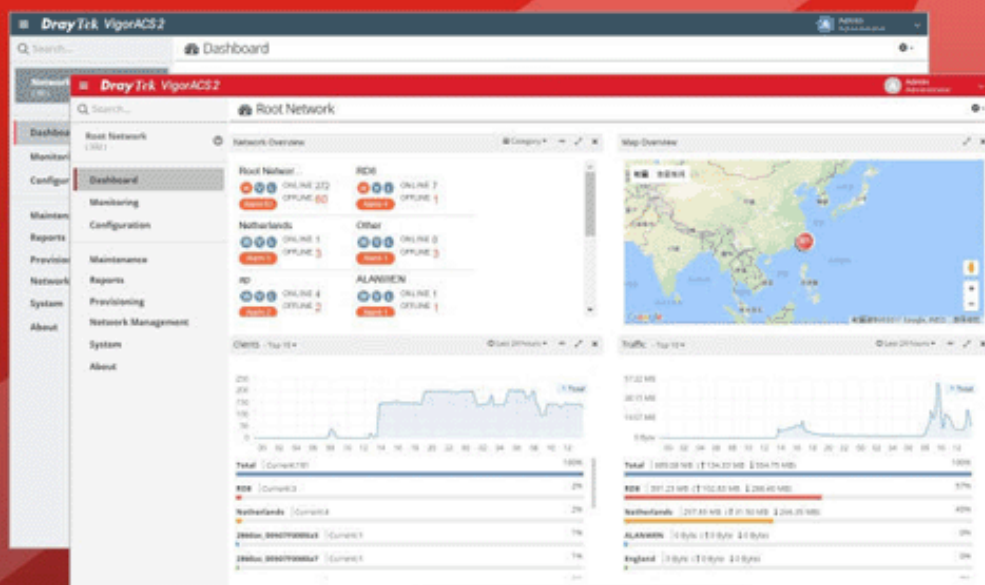


DrayTek

VigorACS 2

Unified Management System

Your reliable networking solutions partner



User's Guide

V1.5

VigorACS 2

Unified Management System

User's Guide

Manual Version: V1.5

Date: January 16, 2020

Software Version: V2.4.0

© 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 2 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 2 (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 does 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 2.

Table of Contents

Part I Introduction	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 7 or 10	5
2.1.1 Installation for Java	5
2.1.2 Installation for MariaDB	9
2.1.3 Installation for VigorACS 2	14
2.1.4 StartMySQL/MariaDB Database	22
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 Database	31
2.2.3 Start InfluxDB	31
2.2.4 Start VigorACS	31
2.2.5 Edit VigorACS IP	32
2.3 Registering VigorACS	32
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 Group	43
3.2.3 Dashboard for Device (CPE, AP)	43
3.2.4 Statistics for Network	45
3.2.5 Statistics for CPE	45
3.2.6 Root Network and Inventory View	46
3.2.7 Network Overview	46
3.2.8 Map Overview	47
3.2.9 Top 10 for Clients	47
3.2.10 Top 10 for Traffic	48
3.2.11 New Added Devices List	48
3.2.12 Icons Used in VigorACS 2	49
3.3 Capture Packets	49
3.4 Set Password	52
3.5 Two-factor Authentication	53

3.6 Change Theme.....	55
3.7 Logout VigorACS.....	56
3.8 About VigorACS.....	57
3.8.1 License Key Information.....	57
3.8.2 License Agreements.....	58
3.9 Operation Procedure.....	58
Applications.....	60
A-1 How to Register a CPE onto VigorACS 2?.....	60
A-2 How to Create a New Network ?.....	62
A-3 How to Assign a New Added CPE to a Network?.....	64
A-4 How to Create a New User Group ?.....	65

Part II SYSTEM MENU, System and User Settings Management 67

Chapter 4 System.....	68
4.1 System Parameter.....	68
4.2 Language.....	75
4.3 External Monitoring Server.....	76
4.3.1 Health Server.....	76
4.3.2 Wireless Client Information Server.....	77
4.4 Block Host.....	78
4.5 Clear Logs.....	79
4.6 Upload Serial Number.....	80
4.7 Google API Key.....	81
4.8 Certificate.....	82
4.8.1 Certificate.....	82
4.8.2 Certificate with private key.....	83
4.8.3 PKC12.....	85
4.9 Backup Database.....	87
4.9.1 Backup Tasks.....	87
4.9.2 Backup Files.....	90
4.9.3 Error Logs.....	91
4.10 Login Bulletin.....	92
4.10.1 General Settings.....	93
4.10.2 Message Settings.....	95
4.11 Adverts Carousel.....	97
4.11.1 General Settings.....	97
4.11.2 Advert Items Settings.....	99
4.12 Logs.....	104
4.13 Delete Logs Actions.....	106

Chapter 5 User	108
5.1 User Management	108
5.2 Group Management	111
5.2.1 Setting	111
5.2.2 Management	113
5.3 Device Group	114
5.4 External Authentication Server	114
5.5 Mail Server	118
5.6 Function Management	119
5.7 Wholesale Wizard	120
5.8 SMS Server	124
5.9 SNMP Server	125
Applications	126
A-1 How to Add a User?.....	126
A-2 How to Add a Group?.....	127

Part III SYSTEM MENU, General Settings for Managing CPE 129

Chapter 6 Network Management	130
6.1 Settings for Network	130
6.2 Settings for Device.....	132
Applications	134
A.1 How to Create a Network for Managing Devices?	134
A.2 How to Change the Network of a Device?	136
Chapter 7 Maintenance	138
7.1 Scheduled Backup.....	138
7.1.1 Networks & Devices	138
7.1.2 Backup Settings Profile	140
7.2 Configuration Restore	142
7.2.1 Apply to Devices	142
7.2.2 Restore Settings Profile	143
7.3 Firmware Upgrade	145
7.4 Device Reboot	147
7.5 System Password Reset	148
7.6 Schedule Profile.....	149
7.7 File Manager	151
Chapter 8 Provisioning	153
8.1 Global Parameters	153
8.2 Network & Devices.....	160
8.3 CPE Set Parameters	161

8.4 CPE Keep Parameters	164
8.5 Firmware Upgrade	165
<i>8.5.1 Firmware Upgrade Job List</i>	165
<i>8.5.2 Exclude Devices</i>	168
Applications	170
<i>A.1 How to Create a Provision Profile with Global Parameters?</i>	170
<i>A.2 How to Modify Provision Profile with Global Parameters?</i>	171
<i>A.3 How to Modify Provision Profile with CPE Set Parameters?</i>	174
Chapter 9 Reports	176
9.1 Report Tasks	176
9.2 Reports	179

Part IV NETWORK MENU for Root Network (VPN and AP Management) 181

Chapter 10 Monitoring for Network	182
10.1 Alarm	183
10.2 Logs	184
10.3 Devices	185
10.4 Clients	186
10.5 Cellular Data Usage	187
10.6 Floor Plan	188
<i>10.6.1 List View</i>	188
<i>10.6.2 Browse View</i>	192
10.7 Rogue AP Detection	194
Applications	196
<i>A.1 How to specify an AP device to an existed Floor Plan Profile?</i>	196
Chapter 11 Configuration for Network	200
11.1 VPN	200
<i>11.1.1 VPN under NETWORK MENU</i>	201
11.2 AP Profile	201
<i>11.2.1 Add New Profile</i>	204
<i>11.2.2 Edit the AP Profile</i>	205
Applications	206
<i>A.1 How to apply an AP profile to AP device(s)?</i>	206

Part V DEVICE MENU for Specified CPE 209

Chapter 12 Monitoring for CPE	210
12.1 Alarm	210
12.2 Logs	212
12.3 Diagnostics	213

12.3.1 Ping.....	213
12.3.2 Trace Route.....	214
12.3.3 Routing Table.....	214
12.3.4 ARP Table.....	215
12.3.5 DHCP Table.....	215
12.3.6 Sessions Table.....	216
Chapter 13 Configuration for CPE	217
13.1 Modifying WAN Settings for CPE.....	219
13.1.1 Internet Access - Check WAN Status.....	219
13.1.2 Connection Detection.....	221
13.1.3 Multi-PVC/VLAN.....	221
13.1.4 WAN IPv6.....	222
13.1.5 WAN Budget.....	223
13.1.6 DSL.....	224
13.2 Modifying LAN Setting for CPE.....	224
13.2.1 General Setup.....	224
13.2.2 IP Routed Subnet.....	226
13.2.3 VLAN.....	226
13.2.4 Bind IP to MAC.....	227
13.2.5 DHCP Option Setup.....	228
13.2.6 InterLAN Routing.....	228
13.2.7 LAN IPv6.....	229
13.3 Hotspot Web Portal for CPE.....	231
13.3.1 Profile Setup.....	231
13.4 Routing Settings for CPE.....	232
13.4.1 Load Balance/Policy Route.....	232
13.4.2 Static Route IPv4 / IPv6.....	233
13.4.3 BGP.....	235
13.5 NAT Settings for CPE.....	236
13.5.1 Port Redirection.....	236
13.5.2 DMZ Host.....	237
13.5.3 Open Ports.....	237
13.5.4 Port Triggering.....	239
13.5.5 ALG.....	239
13.6 Hardware Acceleration Settings for CPE.....	240
13.7 Firewall Settings for CPE.....	242
13.7.1 General Setup.....	242
13.7.2 Default Rule.....	242
13.7.3 Filter Rules.....	243

13.7.4 DoS Defense	245
13.7.5 APP Enforcement	246
13.7.6 URL Content Filter	247
13.7.7 Web Content Filter	248
13.7.8 DNS Filter	250
13.8 User Management Settings for CPE	251
13.8.1 General Setup	251
13.8.2 User Profile	251
13.8.3 User Group	252
13.9 Modifying Objects Settings for CPE	254
13.9.1 Create / Edit an IP Object Profile	254
13.9.2 Create / Edit an IP Group Profile	255
13.9.3 Create / Edit an IPv6 Object Profile	256
13.9.4 Create / Edit an IPv6 Group Profile	257
13.9.5 Create / Edit a Service Type Object Profile	258
13.9.6 Create / Edit a Service Type Group Profile	259
13.9.7 Create / Edit a Keyword Object Profile	260
13.9.8 Create / Edit a Keyword Group Profile	261
13.9.9 Create / Edit a File Extension Object Profile	262
13.9.10 Create / Edit a SMS Service Object Profile	263
13.9.11 Create / Edit a Mail Service Object Profile	264
13.9.12 Create / Edit a Notification Object Profile	266
13.9.13 Create / Edit a String Object	267
13.10 QoS Settings for CPE	268
13.10.1 QoS WAN	268
13.10.2 QoS Class	269
13.10.3 QoS Service Type	270
13.10.4 Others	271
13.11 Applications Settings for CPE	272
13.11.1 Dynamic DNS	272
13.11.2 LAN DNS / DNS Forwarding	274
13.11.3 DNS Security	275
13.11.4 Schedule	275
13.11.5 External RADIUS	276
13.11.6 Internal RADIUS	277
13.11.7 External TACACS+	277
13.11.8 Active Directory/LDAP	278
13.11.9 UPnP	279
13.11.10 IGMP	280

13.11.11	Wake on LAN	280
13.11.12	SMS/Mail Alert Service	281
13.11.13	Bonjour	284
13.11.14	High Availability	285
13.11.15	Local 802.1X General Setup	286
13.12	VPN Settings for CPE	287
13.12.1	VPN Wizard	287
13.12.2	Create LAN to LAN Profile for VPN Connection	290
13.12.3	Create Remote Dial-in User Profile for VPN Connection.....	293
13.13	VoIP Settings for CPE	295
13.13.1	General Setting	295
13.13.2	SIP Accounts	296
13.13.3	Phone Book	297
13.13.4	Digit Map.....	298
13.13.5	Call Barring.....	300
13.13.6	Regional.....	301
13.13.7	PSTN Settings.....	302
13.13.8	Phone Setting	303
13.13.9	Log	304
13.14	LTE Settings for CPE	305
13.14.1	General Setup.....	305
13.14.2	SMS-Inbox	306
13.14.3	Send SMS.....	306
13.14.4	Router Commands	307
13.14.5	Status.....	307
13.15	Wireless LAN Settings for CPE.....	308
13.15.1	General Setting for 2.4G/5G	308
13.15.2	General SSID for 2.4G/5G	308
13.15.3	Security for 2.4G/5G.....	310
13.15.4	Access Control for 2.4G/5G.....	311
13.15.5	WPS for 2.4G/5G	311
13.15.6	Bandwidth Management for 2.4G/5G	312
13.15.7	WDS for 2.4G/5G	313
13.15.8	Airtime Fairness for 2.4G/5G	313
13.15.9	Advanced Setting for 2.4G/5G	314
13.15.10	Band Steering for 2.4G/5G	314
13.15.11	AP Discovery for 2.4G/5G.....	315
13.15.12	Station List for 2.4G/5G	316
13.15.13	Roaming for 2.4G/5G.....	316

13.15.14 Station Control for 2.4G/5G	317
13.16 Bandwidth Management Settings for CPE	318
13.16.1 Sessions Limit	318
13.17 USB Applications Settings for CPE	319
13.17.1 General Settings	319
13.17.2 User Management	319
13.17.3 Temperature Sensor	321
13.17.4 Disk Status	321
13.17.5 Modem Status	322
13.17.6 Printer Status	323
13.17.7 Sensor Status	323
13.18 System Settings for CPE	324
13.18.1 Maintenance	324
13.18.2 Time Settings	325
13.18.3 Admin Account	325
13.18.4 Admin Local User	326
13.18.5 SNMP Settings	327
13.18.6 Management	327
13.18.7 TR069 Settings	328
13.18.8 SysLog Settings	328
13.18.9 Mail Alert	329
13.19 Copy Parameter for CPE	330
13.19.1 Copy Parameter	330
13.19.2 Checking the Copying Parameters Status	334
13.20 Advanced Settings for CPE	335
13.20.1 Parameter Tree	335
13.20.2 Exclude Parameters	335
Applications	336
A.1 How to create a VPN by using VPN Wizard?	336
A.2 How to create a VPN Connection with Advanced Settings by using VPN Wizard ?	342
Chapter 14 Trouble Shooting	346
14.1 Contacting DrayTek	346
Chapter 15 Reference Information	348
15.1 For Linux System	348
15.2 For Windows XP System	349

Part I Introduction

Chapter 1 Introduction

≡ DrayTek VigorACS2

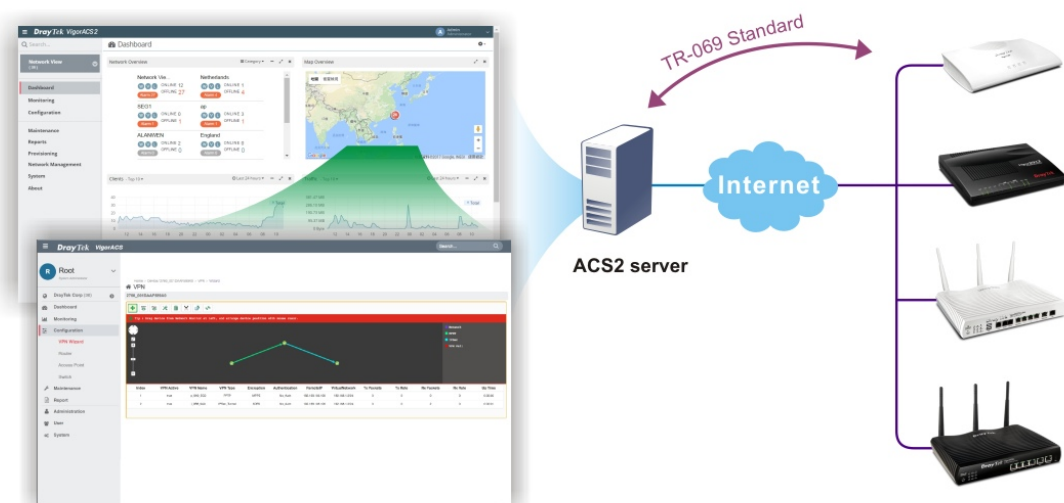
VigorACS 2 is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway and wireless AP. VigorACS 2 has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore and parameter profile for mass deployment of CPE devices. It is easy to use through intuitive Web-based GUI with security management. VigorACS 2 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 2 server can be installed in Windows and Linux.
- Intuitive Web-based GUI can be executed on all browsers like IE, 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 2 and CPE devices. With TR-069 protocol, VigorACS 2 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

DrayTek VigorACS2

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



Info

VigorACS 2 can be operated only by a host with 64-bit operation system.

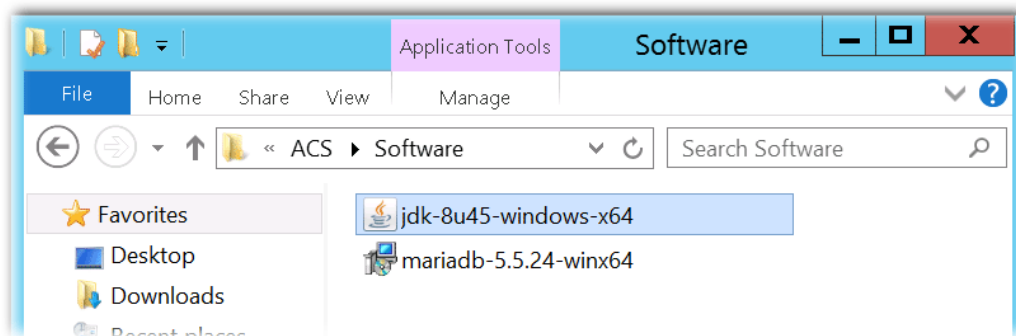
2.1 Platform for Windows 7 or 10

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

- (I) Installation for Java,
- (II) Installation for MariaDB
- (III) Installation for VigorACS 2
- (IV) Start MySQL/MariaDB Database.
- (V) Edit VigorACS ip.
- (VI) Start VigorACS.

2.1.1 Installation for Java

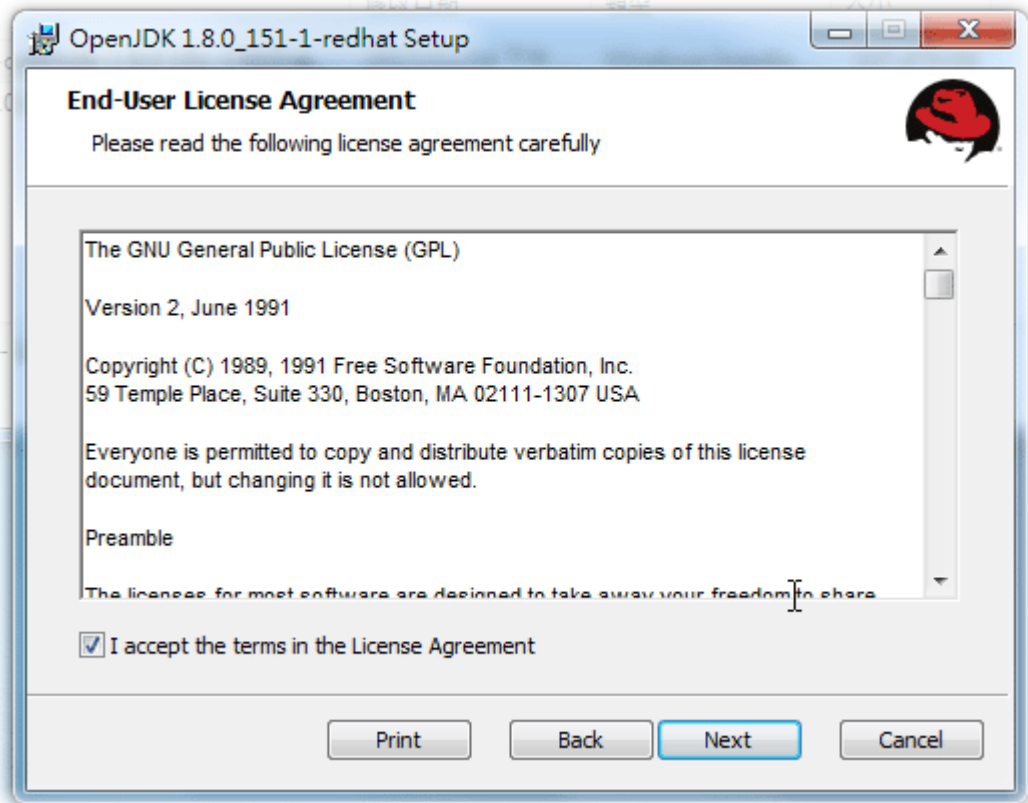
1. Install Java by clicking "jdk-8u45-windows-x64" it to execute the installation.



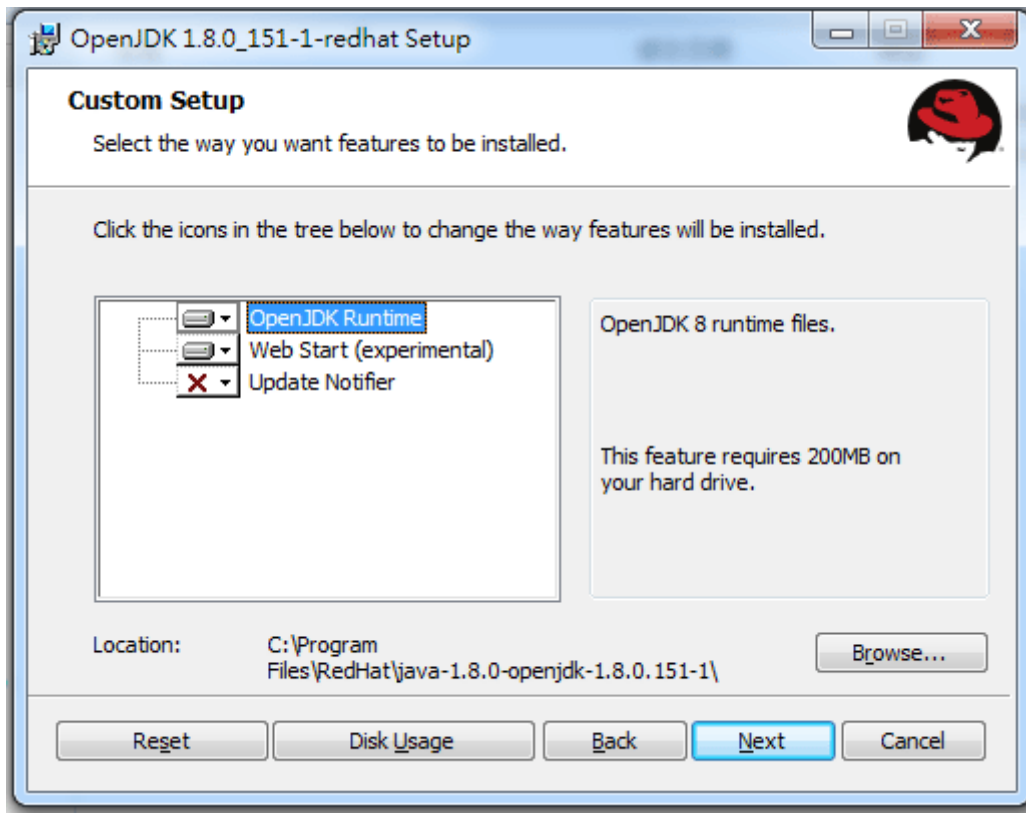
2. The first page will be shown as follows. Click **Next** to get into next page.



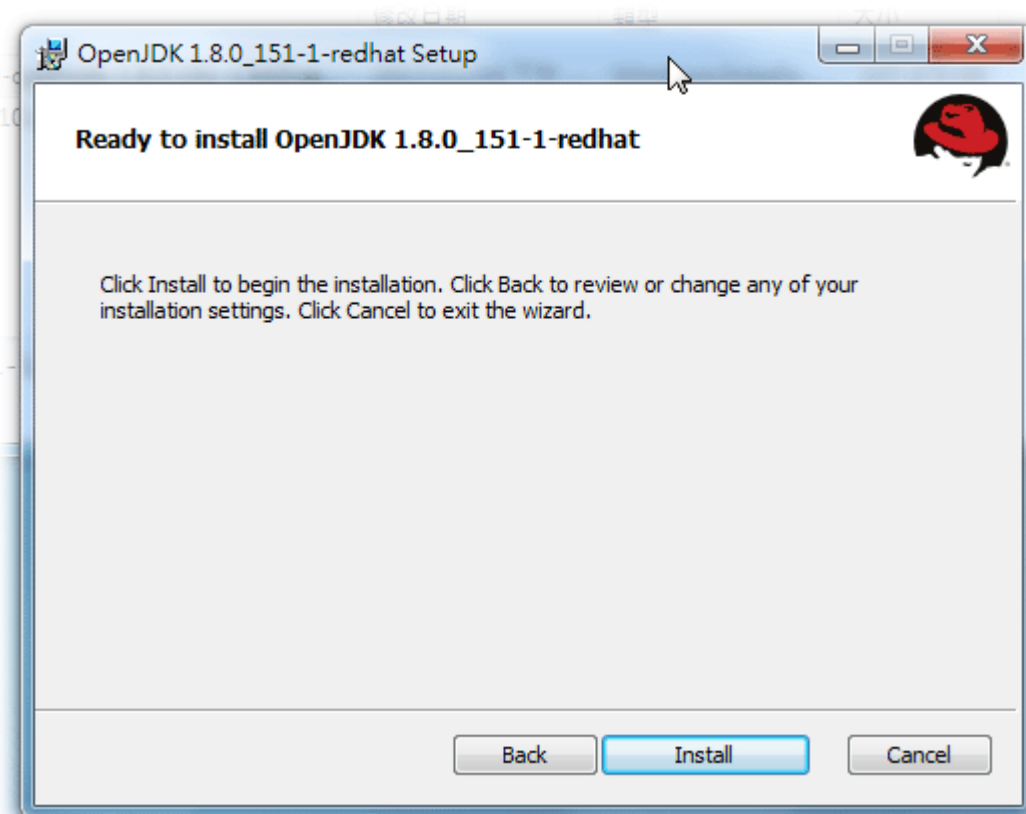
3. Then, check "I accept the terms..." and click the **Next** button.



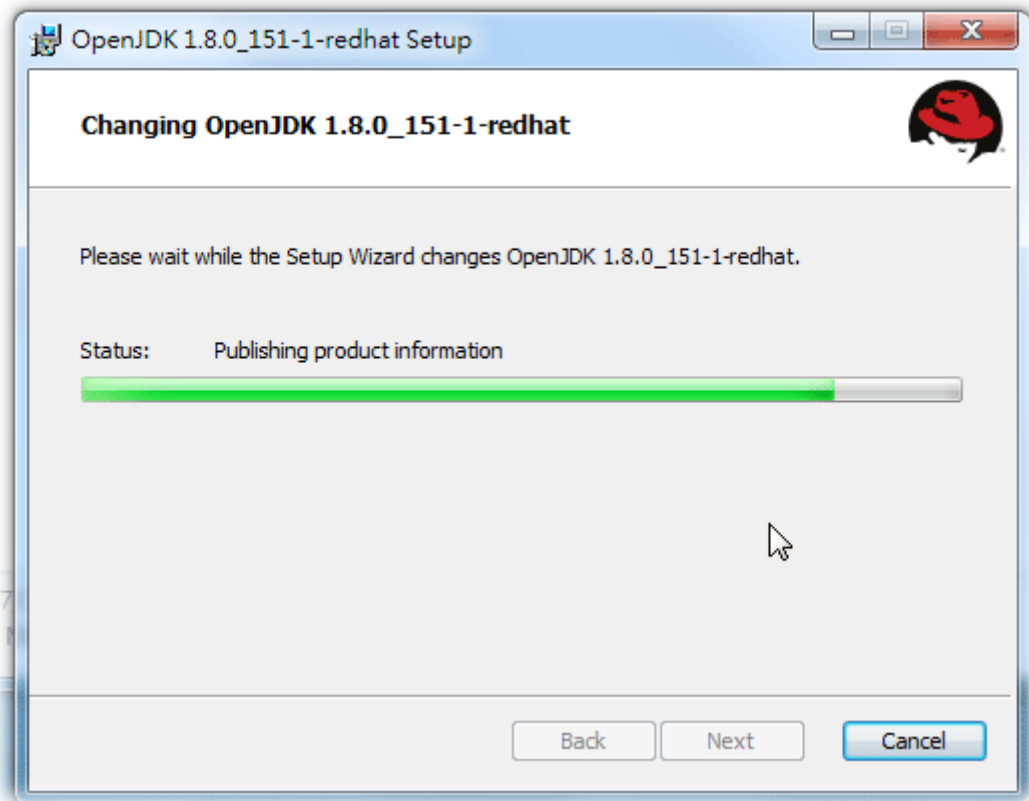
4. In this page, optional features will be listed for you to specify the destination folder for JAVA driver installation. Choose the one you need and click **Next**.



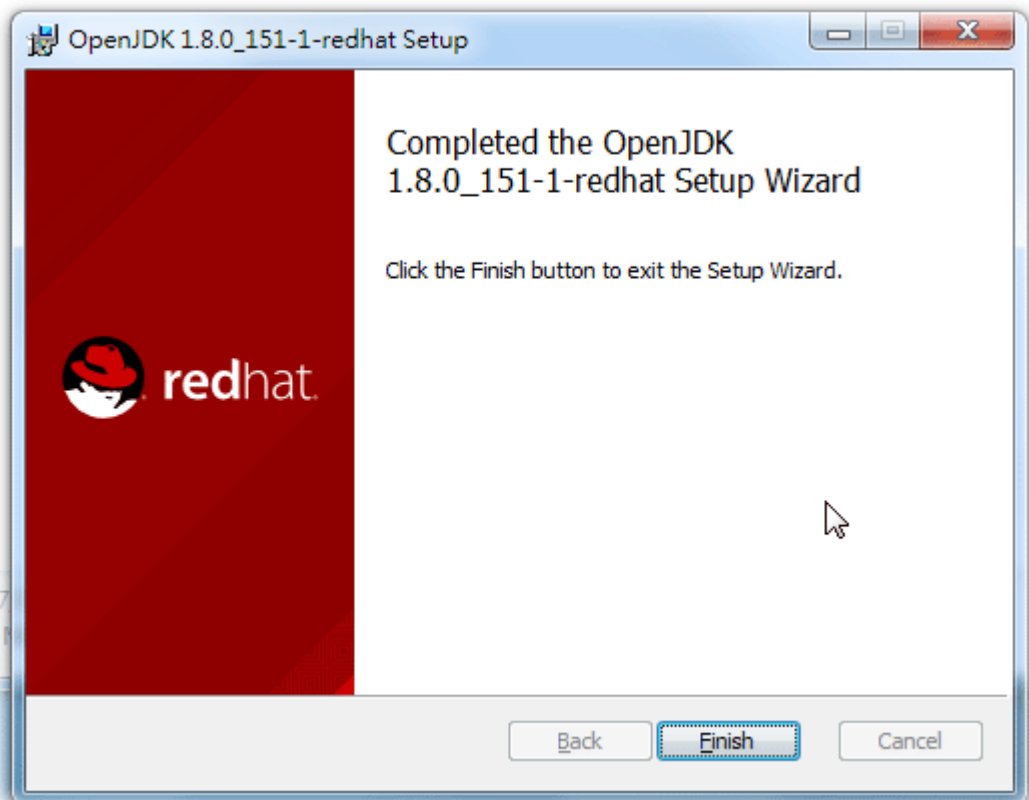
5. In the following page, just click **Install**.



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

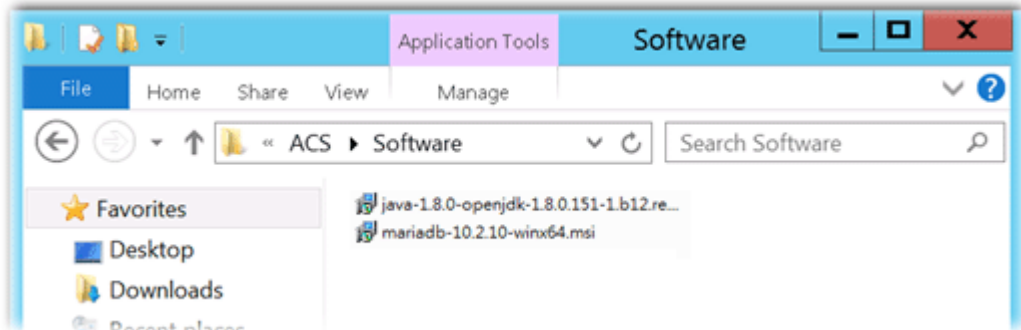


7. When the following page appears, the installation is completed. Click Close to exit the installing program.

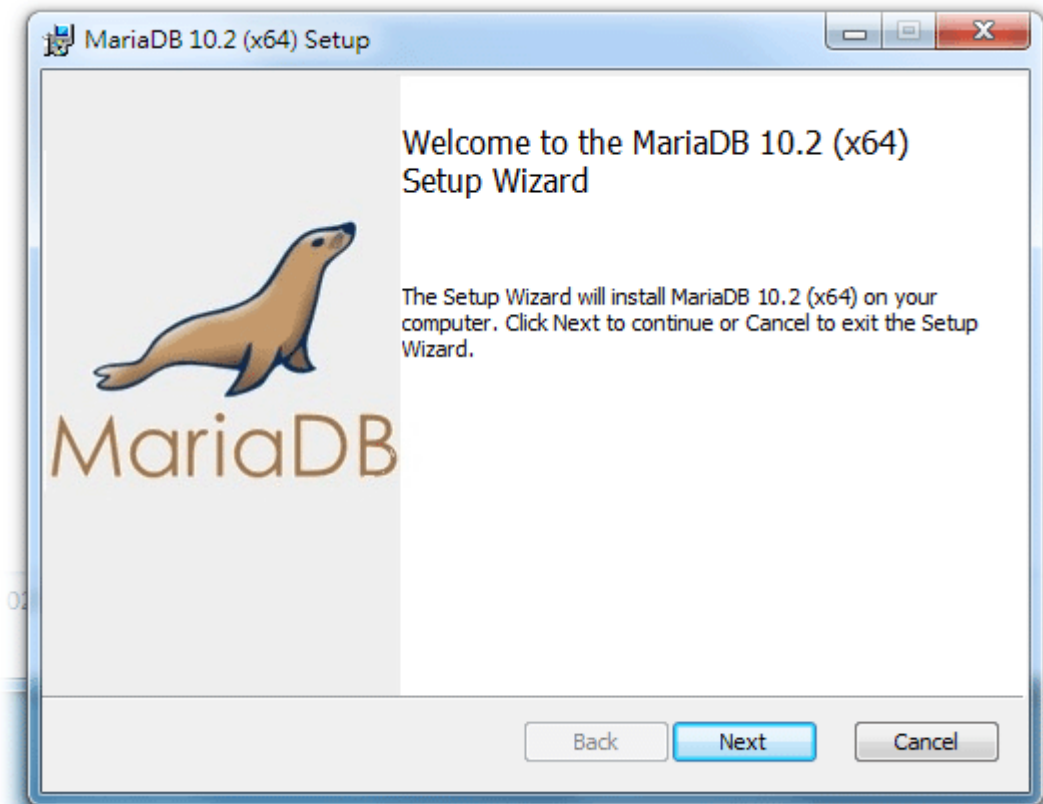


2.1.2 Installation for MariaDB

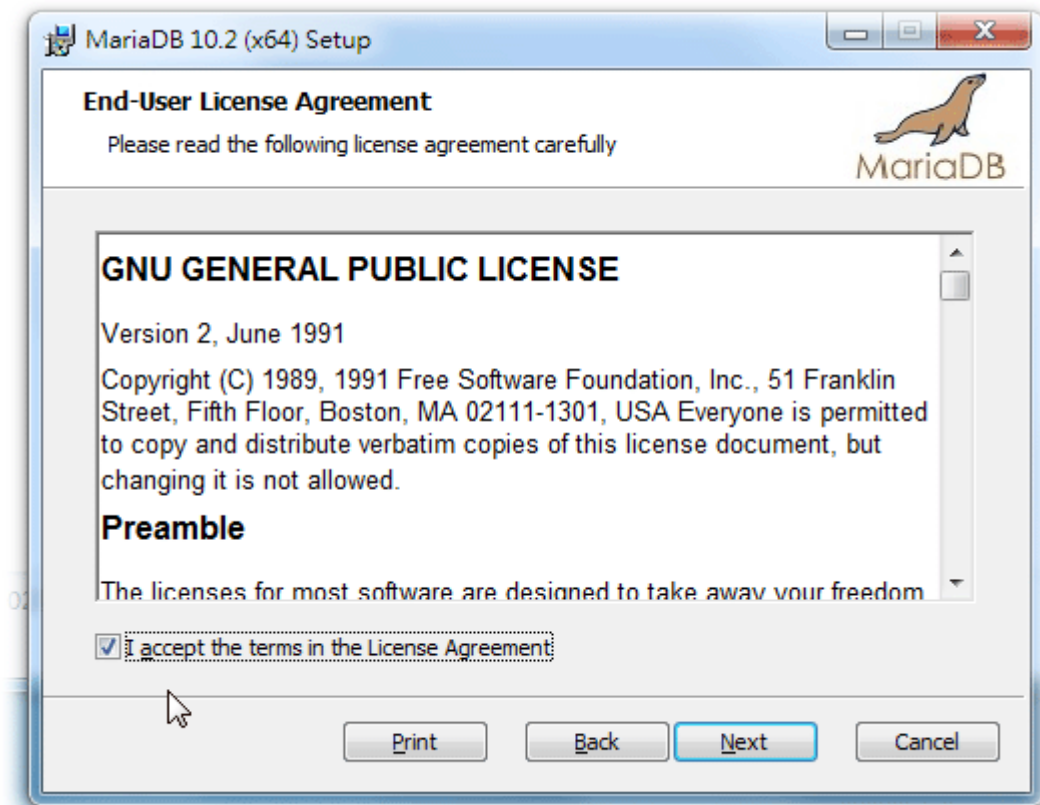
1. Install MariaDB by clicking "mariadb-10.2.10-winx64" (based on your PC condition) it to execute the installation.



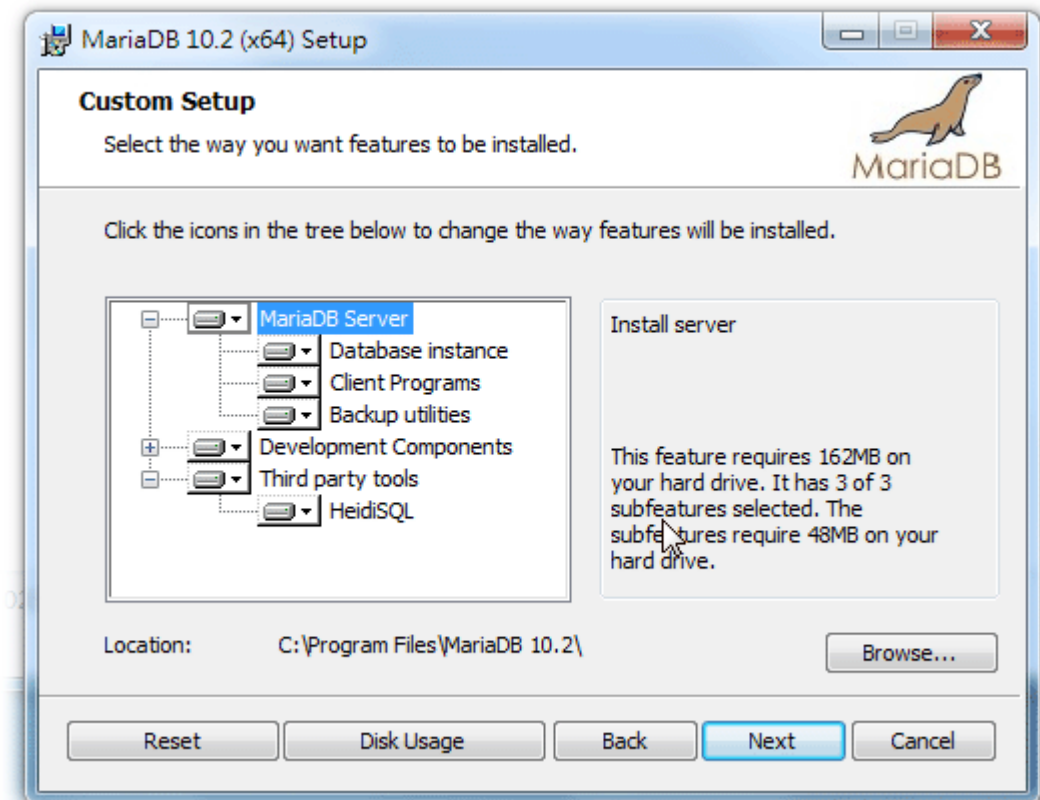
2. When the welcome screen appears, please click Next for next step.



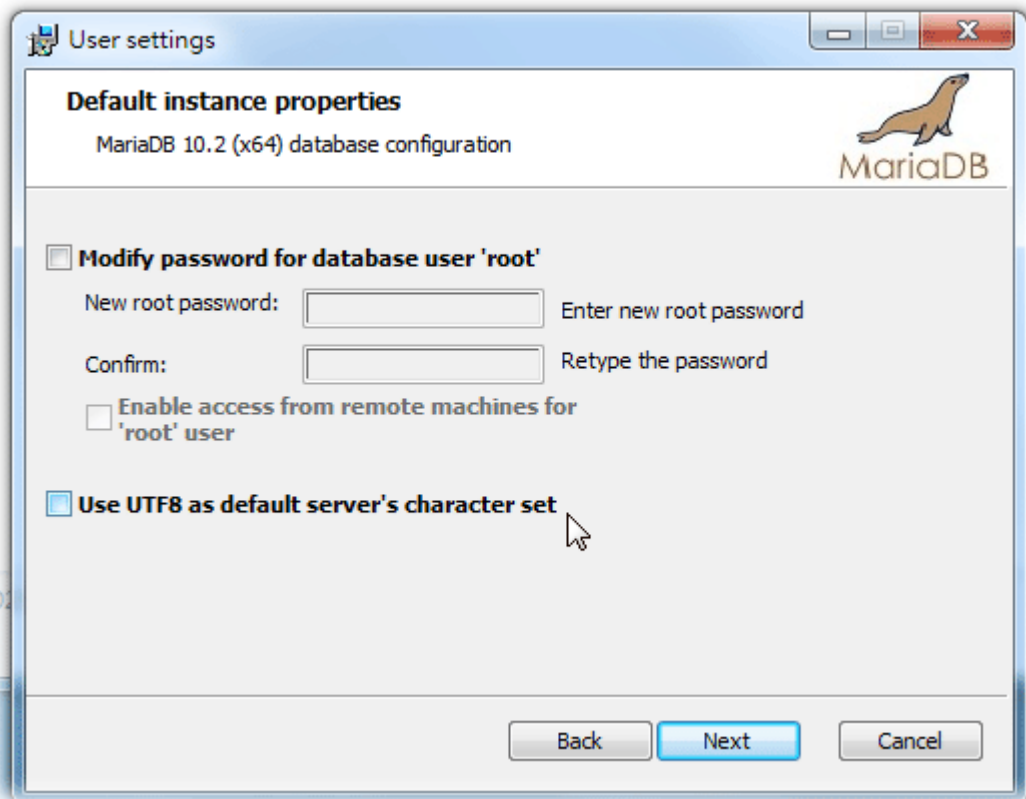
3. On this dialog box, check the box of "I accept the terms...." and click Next.



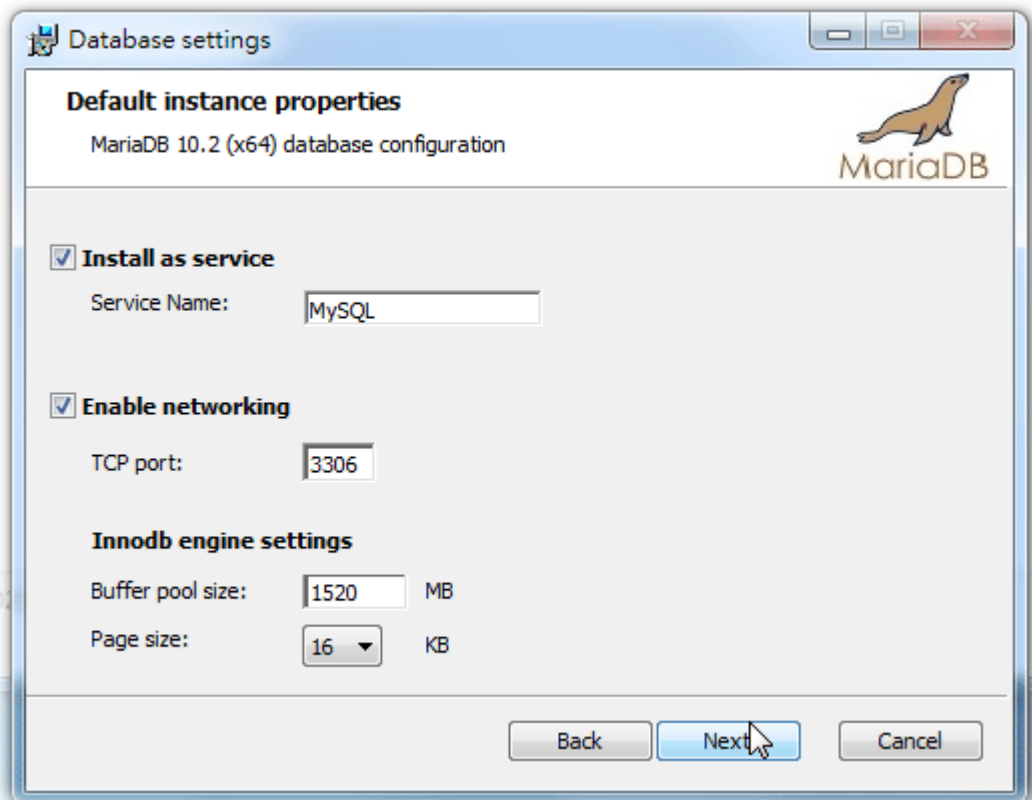
4. Select the way for the features to be installed. Then click Next.



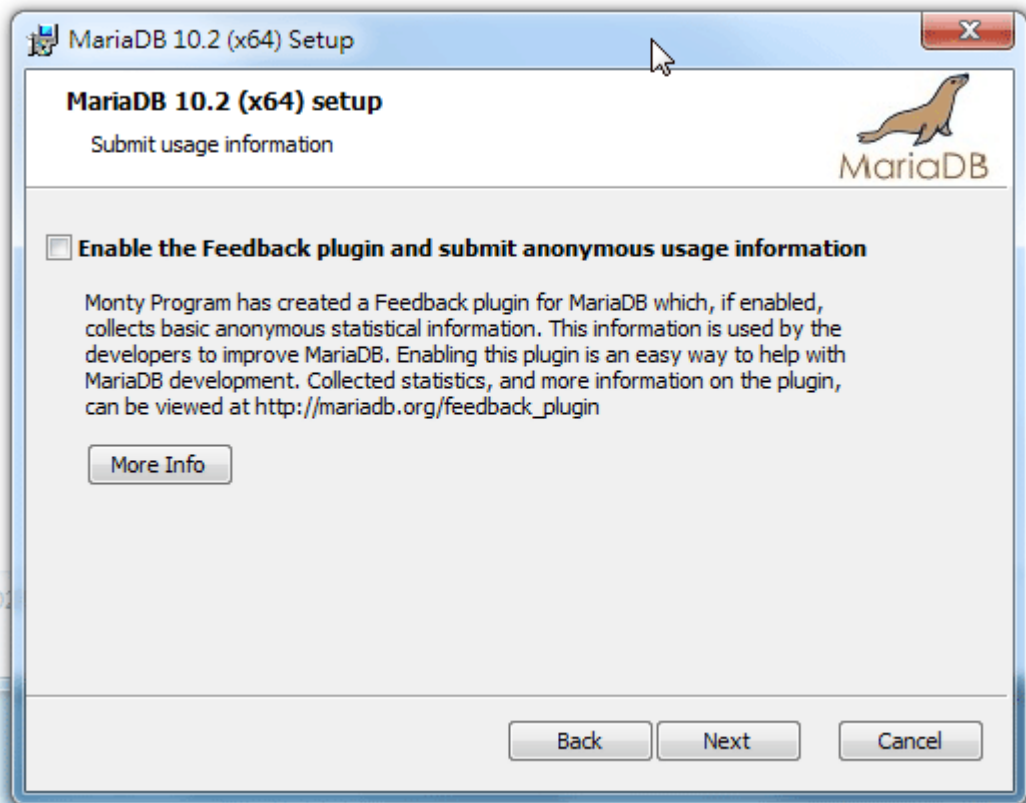
5. If you want to configure password for MariaDB server, please check **Modify password...** and type the password. It depends on your request. Otherwise, simply click **Next**.



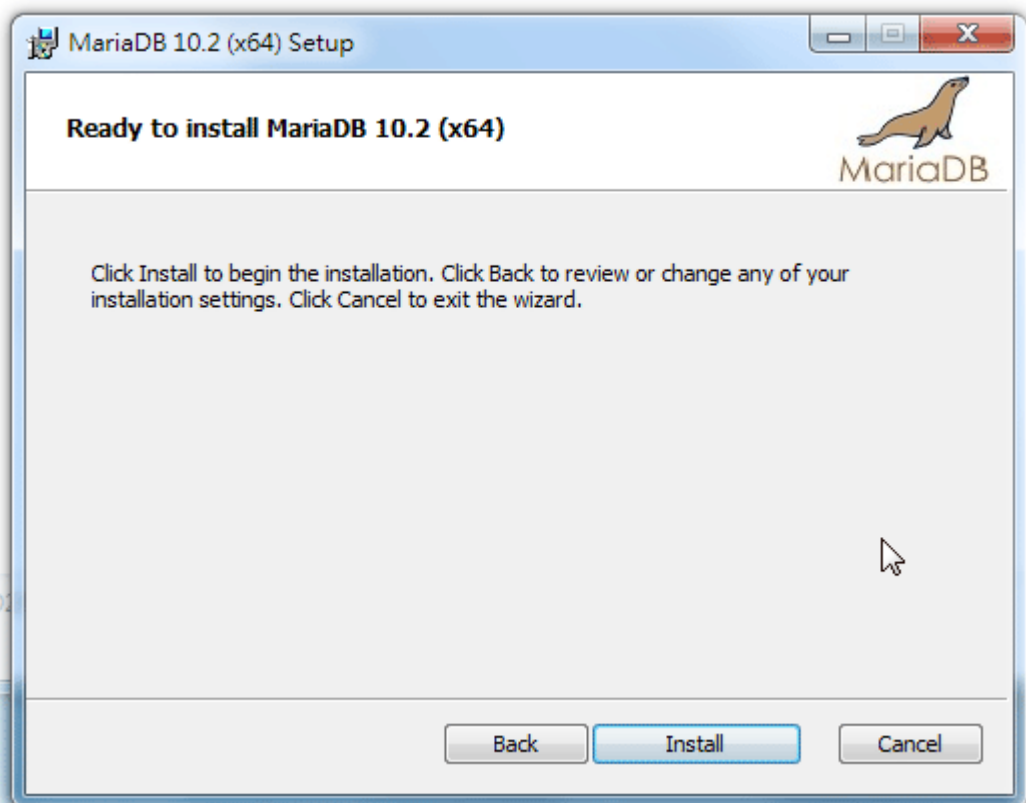
6. Modify the default instance properties if required. Then click **Next**.



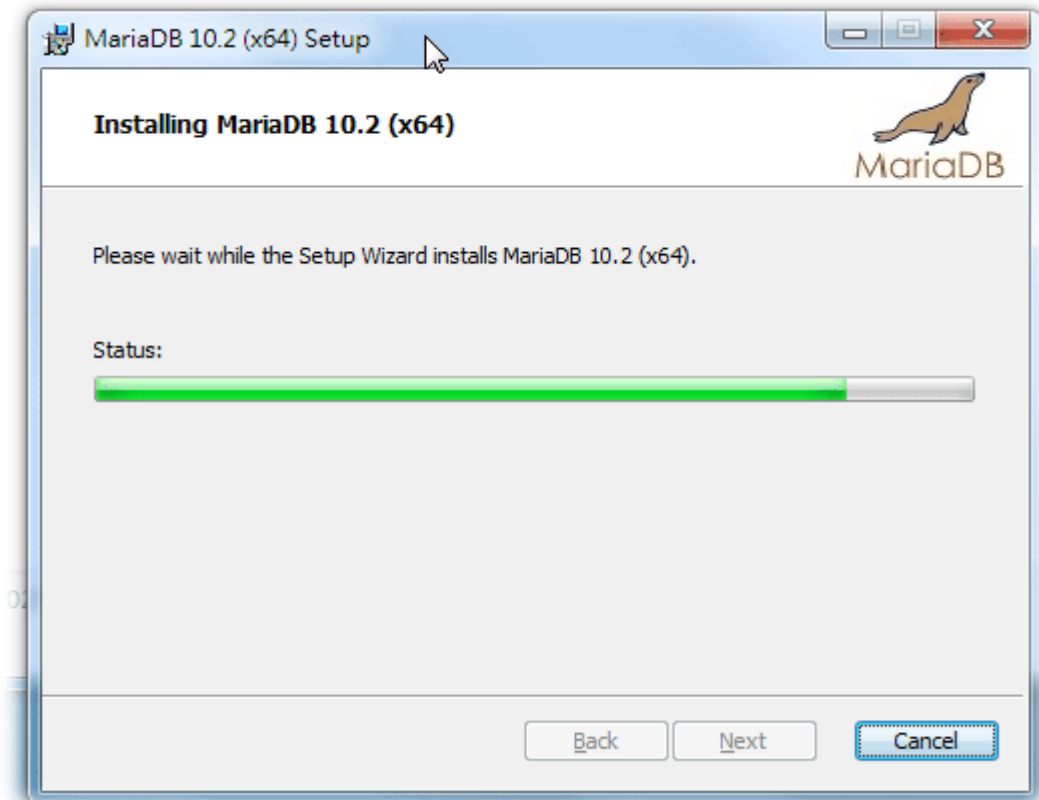
7. On this dialog box, click Next.



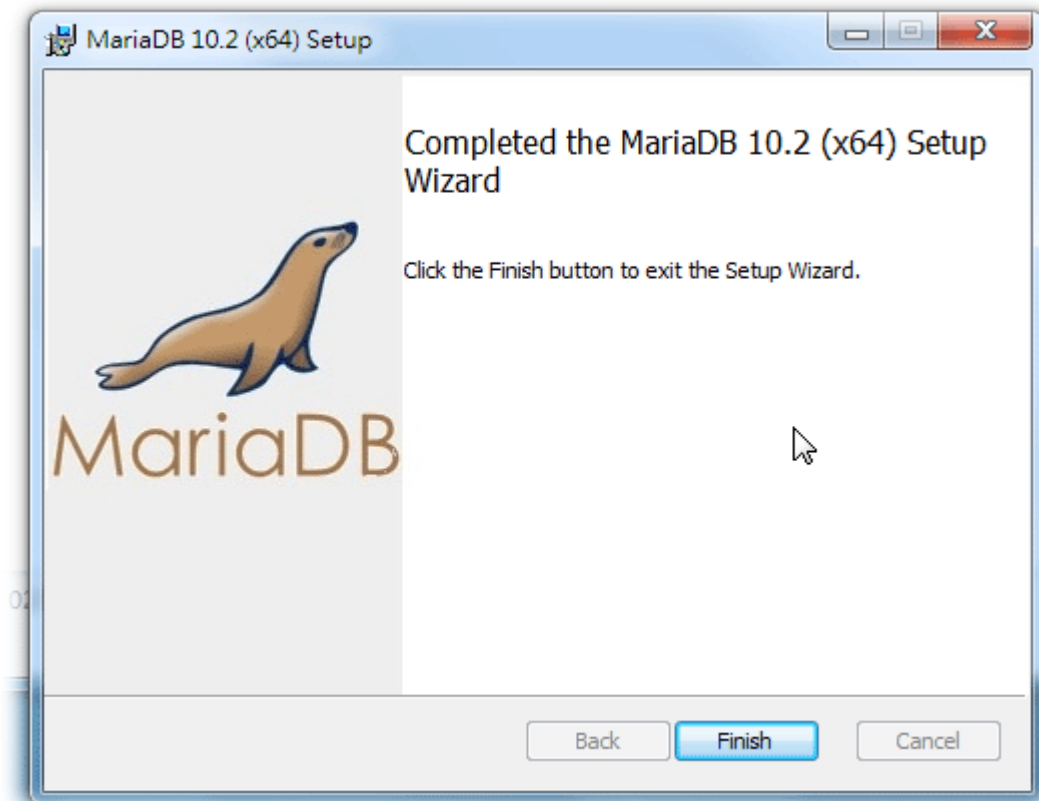
8. On this dialog box, click Install.



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



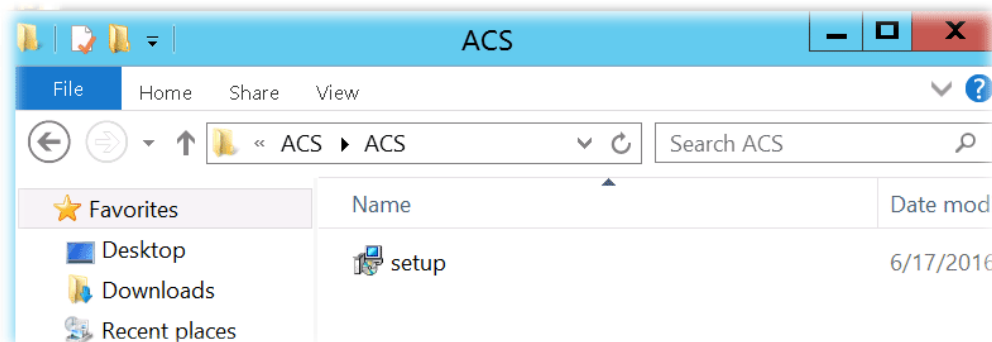
10. After finishing the configuration, please click **Finish** to exit the wizard.



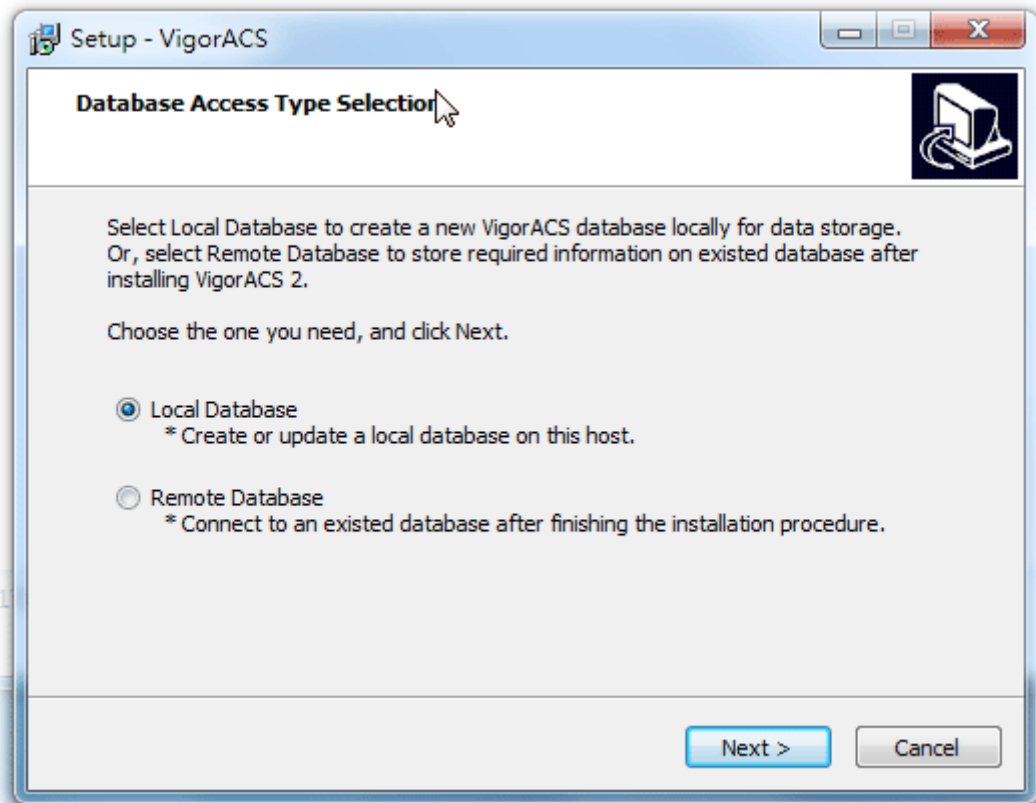
2.1.3 Installation for VigorACS 2

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

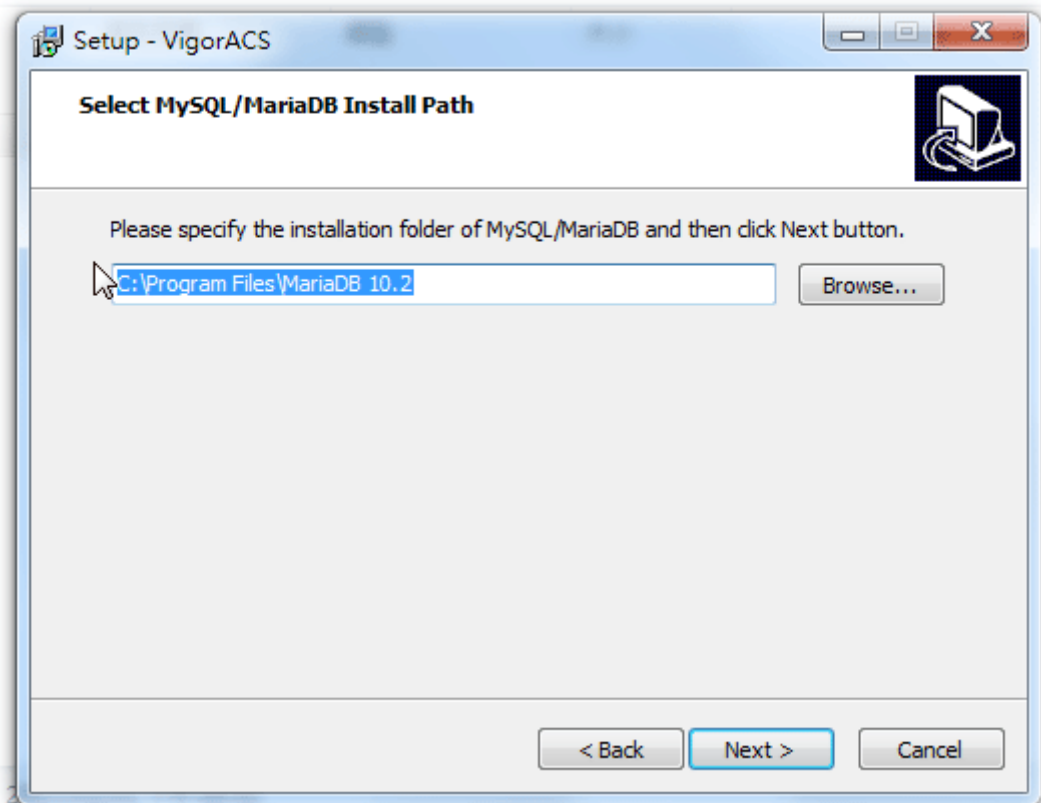
1. Click Setup to run VigorACS 2 setup wizard.



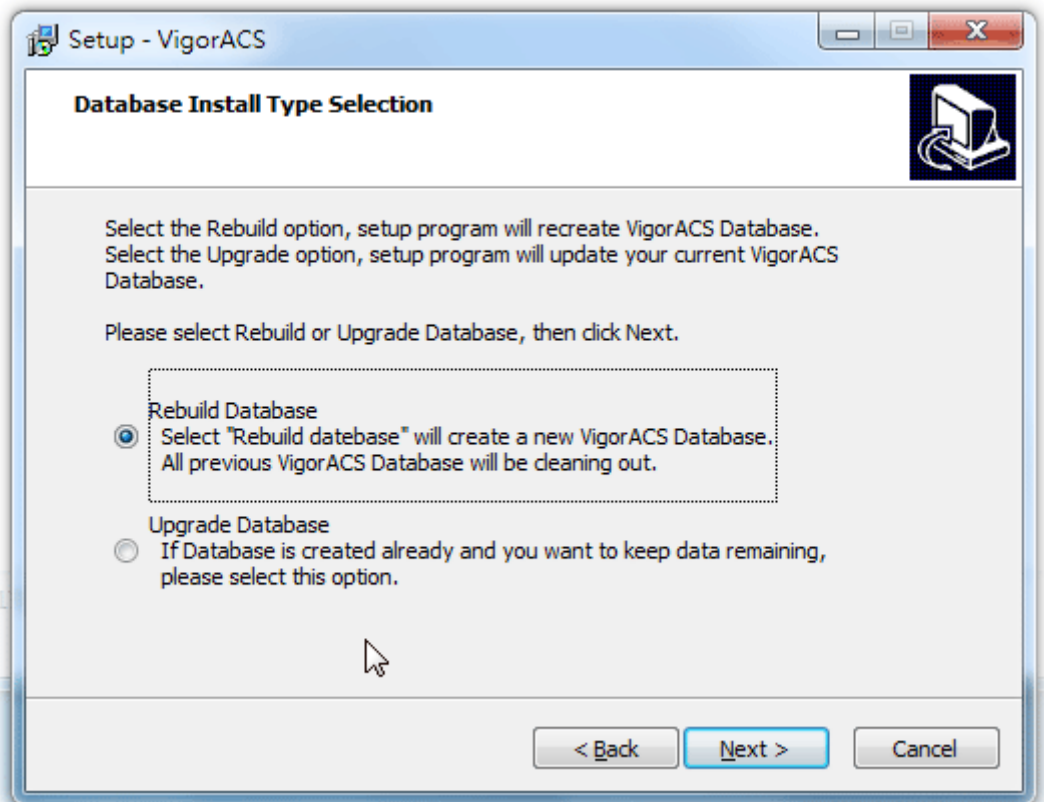
2. When the following dialog appears, choose Local Database / Remote Database and click Next.



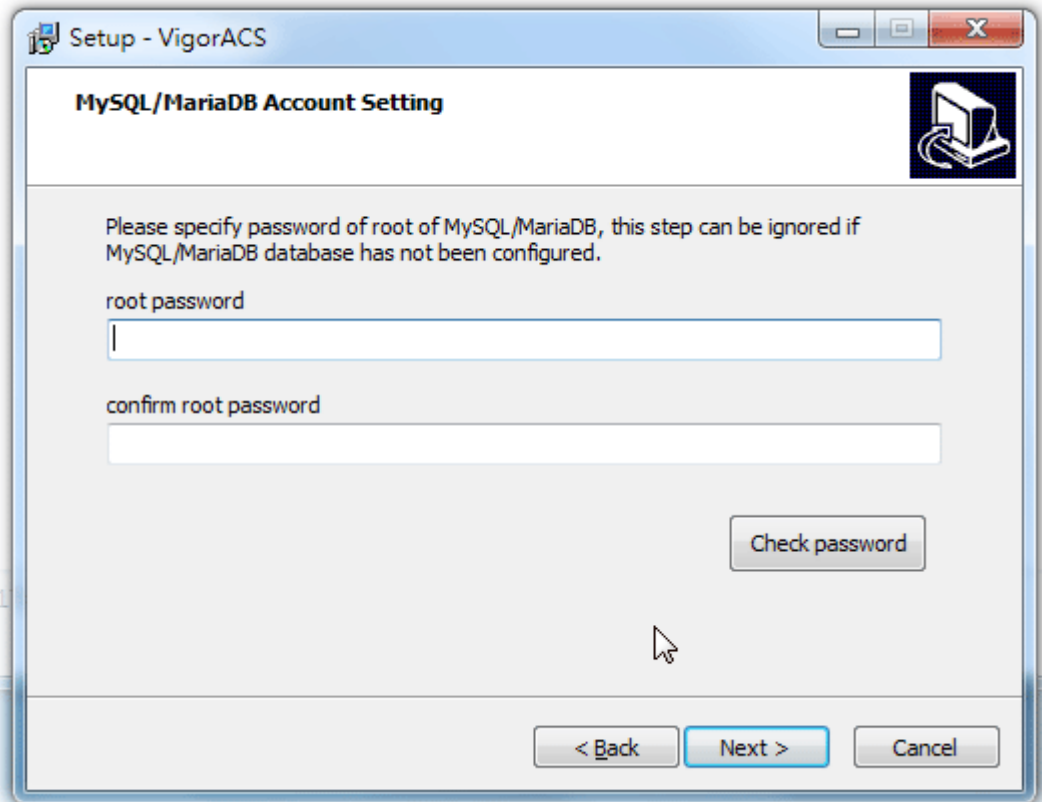
3. Select the directory that MariaDB being installed (done in 2.1.2) and click Next



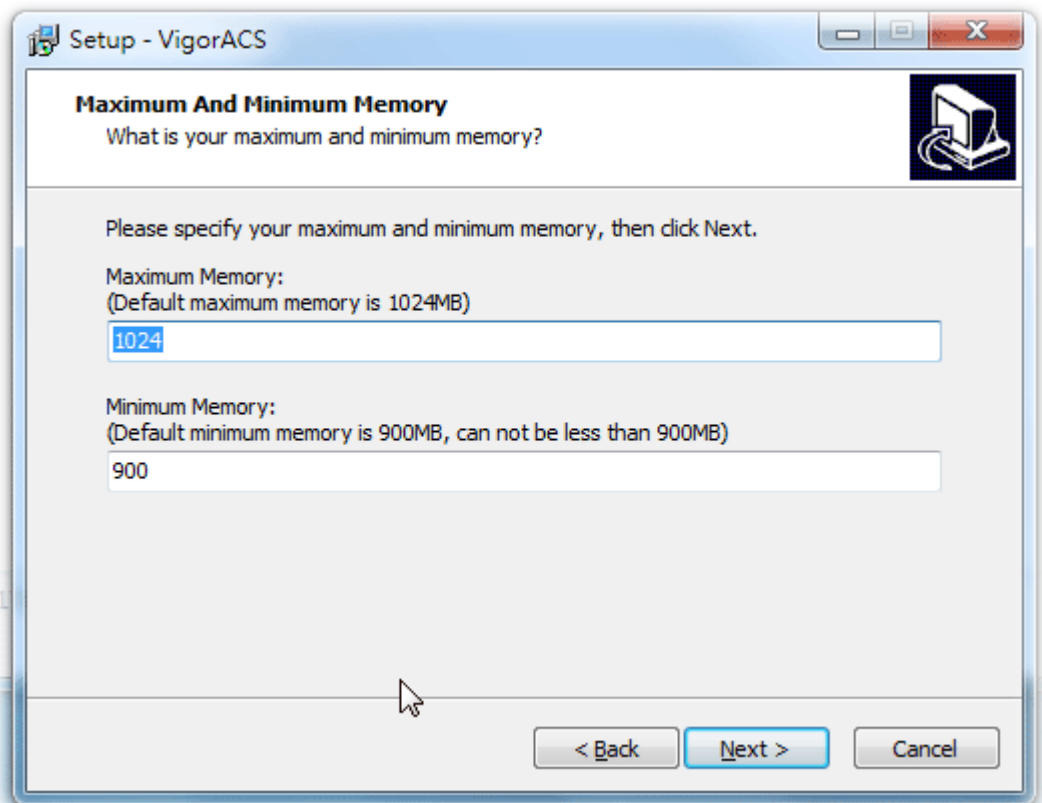
4. In this dialog box, choose **Rebuild Database** (for rebuilding the VigorACS database) or **Upgrade Database** (for upgrading the database). For the first time using, please choose **Rebuild Database**. Then click Next.



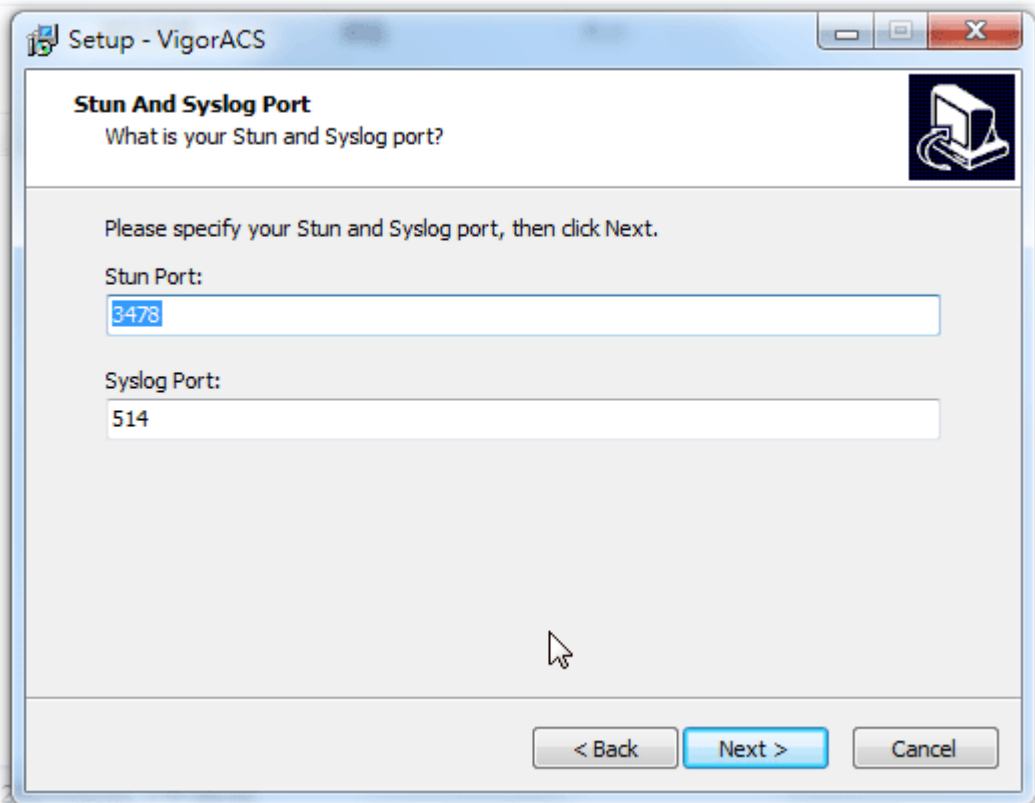
5. Click **Next**. If you have configured MySQL/MariaDB previously and specified password for it, you have to type the password in this page and then click **Next**.



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



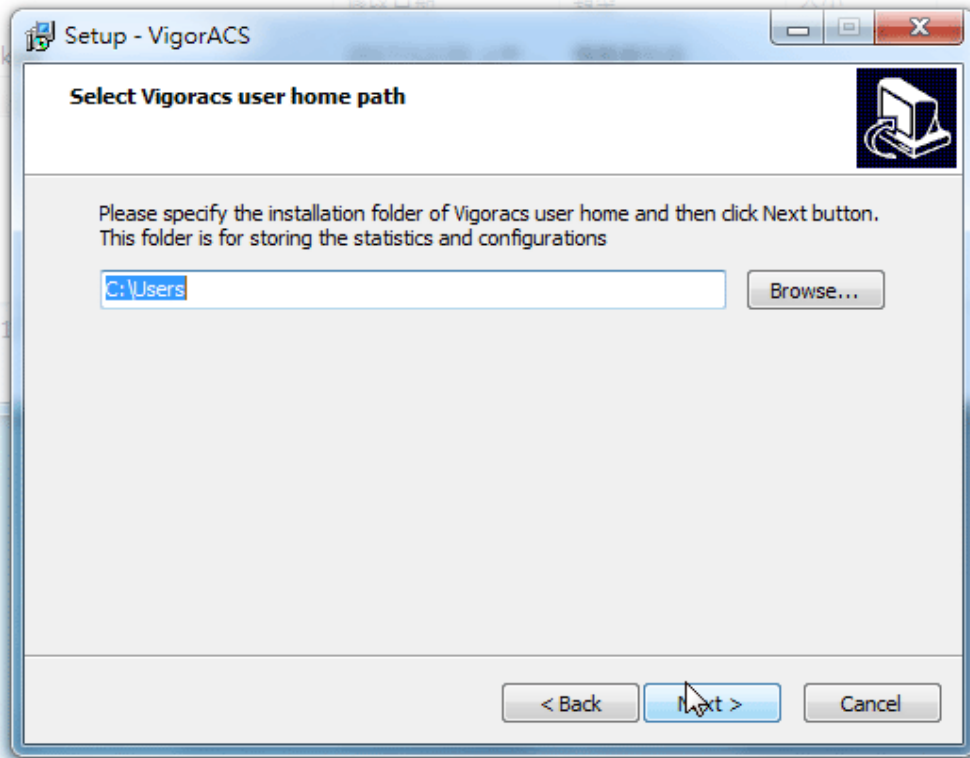
7. Setup ACS HTTP and HTTPS port, we'll suggest using others port instead of default 80 and 443 port to prevent conflict.



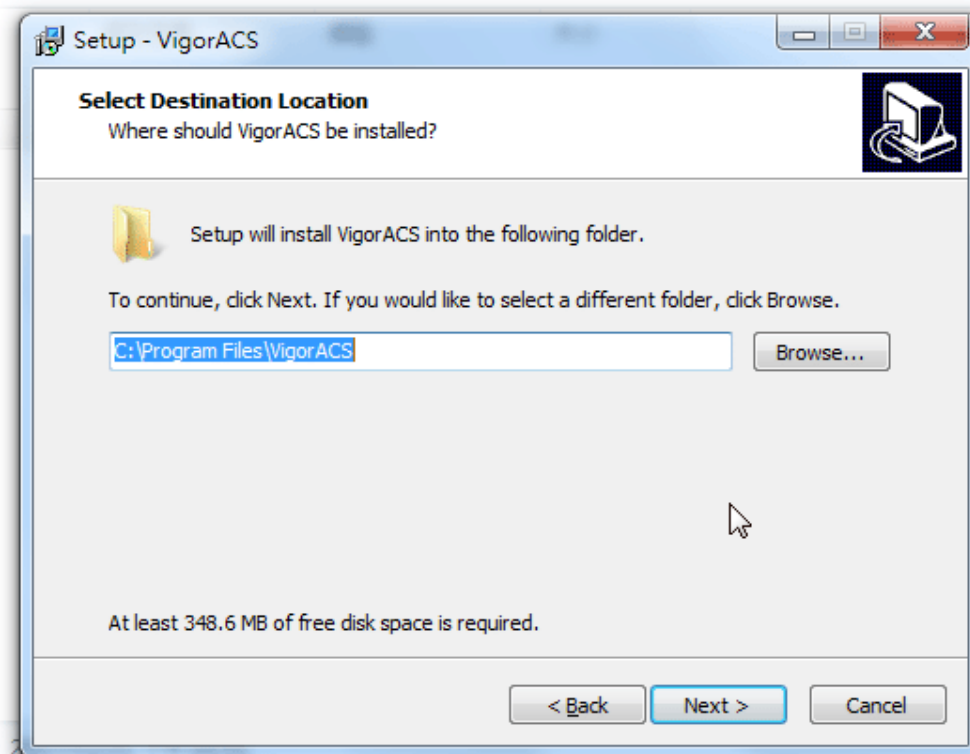
Info

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

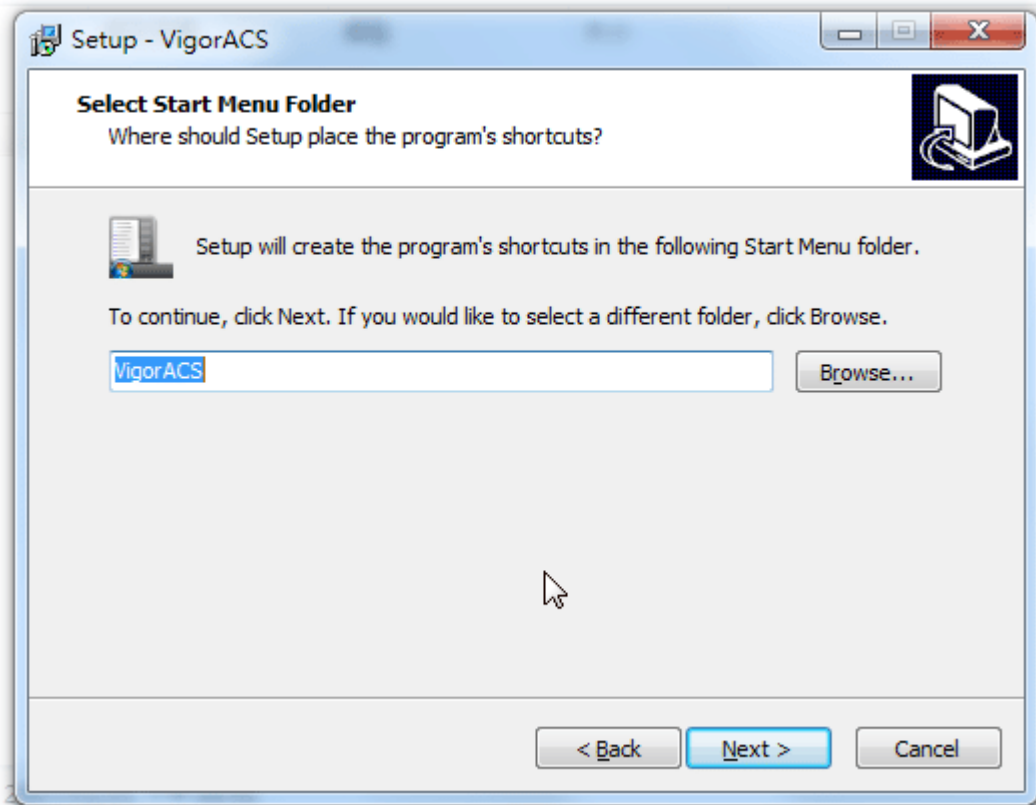
- Determine the home path and click **Next**. The default directory used by this program is *C:\Users*. You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



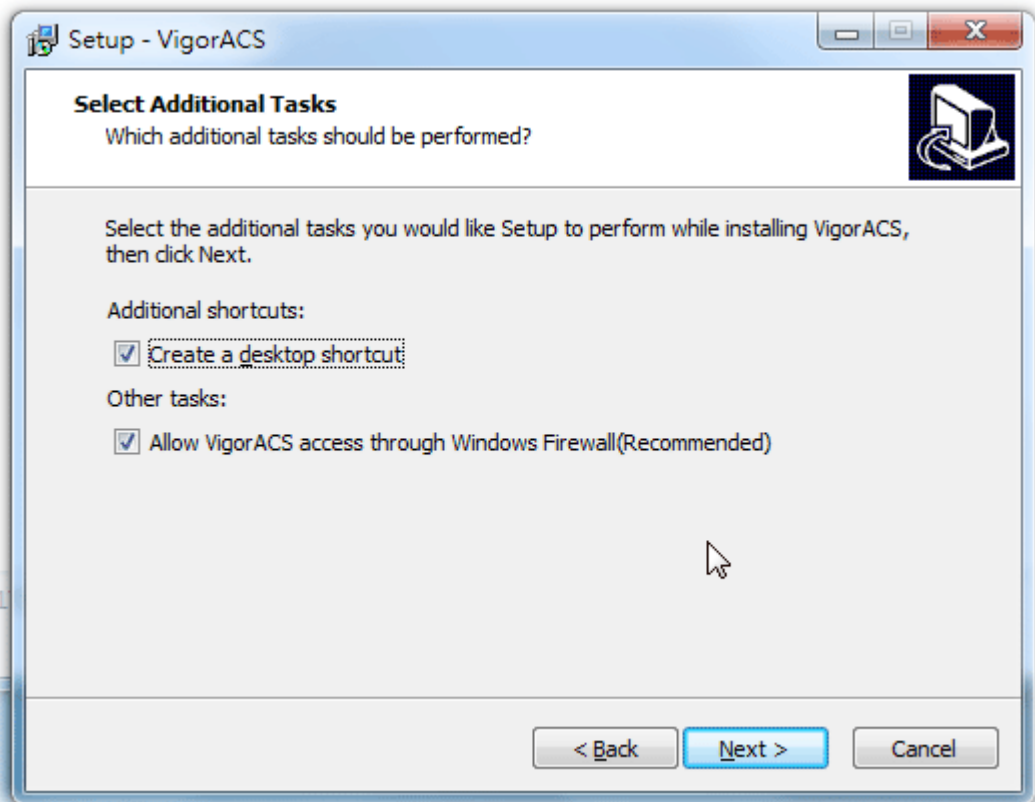
- Determine the destination folder and click **Next**. The default directory used by this program is *C:\Program Files\VigorACS*. You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



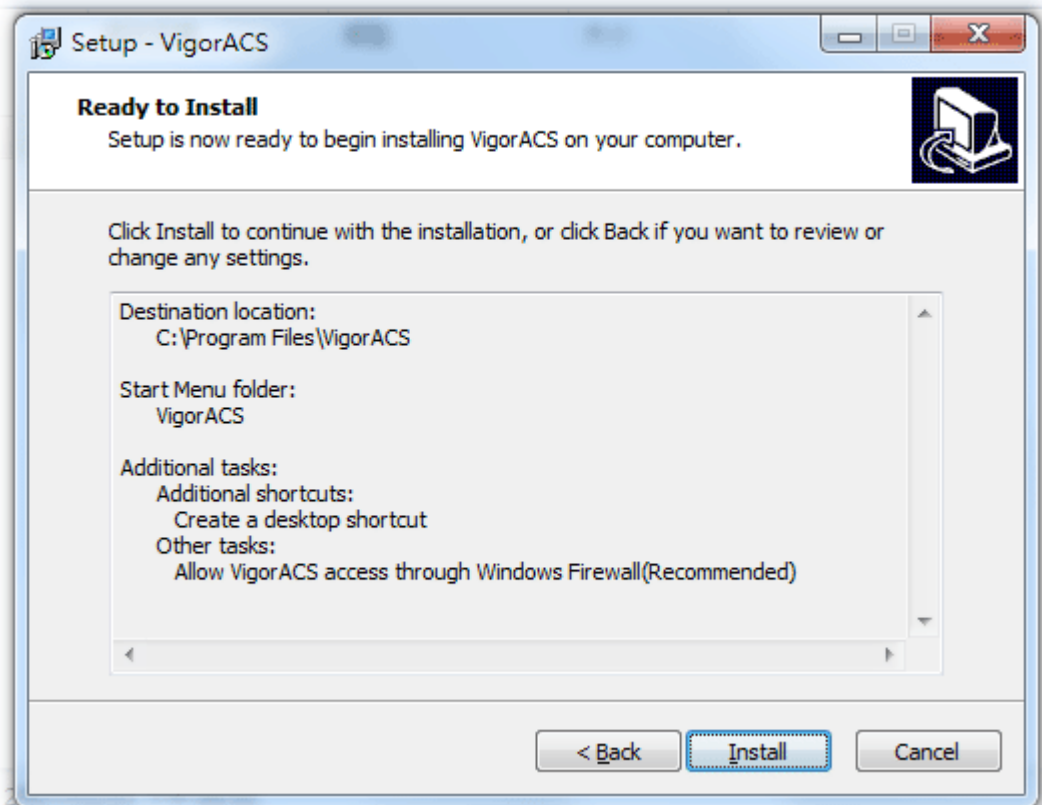
10. Determine the start menu folder and click **Next**. The default directory used by this program is *VigorACS*. You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



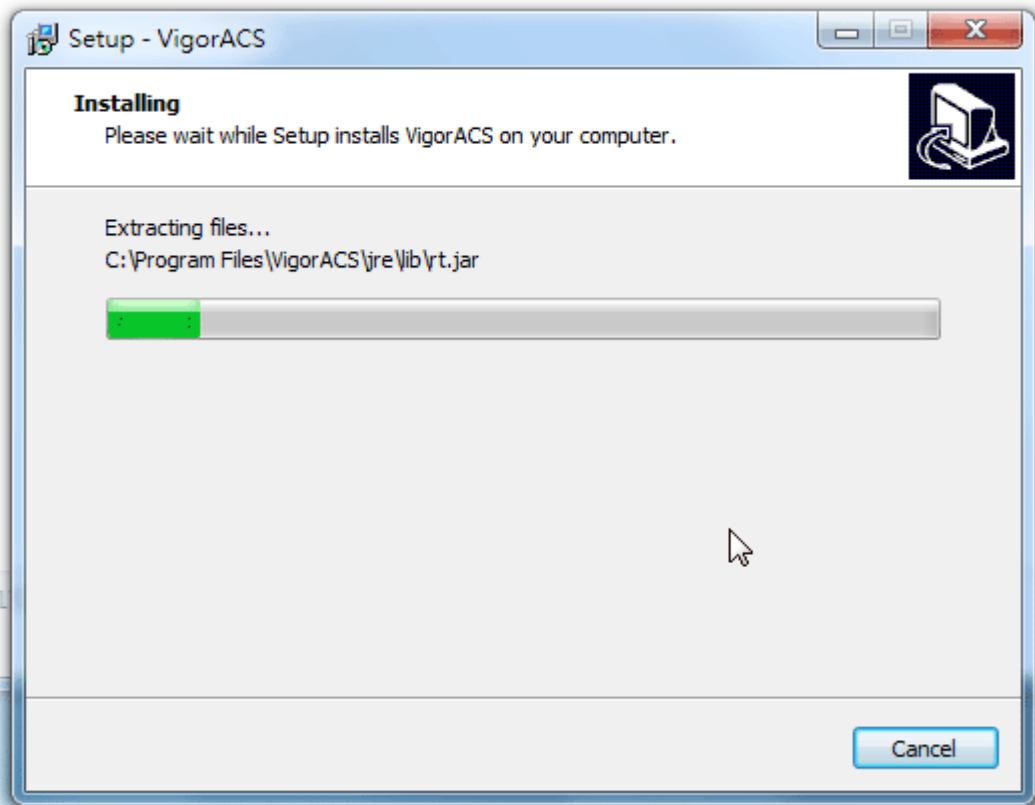
11. In this dialog, check the box of "Create a desktop shortcut" for your necessity. Click Next.



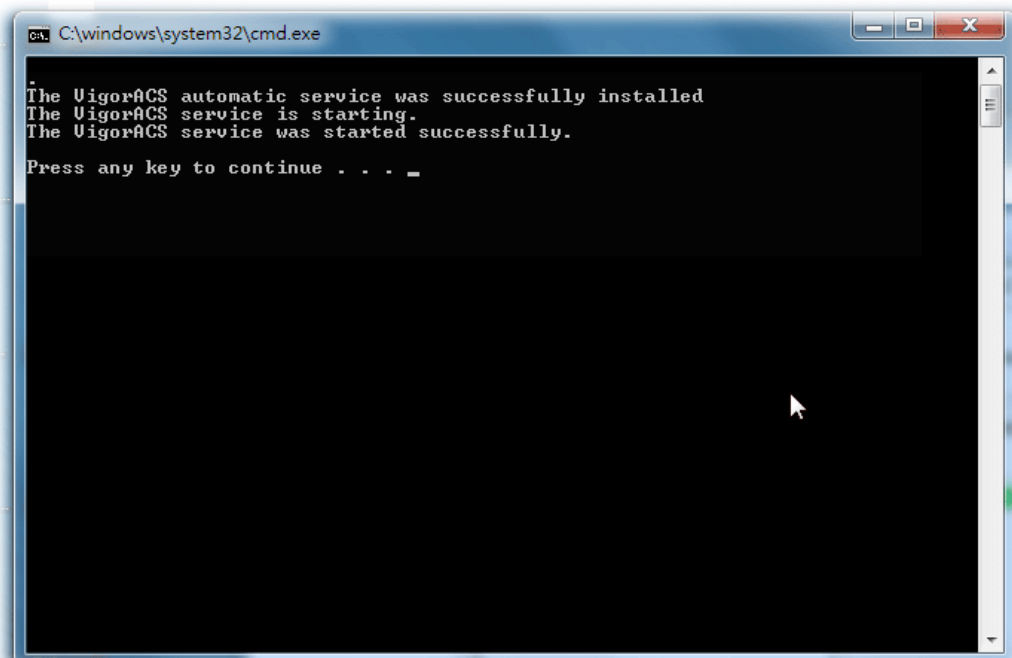
12. Now, the program is ready to install necessary features and files to your computer. Please click **Install** to start.



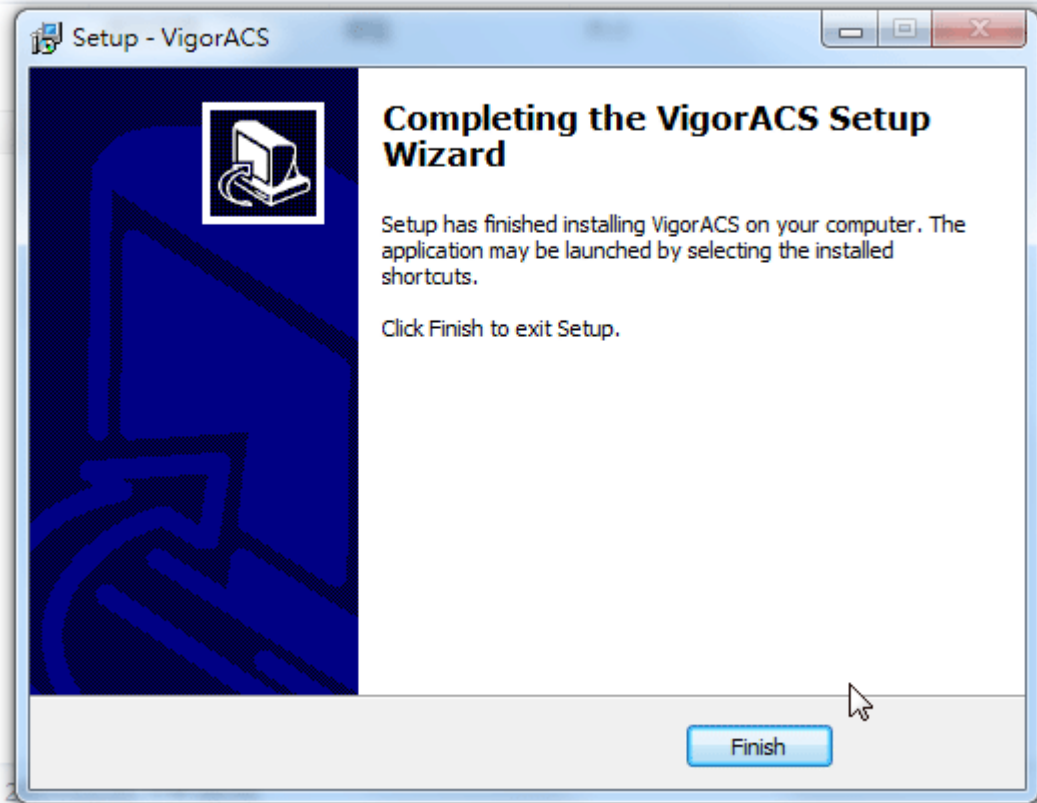
13. Please wait for a while to complete the installation.



14. While installing, the following screen will appear to show that MariaDB has been activated. Please wait for next dialog appearing.



15. Now the program has completed the installation of VigorACS 2. Click Finish to exit it.



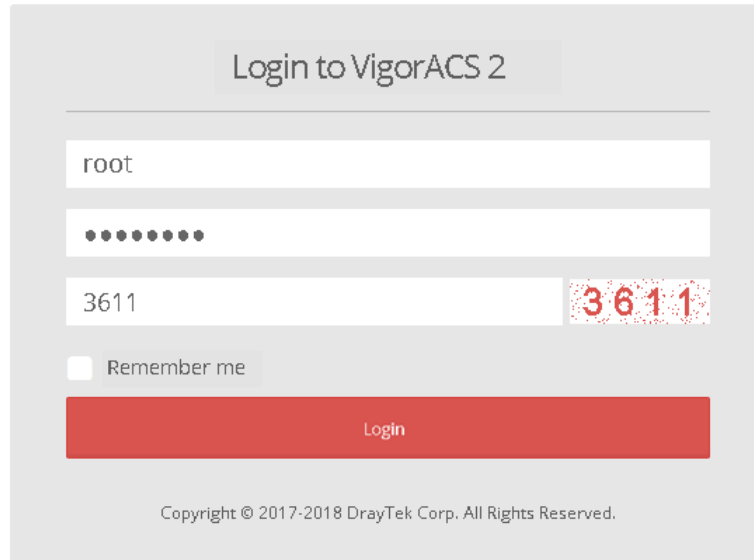
2.1.4 StartMySQL/MariaDB Database

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

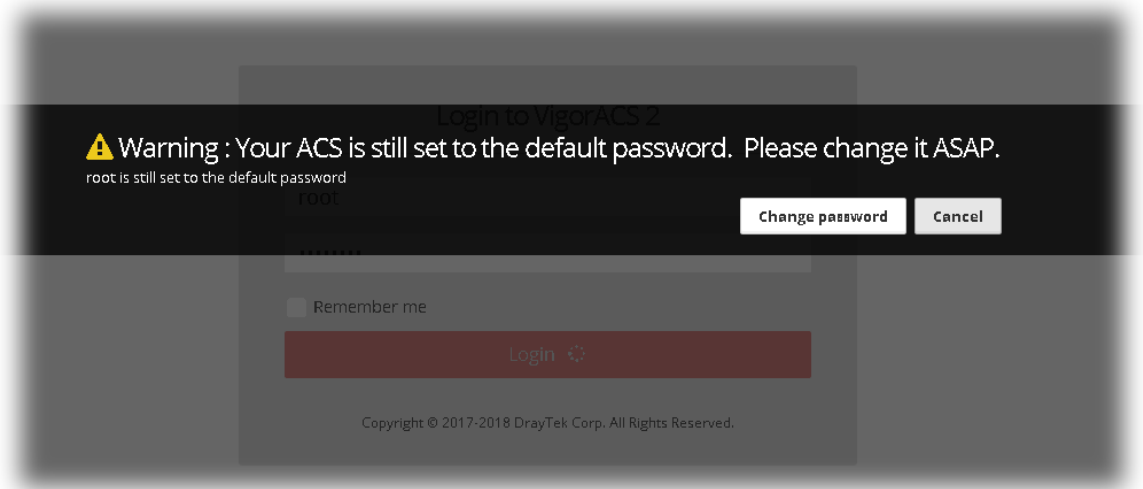
Normally, you don't need to worry about this step on Windows. But if you find any problems on VigorACS, you should check mysql/mariadb first. Please go to Windows Service check the MySQL/MariaDB Service starts or not.

2.1.5 Start VigorACS

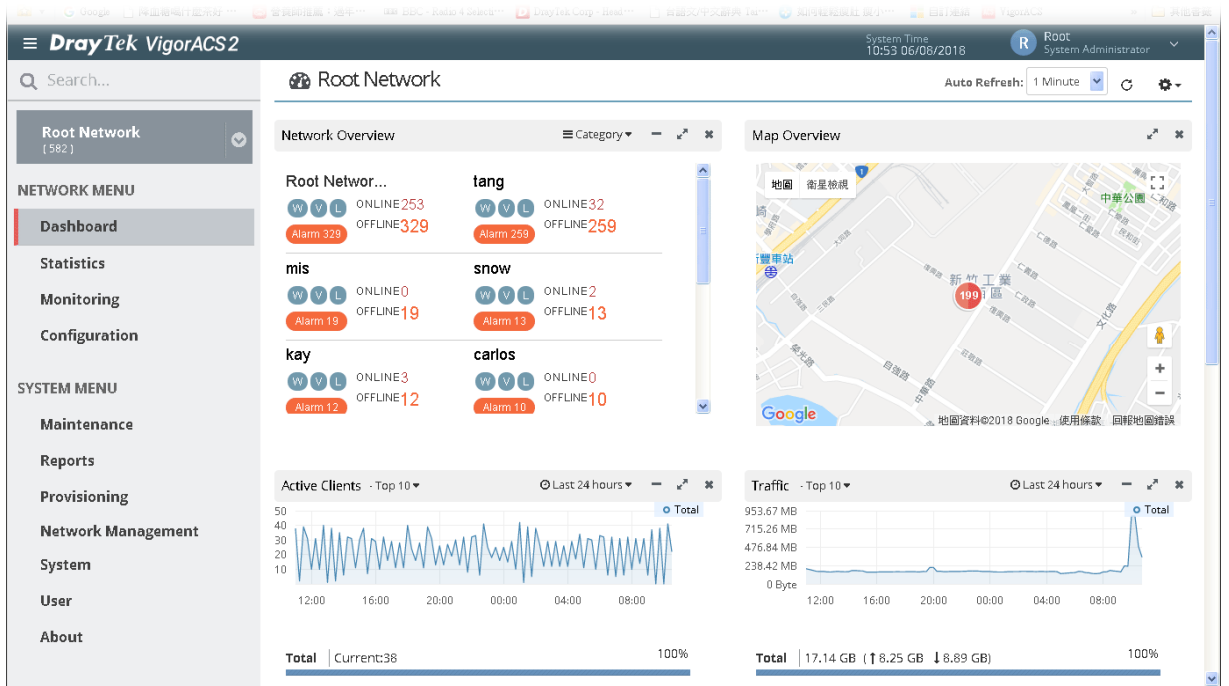
1. Login VigorACS. Use a web browser and type "*localhost:portnumber*". Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be "*localhost:8011*".
2. The login page of VigorACS will be shown as 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 2 will be shown as below.



Info

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

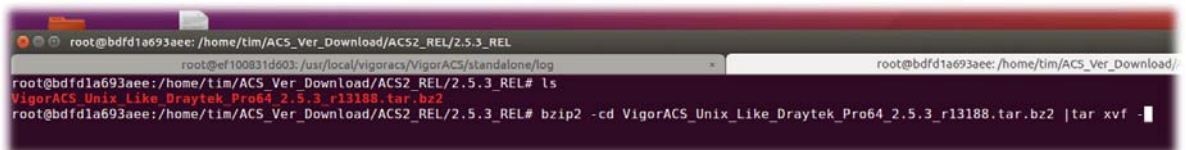
Follow the steps listed below to install VigorACS under Linux:

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_XXXXXXX_XXXXXX.tar.bz2 | tar xvf -  
or  
#tar -jxv -f VigorACS_Unix_Like_XXXXXXX_XXXXXX.tar.bz2
```

3. Decompress the setup packages

```
bzip2 -cd VigorACS_Unix_Like_XXXXXXX_XXXXXX.tar.bz2 |tar xvf -
```



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

```
chmod 755 ./install.sh  
chmod 755 ./uninstall.sh
```

```

-rw-r--r-- 1 root root      1807 Oct  9 11:39 Install VigorACS Guide.txt
-rw-r--r-- 1 root root      2972 Oct  9 11:39 Quick Start Guide.txt
-rw-rw-r-- 1 1000 1000 1337654060 Jan 10 16:18 VigorACS_Unix_Like_Draytek_Pro64_2.5.3_r13188.tar.bz2
drwxr-xr-x 2 root root      4096 Jan 10 16:38 acs/
-rw-r--r-- 1 root root     10968 Oct 17 01:00 acs_lib.sh
drwxr-xr-x 2 root root      4096 Jan 10 16:38 font/
-rw-r--r-- 1 root root       631 Oct  9 11:39 install.conf
-rw-r--r-- 1 root root     64660 Oct 31 11:10 install.sh
drwxr-xr-x 2 root root      4096 Jan 10 16:38 jcelib/
drwxr-xr-x 2 root root      4096 Jan 10 16:39 linux/
drwxr-xr-x 3 root root      4096 Jan 10 16:39 scripts/
-rw-r--r-- 1 root root      2422 Oct  9 11:43 uninstall.sh
root@bdf1a693aee:/home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL# chmod 755 install.sh
root@bdf1a693aee:/home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL# chmod 755 uninstall.sh
root@bdf1a693aee:/home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL# █

```

5. Execute ./install.sh installation file.

```

-rw-r--r-- 1 root root       631 Oct  9 11:39 install.conf
-rwxr-xr-x 1 root root     64660 Oct 31 11:10 install.sh*
drwxr-xr-x 2 root root      4096 Jan 10 16:38 jcelib/
drwxr-xr-x 2 root root      4096 Jan 10 16:39 linux/
drwxr-xr-x 3 root root      4096 Jan 10 16:39 scripts/
-rwxr-xr-x 1 root root      2422 Oct  9 11:43 uninstall.sh*
root@bdf1a693aee:/home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL# ./install.sh
ping IPv4 address success

entering /home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL/linux.....

```

Please make sure you have /usr/bin/sh first. If you don't have /usr/bin/sh, please enter the command on the screen:

```
#ln -s /bin/sh /usr/bin/sh
```

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

```

drwxr-xr-x 2 root root      4096 Jan 10 16:38 jcelib/
drwxr-xr-x 2 root root      4096 Jan 10 16:39 linux/
drwxr-xr-x 3 root root      4096 Jan 10 16:39 scripts/
-rwxr-xr-x 1 root root      2422 Oct  9 11:43 uninstall.sh*
root@bdf1a693aee:/home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL# ./install.sh
ping IPv4 address success

entering /home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL/linux.....

Please create /usr/local/vigoracs
Create it now? (y/n)
y█

```

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

```

entering /home/tim/ACS_Ver_Download/ACS2_REL/2.5.3_REL/linux.....

Please create /usr/local/vigoracs
Create it now? (y/n)
y

We'll install the following packages for showing captcha (For some Linux version e.g. Ubuntu, Debian):
- xfonts-base
- fontconfig
- libncurses5
Install now(y/n)?
y█

```


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.

```
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for systemd (229-4ubuntu19) ...

You must restart this ACS Server manually to finish the installation process

Notice:
* Installation ACS Server requires root privileges.
* After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
█
```

- (1) Install MySQLI/MariaDB
- (2) Change root password and security configuration of MySQLI/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 :



Info

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'
```



Info

The password set in this step is used for VigorACS 2 to login database.

```

You must restart this ACS Server manually to finish the installation process
Notice:
  * Installation ACS Server requires root privileges.
  * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
1
Do you want to install mariadb(mariadb-10.3.12) ... (y/n)?

```

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.

```

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
2

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):

```



Info

The password set in this step is used for VigorACS 2 to login database.

11. Input 3 to install InfluxDB.

```

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
3
Do you want to install influxdb(influxdb-1.6.1) ... (y/n)?

```

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

12. Input 4 to install Java.

```

ln -s /usr/local/InfluxDB/bin influxdb

If you upgrade the ACS (from the version before 2.4.0) for the first time,
please remember to run the rrd2influxdb tool to convert the existed/old data after ACS upgrade.
It will on the /usr/local/vigoracs/VigorACS/convert_rrd2_Influxdb/ path. For more explanation,
you may refer the /usr/local/vigoracs/VigorACS/convert_rrd2_Influxdb/readme.txt document.

Notice:
  * Installation ACS Server requires root privileges.
  * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
4
Do you want to install jdk(openjdk-12.0.2.9) ... (y/n)?

```

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.

```

openjdk-12.0.2.9-linux-x64/man/man1/rmid.1
openjdk-12.0.2.9-linux-x64/man/man1/rmiregistry.1
openjdk-12.0.2.9-linux-x64/man/man1/serialver.1
openjdk-12.0.2.9-linux-x64/man/man1/unpack200.1
openjdk-12.0.2.9-linux-x64/release
ln -s /usr/local/openjdk-12.0.2.9-linux-x64 /usr/javase

Notice:
  * Installation ACS Server requires root privileges.
  * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
5
[Install VigorACS]
[Warning] It will clear the existing ACS database and create a new one. Do you want to continue? (y/n)

```

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

```

input select num :
5
[Install VigorACS]

[Warning] It will clear the existing ACS database and create a new one.Do you want to continue? (y/n)
y
Do you want to use remote/local database? (1: Local side database, 2: Remote side database, Enter for Local side database)

Which Mysql do you want to use ? (1: ACS , 2: OS default, Enter for ACS mysql)

MySQL is running!!
Please keyin password of root of MySQL/MariaDB.

Do you want to test password now?(y/n)
y

Access Database Success
Start to install VigorACS...

```

```

1. standalone-secure.xml
   * Supported Protocols: TLS 1.3 only
2. standalone.xml (Recommended)
   * Supported Protocols: TLS 1.2 only
3. standalone-compatible.xml
   * Supported Protocols: TLS 1.0 or above

Note that:
- The TLS 1.2 and TLS 1.3 protocols might cause the CPE with older firmware failing to register on VigorACS.
- JAVA 11 will be a mandatory requirement to run the configuration in standalone-secure.xml.
2
Current JBoss Configuration: standalone.xml
Generate default tr069.keystore...
After installing VigorACS , tr069 will be created automatically.
Start to create tr069 database ....
Drop and Create tr069 database NOW !!
Create tr069 database successfully....
Create tr069 database table....

```

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

```

Notice:
  * Installation ACS Server requires root privileges.
  * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB ( Default root password is blank )
[3] Install InfluxDB
[4] Install or Upgrade Java
[5] Install VigorACS ( It will build one MySQL/MariaDB database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :
7
Please keyin IP:Port of root of Remote MySQL/MariaDB.
Please keyin IP (default IP: 127.0.0.1) :

```

15. Input 7 to finish and exit the installation.



Info 1

Step 13 is required for establishing remote database only. You can ignore it while building local database.

Info 2

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 Database

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.

```
root@bdf1a693aee:/usr/local/vigoracs/VigorACS/bin# ./vigoracs.sh
Mysql process id : 1286 1388
InfluxDB process id : 1430
VigorACS process id :
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
Input select num :
```

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.

```
root@bdf1a693aee:/usr/local/vigoracs/VigorACS/bin# ./vigoracs.sh
Mysql process id : 1286 1388
InfluxDB process id : 1430
VigorACS process id :
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
Input select num :
```

Select item 3 to start InfluxDB.

2.2.4 Start VigorACS

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

```
root@bdf1a693aee:/usr/local/vigoracs/VigorACS/bin# ./vigoracs.sh
Mysql process id : 1286 1388
InfluxDB process id : 1430
VigorACS process id :
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
Input select num :
```

Select item 5 to start VigorACS.

```

Mysql process id : 1286 1388
InfluxDB process id : 1430
VigorACS process id :
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
Input select num :
5
Which HTTP port do you want to bind for VigorACS service ( port number or Enter for 80 port)?
Which HTTPS port do you want to bind for VigorACS service ( port number or Enter for 443 port)?
Which ip address do you want to bind for VigorACS service ( x.x.x.x or Enter for bind 0.0.0.0 address)?
Which STUN port do you want to bind for VigorACS service ( port number or Enter for 3478 port)?
Which syslog port do you want to bind for VigorACS service ( port number or Enter for 514 port)?
How many memory do you want to set for VigorACS service? (Enter for default MAX Memory is 1024, MIN Memory is 900 MB)
MAX Memory What you want? (Unit: MB)
MIN Memory What you want? (Unit: MB)
* Starting WildFly Application Server 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.



Info 1

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.

Info 2

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.

Registration for VigorACS via Windows Platform

Below shows the steps to register VigorACS:

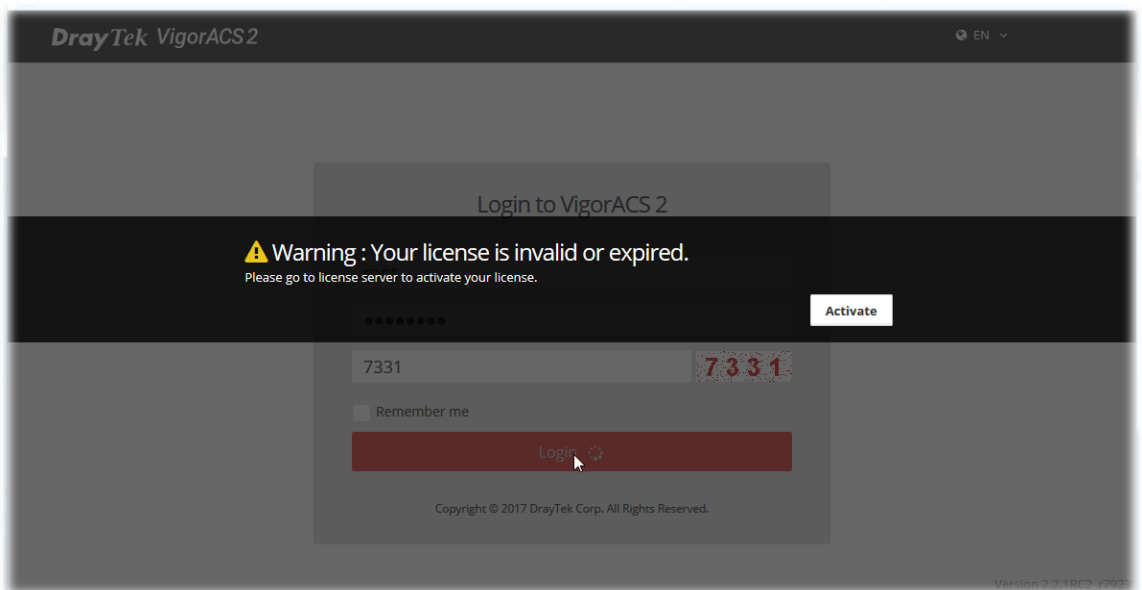
1. Login VigorACS. Use a web browser and type *"localhost:portnumber"*. Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be *"localhost:8011"*.
2. The login page of VigorACS will be shown as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



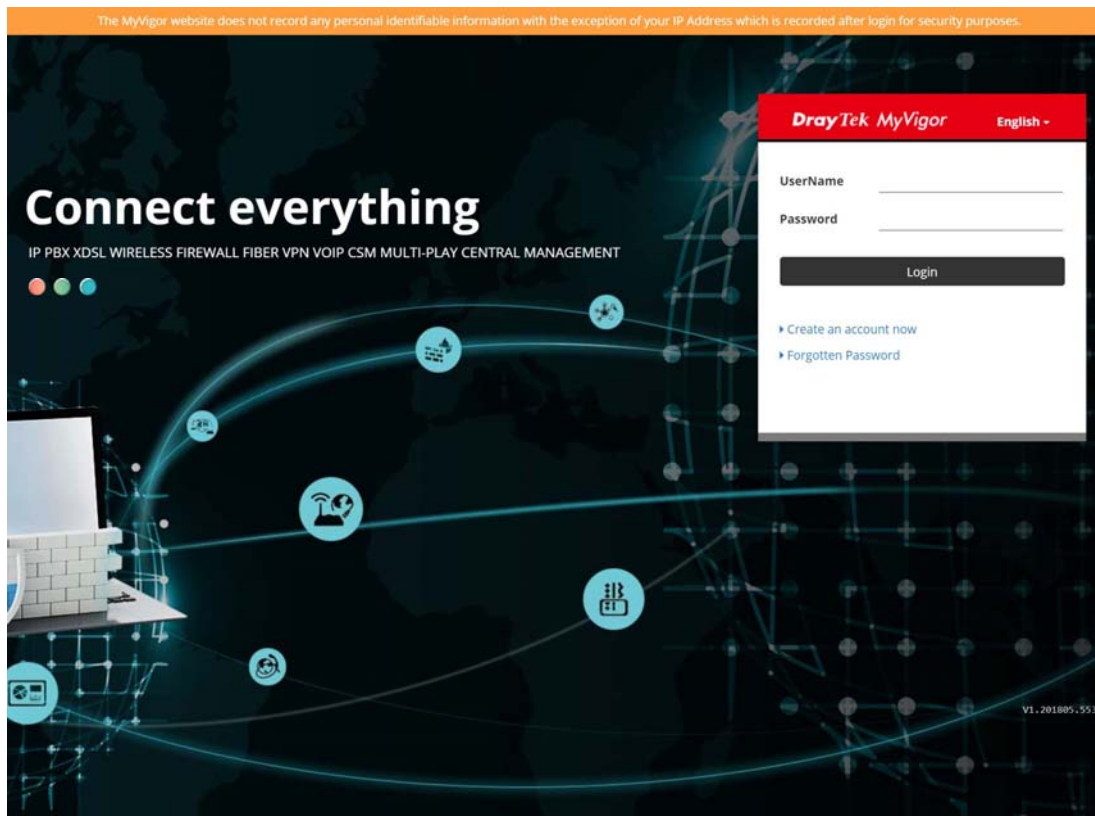
Info

“root” and “admin123” are default settings.

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



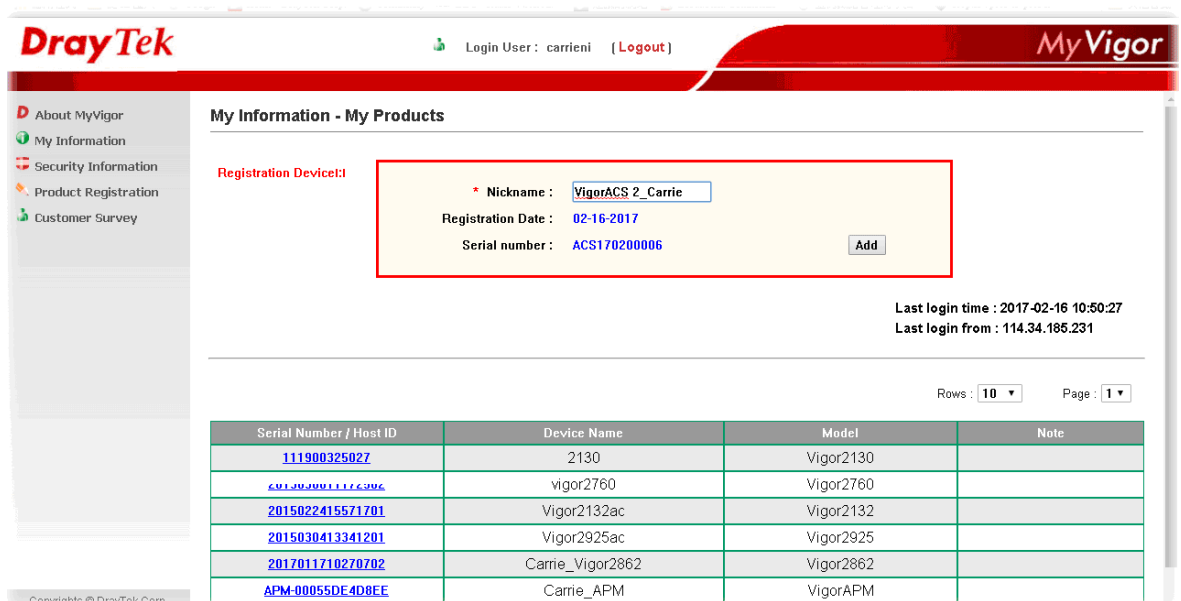
- A login page for MyVigor web site will be popped up automatically. Type your account (user name) and password in this page. Check the box of "I'm not a robot". Then, click Login.



Info

If you do not have any account, simply click [Create an account now](#) to create a new one for using the service provided by MyVigor web site.

- 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.



- Type a nickname for VigorACS and click Add.

My Information - My Products

Registration Device!:

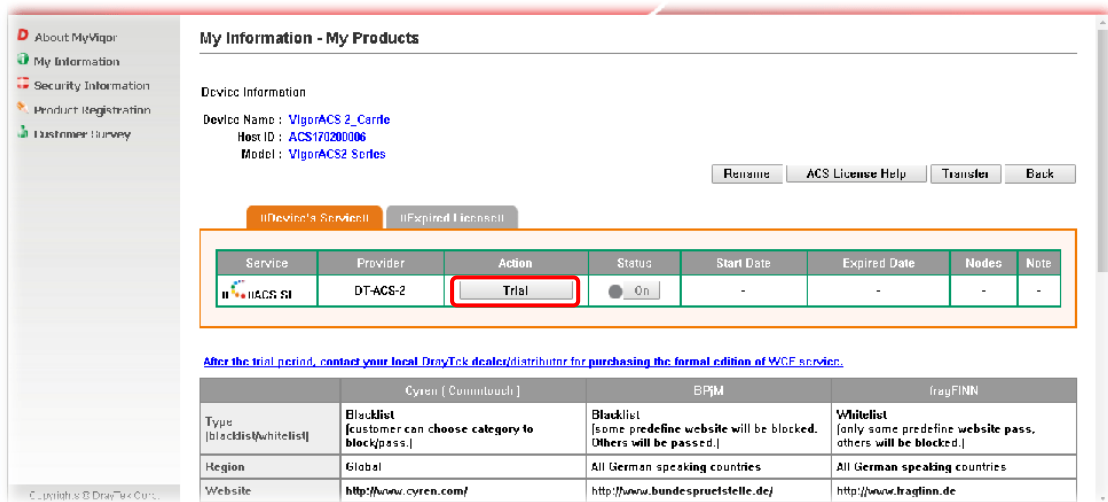
* Nickname :	<input type="text" value="VigorACS 2_Carrie"/>
Registration Date :	02-16-2017
Serial number :	ACS170200006
	<input type="button" value="Add"/>

7. After clicking **Add**, you can see the following screen. Click **OK**.



Your device has been successfully added to the database.

8. You will get a device information page as shown below. If you are the new user of VigorACS, you can get a free charge of 30-day service of VigorACS. Simply click the **Trial** button.



My Information - My Products

Device Information

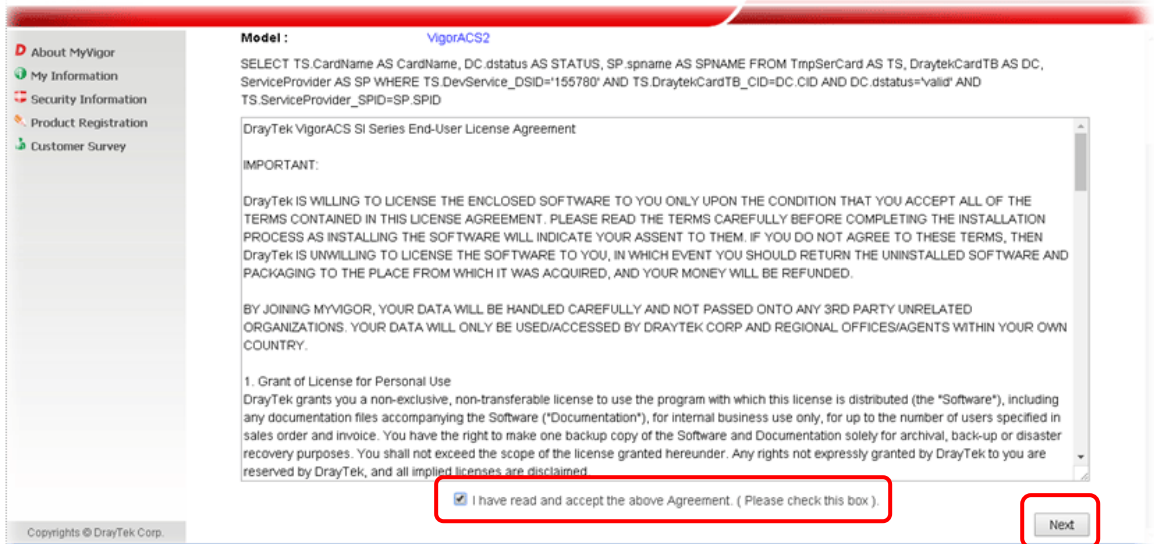
Device Name : VigorACS 2_Carrie
Host ID : ACS170200006
Model : VigorACS2 Series

Service	Provider	Action	Status	Start Date	Expired Date	Nodes	Note
VigorACS SI	DT-ACS-2	<input type="button" value="Trial"/>	<input type="checkbox"/> On	-	-	-	-

[After the trial period, contact your local DrayTek dealer/distributor for purchasing the formal edition of WCF service.](#)

	Cyren (Commitouch)	BPJM	fragFINN
Type [blacklist whitelist]	Blacklist [customer can choose category to block/pass.]	Blacklist [some predefine website will be blocked. Others will be passed.]	Whitelist [only some predefine website pass, others will be blocked.]
Region	Global	All German speaking countries	All German speaking countries
Website	http://www.cyren.com/	http://www.bundespruetzstelle.de/	http://www.fragfinn.de

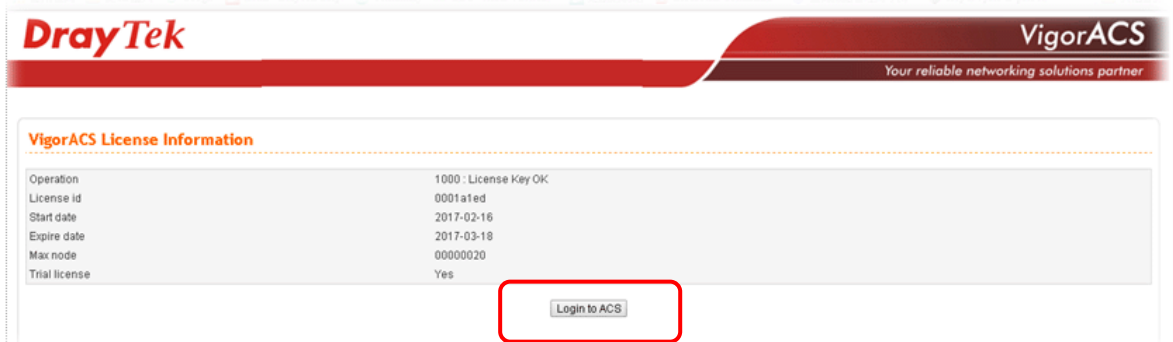
9. From the following screen, check the box of "I have read and accept the above...." and click **Next**.



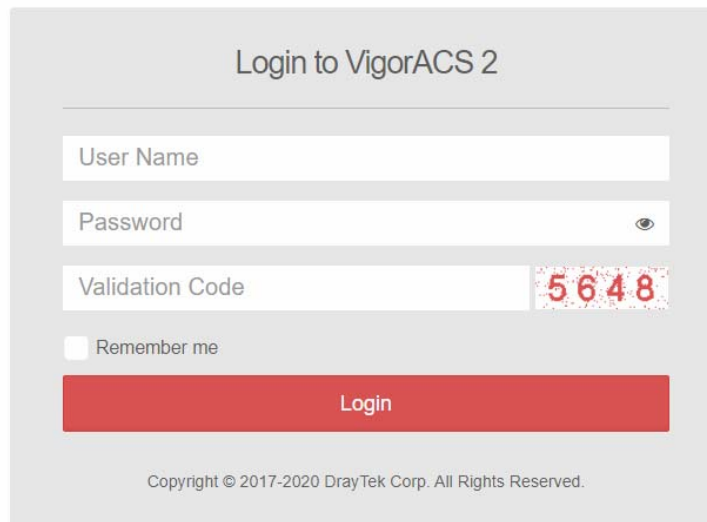
10. In the page below, click Register.



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

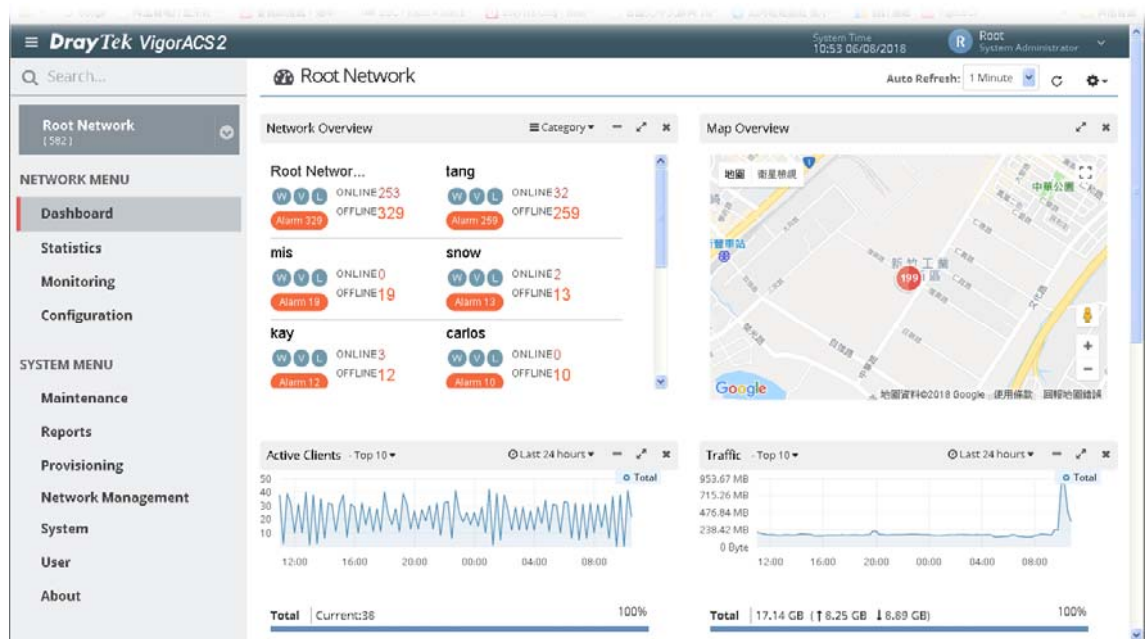


12. The login page will appear as follows. Type the default settings of User Name (root) and Password (admin123) and type the authentication code. Then, click Login.



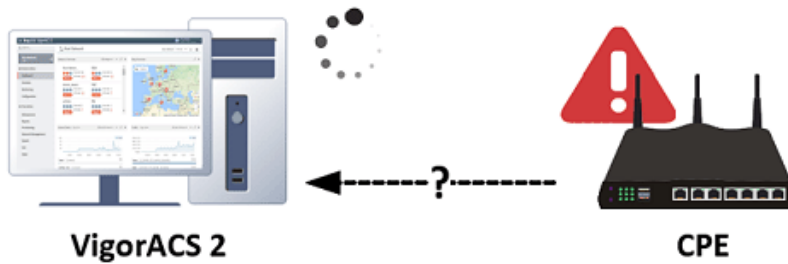
Copyright © 2017-2020 DrayTek Corp. All Rights Reserved.

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



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.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name: FAE_2926		
<input checked="" type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access		
Internet Access Control <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed: <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input checked="" type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input type="checkbox"/> Disable PING from the Internet		
Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports		
Telnet Port: 8023 (Default: 23)		
HTTP Port: 8080 (Default: 80)		
HTTPS Port: 443 (Default: 443)		
FTP Port: 8021 (Default: 21)		
TR069 Port: 8069 (Default: 8069)		
SSH Port: 50822 (Default: 22)		
Brute Force Protection <input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server		

- 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.

System Maintenance >> TR-069 Setting

ACS and CPE Settings	Health Parameters	Export Parameters
Tr069: <input type="radio"/> Disable <input checked="" type="radio"/> Enable		
ACS Server On: LAN/VPN		
ACS Server URL: http://acsfaq.draytek.com/ACSServer/services/ACSServlet Wizard <input type="checkbox"/> Acquire URL from DHCP option 43 Username: fae Password: ***** Test With Inform: <input type="checkbox"/> Event Code: PERIODIC		
Last Inform Response Time: Mon Nov 19 13:19:49 2018		
CPE Client <input type="radio"/> Http <input checked="" type="radio"/> Https Note: Https mode only works when Vigor ACS SI is 1.1.6 and above version. URL: https://192.168.66.1:8069/cwm/CRN.html Port: 8069 Username: vigor Password: *****		
Periodic Inform Settings <input type="radio"/> Disable <input checked="" type="radio"/> Enable Interval Time: 900 second(s)		

- 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 2

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.

STUN Settings

Disable
 Enable

Server Address:

Server Port:

Minimum Keep Alive Period: second(s)

Maximum Keep Alive Period: second(s)

- Check the ACL setting

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

DrayTek Vigor2926 Series

System Maintenance >> Management

IPv4 Management Setup

Router Name: DrayTek

Default: Disable Auto-Logout
 Enable Validation Code in Internet/LAN Access

Internet Access Control

Allow management from the Internet
 Domain name allowed:

FTP Server
 HTTP Server Enforce HTTPS Access
 HTTPS Server
 Telnet Server
 TR069 Server
 SSH Server
 SNMP Server

Disable PING from the Internet

Access List from the Internet

List	Index in IP Object	IP / Mask
1	1	11.22.33.44/255.255.255.255
2		
3		

Management Port Setup

User Define Ports Default Ports

Telnet Port: (Default: 23)
 HTTP Port: (Default: 80)
 HTTPS Port: (Default: 443)
 FTP Port: (Default: 21)
 TR069 Port: (Default: 8069)
 SSH Port: (Default: 22)

Brute Force Protection

Enable brute force login protection

FTP Server
 HTTP Server
 HTTPS Server
 Telnet Server
 TR069 Server
 SSH Server

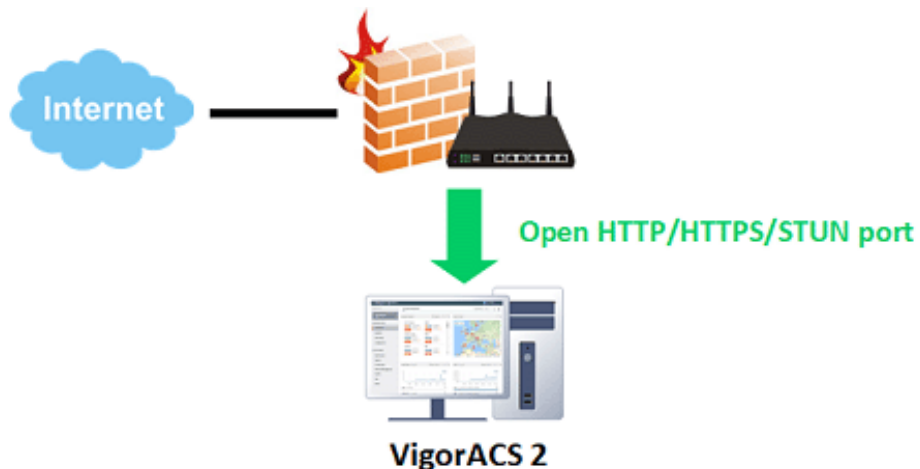
Maximum login failures: times
 Penalty period: seconds

Blocked IP List

- Check the firewall on ACS server

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

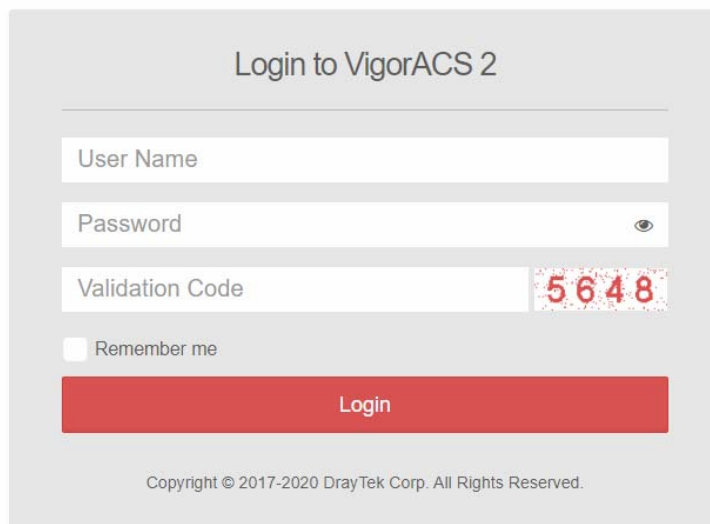
- HTTP port (Default tcp port 80)
- HTTPS port (Default tcp port 443)
- STUN port (Default udp port 3478)



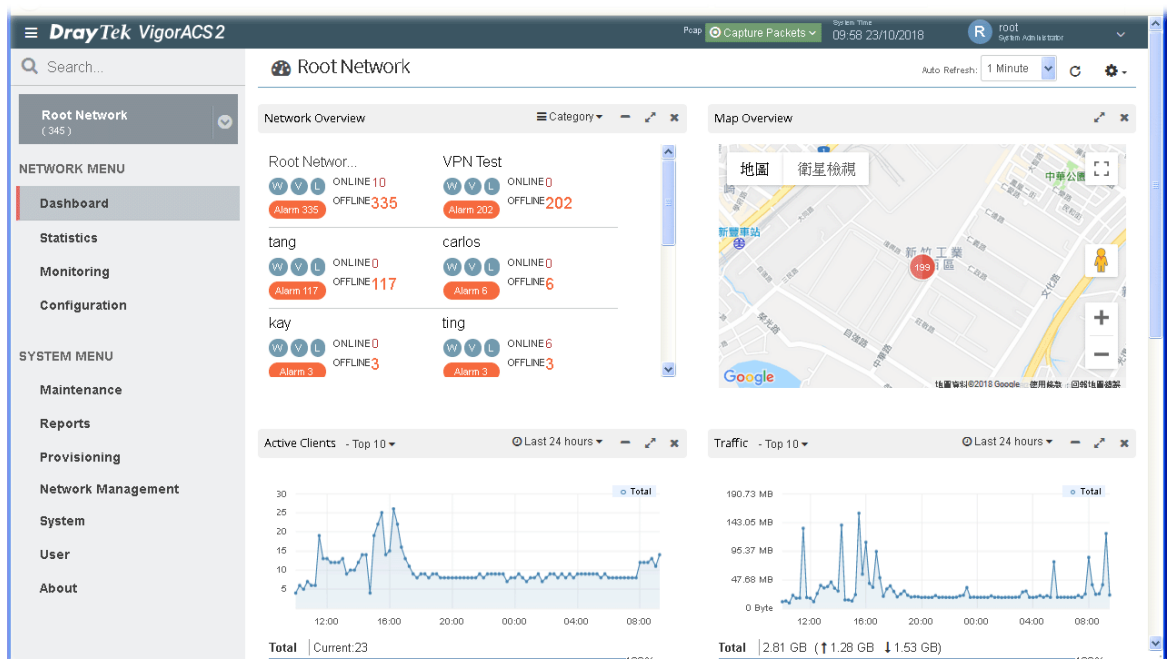
Chapter 3 Getting Started

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”*.

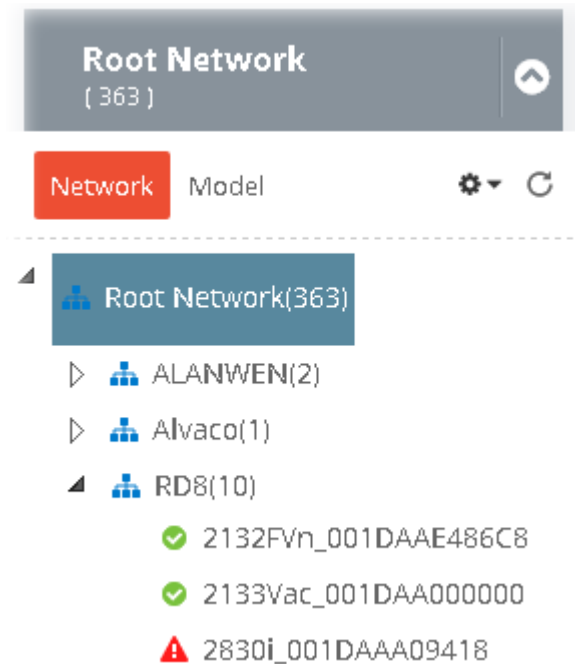


2. After clicking Login, main screen of VigorACS 2 will be shown as below.



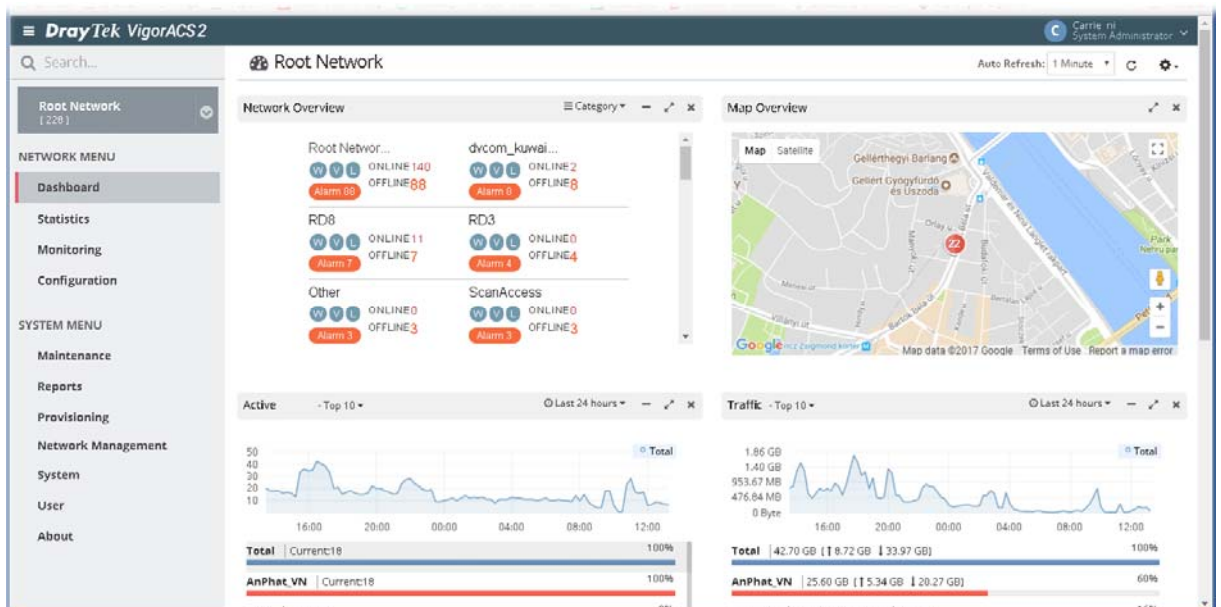
3.2 Dashboard

The information displayed on dashboard will be changed based on the network, group or device selected. To switch the dashboard among network, group and device, simply click Root Network on the home page to expand the tree view.



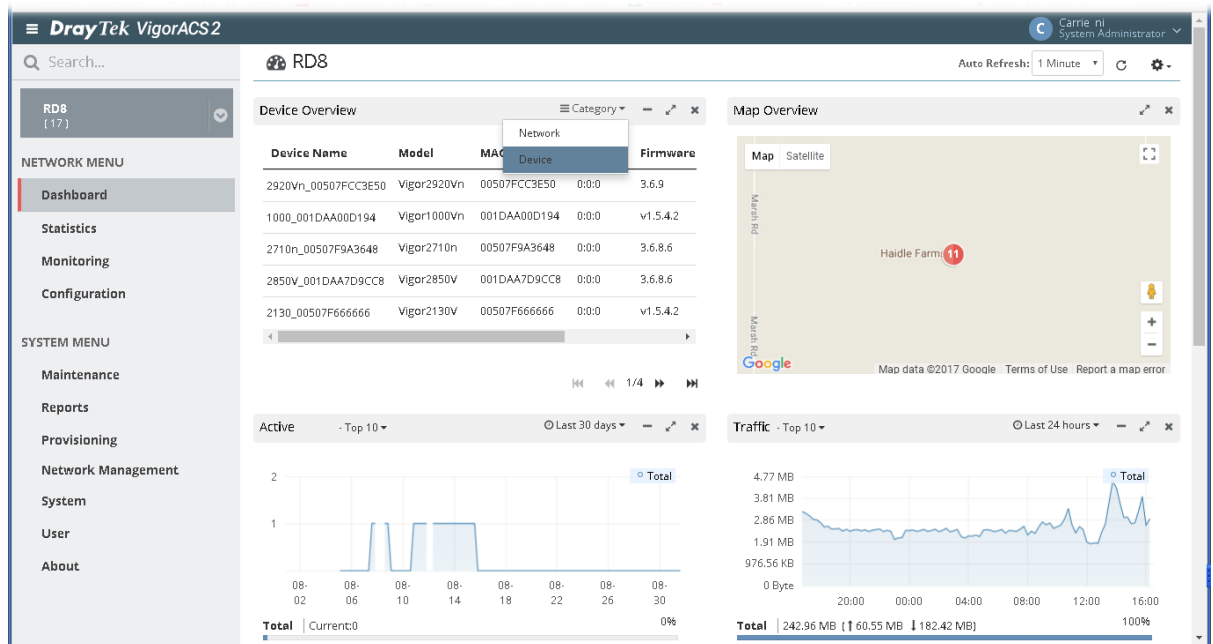
3.2.1 Dashboard for Root Network

The dashboard displays brief and quick overview information for the devices (CPE, Access Point) managed by VigorACS.



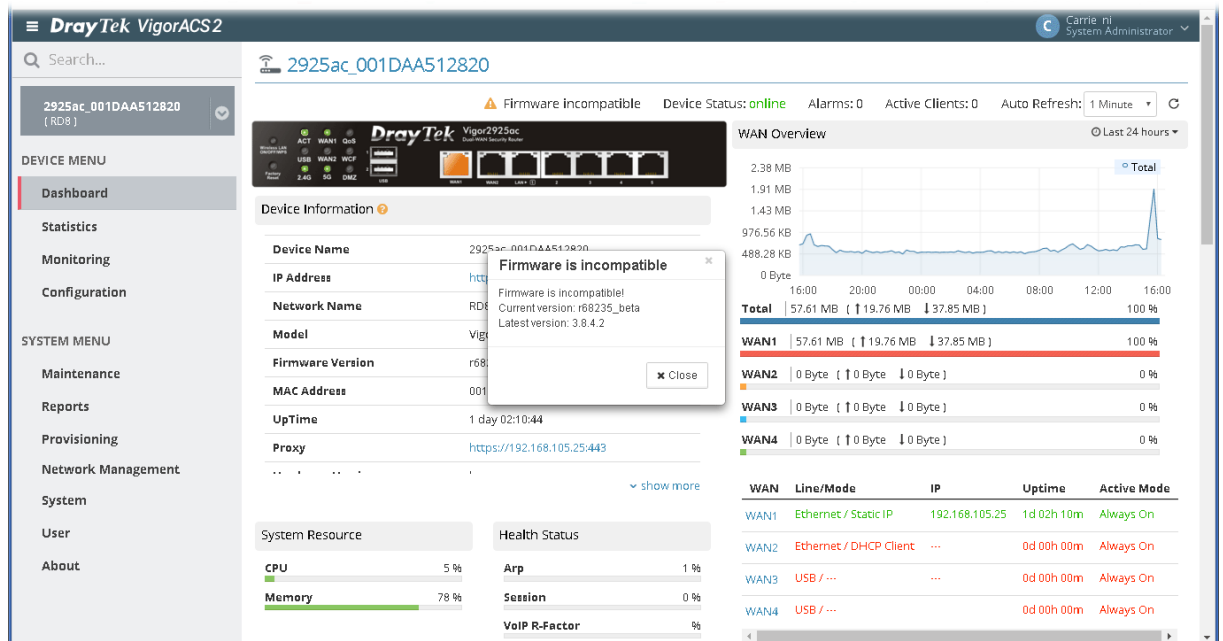
3.2.2 Dashboard for Group

This page offers information about device overview (including device name, model, MAC, up time, firmware version, LAN clients, and VPN), top 10 clients, new devices, map overview, traffic top 10 for the selected group.



3.2.3 Dashboard for Device (CPE, AP)

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, Map, and Quick Tools for the selected device.



Move the mouse cursor on the dashboard. When the mouse cursor becomes a "hand" on certain place, simply click it to access into the configuration page of that option.

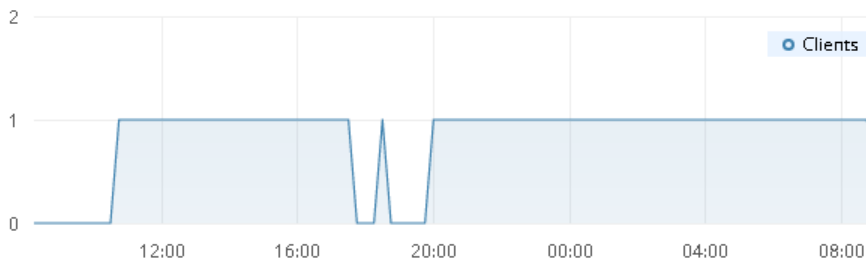
Quick Tools

[Backup Config](#) | [Restore Last Config](#) | [Download Last Config](#)

WAN	Line/Mode	IP	Uptime	Active Mode
WAN1	DSL / Static IP	192.168.105.60	0d 00h 13m	Always On
WAN2	Ethernet / DHCP Client	---	0d 00h 00m	Always On
WAN3	USB / ---	---	0d 00h 00m	Always On
WAN4	USB / ---	---	0d 00h 00m	Always On

LAN Overview

Last 24 hours ▾

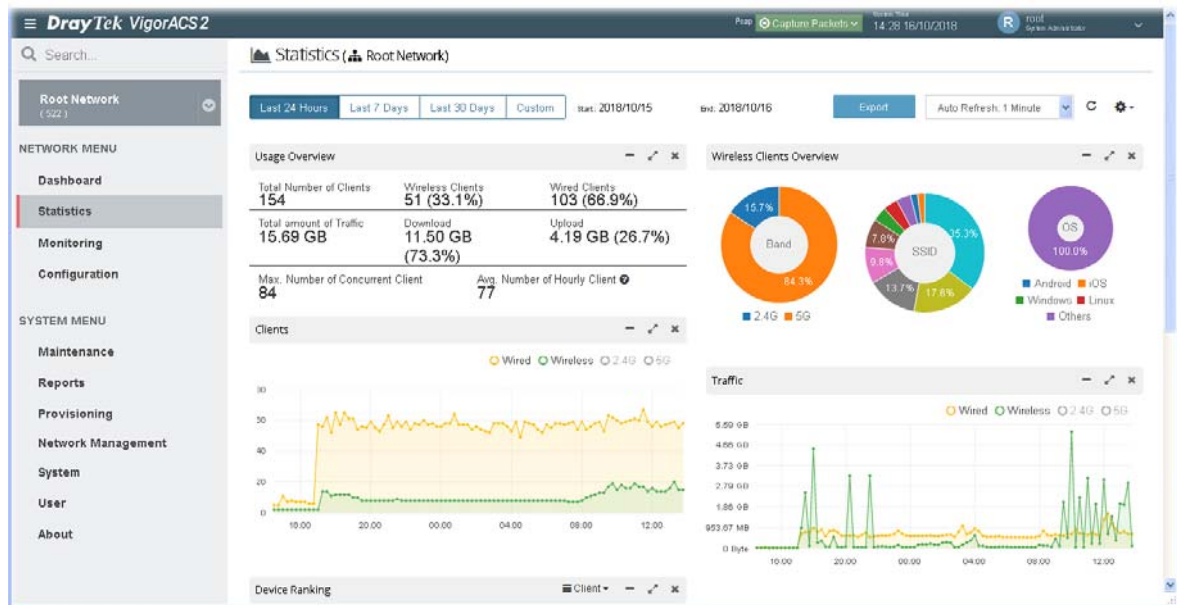


LAN	Status	IP/Mask	DHCP	Clients
LAN1	Enable	192.168.60.1 /24	On	0 (0%)

[show more](#)

3.2.4 Statistics for Network

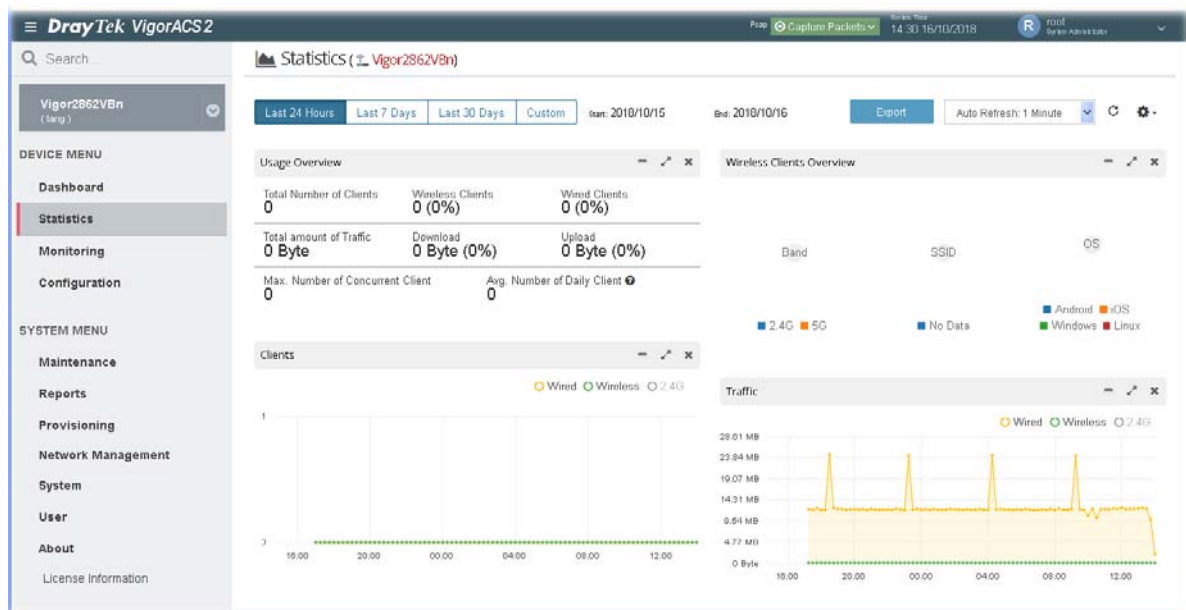
The page offers statistics for all the devices listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various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

3.2.5 Statistics for CPE

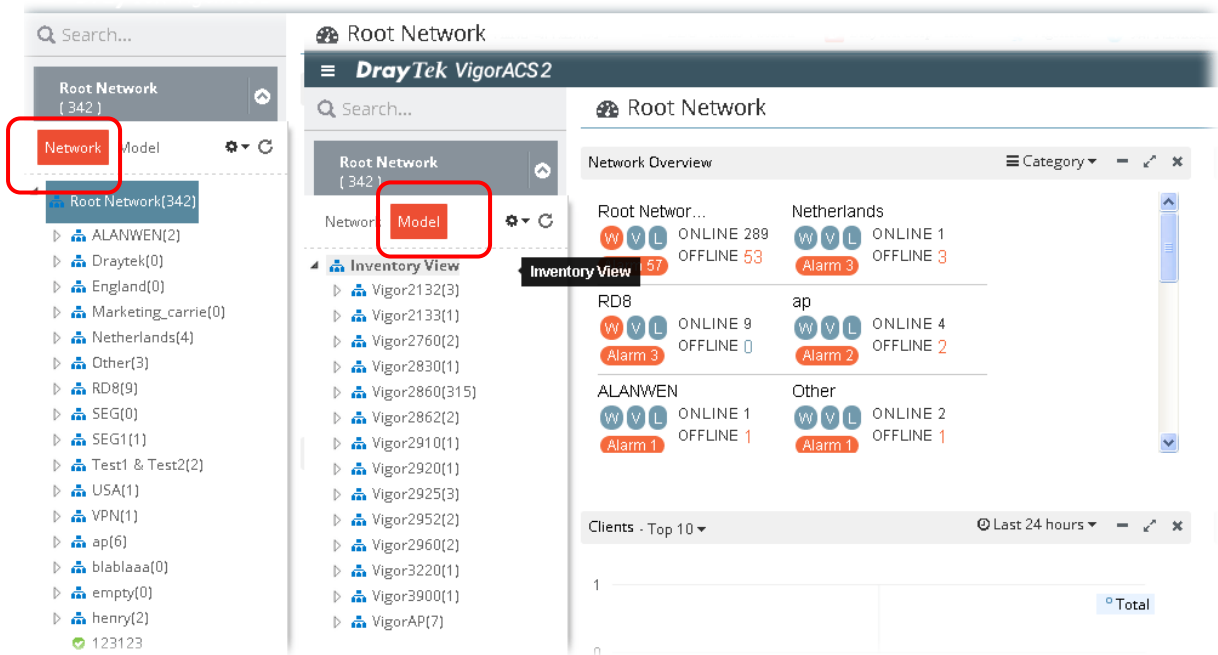
The page offers statistics for the selected device listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain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



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

3.2.6 Root Network and Inventory View

Root Network shows a tree view for all of the managed devices (CPE, Access Point) grouped under different networks. Inventory view allows the devices to be divided and categorized with the model series, such as Vigor2860 series, Vigor3900 series, and so on.

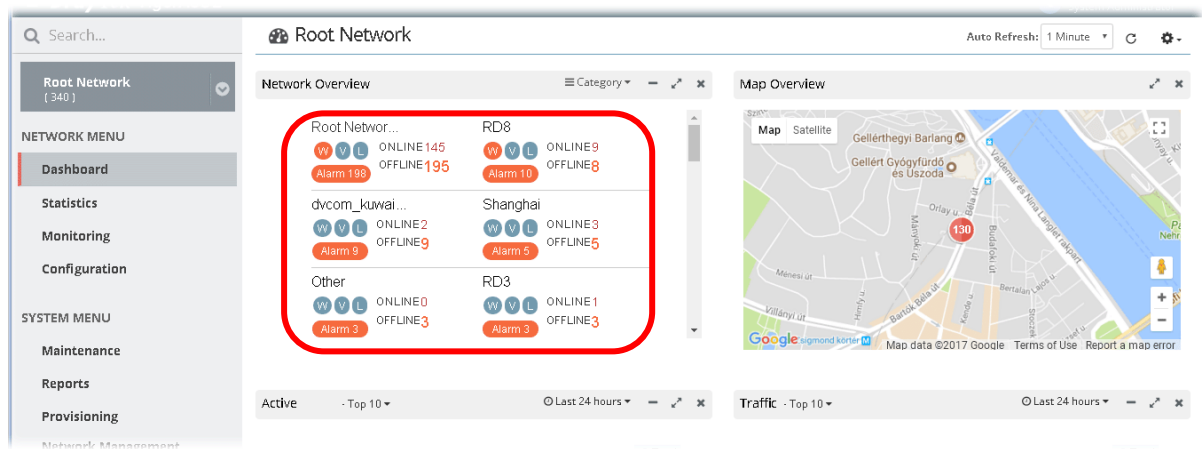


Click Network to display Root Network view; click Model to display the Inventory view.

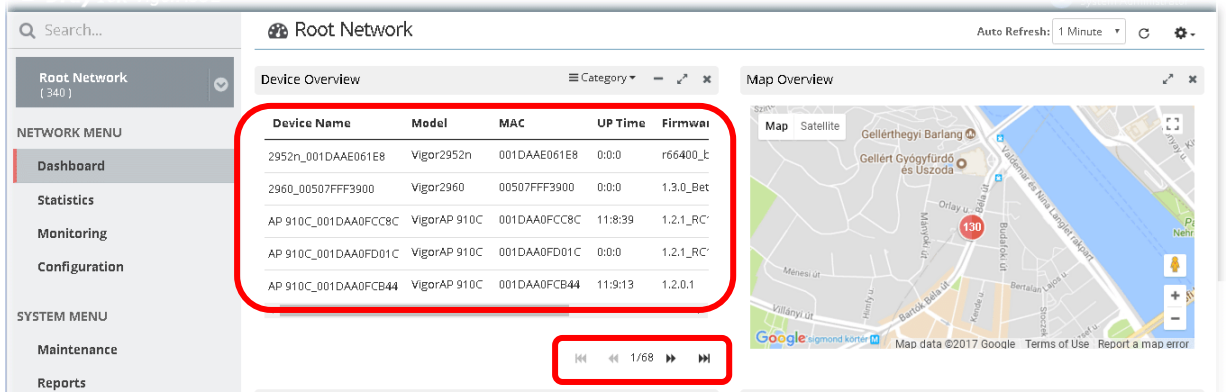
3.2.7 Network Overview

The network overview can be displayed by two methods, the Network Overview and the Device Overview. Click Category to switch these two methods.

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.



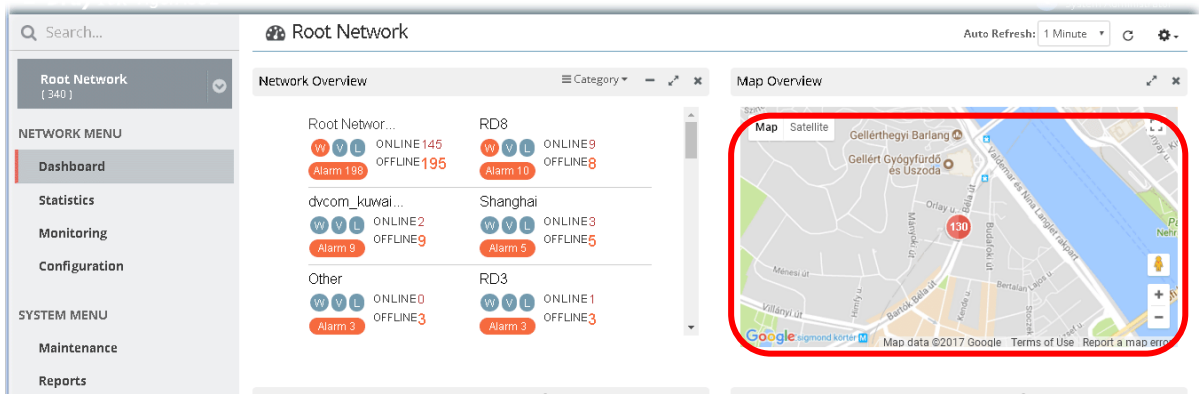
Under Device Overview, move the scroll bar left and right to check basic information for each device. Click >> (Next) or << (Previous) arrow to display next page for checking information for other devices.



3.2.8 Map Overview

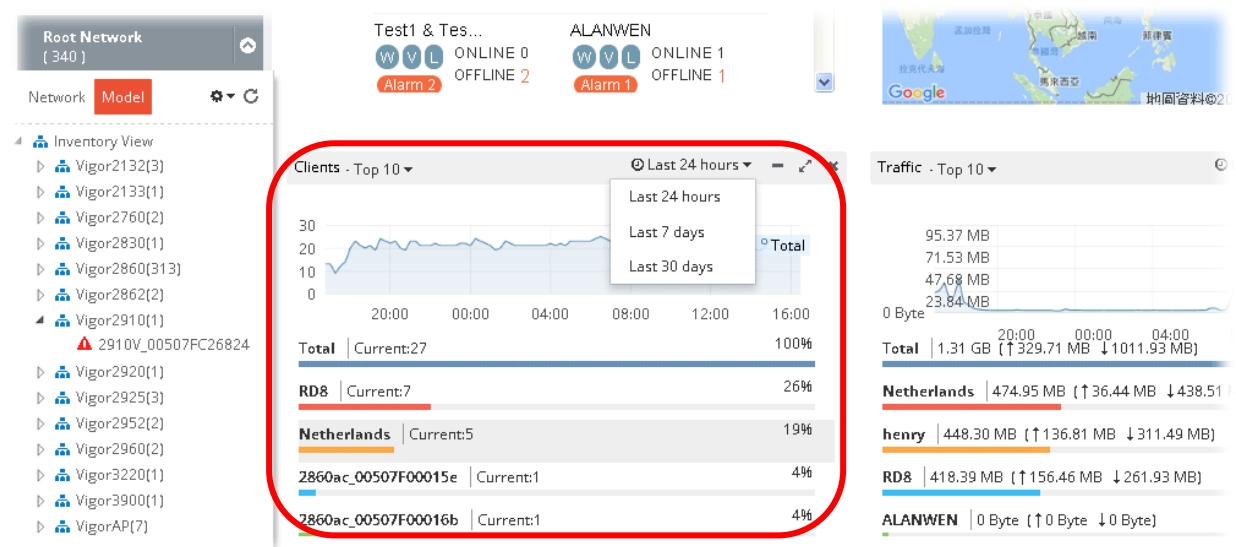
This map displays the location of the devices managed by VigorACS. The number on the map points the quantity of the devices classified under the root network or network group. Move your mouse on the number and click it. The map will be zoomed in with more detailed information.

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



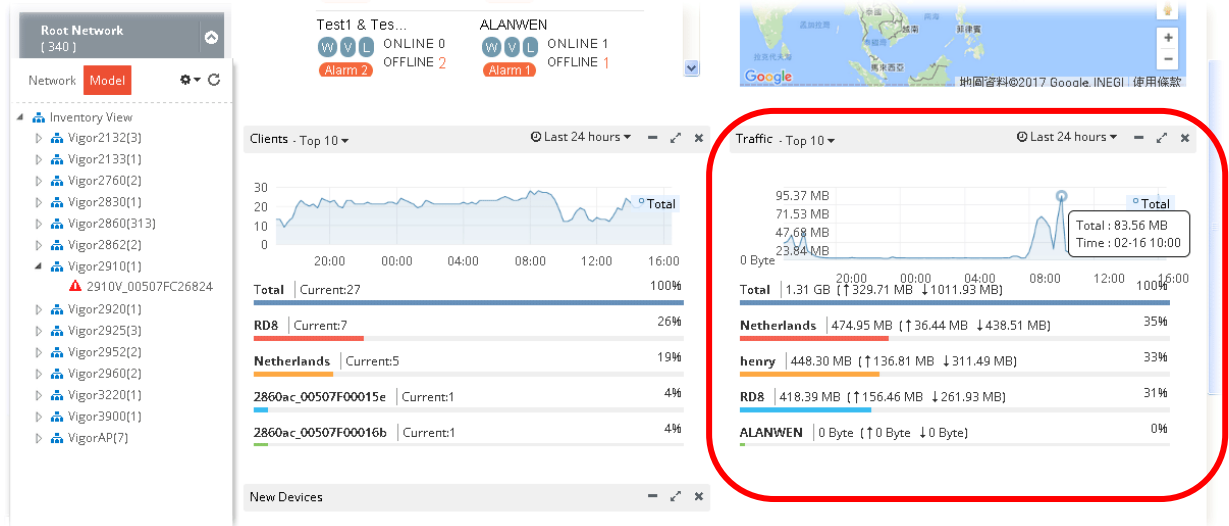
3.2.9 Top 10 for Clients

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



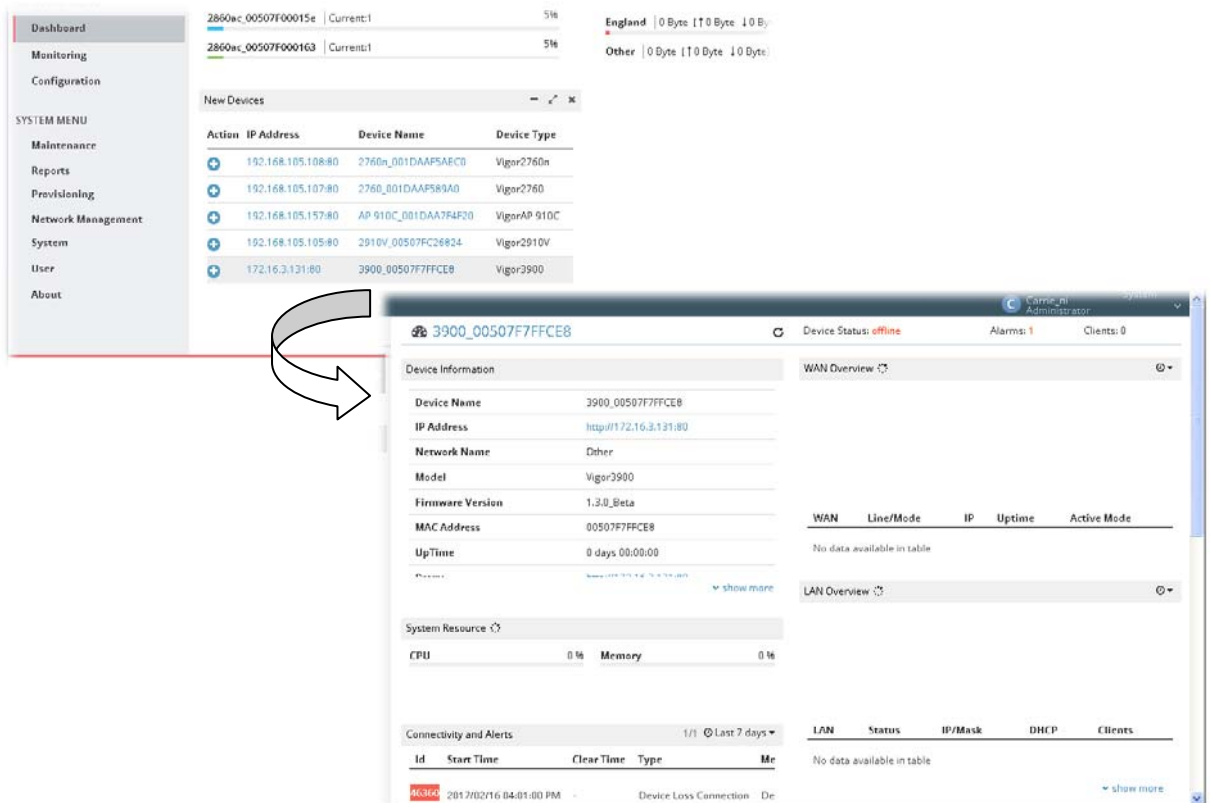
3.2.10 Top 10 for Traffic

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




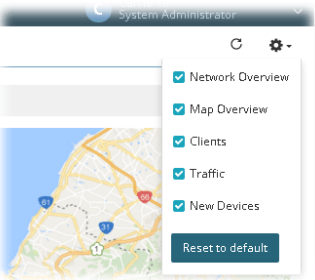


3.2.11 New Added Devices List

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



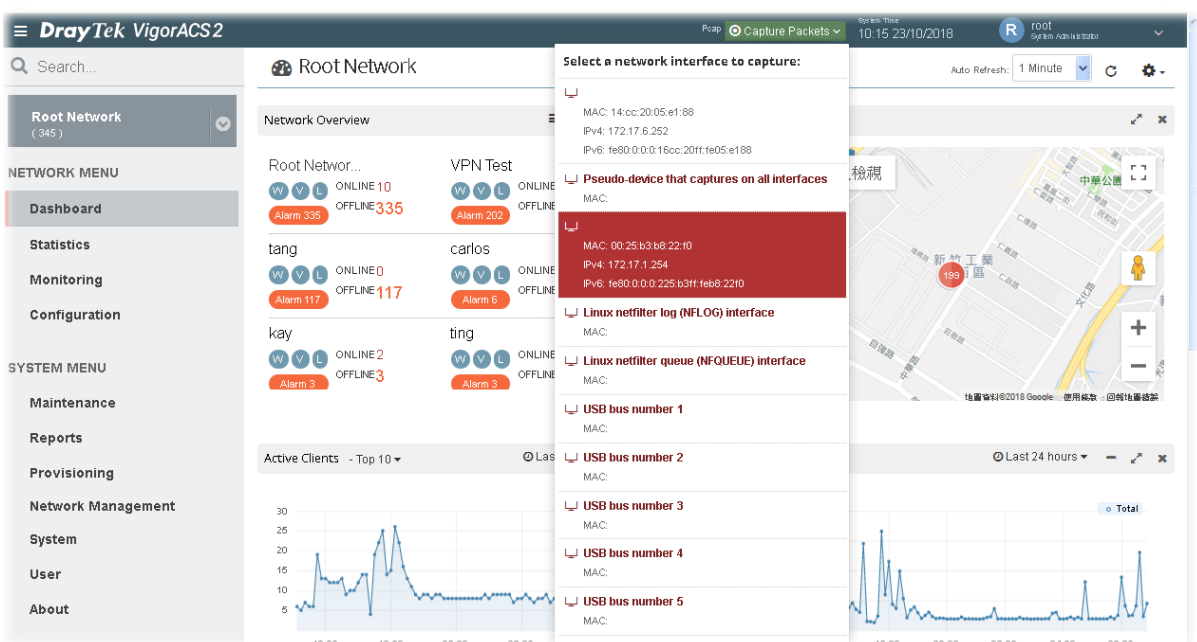
3.2.12 Icons Used in VigorACS 2

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.  - means "Enable".  - means "Disable".
	The type of widget can be chosen on the top-right of VigorACS web user. Check the one(s) you want to display on the web page; or uncheck the one(s) you want to hide on the web page.

3.3 Capture Packets

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 MENU>>System>>System Parameter**, ID 81 PacketCaptureTool.





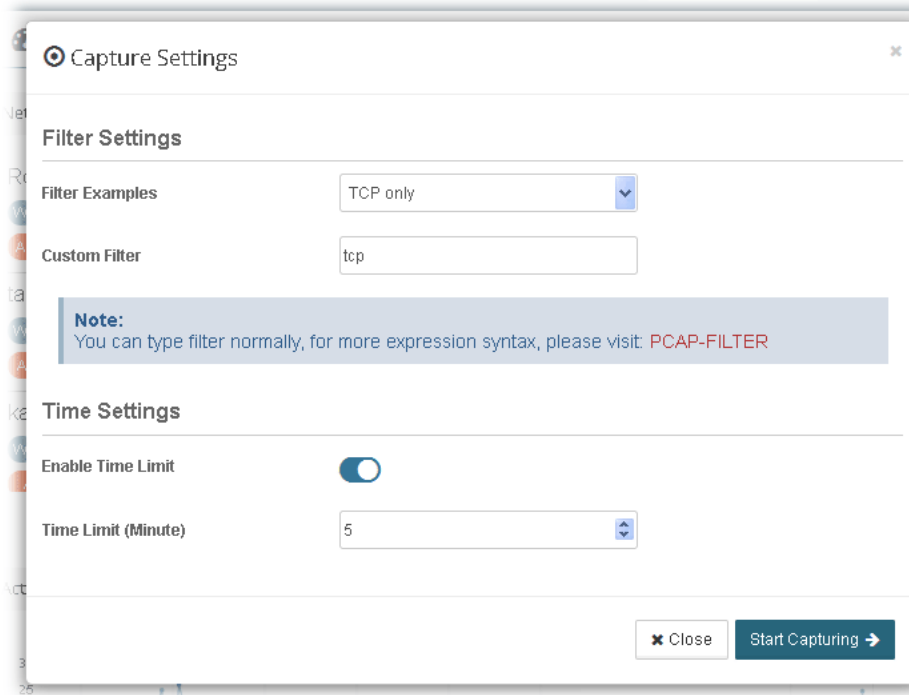
Info

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

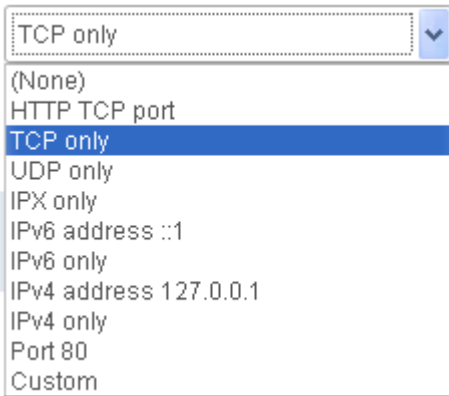
Pcap **No network device detected, please check if libpcap/WinPcap is installed.**

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.

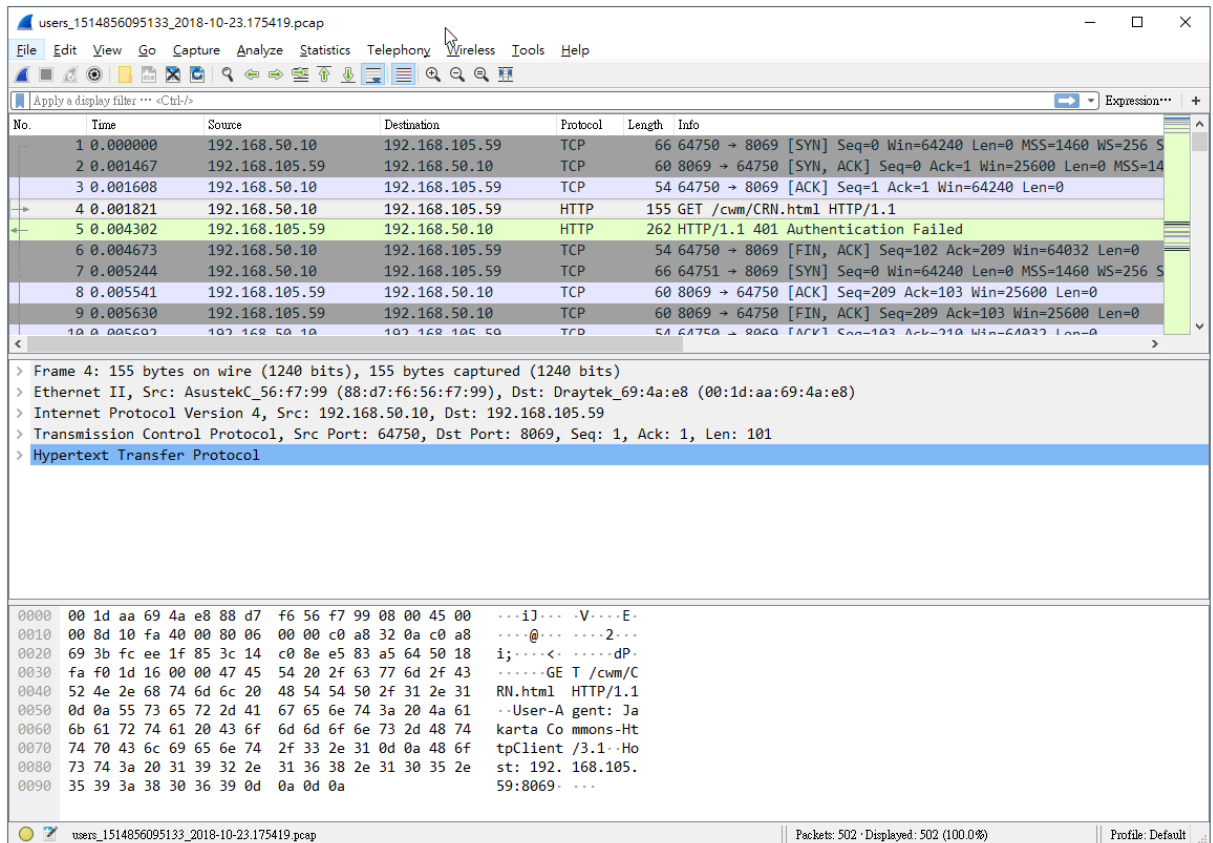


These parameters are explained as follows:

Item	Description
Filter Settings	<p>Filter Examples - Choose a filter for filtering the packet corresponding to the type selected.</p>  <p>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</p>

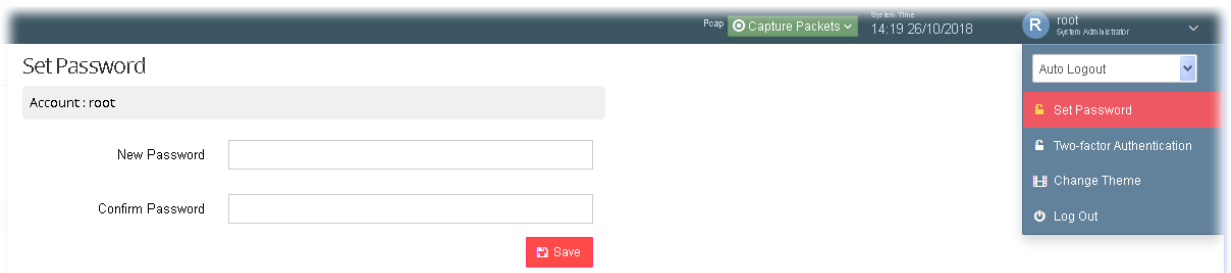
	<p>only the packets coming from/sending to that IP address will be captured and recorded.</p> <p>Custom Filter - Variation of Filter Examples will change the setting in Custom Filter. However, the system administrator can define the filter by entering correct syntax (e.g., host 172.16.2.222) if required. Packet capturing will be executed according to Custom Filter setting.</p>
<p>Time Settings</p>	<p>Enable Time Limit - If enabled, VigorACS server will capture the packets within the time limit defined below.</p> <p>Time Limit (Minute) - Enter a value as a time limit.</p>
<p>Start Capturing</p>	<p>Click it to start packets capturing.</p> <ul style="list-style-type: none"> 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. <div data-bbox="683 792 1453 853" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> </div> <div data-bbox="683 882 1230 943" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> </div> <ul style="list-style-type: none"> 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. <div data-bbox="707 1144 1453 1205" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> </div> <ul style="list-style-type: none"> 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. 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. <div data-bbox="707 1525 1477 1563" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> </div> <p>Click the Refresh button on the right side of Pcap status bar to check if someone else uses Pcap or not.</p>

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.



3.4 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.

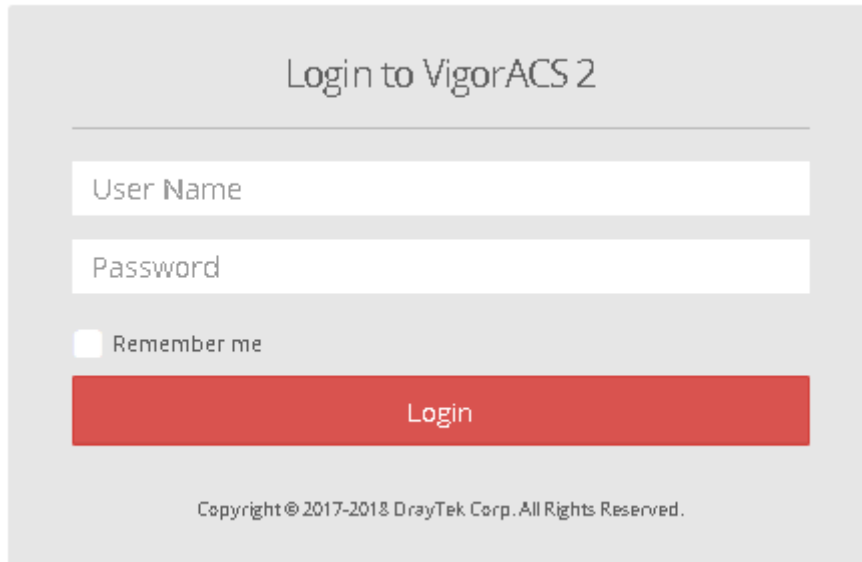


3.5 Two-factor Authentication

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 2 by using the user account and password.



Login to VigorACS 2

User Name

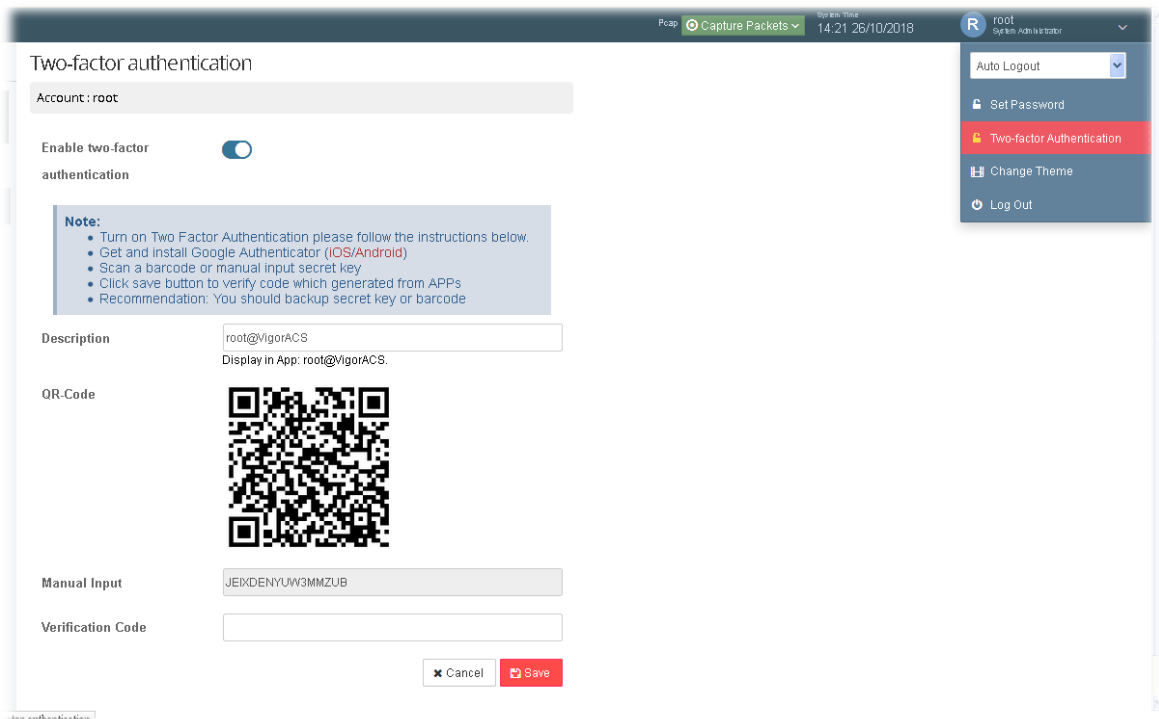
Password

Remember me

Login

Copyright © 2017-2018 DrayTek Corp. All Rights Reserved.

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



Two-factor authentication

Account: root

Enable two-factor authentication

Note:

- Turn on Two Factor Authentication please follow the instructions below.
- Get and install Google Authenticator (iOS/Android)
- Scan a barcode or manual input secret key
- Click save button to verify code which generated from APPs
- Recommendation: You should backup secret key or barcode

Description: root@vigorACS
Display in App: root@vigorACS.

QR-Code

Manual Input: JEIKDENYUW3MMZUB

Verification Code

Cancel Save

4. Use your cell phone to scan the QR-Code shown on the page or enter the secret key displayed on the box of **Manual Input**.

QR-Code



Manual Input

FBSBOPNJG7ZTFGDZ

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.

Verification Code

6. Logout VigorACS 2.
7. Re-login VigorACS 2. The first login web page requires you to enter the original user account and password. After clicking the Login button, the *second* login web page appears. Please enter the authentication code (created randomly) obtained from the APP (Google Authenticator) on your cell phone and click the Verify Code button.

Login to VigorACS 2

Two-factor Authentication code

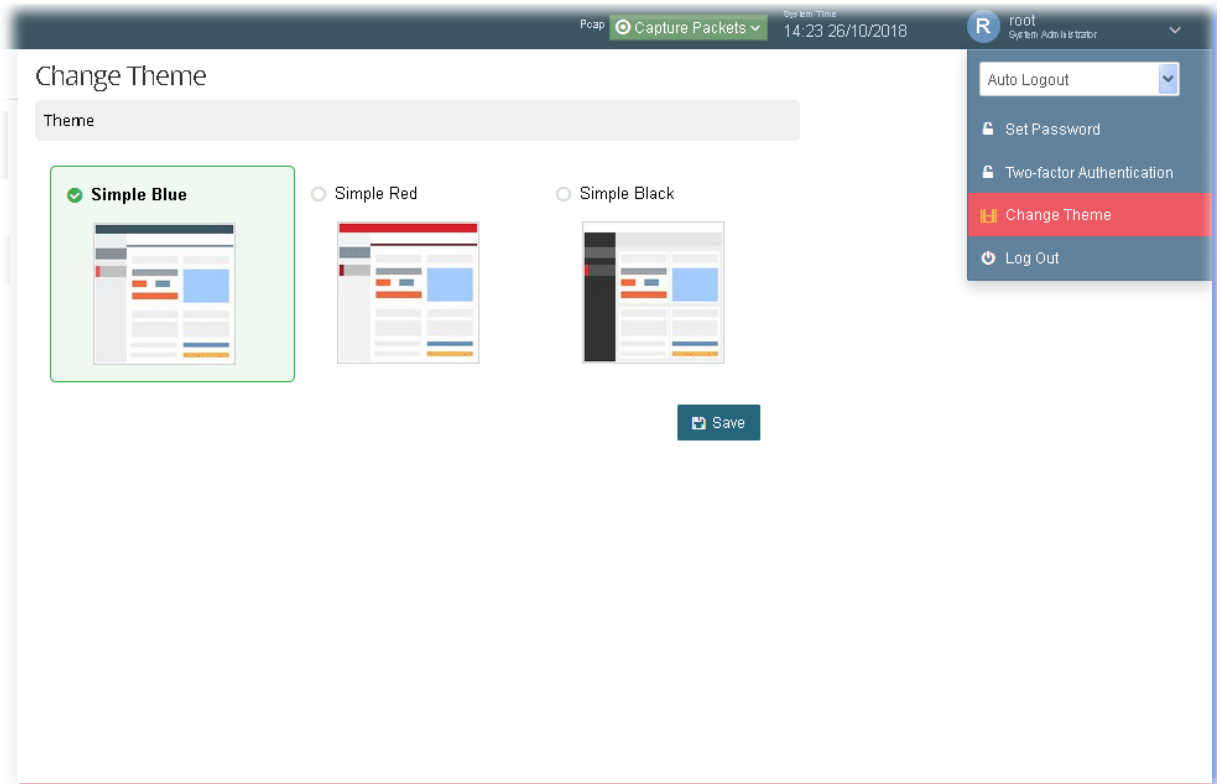
Verify Code

Abort

Copyright © 2017 DrayTek Corp. All Rights Reserved.

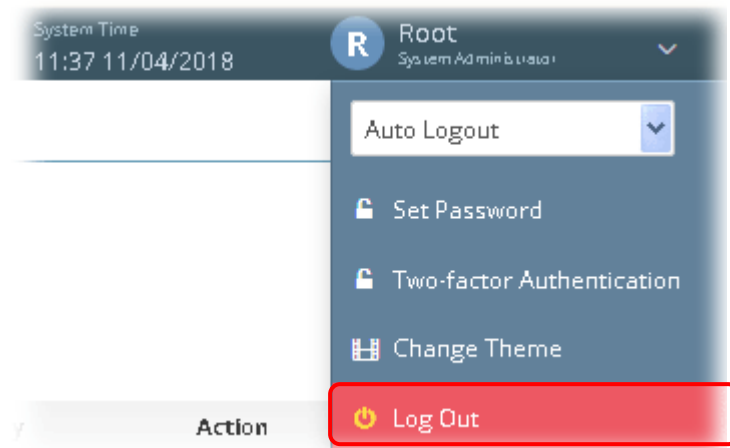
3.6 Change Theme

The theme of VigorACS web user interface can be changed with different color. Choose the color you want and click Save.



3.7 Logout VigorACS

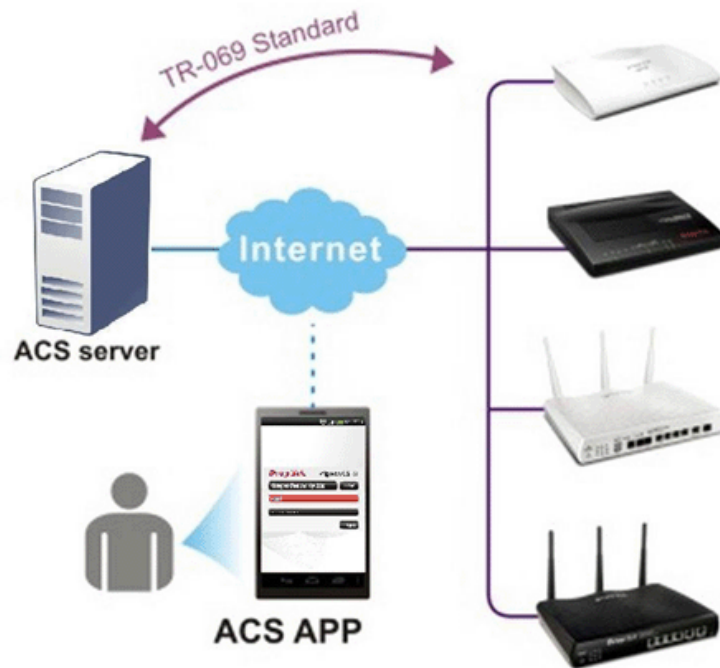
Simply click Logout icon to logout VigorACS.



3.8 About VigorACS

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.



3.8.1 License Key Information

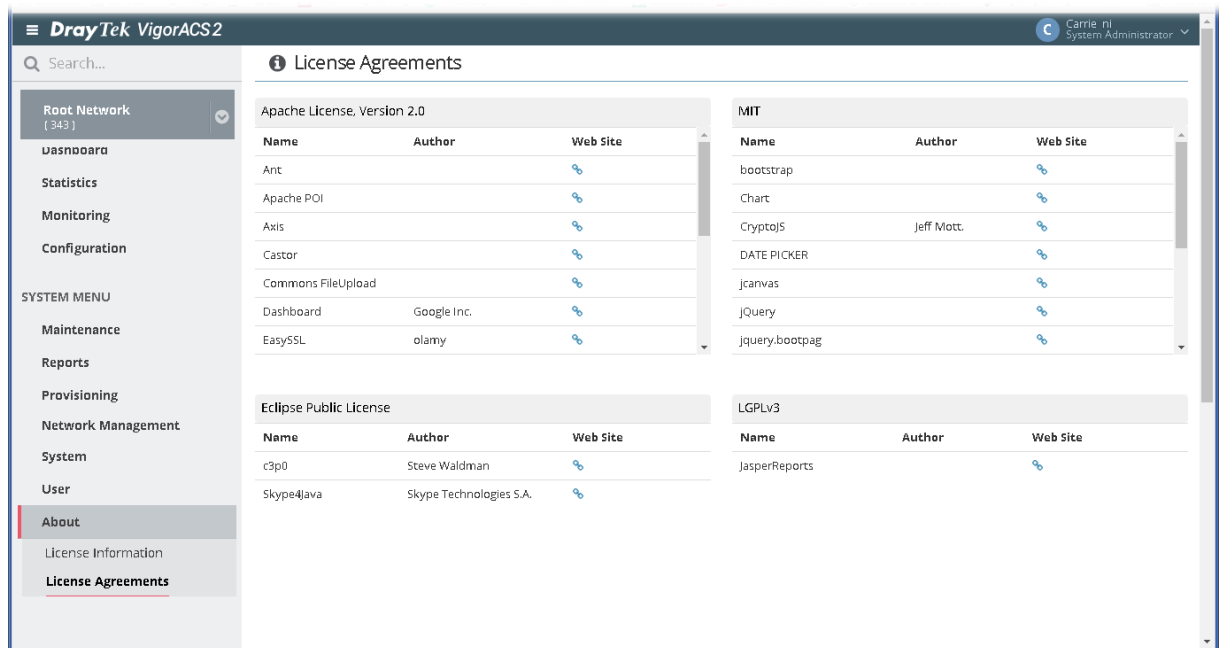
This page displays relational information for license key current used by VigorACS 2. In addition, it offers a channel to new the license key for VigorACS 2 when it is going to be expired.

License Information

License Information			
Host ID	ACS170200004		
License ID	0001a181		
Start Date	2017-02-14		
Expire Date	2099-03-15		
Max Node	200000		
Trial License	YES		

3.8.2 License Agreements

This page displays relational license information required by VigorACS 2.



The screenshot shows the DrayTek VigorACS2 web interface. The top navigation bar includes the DrayTek logo, a search bar, and the user name 'Carrie ni System Administrator'. The left sidebar contains a navigation menu with options like Root Network, Dashboard, Statistics, Monitoring, Configuration, SYSTEM MENU, Maintenance, Reports, Provisioning, Network Management, System, User, and About. The main content area is titled 'License Agreements' and displays a list of license agreements. The agreements are organized into five sections: Apache License, Version 2.0; MIT; Eclipse Public License; and LGPLv3. Each section contains a table with columns for Name, Author, and Web Site. The Apache License, Version 2.0 section lists various licenses like Ant, Apache POI, Axis, Castor, Commons FileUpload, Dashboard, and EasySSL. The MIT section lists licenses like bootstrap, Chart, CryptoJS, DATE PICKER, jcanvas, JQuery, and jquery.bootpag. The Eclipse Public License section lists licenses like c3p0 and Skype4Java. The LGPLv3 section lists the JasperReports license.

Apache License, Version 2.0		
Name	Author	Web Site
Ant		🔗
Apache POI		🔗
Axis		🔗
Castor		🔗
Commons FileUpload		🔗
Dashboard	Google Inc.	🔗
EasySSL	olamy	🔗

MIT		
Name	Author	Web Site
bootstrap		🔗
Chart		🔗
CryptoJS	Jeff Mott.	🔗
DATE PICKER		🔗
jcanvas		🔗
JQuery		🔗
jquery.bootpag		🔗

Eclipse Public License		
Name	Author	Web Site
c3p0	Steve Waldman	🔗
Skype4Java	Skype Technologies S.A.	🔗

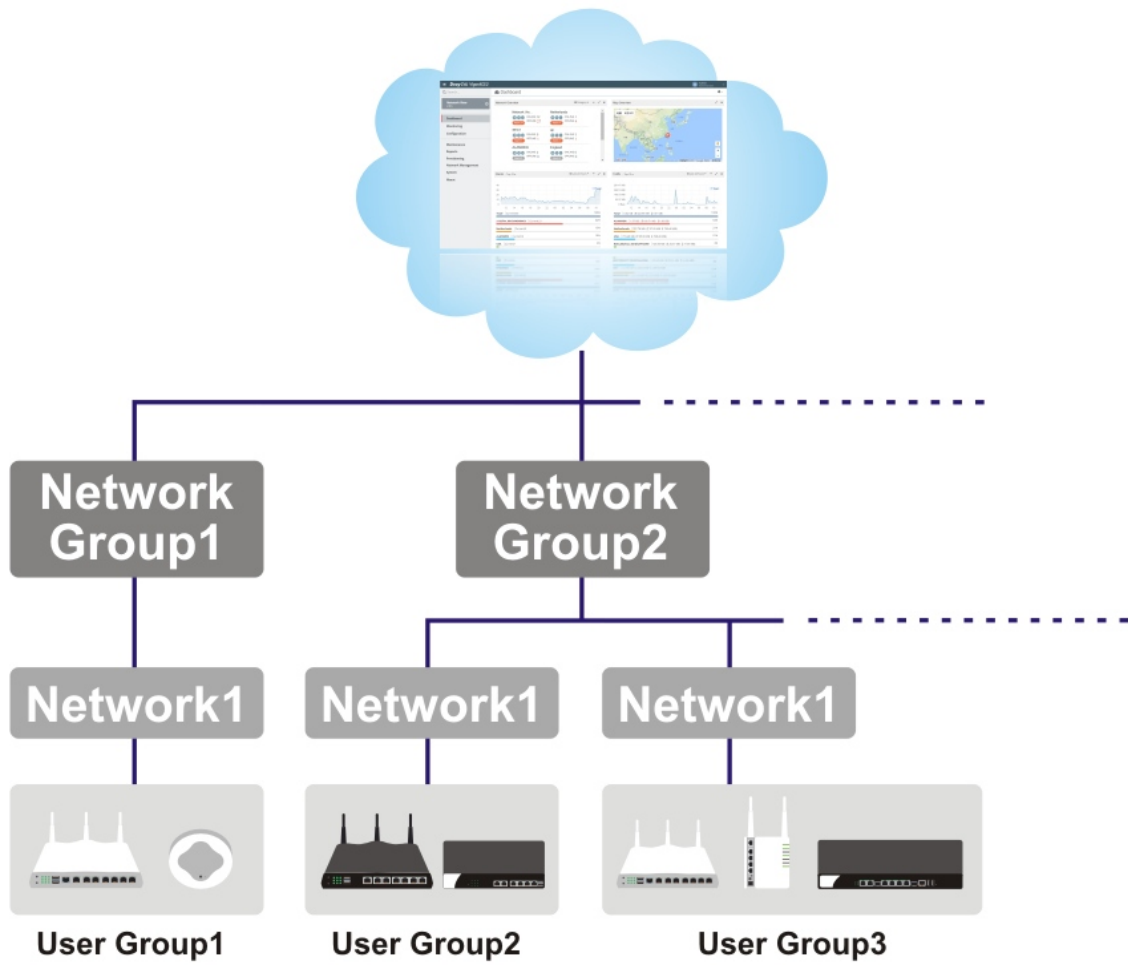
LGPLv3		
Name	Author	Web Site
JasperReports		🔗

3.9 Operation Procedure

Follow the instruction listed below to operate VigorACS 2:

- 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 2?

This section briefly shows a simple way to register a CPE onto VigorACS 2 with few steps. For detailed information, refer to Chapter 4.

The CPE to be managed by VigorACS 2 must be configured and restarted. Here we take Vigor2925 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 2 and Vigor device up.

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

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup
Router Name <input type="text" value="DrayTek"/>	
<input type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports
Internet Access Control <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/>	Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22)
<input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input checked="" type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server	TLS/SSL Encryption Setup <input checked="" type="checkbox"/> Enable TLS 1.2

- Allow management from the Internet - Enabled.
- TR-069 Server - Enabled.

- Open System Maintenance>>TR-069.

System Maintenance >> TR-069 Setting

ACS and CPE Settings **Health Parameters**

ACS Server On LAN/VPN

ACS Server

URL

Acquire URL from DHCP option 43

Username

Password

 Event Code PERIODIC

Last Inform Response Time : Sat Jan 1 0:12:57 2000 ●

CPE Client

Disable

Enable

Http Https

URL

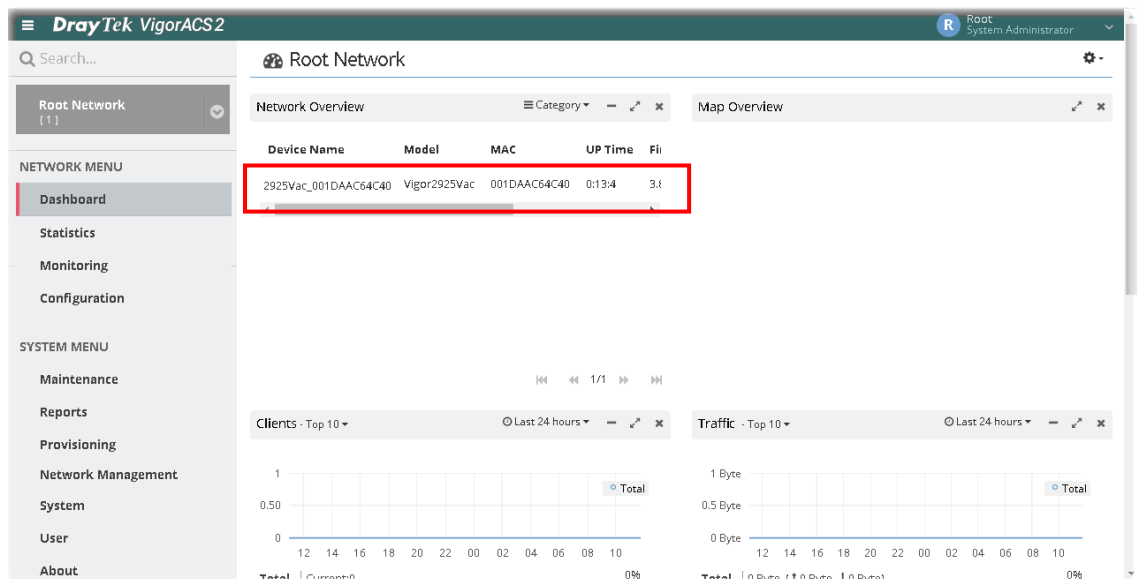
Port

Username

Password

Periodic Inform Settings

- Specify the interface for ACS Server On.
 - Set URL, username, password for network group.
 - Enable CPE Client.
- 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.
 - Open the homepage of VigorACS 2.
 - Now, Vigor2925 has been registered onto VigorACS 2 and displayed on the homepage.

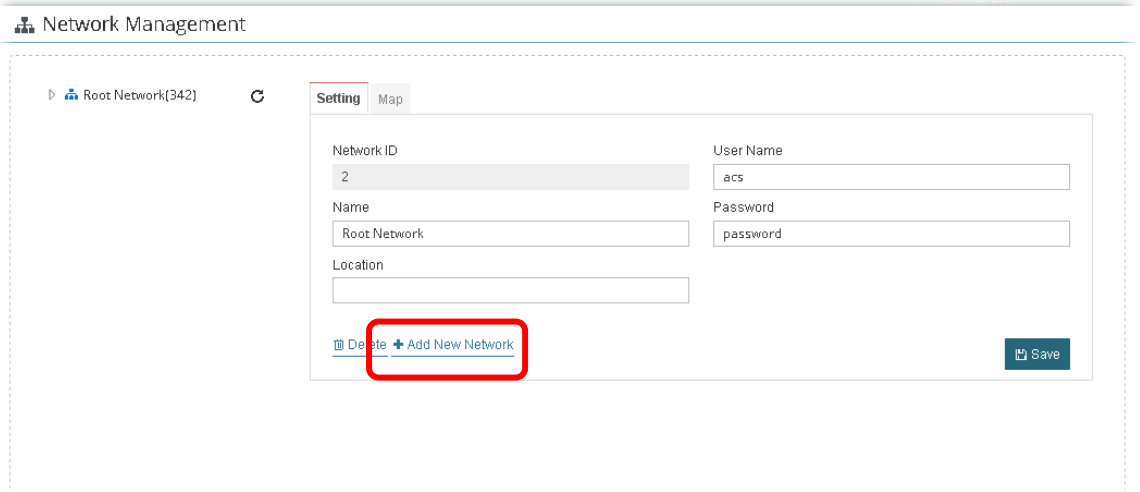


Click the icon to list all the devices.

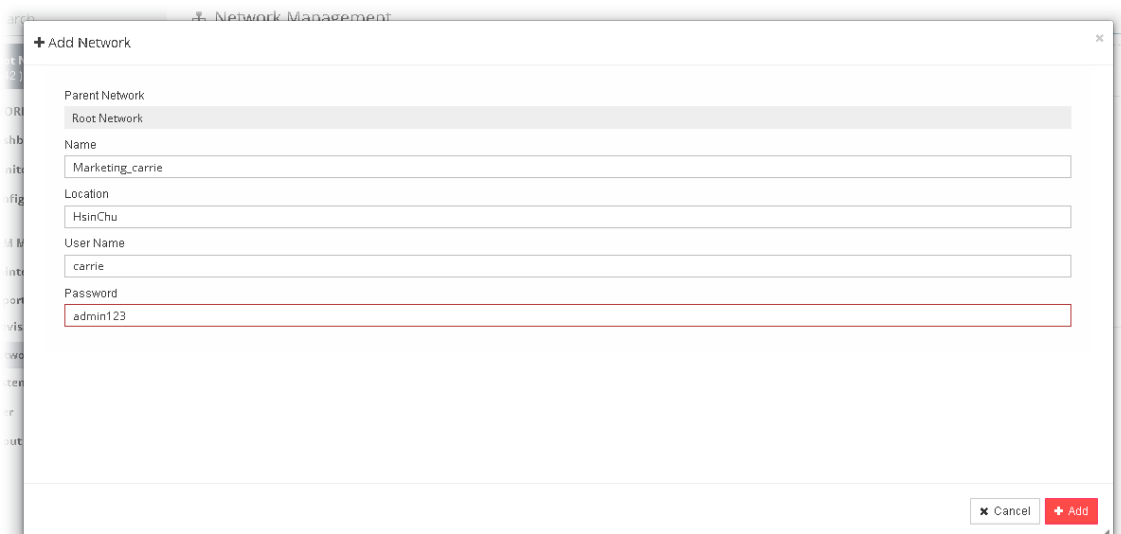
A.2 How to Create a New Network ?

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

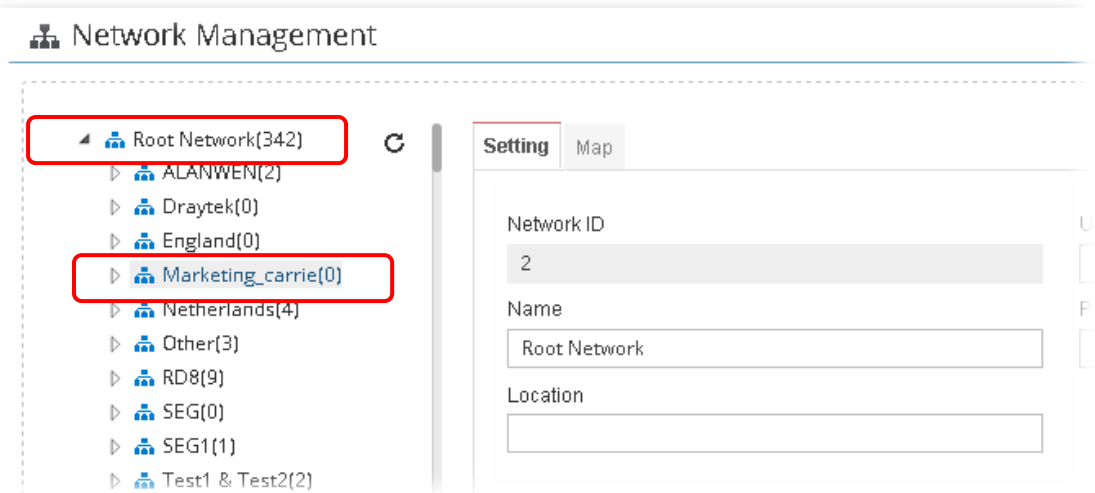


4. A pop-up window appears. Type the required information.

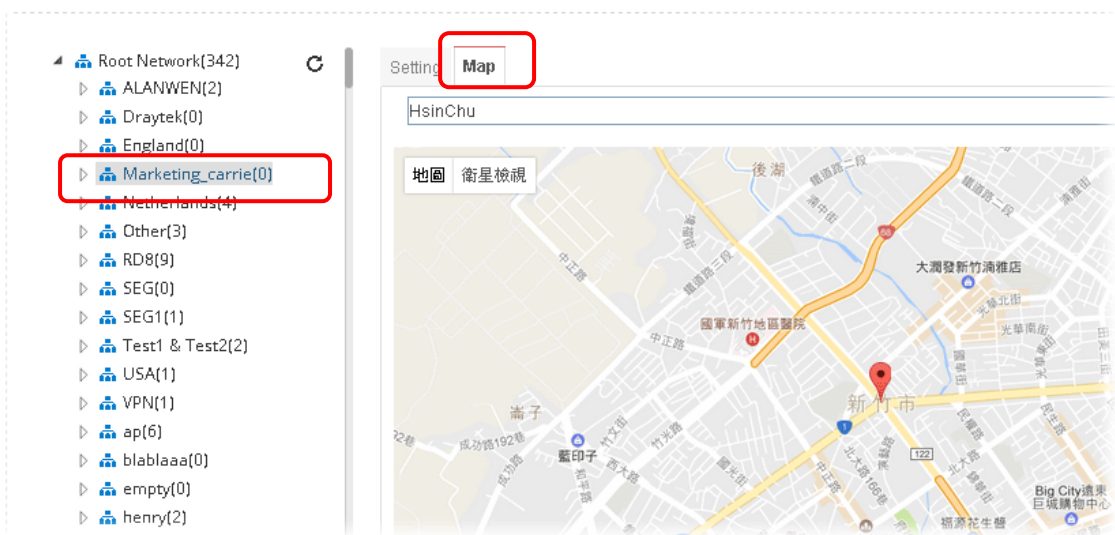


1. **Name** - Type a new name of the network.
2. **Location** - Define the location of such network.
3. **User Name** - Type a user name for such network.
4. **Password** - Type a password for such network.

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 Vigor3900 as an example.

The screenshot shows the VigorACS2 dashboard. On the left is a navigation menu with options like Dashboard, Statistics, Monitoring, Configuration, etc. The main area displays network statistics for various regions like Netherlands, henry, RD8, and ALANWEN. Below this is a 'New Devices' table with the following data:

Action	IP Address	Device Name	Device Type
+	192.168.105.108:80	2760n_001DAAF5AEC0	Vigor2760n
+	192.168.105.107:80	2760_001DAAF589A0	Vigor2760
+	192.168.105.157:80	AP 910C_001DAA7F4F20	VigorAP 910C
+	192.168.105.105:80	2910V_00507FC26824	Vigor2910V
+	172.16.3.131:80	3900_00507F7FFCE8	Vigor3900

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

The 'Add New Device' dialog box contains the following fields and options:

- Add to network:** Marketing_carrie (dropdown menu)
- Device name:** 3900_00507F7FFCE8 (text input)
- Location:** (empty text input)
- Emergency phone:** (empty text input)
- Set to known device:**

Buttons at the bottom: Cancel, Apply

Add to network - Choose the network from the drop down list.

Location - Type the location of the selected device.

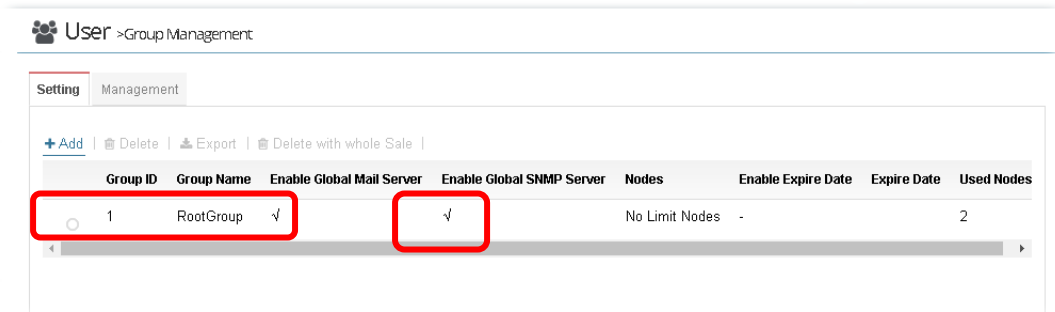
Emergency phone - Type the mobile phone for communication.

Set to known device - Click it to make the device visibly or invisibly.

3. Click Apply to save the changes.

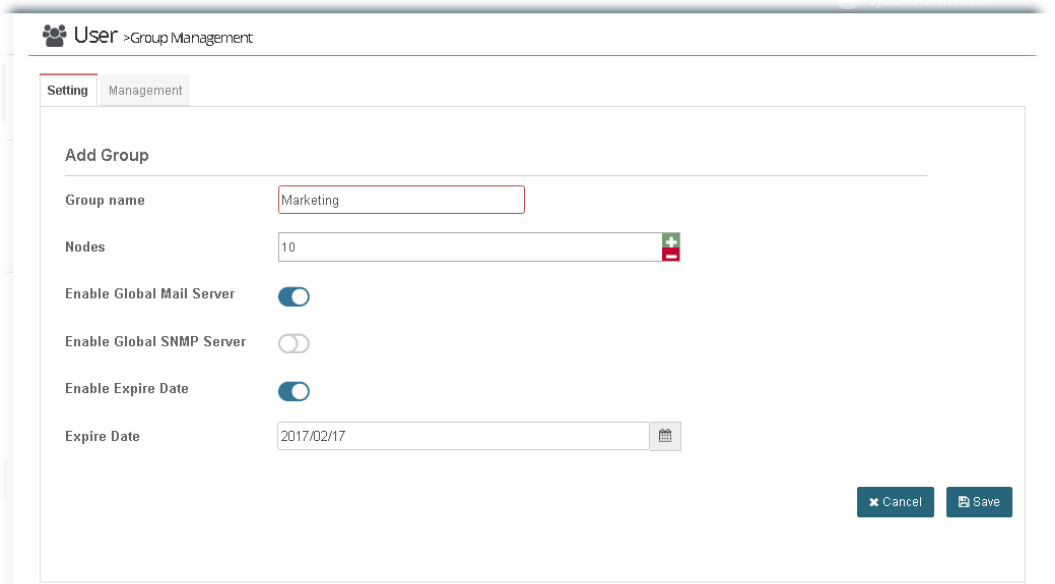
A-4 How to Create a New User Group ?

1. Only the administrator has the right to create a new user group.
2. From the **SYSTEM MENU**, open the User menu.
3. Click **Group Management**. The following page will appear.



RootGroup is a default setting.

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



Group name - Type a new name.

Nodes - Use + or - to add or decrease the number of nodes.

Enable Global Mail Server - Click it to enable or disable the service.

Enable Global SNMP Server - Click it to enable or disable the service.

Enable Expire Date - Click it to enable the Expire Date mechanism.

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

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

Setting Management

[+ Add](#) | [Delete](#) | [Export](#) | [Delete with whole Sale](#)

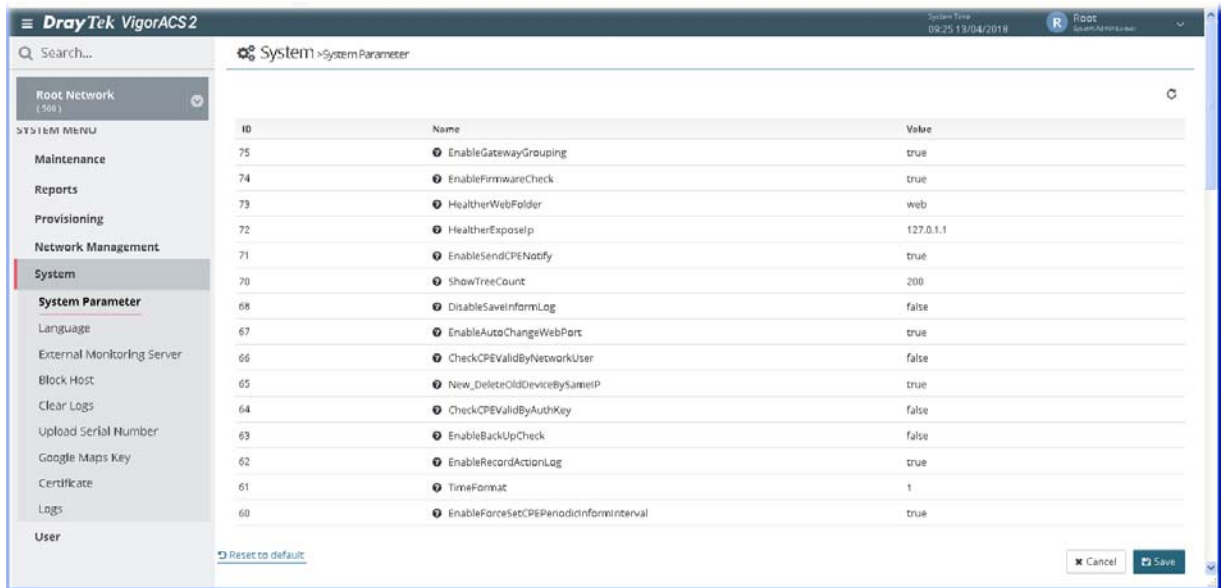
	Group ID	Group Name	Enable Global Mail Server	Enable Global SNMP Server	Nodes	Enable Expire Date	Expire Date	Used Nodes
<input type="radio"/>	1	RootGroup	√	√	No Limit Nodes	-		2
<input checked="" type="radio"/>	2	Marketing	√	-	10	√	2017/02/17	0

Part II SYSTEM MENU, System and User Settings Management

Chapter 4 System

4.1 System Parameter

Open SYSTEM MENU>>System and click System Parameter to get the following web page:



These parameters are explained as follows:

ID No.	Description
	<p>Reset to default Click the link to reset all of the system parameters with factory default values.</p>
1	<p>ProvisionKeepParameter It can be set with true or false. True - Enable the function of Keep Profile (profile or parameters in provision). False - VigorACS will disable the function of Keep Profile.</p>
2	<p>ProvisionWaitCount 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.</p>
3	<p>ProvisionFactoryResetEnable True - The function of keep profile will perform immediately for CPE without reaching the value of 'ProvisionWaitCount'.</p>

4	<p>FirmwareUpgradeCount</p> <p>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.</p>
5	<p>ProvisionDeviceAutoEnable</p> <p>False - The CPE would not be added in Homepage when a profile defines a CPE with different names but with the same serial number.</p> <p>True - The CPE would be added in Homepage when a profile defines a CPE with different names but with the same serial number.</p>
6	<p>ProvisionChangeDeviceNameEnable</p> <p>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.</p>
7	<p>SettingProfileSpaceSetEnable</p> <p>True - Users can use space as character in parameter values. For example, users can use the space character as their password.</p>
8	<p>ParameterListLongWaitCount</p> <p>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. It will take effect after VigorACS restarts. Default is 1200.</p>
12	<p>GetSetParameterCount</p> <p>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.</p> <p>Set this value properly to prevent CPEs from crashing or improve the efficiency.</p>
13	<p>IsDownloadUsedHttps</p> <p>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.</p>
14	<p>ProvisionProfileFormat</p> <p>It can be set with 1, 2, 3 or 4.</p> <p>This value indicates the format of text configured profile.</p> <p>If the value is set with 1, the format is defined as serial number, network_device name, isreboot, and [parameter1, parameter2,.. and so on].</p> <p>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].</p> <p>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].</p> <p>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].</p>
15	<p>IsRebootAfterDownload</p> <p>True- After downloading and upgrading the firmware, reboot the CPE.</p> <p>False - Users must reboot the CPE manually.</p>

16	<p>KeepProfileUpdateRule</p> <p>It can be set with is 1, 2 or 3.</p> <p>The value 1 means after uploading profile, keep original Keep Profile settings and add extra parameter settings (if the profile contains more parameter settings).</p> <p>The value 2 means after uploading profile, delete original Keep Profile setting if the device name changed.</p> <p>The value 3 means after uploading profile, delete original Keep Profile settings every time.</p>
17	<p>IsSetGlobalParameter</p> <p>False - Disable global parameter configuration function. When it is disabled, even users set global parameters, these parameters won't be applied.</p>
19	<p>IsTurnOffPeriodicInform</p> <p>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.</p> <p>False - After adjusting the PeriodicInform (configured in 59. CPEPeriodicInformInterval) of CPEs, remember to set this value false.</p>
20	<p>PollingDeviceCount</p> <p>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.</p> <p>Note: After changing this parameter value, restart VigorACS to apply the change.</p>
21	<p>DeviceAutoEnable</p> <p>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.</p> <p>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.</p>
22	<p>PollingInterval</p> <p>Set the polling interval for VigorACS to examine CPE. The unit is milliseconds. Default is 900000.</p>
23	<p>CPEWebUiPort</p> <p>Set a port number for VigorACS system accesses into CPE's WUI.</p>
26	<p>VPNIPSecDefaultSecurity</p> <p>Set the default security method for establishing VPN based on IPsec.</p>
27	<p>CheckDeviceStatusCount</p> <p>Determine how many times shall VigorACS system check the device before the device becomes offline.</p>
28	<p>VPNChangeEnable</p> <p>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.</p> <p>False - Default value.</p>
29	<p>WANSeverity</p> <p>Set the severity (critical, major, minor, warning and normal) for WAN connection.</p>
30	<p>VPNSeverity</p> <p>Set the severity (critical, major, minor, warning and normal) for VPN connection.</p>

32	EnableHttpChunkedMode True - Use chunked mode (chunked transfer encoding) for HTTP. False - Default value.
33	CPEWebUiProtocol Set HTTP (default) or HTTPS as the protocol for accessing CPE's web user interface.
34	EnableValidateCodeCheck True - Enable the function of validating code check on the login page. False - Disable the function. It is the default value.
35	VPNIPSecDefaultMode Set the default mode for IPSec VPN connection. Main Aggressive
36	StatisticsStep Set the time interval (default is 900) for data collection for RRD traffic.
38	EnableWebServices True - The third party software can get/set VigorACS functions through web services. False - Default value.
41	HidePassword True - Hide the password value on provision page. False - Default value.
43	VPNEnablePingKeepAlive True - Enable the function of Enable PING to keep VPN alive for CPE while creating VPN by using the VPN wizard. False - Default value.
44	CPEDetectMode Set the CPE detection mode. 0 means TR069; 1 means ping.
46	EnableRRD True - Enable the function of data collection (StatisticsStep) for RRD traffic.
47	AutoDetectRouteName True - Get CPE's router name. False - Default value.
49	DefaultSetDeviceKnown True - Set the new added CPE as a known device. False - Default value.
50	KeepProfileRebootByBOOTSTRAP True - VigorACS will ask the CPE to reboot if receiving CPE request including BOOTSTRAP. False - Default value.
51	DisableAlarmMailByACSReboot True - VigorACS will not send alarm message within 15 minutes after turning on VigorACS. False - Default value.
52	DeleteOldDeviceBySameIP 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. False - Default value.

54	<p>DisablePolling</p> <p>True - Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration. False - Default value.</p>
55	<p>DisableAlarmMailByClear</p> <p>True - Disable the function of sending alarm e-mail when alarm status is clear. It is the default setting. False - VigorACS will send alarm e-mail when alarm status is clear.</p>
56	<p>UseStunAddressForVpn</p> <p>True - Remote IP address will use the STUN IP address for VPN connection. False -Default value.</p>
57	<p>EnableChangeNetworkByNetworkUser</p> <p>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. False - Disable such function.</p>
58	<p>FWUpgradeFailInterval</p> <p>If the firmware upgrade failed, the next firmware upgrade will execute after the time interval configured here. Default value is 86400 seconds.</p>
59	<p>CPEPeriodicInformInterval</p> <p>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.</p>
60	<p>EnableForceSetCPEPeriodicInformInterval</p> <p>True -Default value. Enable the function of CPEPeriodicInformInterval. False - Disable the function of CPEPeriodicInformInterval.</p>
61	<p>TimeFormat</p> <p>Display the time format. 0 means 24-hour clock; 1 means 12-hour clock.</p>
62	<p>EnableRecordActionLog</p> <p>True - Enable the function of record action log. It is the default value. False - Disable the function of record action log.</p>
63	<p>EnableBackupCheck</p> <p>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. False - Default value.</p>
64	<p>CheckCPEValidByAuthKey</p> <p>True - VigorACS will check if the authentication key informed by CPE is valid or not. False - Default value.</p>
65	<p>New_DeleteOldDeviceBySameIP</p> <p>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. False - Default value.</p>

66	<p>CheckCPEValidByNetworkUser</p> <p>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.</p> <p>False - Default value.</p>
67	<p>EnableAutoChangeWebPort</p> <p>True - Enable for changing web port automatically. It is the default setting.</p> <p>False - Disable the function.</p>
68	<p>DisableSaveInformLog</p> <p>True - Disable the function of Save Inform Log.</p> <p>False - Default value.</p>
70	<p>ShowTreeCount</p> <p>Set how many devices will be shown on the home device tree. Default value is 100.</p>
71	<p>EnableSendCPENotify</p> <p>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.</p> <p>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.</p>
72	<p>HealthierExposelp</p> <p>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.</p>
73	<p>HealthierWebFolder</p> <p>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.</p> <p>Default folder name is set as "web".</p>
74	<p>EnableFirmwareCheck</p> <p>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.</p>
75	<p>EnableGatewayGrouping</p> <p>True - Enable the function of grouping VigorAP devices by using gateway addresses and displaying AP devices behind the gateway routers.</p> <p>False - Default value.</p>
76	<p>EnableUIGraph</p> <p>True - Enable the function of displaying graph of web user interface. It is the default value.</p> <p>False - Disable the function.</p>
77	<p>ACSHttpsProtocol</p> <p>Specify the SSL protocol (TLSv1, TLSv1.1 or TLSv1.2) for HTTPS connection.</p> <p>The default is TLSv1.2 for more secure communications.</p>

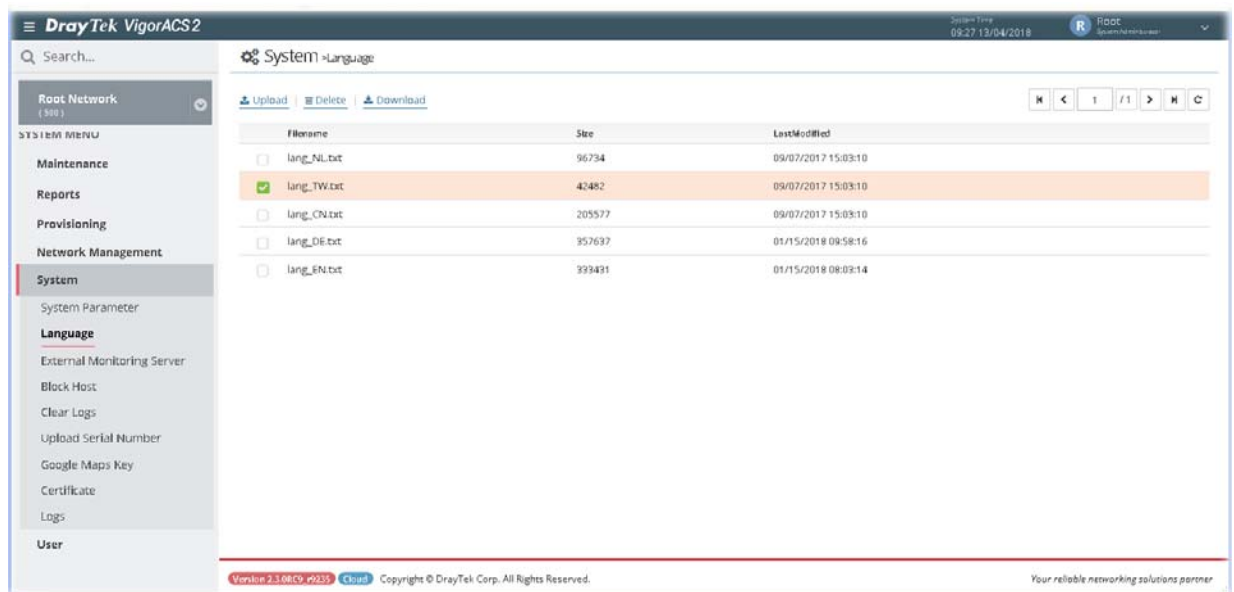
78	<p>EnableAuditorActionLog</p> <p>True - The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions.</p> <p>False - Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded.</p>
79	<p>EnableAuditorDeletedLog</p> <p>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.</p> <p>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.</p>
80	<p>HttpProxyPort</p> <p>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.</p>
81	<p>PacketCaptureTool</p> <p>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.</p> <p>False - Default value.</p>
82	<p>ClientRecordAliveTimeInDays</p> <p>Set the number of days for reserving the record (about client traffic). When exceeding the day limit, VigorACS will delete the record.</p> <p>Default value is 30(days).</p>
83	<p>IsDeleteExpiredClientTrafficByTimestamp</p> <p>True - Enable the function of ClientRecordAliveTimeInDays.</p> <p>False - Default setting.</p>
84	<p>EnableClientRecord</p> <p>True - Default value. Enable the function of recording client traffic and displaying related information on NETWORK MENU >> Monitoring >>Clients.</p>

4.2 Language

VigorACS 2 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 2. If necessary, you can download a text file with VigorACS 2 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.

4.3 External Monitoring Server

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

4.3.1 Health Server

The screenshot shows the DrayTek VigorACS2 web interface. The top navigation bar includes the DrayTek logo, the title 'VigorACS2', and the user 'Root' with a dropdown arrow. The left sidebar menu is expanded to 'System', which includes sub-items like 'System Parameter', 'Language', 'External Monitoring Server', 'Block Host', 'Clear Logs', 'Upload Serial Number', 'Google Maps Key', 'Certificate', 'Logs', and 'User'. The main content area is titled 'System -> External Monitoring Server'. It features a 'Health Server' section with a sub-section 'Wireless Client Information Server'. The 'Enable Server' toggle is turned on. Below it are input fields for 'URL' (10.10.10.10), 'User Name' (123), 'Password' (123), and a dropdown menu for 'API' (Health_Default_GLOBAL). At the bottom right, there are 'Cancel' and 'Save' buttons. The footer contains 'VigorACS 2.3.0.0 (v233) Copyright © DrayTek Corp. All Rights Reserved.' and 'Your reliable networking solutions partner'.

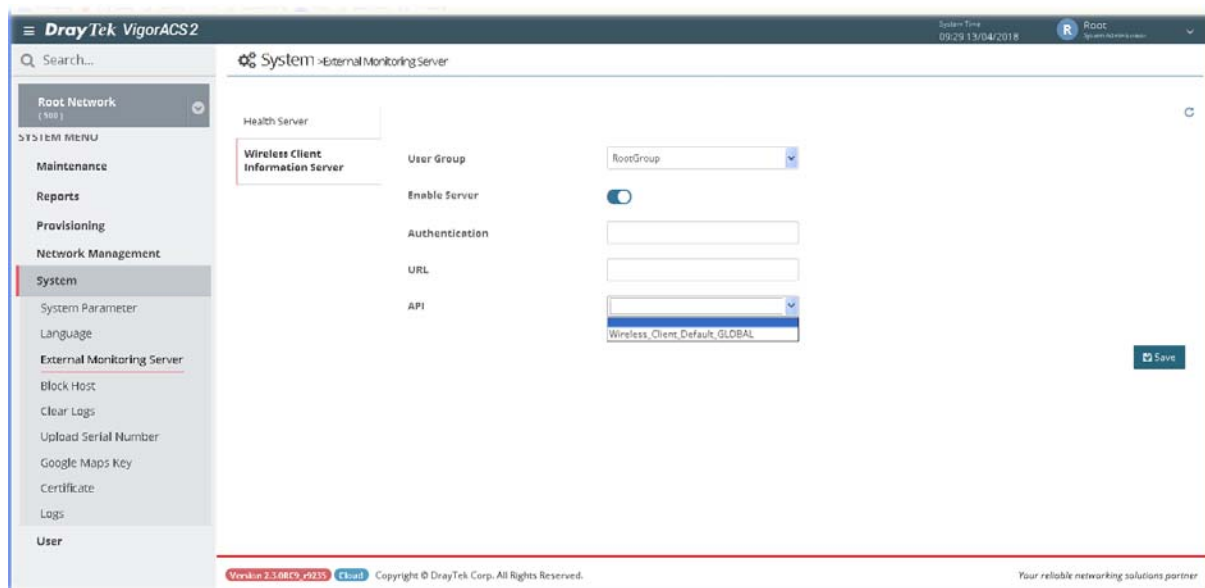
These parameters are explained as follows:

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.

After finished the above settings, click **Save** to save the change.

4.3.2 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:

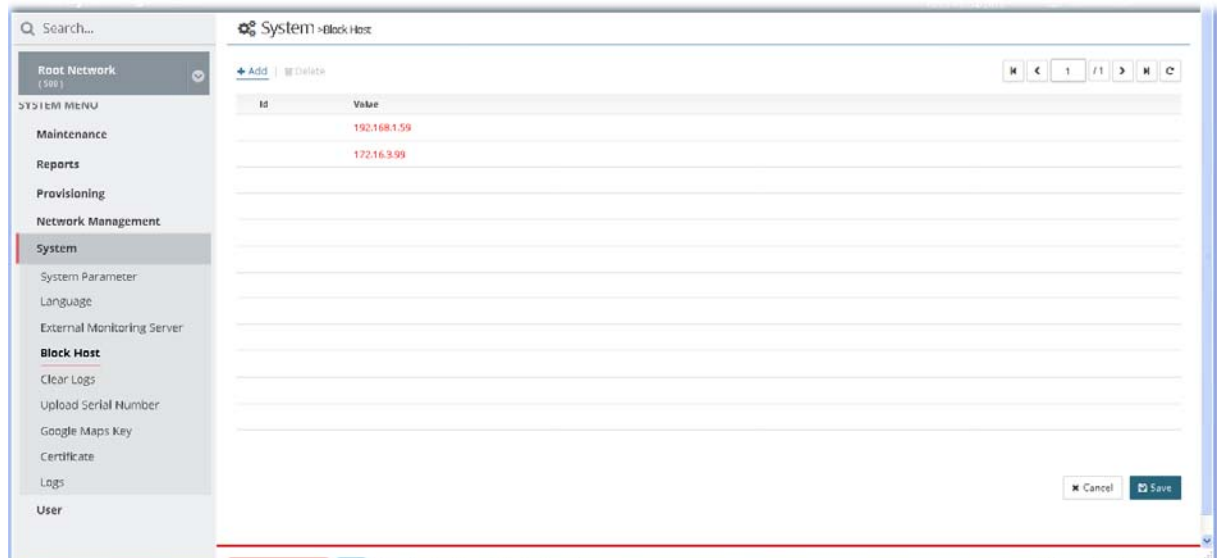
Item	Description
User Group	Use the drop down list to specify a user group. In which, RootGroup contains all of the users with the role of system administrator in default.
Enable Server	Click the icon to enable / disable the server.
Authentication	Enter a string for authentication.
URL	Enter the URL 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.

After finished the above settings, click Save to save the change.

4.4 Block Host

Such feature can deny some CPE (with IP address) for connecting to VigorACS or registering to VigorACS due to some reasons (e.g., attacked by someone or device removed).

Due to the limitation of the number of the nodes, if a remote CPE is no longer to be managed by VigorACS, and the TR-069 settings about VigorACS in CPE are unable to be rewritten or cleared, the administrator can remove or block the IP address of such CPE by using this feature. Then VigorACS will not receive any information coming from the CPE periodically and prevent from management troubles.



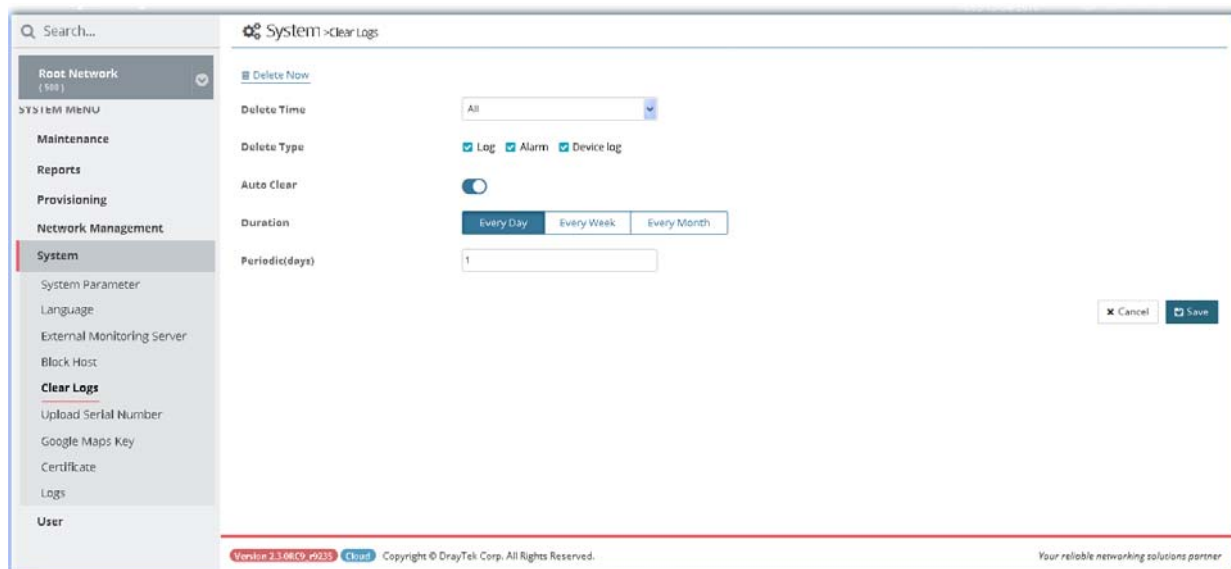
These parameters are explained as follows:

Item	Description
+Add	Click it to add a specified host to be blocked by VigorACS.
Delete	Click it to unblock a host which is listed on the blocked hosts list.
Id	The number appears here is given by VigorACS randomly.
Value	Type an IP address which represents a host.
Cancel	Discard current settings and restore the default settings.
Save	Save and activate the current settings.

After finished the above settings, click **Save** to save the change.

4.5 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 Now	Click it to delete the log information immediately.
Delete Time	Use the drop down list to specify the timing to delete the log. All - All of the logs recorded. Before 1, 3, 6 Month - Log recorded before 1, 3 or 6 month ago. 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. Every Week - VigorACS deletes the log every week. 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 VigorACS 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 VigorACS will delete the log on Saturday every week.
Cancel	Discard current settings and restore the default settings.

Save	Save and activate the current settings.
------	---

After finished the above settings, click Save to save the change.

4.6 Upload Serial Number

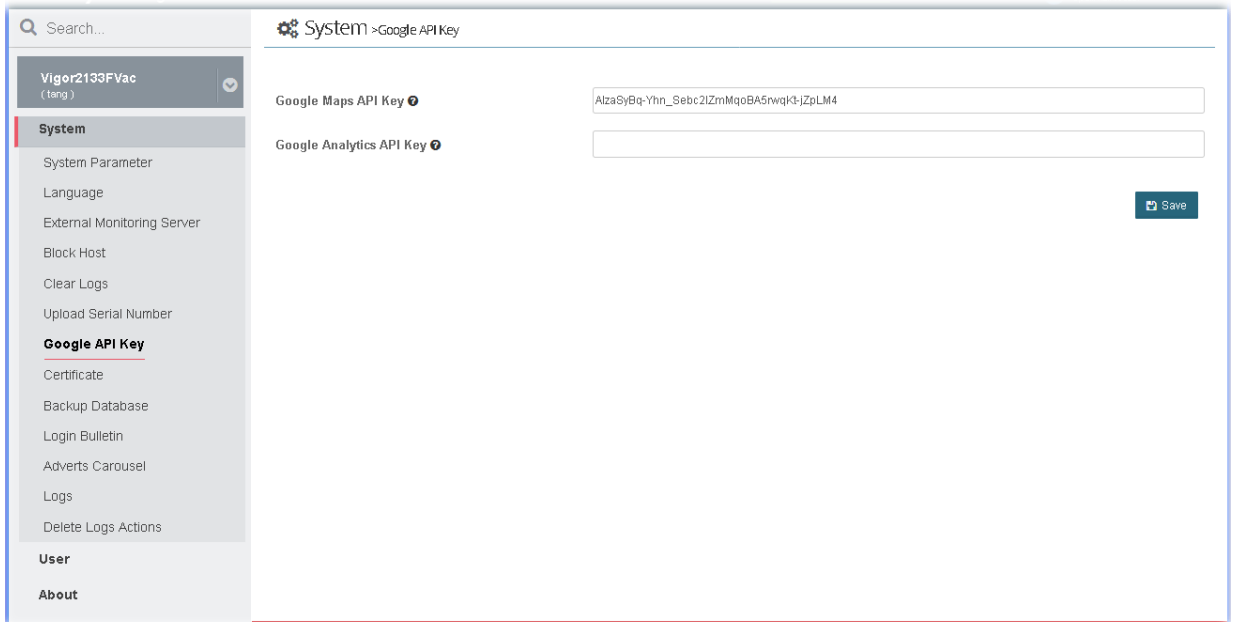
The information for serial number on the rear side / bottom of the CPE or VigorAP can be uploaded onto VigorACS as a reference to be inspected by the administrator.

These parameters are explained as follows:

Item	Description
Upload	Click it to upload a ".CSV" file (located on host) to VigorACS. 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.

4.7 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.



The screenshot shows the 'System > Google API Key' configuration page in the VigorACS interface. On the left is a sidebar menu with sections for 'System', 'Google API Key', 'User', and 'About'. The 'System' section is expanded, showing options like 'System Parameter', 'Language', 'External Monitoring Server', 'Block Host', 'Clear Logs', 'Upload Serial Number', 'Certificate', 'Backup Database', 'Login Bulletin', 'Adverts Carousel', 'Logs', and 'Delete Logs Actions'. The 'Google API Key' section is also expanded, showing 'Google Maps API Key' and 'Google Analytics API Key'. The 'Google Maps API Key' field contains the value 'AlzaSyBq-Yhn_Sebr2IZmMqoBA5nwqk3-JzPLM4'. The 'Google Analytics API Key' field is empty. A 'Save' button is located at the bottom right of the configuration area.

Search...

Vigor2133Fvac (tang)


System


- System Parameter
- Language
- External Monitoring Server
- Block Host
- Clear Logs
- Upload Serial Number
- Google API Key**
- Certificate
- Backup Database
- Login Bulletin
- Adverts Carousel
- Logs
- Delete Logs Actions

User

About

System > Google API Key

Google Maps API Key 

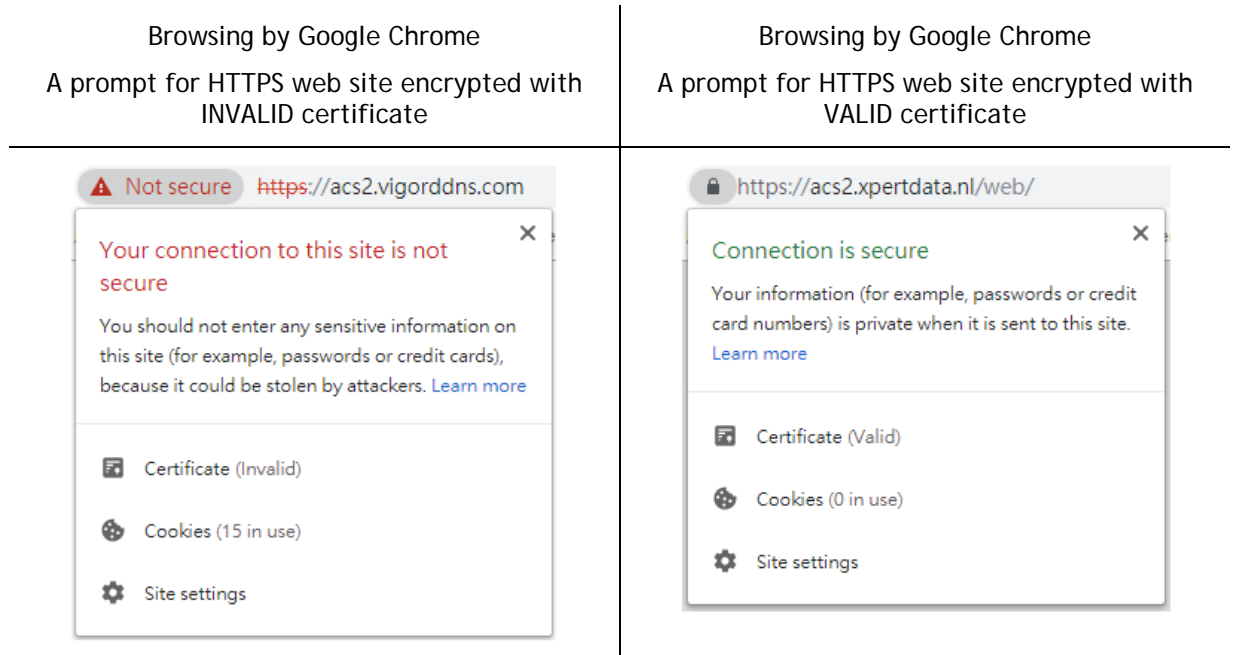
Google Analytics API Key 

Save

4.8 Certificate

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

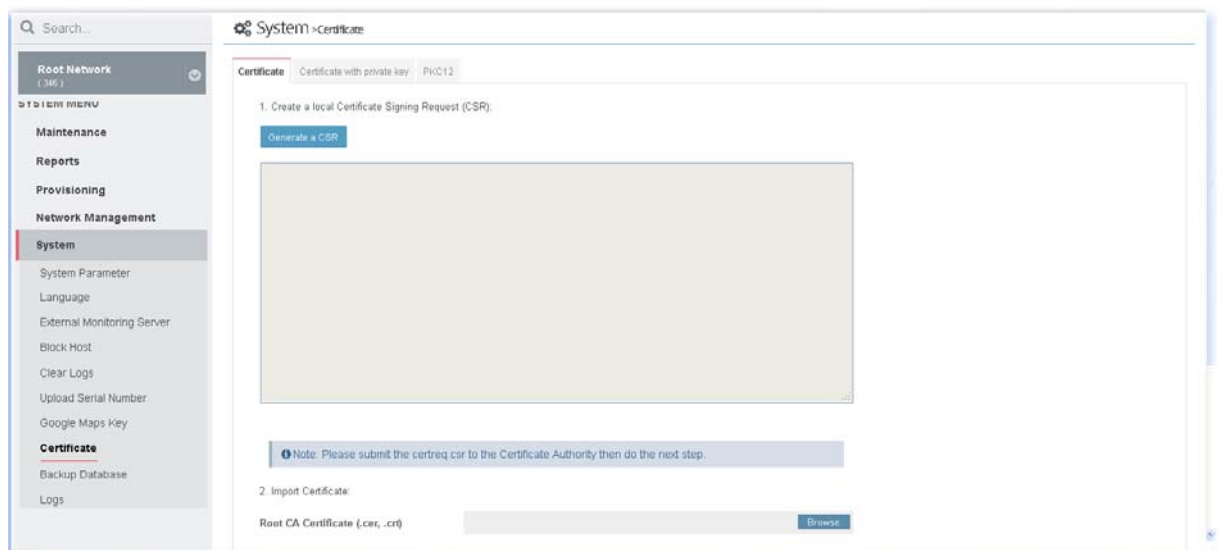
It is suggested to use HTTPS protocol for encrypting the connection between the browser and the web server for every website to prevent private information (such as account, password, personal data, credit number, and others) entered by users from leakage.

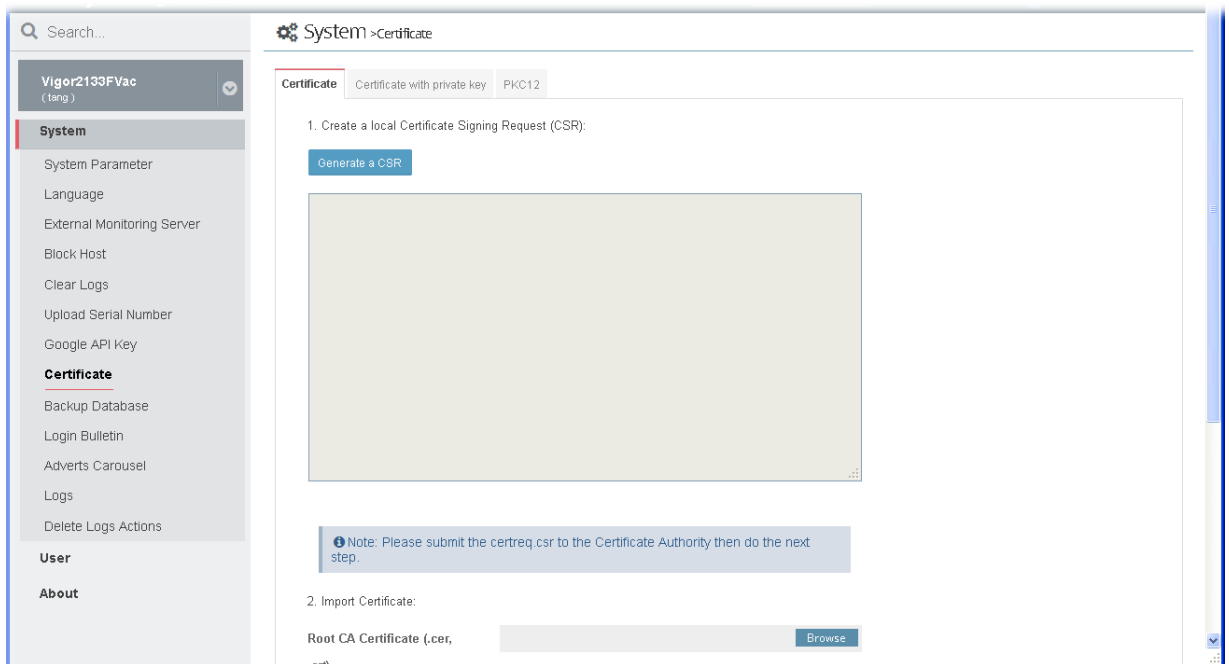


4.8.1 Certificate

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 it to generate a CSR certificate.
Import Certificate	Click the Browse button to specify a file to apply the HTTPS certificate. <ul style="list-style-type: none"> ● Root CA Certificate ● Intermediate CA Certificate ● Trusted Certificate
Save	Save current settings and uploading/pasting the certificate.

4.8.2 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.

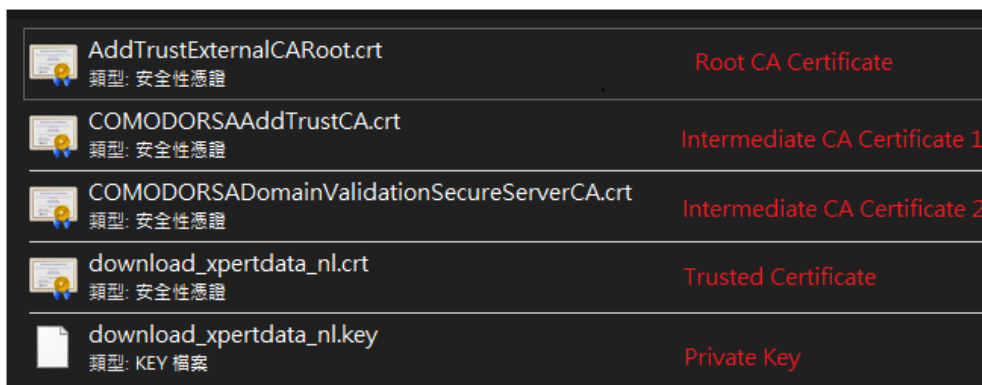
These parameters are explained as follows:

Item	Description
Certificate form	<p>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.</p> <ul style="list-style-type: none"> ● With Root and Intermediate Certificate(s) ● With CA Bundle ● One PEM File - The certificate issued by the certificate authority contains only one PEM file. ● None of above - The certificate issued by the certificate authority contains only one certificate (CRT file) with a private key.
Import Method	<p>Upload Files - The content of the certificate / key shall be obtained by uploading a file.</p> <p>Paste Contents Directly - The content of the certificate / key shall be pasted from clipboard.</p>
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)	<p>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.</p> <p>Add - If there is more than one intermediate CA certificate file, click it to import more.</p>
When With CA Bundle is selected	

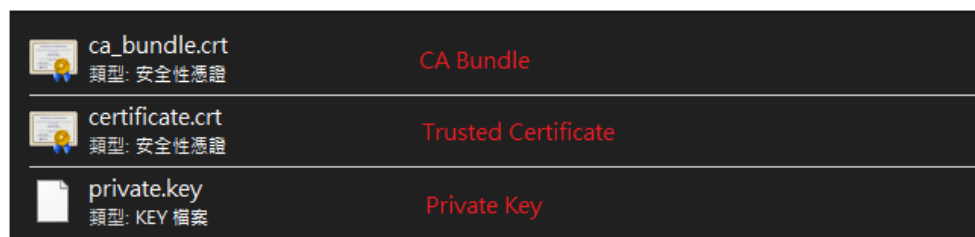
CA Bundle (.cer, .crt)	Click the Browse button to select one certificate or obtain the content of the certificate from the clipboard.
When One PEM File is selected	
PEM File (.pem)	Click the Browse button to select one PEM file.
Save	Save current settings and uploading/pasting the certificate.

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:

```

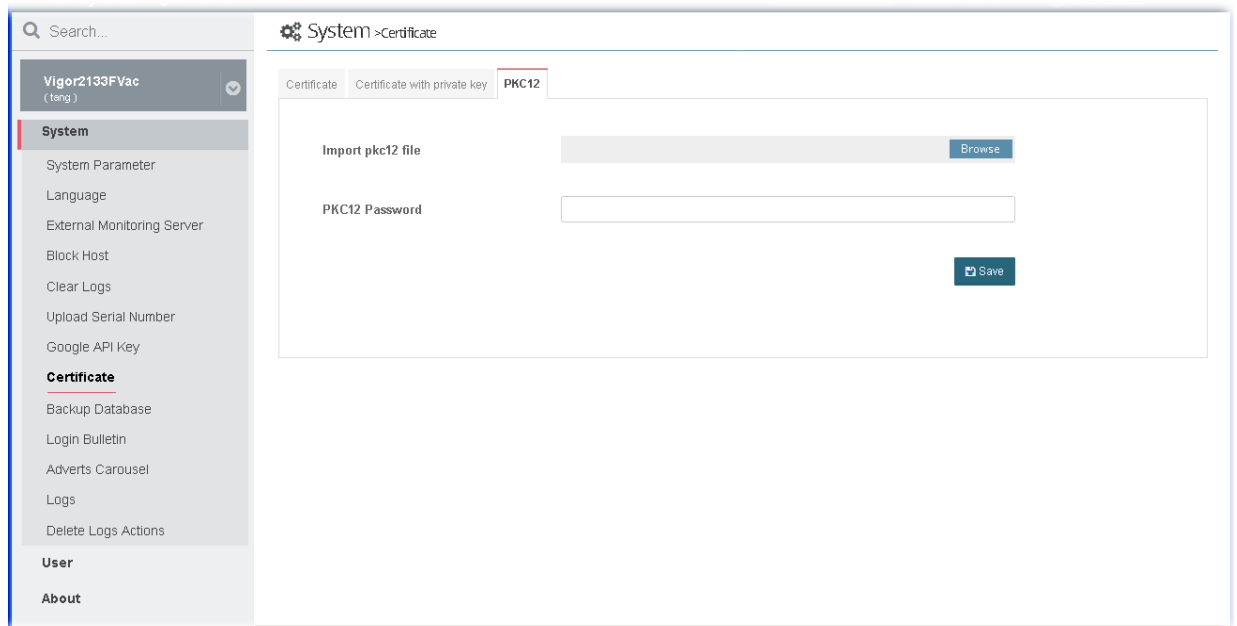
-----BEGIN PRIVATE KEY-----
MIIEkjC....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGDjCCBPag....
-----END CERTIFICATE-----

```

4.8.3 PKC12

PKC 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 PKC 12 file and applying to VigorACS server with specified password.



These parameters are explained as follows:

Item	Description
Import pkc12 file	Click the Browse button to specify the file.
PKC12 Password	Enter a string as password for PKC12 certificate.
Save	Save and activate the current settings.

4.9 Backup Database

Open System>>Backup Database to get the following web pages.

4.9.1 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.

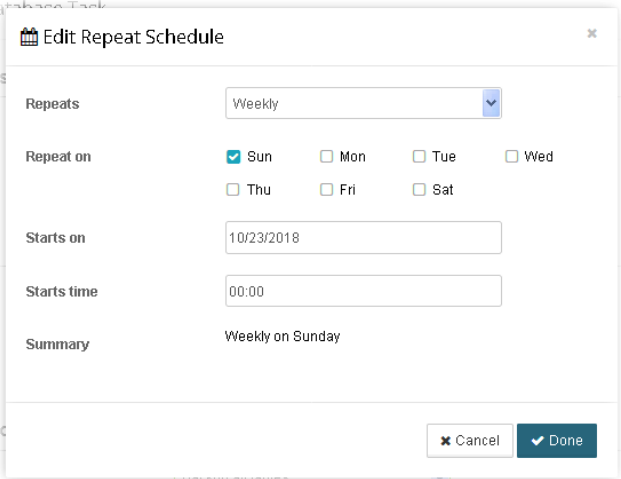
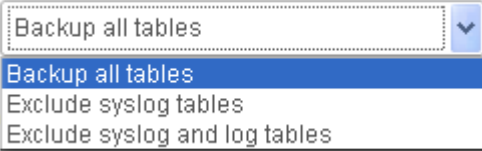
These parameters are explained as follows:

Item	Description
Filter Task List by User Group	Use the drop down list to specify a user group. In which, RootGroup contains all of the users with the role of system administrator in default.
Search Profile Name / Created by	Specify the conditions (type the profile name, creator) for database task searching.
+Add Backup Database Task	Click it 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 it to modify, change the selected profile. Delete - Click it to delete the selected profile.

The following setting page appears when +Add Backup Database Task is clicked.

These parameters are explained as follows:

Item	Description
Task Settings	<p>Enable This Task - Click it to enable the task.</p> <p>Task Name - Type a name for the new task.</p>
Scheduling	<p>Run Backup - Choose Once to perform the backup immediately or at certain time. Choose Repeat to perform the backup periodically.</p> <ul style="list-style-type: none"> ● Later / Now - It is available when Once is selected as Run Backup. ● 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.

	
<p>Backup Options</p>	<p>Backup Type - Choose an option to perform the backup.</p>  <p>Ignore License Tables - VigorACS system performs the database backup by ignoring the tables concerning of backup and license (such as syscd, sysn, dslpmid, dslpmshow and etc..) to prevent from license error while transferring VigorACS server. The default value is "Enabled".</p> <p>After backup delete log tables - Delete the log tables immediately when VigorACS server finishes the backup job</p>
<p>Email Notification</p>	<p>Enable Email Notification - If enabled, VigorACS server will send a notification email about database backup to the recipient.</p> <ul style="list-style-type: none"> ● Email Subject - Enter the subject for the email. ● Email From - Enter the email address of the sender/agent/registrar. ● Email Content - Enter the content of the email. ● Email To - Enter the email address of the recipient. ● +Add recipient - Add more recipients to receive the email from VigorACS server.
<p>Cancel</p>	<p>Discard current settings.</p>
<p>Save</p>	<p>Save the current settings and exit the page.</p>

4.9.2 Backup Files

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

The screenshot shows the 'System > Backup Database' interface. On the left is a navigation menu with sections for System, Backup Database, User, and About. The main area has tabs for Backup Tasks, Backup Files (selected), and Error Logs. Below the tabs are 'Delete' and 'Download' icons, and a pagination control showing page 1 of 21. A table lists backup files with columns for Filename, Size, and Last Modified.

Filename	Size	Last Modified
backup_ACS_2.4.0RC2_r10585_ExcludeSyslogAndLogVer_2018-11-28.0950.sql	524.16 MB	11/28/2018 09:50:21
backup_ACS_2.4.0RC2_r10585_FullVer_2018-11-27.1145.sql	896.78 MB	11/27/2018 11:45:48
backup_ACS_2.4.0RC2_r10585_ExcludeSyslogAndLogVer_2018-11-27.0950.sql	524.15 MB	11/27/2018 09:50:26
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-26.1000.sql	524.58 MB	11/26/2018 10:00:17
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-26.0950.sql	524.58 MB	11/26/2018 09:50:29
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-26.0830.sql	524.58 MB	11/26/2018 08:30:28
backup_ACS_2.4.0RC1_r10374_FullVer_2018-11-25.1145.sql	897.17 MB	11/25/2018 11:45:46
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-25.0950.sql	524.58 MB	11/25/2018 09:50:50
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-25.0830.sql	524.58 MB	11/25/2018 08:30:22
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-24.0950.sql	524.58 MB	11/24/2018 09:50:31
backup_ACS_2.4.0RC1_r10374_ExcludeSyslogAndLogVer_2018-11-24.0830.sql	524.58 MB	11/24/2018 08:30:30
backup_ACS_2.4.0RC1_r10374_FullVer_2018-11-23.1145.sql	897.15 MB	11/23/2018 11:45:41

These parameters are explained as follows:

Item	Description
Delete	Click it to remove the selected filename.
Download	Click it to download the file from the hard disk of VigorACS server located for restoration or transferring. At present, only the file with the size less than 1GB can be downloaded. For the size more than 1GB, get that file from the directory of "EMS/sql-backup" in VigorACS server.

The screenshot shows the 'System > Backup Database' interface with a red message bar at the top stating: 'Selected file is too big to be downloaded, please get it via following path: EMS>sql-backup>ACS_#build#FullVer_2018-01-29.0848.sql'. The table below shows a list of backup files, with the file 'backup_ACS_#build#FullVer_2018-01-29.0848.sql' highlighted in orange, indicating it is the selected file.

The downloaded file can be used for database restoration or transferring. Before restoring the database, turn off the VigorACS server first. After finishing the restoration, turn on the VigorACS server again. The restoration command is,

- `mysql -f -u root -Dtr069 < filename.sql`

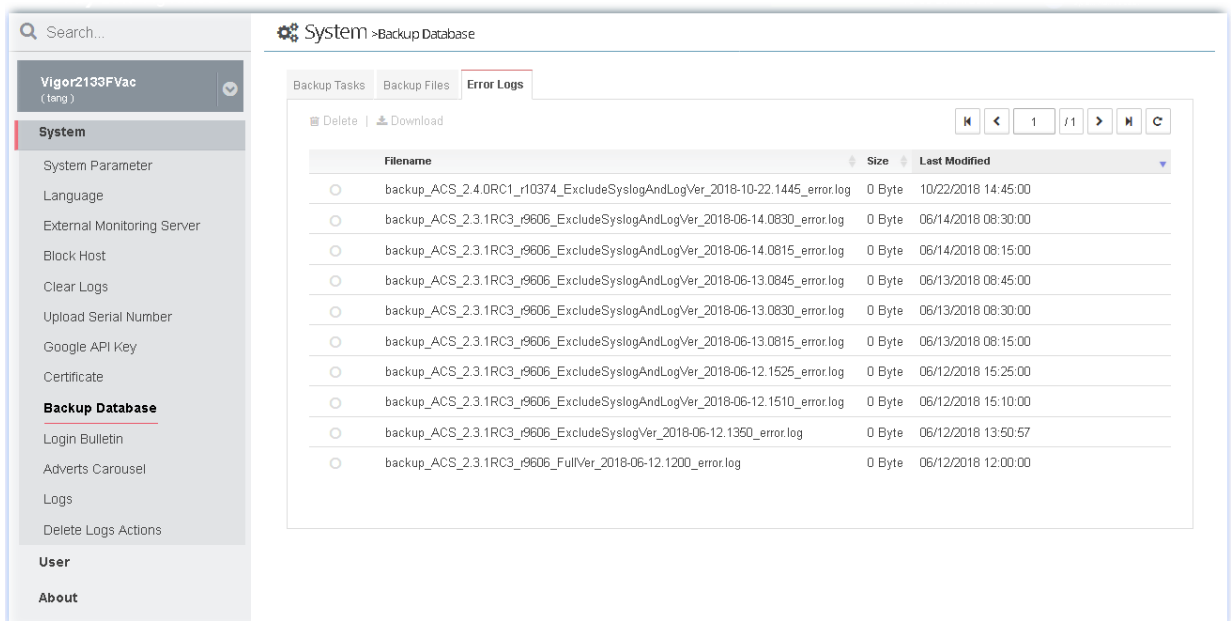
If password is required, restoration command shall be,

- `mysql -f -u root -Dtr069 -p < filename.sql`

Filename	Display the name of the backup file.
Size	Display the size of the backup file.
Last Modified	Display the last modified time.

4.9.3 Error Logs

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

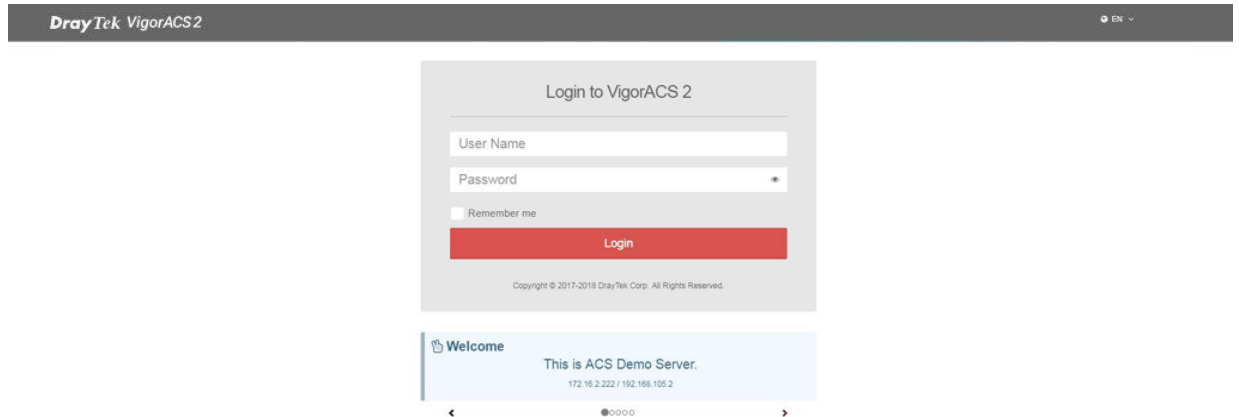
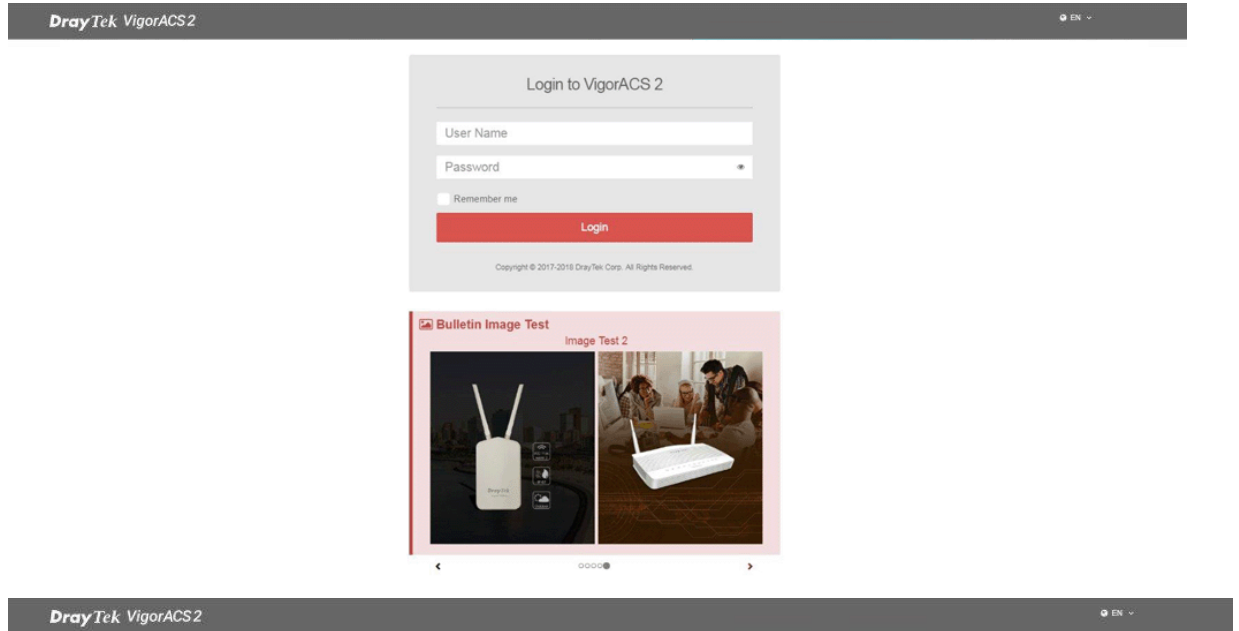


These parameters are explained as follows:

Item	Description
Delete	Click it to remove the selected error log.
Download	Click it to download the selected error log from the hard disk of VigorACS server located. 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. 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.

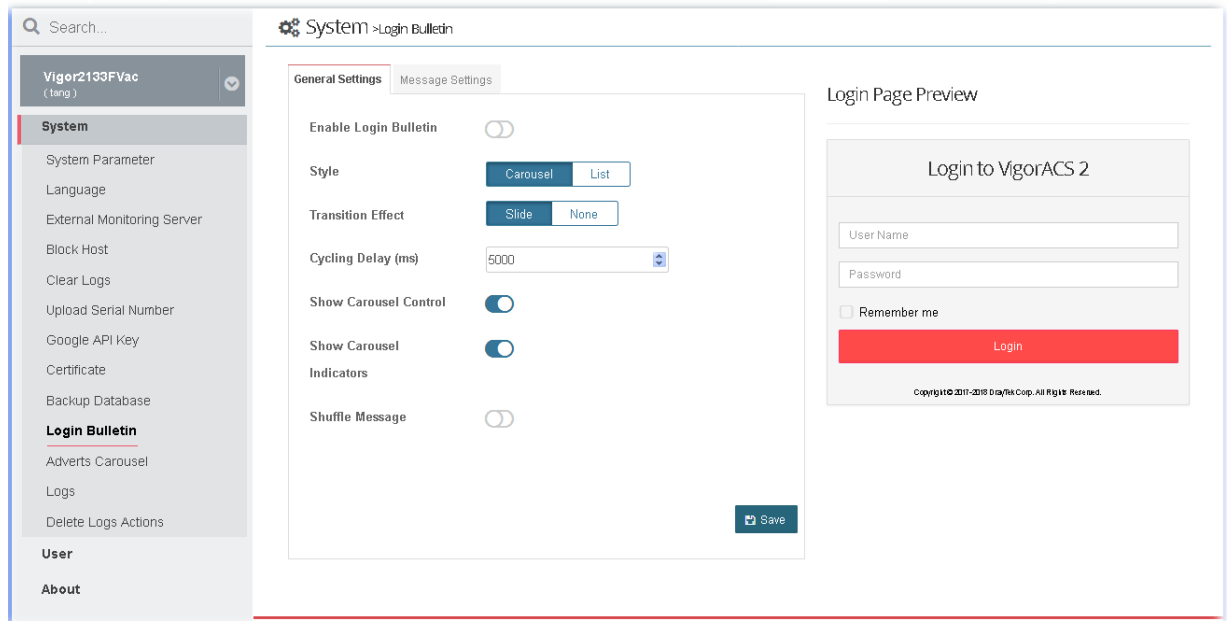
4.10 Login Bulletin

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



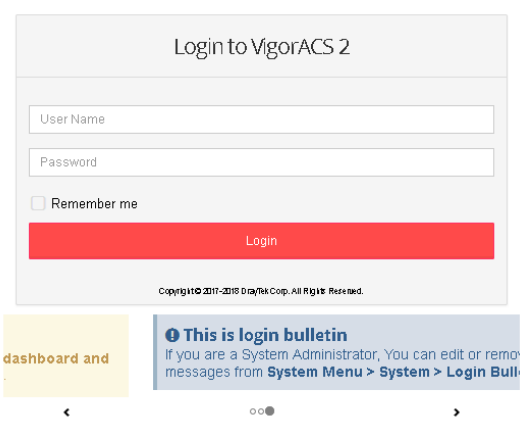
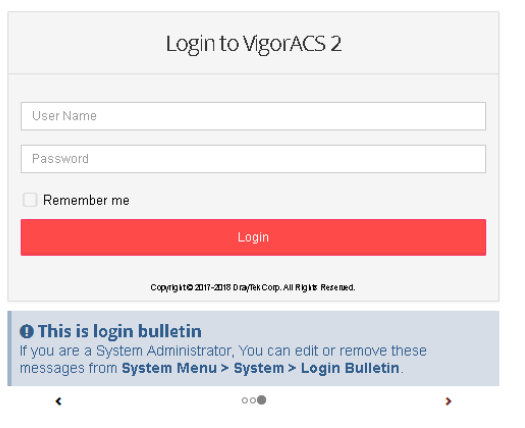
4.10.1 General Settings

Open System>>Login Bulletin and click General Settings to get the following web page.



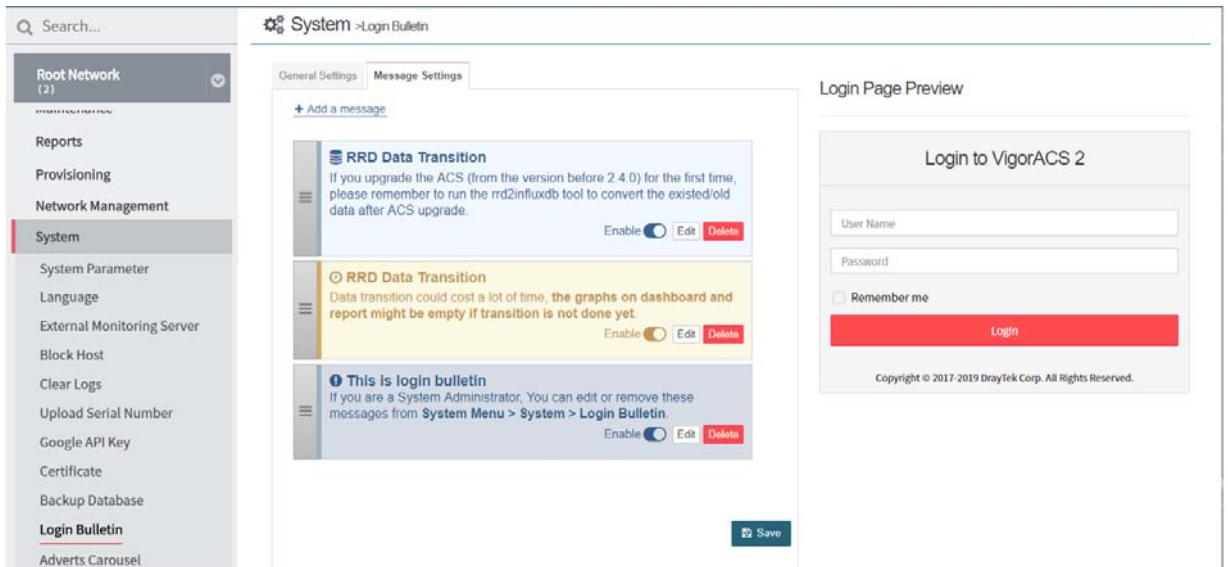
These parameters are explained as follows:

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	<p>The message on the bulletin will be displayed with carousel animation or listed one by one.</p> <p>Carousel - Messages in bulletin will be displayed with carousel animation.</p> <p>List - All of the messages in bulletin will be listed at one time.</p> <p>Login Page Preview</p>

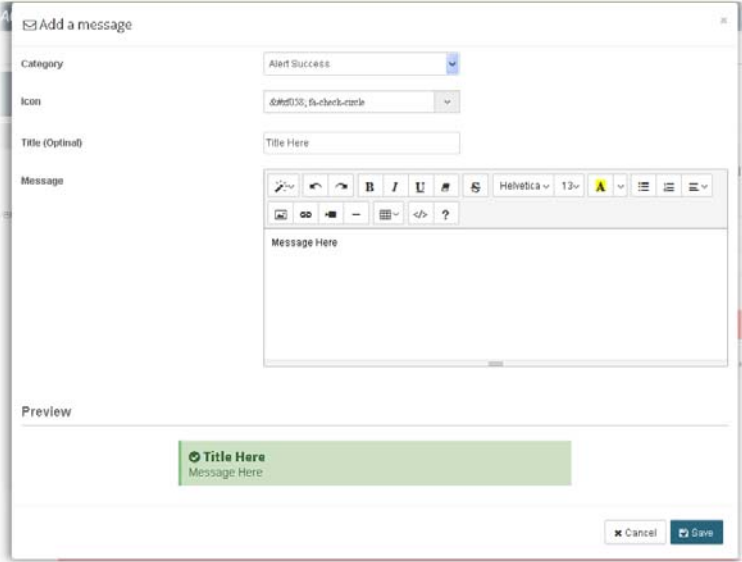
<p>Transition Effect</p>	<p>Slide -The messages will appear automatically from left to right or right to left by sliding.</p> <p>Login Page Preview</p>  <p>None - The message will appear one by one.</p> <p>Login Page Preview</p> 
<p>Cycling Delay (ms)</p>	<p>Set the time delay for every bulletin message item. The available range is 1000 to 60000 ms.</p>
<p>Show Carousel Control</p>	<p>Small arrows below the messages will be shown on the page if this function is enabled.</p>
<p>Show Carousel Indicators</p>	<p>Indicators of the slides below the message will be shown on the page if this function is enabled.</p>
<p>Shuffle Message</p>	<p>The messages will appear randomly if this function is enabled.</p>
<p>Save</p>	<p>Save the current settings.</p>
<p>Login Page Preview</p>	<p>After configuring the settings for login bulletin, click Save to display the messages in this area.</p>

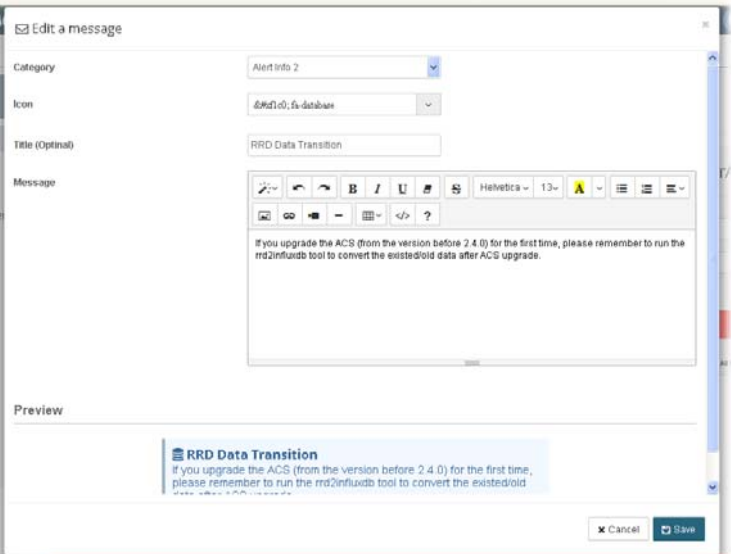

4.10.2 Message Settings

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



These parameters are explained as follows:

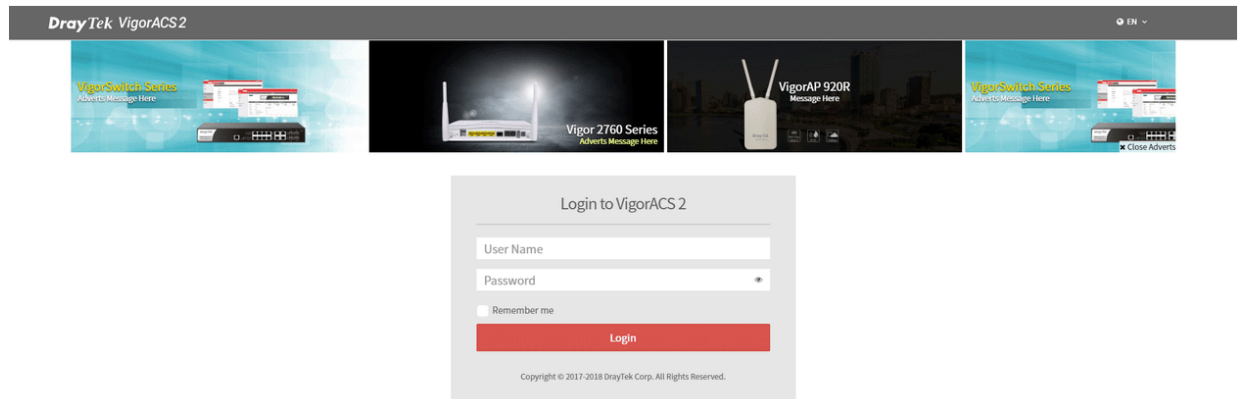
Item	Description
Message Settings Display Area	Display all of the messages. You can change the order of the message by dragging the message up or down.
+Add a message	Create a new message.  <p>Category - Specify the attribute for the message. Icon - Specify one of the types as the icon in the front of the title. Title (Optional) - Enter a string as the heading for the message. Message - Enter the content of the message. Preview - The changes made above will be shown in this area immediately. Save - Save the message and exit the dialog.</p>

<p>Edit</p>	<p>Modify the selected message.</p> 
	<p>Drag this control item to change the sequence of the selected message on the list. After changing, click Save.</p> <p>If the option Shuffle Message in System>>Login Bulletin>>General Settings is enabled, the messages will not be displayed in the order of the list, but will be displayed randomly.</p>
<p>Enable</p>	<p>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.</p>
<p>Delete</p>	<p>Remove the selected message.</p>
<p>Save</p>	<p>Save the current settings.</p>

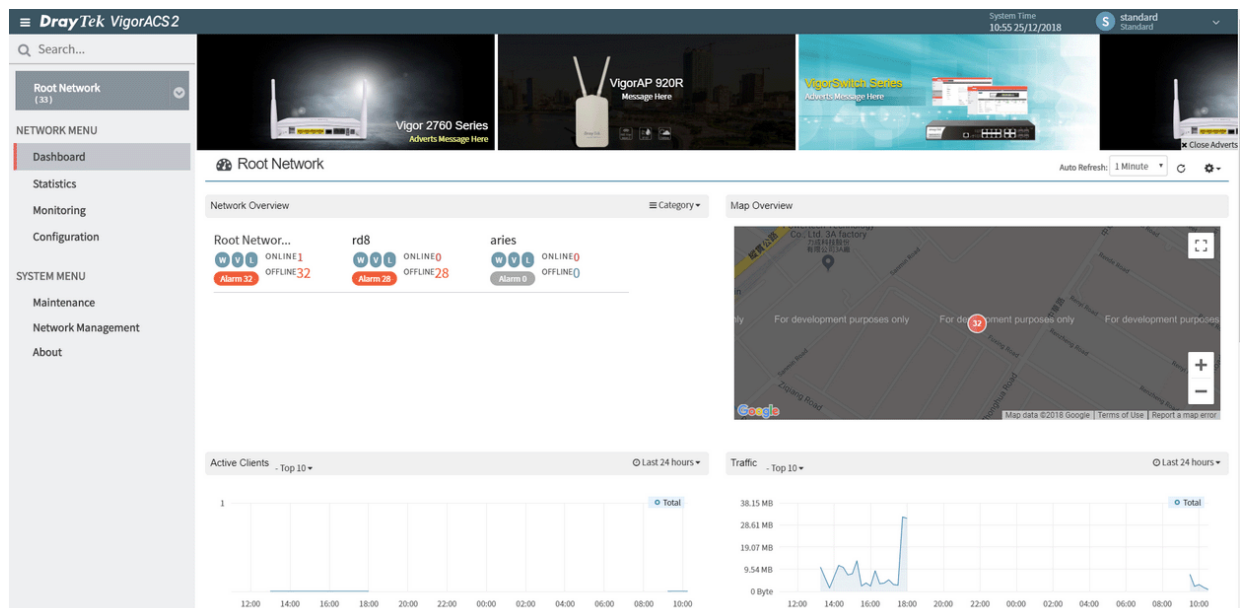
4.11 Adverts Carousel

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

On login page,



On the dashboard,

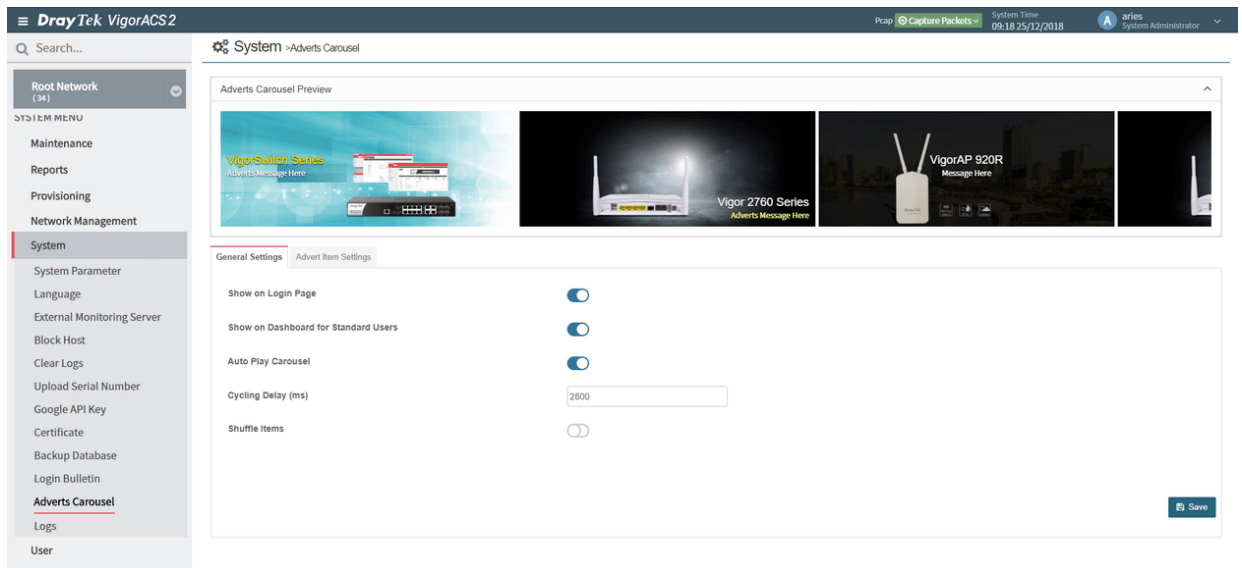


Click the button of Close Adverts on the bottom of the right corner to close the advertisement temporarily. However, the adverts carousel will appear again if switching to other page and returning to this page.

4.11.1 General Settings

Open System>>Adverts Carousel to get the following web page.

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. If disabled, the adverts carousel will NOT be seen on the login page.
Show on Dashboard for Standard Users	It is available only for the VigorACS 2 cloud edition. If enabled, the adverts carousel will be SEEN on the Dashboard. If disabled, the adverts carousel will NOT be seen on the Dashboard.
Auto Play Carousel	If enabled, the adverts carousel will be PLAYED automatically. If disabled, the adverts carousel will NOT be played automatically. 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.

4.11.2 Advert Items Settings

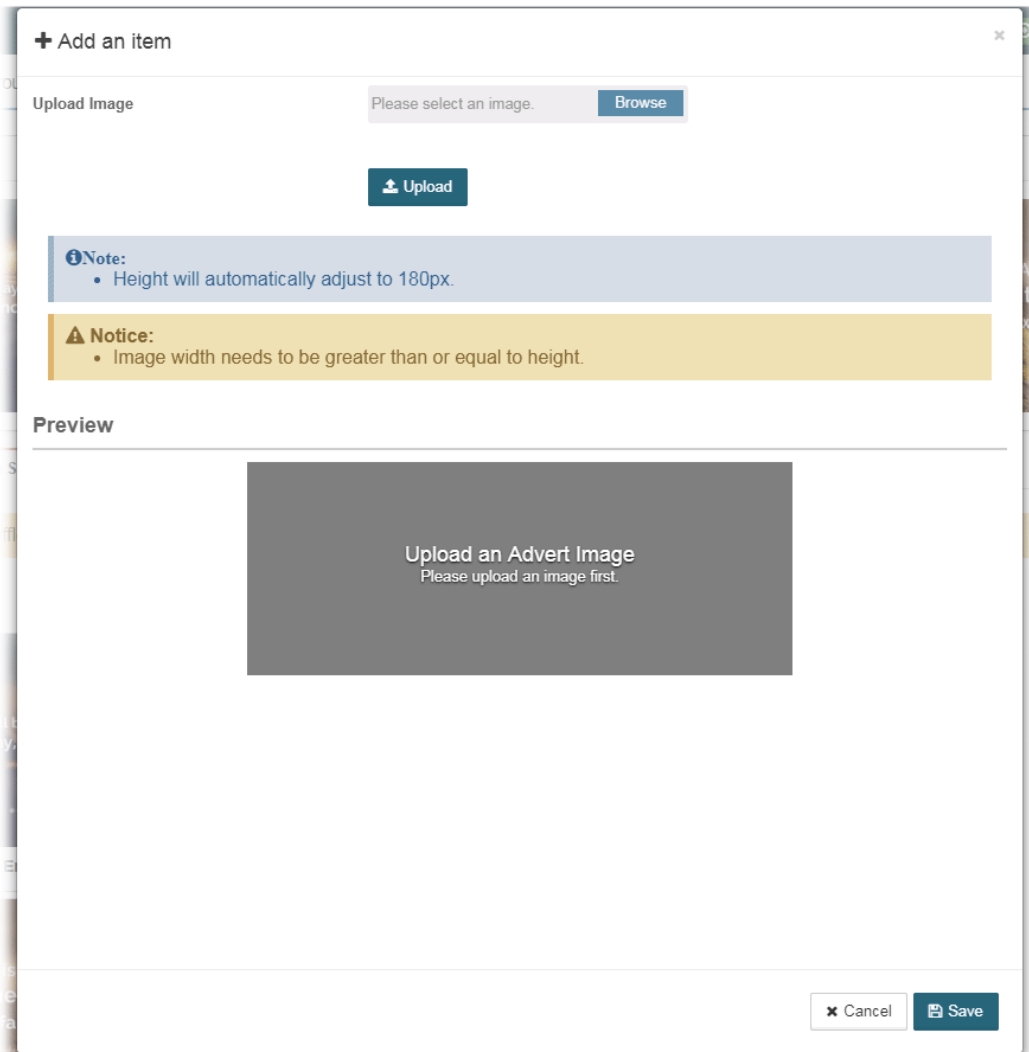
This page is used to upload a selected image onto VigorACS server and enter words (title, message of the image and color specified) on the image for advertisement.

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.




Available settings are listed 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 2 server.
Upload	Upload the selected image to ACS server as the advert image.

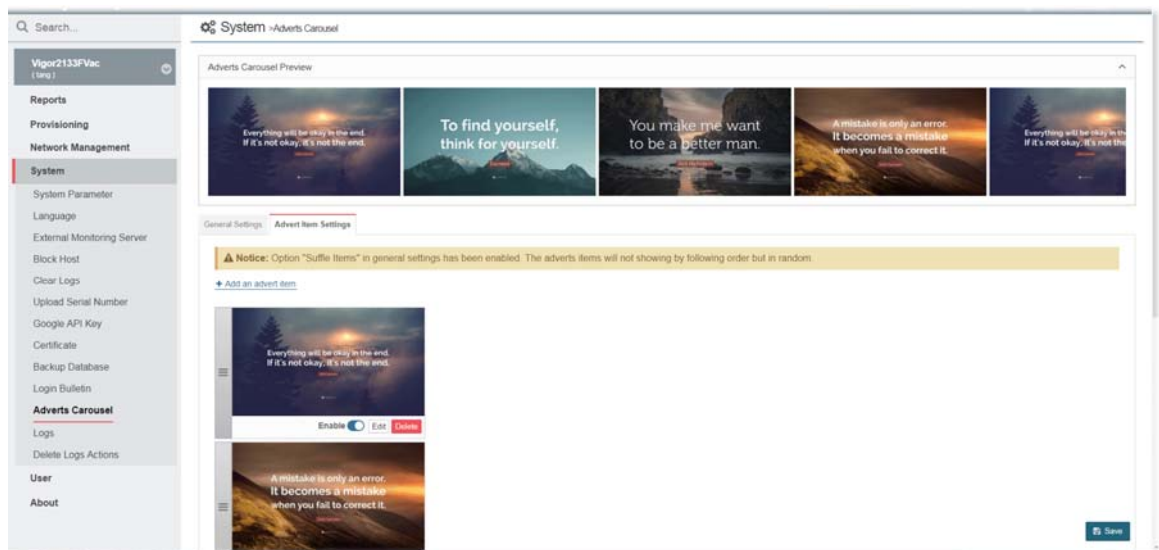
- After specifying an image file, click the **Upload** button. Later, a page with detailed settings will appear as follows:

Available settings are listed as follows:


Item	Description
Upload Image	For change the advert 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 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).

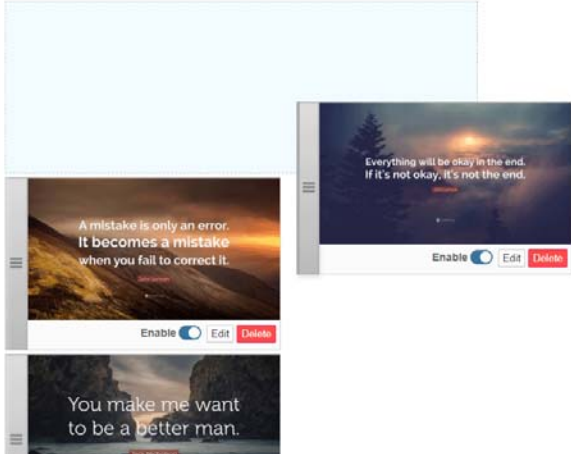
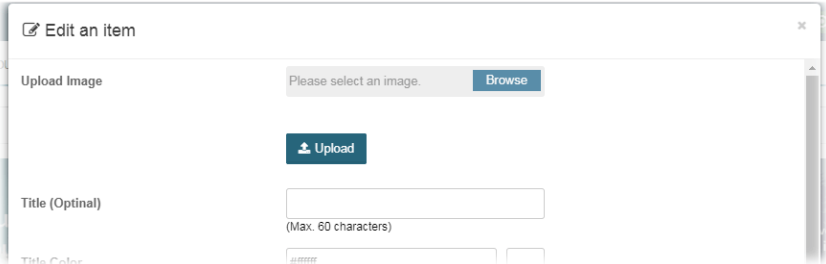
Enable Hyper Link	Choose Enable to activate hyper link for the advertisement.
Link Address	If Enable Hyper Link is enabled, enter the URL of the link.
Text Block Position	Determine the position of the title and message on the advert image.
Preview	Any changes on this setting page will be shown in this field.  <p>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.</p>
Cancel	Discard current settings.
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.



Available settings are listed as follows:

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

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

4.12 Logs

Open System>>Logs to get the following web page. Information displayed here shall be useful for the administration to viewing the status for user access.

ID	User	Severity	Category	Overview	Result	Login IP	Time
2406	kay	Minor	Network Management	Vigor3900 (5454) Device has been deleted.	Succeeded	172.17.6.60	2018/10/16 02:26:36
2405	kay	Minor	Network Management	Vigor3900 (5572) Device has been deleted.	Succeeded	172.17.6.60	2018/10/16 02:22:02
2404	kay	Minor	Network Management	P1260_001DAA06C0CB (5262) Device has been deleted.	Succeeded	118.166.183.34	2018/10/16 02:15:45
2403	kay	Minor	Network Management	DrayTek (5575) Device has been deleted.	Succeeded	118.166.183.34	2018/10/16 02:12:21
2402	kay	Normal	System > System Parameter	Value has been updated.	Succeeded	172.17.6.60	2018/10/16 01:10:50
2401	kay	Normal	System > System Parameter	Value has been updated.	Succeeded	172.17.6.60	2018/10/16 01:10:45
2400	carlos	Major	Maintenance > Firmware Upgrade	(carlos) Job fwu has been deleted.	Succeeded	172.17.6.174	2018/10/16 11:27:04
2399	carlos	Major	Maintenance > Firmware Upgrade	(carlos) Job fwu has been updated.	Succeeded	172.17.6.174	2018/10/16 11:27:00
2398	carlos	Major	Maintenance > Firmware Upgrade	(carlos) Job fwu has been created.	Succeeded	172.17.6.174	2018/10/16 11:26:42
2397	kay	Critical	User > User Management	User kaylee's Profile has been updated.	Succeeded	172.17.6.60	2018/10/16 10:57:15

These parameters are explained as follows:

Item	Description
	Use the drop down list to choose 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 Interval	Specify a period of time for data searching.

ACS System Log	<p>Display the ID, username, login IP, category, overview, severity and time for clients accessing into VigorACS.</p> <p>Select buttons to filter Severity / Category / Result - ??????????</p>
System Log	<p>Display the ID number, model name with MAC address for the CPE, and the action executed in CPE.</p> <p>Export All - Log information can be exported as a file.</p> <p>Delete All - Remove the log for the selected record or remove the log for all of the records.</p>
Login Log	<p>Display the log information, including status, username, login IP, login time and logout time for clients accessing into VigorACS.</p> <p>Export All - Log information can be exported as a file.</p>

4.13 Delete Logs Actions

Open System>>Delete Logs Action to get the following web page.

The screenshot shows a web interface for 'Delete Logs Actions'. On the left is a sidebar with a search bar and a menu. The main area contains a search input, a time interval filter, category filters, and a table with columns for ID, Category, Log Table, Operator, Login IP, Deleted Object, Overview, and Time. The table is currently empty, displaying 'No data available'.

System

- System Parameter
- Language
- External Monitoring Server
- Block Host
- Clear Logs
- Upload Serial Number
- Google API Key
- Certificate
- Backup Database
- Login Bulletin
- Adverts Carousel
- Logs
- Delete Logs Actions**

User

About

System > Delete Logs Actions

search ID / operator / keyword of deleted object Time Interval : 2018/10/29 to 2018/11/28

Category filter: ACS Users | Vigor Devices | Network Clients

ID	Category	Log Table	Operator	Login IP	Deleted Object	Overview	Time
No data available							

This page is left blank.

Chapter 5 User

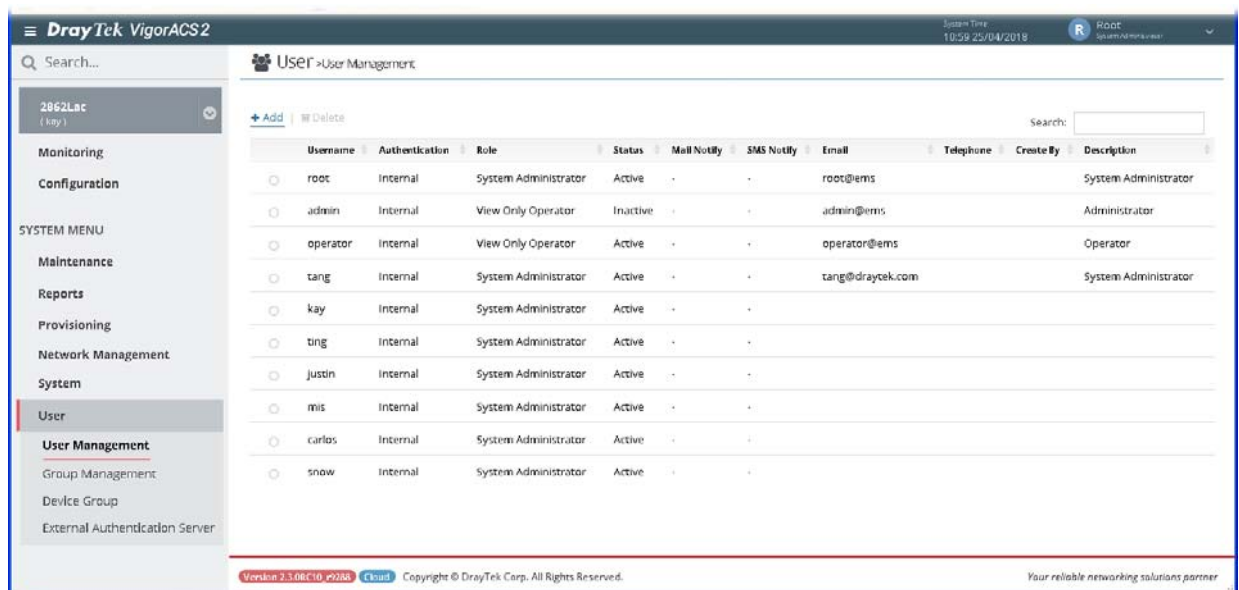
5.1 User Management

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.

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 **SYSTEM MENU**>>**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 it to add a user.
Delete	Click it to remove the selected user.

The following setting page appears when +Add is clicked.

User > User Management

Add User Profile

Enable

Username

Password

Role

SMS Notify

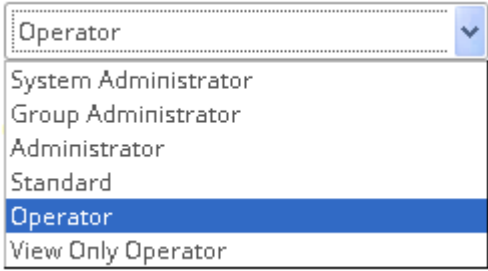
Telephone

Email Notify

Email

Description

Available settings are listed as follows:

Item	Description
Enable	Click it to enable the user profile.
Username	Type a name for the new user.
Password	Type the password for the user.
Role	<p>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.</p>  <p>System Administrator - Have the highest authority. Group Administrator - Have the middle authority high than "Administrator". Administrator - Have the middle authority. Standard - Have the middle authority higher than operator. Operator - Have the low authority higher than View Only Operator. View Only Operator - Have the lowest authority.</p>
SMS Notify	<p>Click it to enable/disable the function.</p> <p>When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms.</p>
Telephone	Type the telephone number for receiving the SMS notification.

Email Notify	Click it to enable/disable the function. When it is enabled, an email will be sent to the user as a notification when the connected device gets alarms.
Email	Type the email for communication between the user and VigorACS server.
Description	Type a brief description for the user.
Cancel	Discard current settings.
Save	Save the current settings and exit the page.

After finished the above settings, click **Save** to save the change.

5.2 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**.

5.2.1 Setting

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

Group Name	License Type	License Date	License Nodes	Used Nodes	Enable Global Mail Server	Enable Global SNMP Server
key	Standard	2018-03-29 ~ 2019-03-29	50	7	<input type="checkbox"/>	<input type="checkbox"/>
ting	Standard	2018-03-29 ~ 2019-03-29	50	19	<input type="checkbox"/>	<input type="checkbox"/>
justin	Standard	2018-03-29 ~ 2019-03-29	50	8	<input type="checkbox"/>	<input type="checkbox"/>
carlos	Standard	2018-03-29 ~ 2019-03-29	50	8	<input type="checkbox"/>	<input type="checkbox"/>
tang	Standard	2018-03-29 ~ 2019-03-29	500	263	<input type="checkbox"/>	<input type="checkbox"/>
snow	Standard	2018-03-29 ~ 2019-03-29	50	4	<input type="checkbox"/>	<input type="checkbox"/>
RootGroup	Root	2017-04-27 ~ 2018-05-27	1000	214	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
mis				0	<input type="checkbox"/>	<input type="checkbox"/>
FAEtest				0	<input type="checkbox"/>	<input type="checkbox"/>

These parameters are explained as follows:

Item	Description
+Add	Click it to add a user group.
Renew License	Click it to renew the license for the selected entry.
Export	Click it to open a dialog for typing SQL syntax to export the settings.
Delete	Click it to clear the selected group. Before using such function, check if the group is blank or not by switching to the Management tab. 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 it to open a dialog for typing SQL syntax to export the settings.
Delete with Whole Sale	Click it to delete the selected user group.
Group ID	Display the index number for the 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.

The screenshot shows the 'Edit Group' configuration page. The breadcrumb is 'USER > Group Management'. There are two tabs: 'Setting' and 'Management'. The 'Edit Group' section contains the following fields:

- Group name:** A text input field containing 'kay'.
- License Type:** A dropdown menu with 'Standard' selected.
- License Date:** A date range field showing '2018-03-29 ~ 2019-03-29'.
- License Nodes:** A text input field containing '50'.
- Enable Global Mail Server:** A toggle switch that is turned on.
- Enable Global SNMP Server:** A toggle switch that is turned on.

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

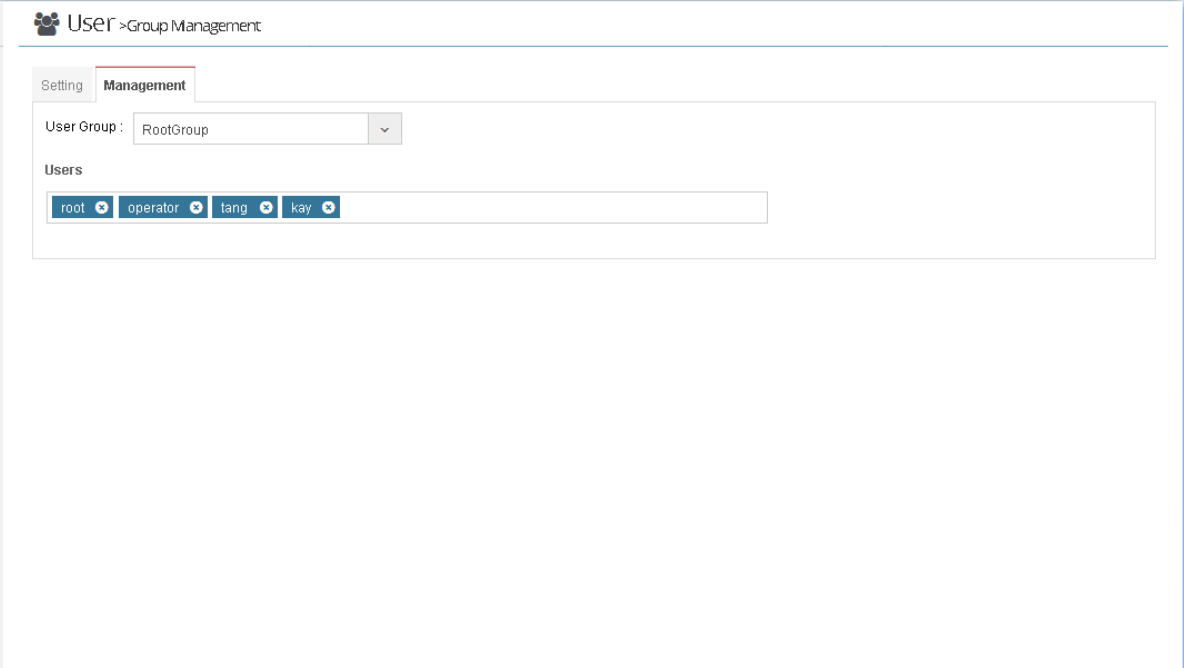
Available settings are listed as follows:

Item	Description
Group Name	Type the name (e.g., Marketing) that can represent the user group.
License Type	Display the type of the license for such group.
License Date	Display the valid date of the license for such group.
License Nodes	Display the number of license nodes for such group.
Enable Global Mail Server	If it is enabled, such group will be allowed to use global mail server.
Enable Global SNMP Server	If it is enabled, such group will be allowed to use global SNMP server.
Cancel	Discard current settings.
Save	Save the current settings and exit the page.

After finished the above settings, click **Save** to save the change.

5.2.2 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. 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. 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.

5.3 Device 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.

5.4 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.

The following setting page appears when +Add is clicked.

The screenshot shows the 'External Authentication Server' configuration page. The 'Enable' toggle is turned on. The 'Server IP Address' is 172.16.3.98 and the 'Destination Port' is 389. The 'Authentication Server Type' is set to 'Active Directory / LDAP' and 'RADIUS'. The 'Use SSL' toggle is off. The 'Bind Type' is set to 'Simple Mode'. There are empty input fields for 'Regular DN' and 'Regular Password'. Below the settings is a table with columns: Id, Profile Name, Common Name, Base Distinguished Name, Additional Filter, Group Distinguished Name, and Action. The table contains the text 'No data available'. At the bottom right are 'Cancel' and 'Save' buttons.

Available settings are listed as follows:

Item	Description
Enable	Click it 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	<p>Active Directory / LDAP -</p> <ul style="list-style-type: none"> ● Use SSL - Enable it to use the port number specified for SSL. ● Bind Type - There are three types of bind type supported: <ul style="list-style-type: none"> ◆ Simple Mode - Just simply do the bind authentication without any search action. ◆ Anonymous - Perform a search action first with Anonymous account then do the bind authentication. ◆ 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. ● Regular DN -Type this setting if Regular Mode is selected as Bind Type. ● Regular Password - Specify a password if Regular Mode is selected as Bind Type. <p>RADIUS -</p> <ul style="list-style-type: none"> ● 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. ● Confirm Shared Secret - Re-type the Shared Secret for confirmation.

Cancel	Discard current settings.
Save	Save the current settings and exit the page.

To create an Active Directory / LDAP profile, click the +Add link in this page to get the following page:

User > External Authentication Server

Profile Name: test

Common Name Identifier: uid

Base Distinguished Name:

Additional Filter:

Note:

- Please type in your additional filter for BaseDN search request. For example,
 - 1) For OpenLDAP: (gidNumber=500)
 - 2) For AD: (msNPAllowDialin=TRUE)

Group Distinguished Name:

Cancel Save

Available settings are listed as follows:

Item	Description
Profile Name	Type a name for such profile.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server.
Additional Filter	Type the condition for additional filter.

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.

User > External Authentication Server

Enable

Server IP Address

Destination Port

Authentication Server Type Active Directory / LDAP RADIUS

Use SSL

Bind Type Simple Mode Anonymous Regular

Regular DN

Regular Password

[+ Add](#)

Id	Profile Name	Common Name	Base Distinguished Name	Additional Filter	Group Distinguished Name	Action
1	...					Delete
2	test	UID	MARKET		GROUP	Delete

Now, click the Save button on the bottom of this page to store the settings. Then, an external authentication server profile just created will be shown on the screen.

User > External Authentication Server

[+ Add](#) | [Delete](#)

Enable	Server IP Address	Authentication Server Type	Destination Port	
<input type="checkbox"/>	true	172.16.3.98	AD/LDAP	389

5.5 Mail Server

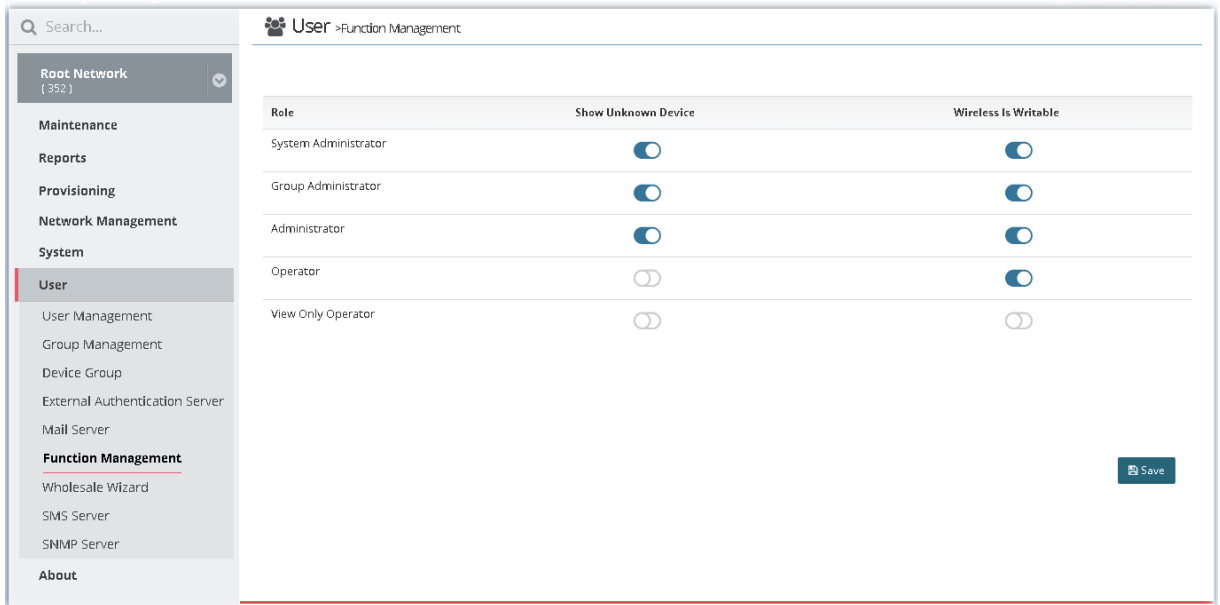
Such feature is used to configure the mail server for sending e-mail. All of the user groups can apply the mail server settings configured in this page.

These parameters are explained as follows:

Item	Description
Send Test Email	Click it 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.
Reset To Default	Click it to reset the mail server to default settings.
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 it 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.

5.6 Function Management

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



The screenshot shows the 'User > Function Management' interface. On the left is a navigation menu with categories: Root Network (352), Maintenance, Reports, Provisioning, Network Management, System, User (selected), User Management, Group Management, Device Group, External Authentication Server, Mail Server, Function Management (with sub-items: Wholesale Wizard, SMS Server, SNMP Server), and About. The main area displays a table with columns: Role, Show Unknown Device, and Wireless Is Writable. A 'Save' button is located at the bottom right of the table area.

Role	Show Unknown Device	Wireless Is Writable
System Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operator	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Only Operator	<input type="checkbox"/>	<input type="checkbox"/>

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.

5.7 Wholesale Wizard

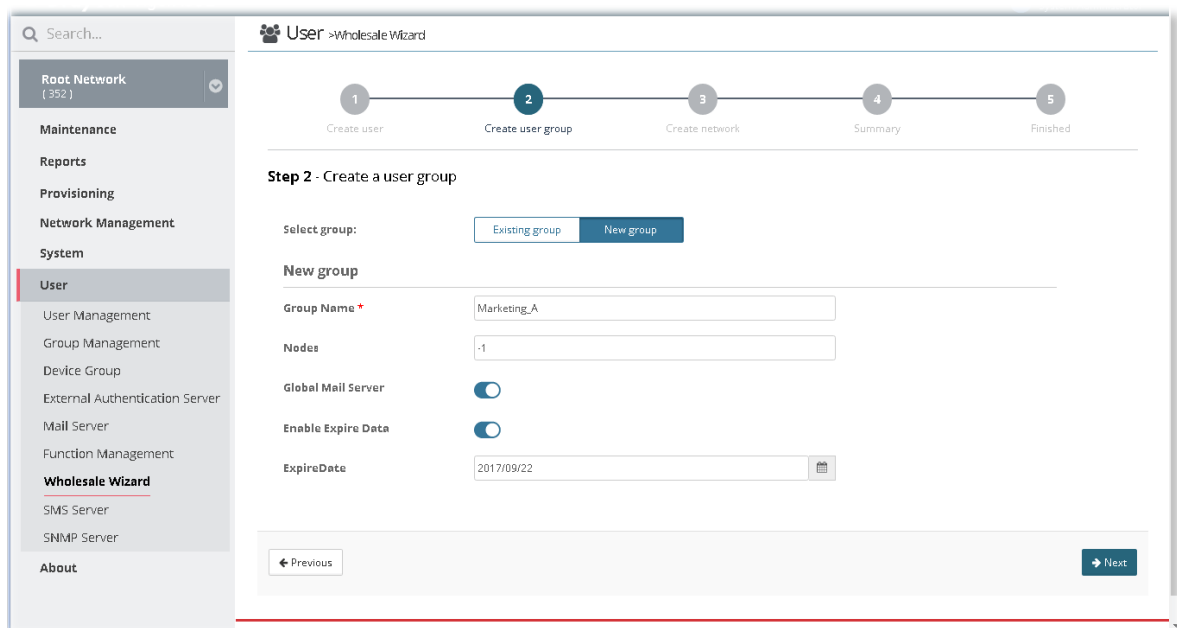
This section can guide the administrator to a create user, user group and network profile via a wizard. Please follow the steps listed below to create:

1. Open **SYSTEM MENU**>>**User** and choose **Wholesale Wizard**.

These parameters are explained as follows:

Item	Description
Username	Type a new name for a new user.
Password	Type a new password.
Telephone	Type the telephone number of such user for receiving the SMS notification.
Email	Type 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.
Previous	Back to previous configuration page.
Next	Go to next configuration page.

- 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:

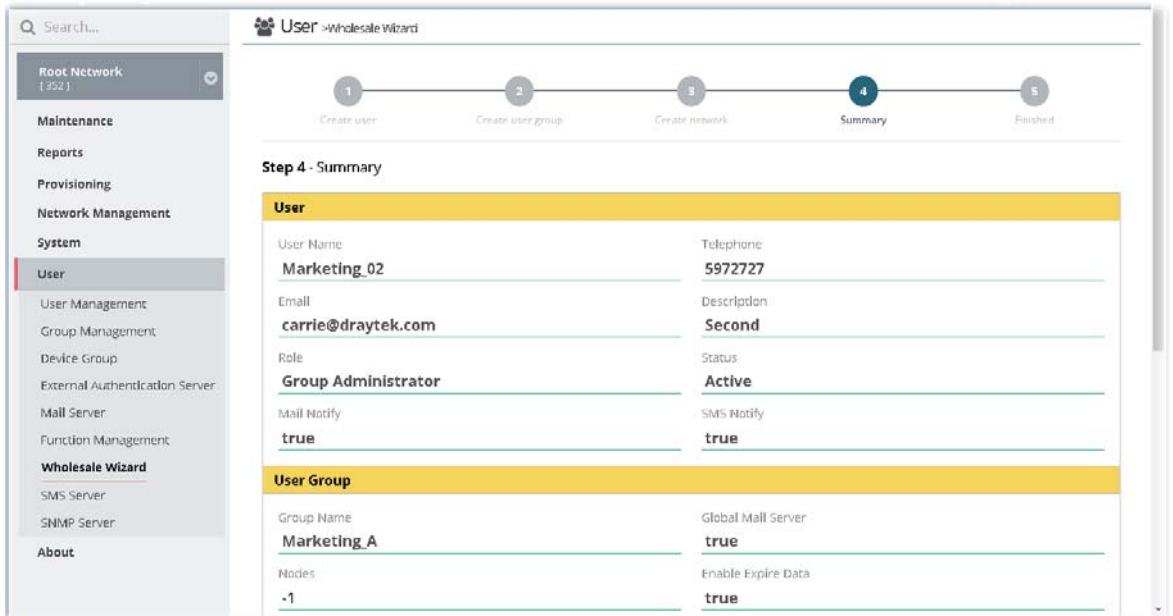
Item	Description
Select group	Determine the group source by choosing Existing group or New group.
Existing group	It is available when Existing group is selected as Select group. User group - Use the drop down list to choose the group you want.
New group	It is available when New group is selected as Select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

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

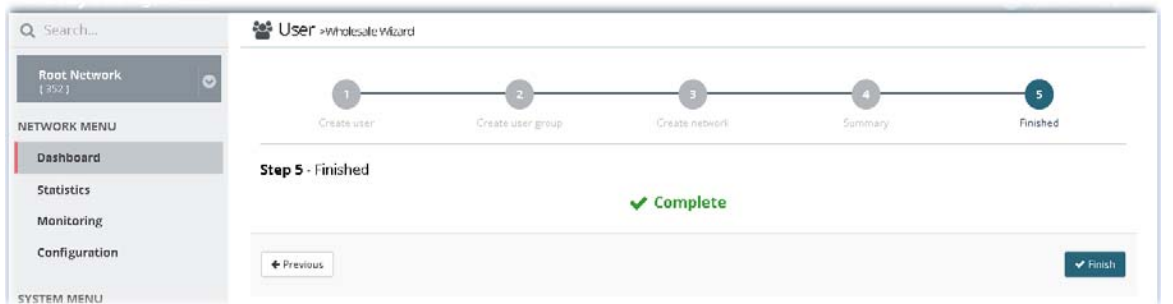
These parameters are explained as follows:

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. 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. Parent Network - Choose one of the existing networks as the Parent Network. Network Name - Type a name for the new network. User Name - Type a name (e.g., market) for the new network. Password - Type a password (e.g., market) for such new network. Location - Type a brief description for the new network.
Previous	Back to previous configuration page.
Next	Go to next configuration page.

- 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.



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



- Click **Finish** to save the settings.
- Open **SYSTEM MENU**>>**User** and choose **User Management**.

5.8 SMS Server

Such feature 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. For example, device loss connection will be treated as "Critical" event.
Save	Save the current settings.

5.9 SNMP Server

Such feature 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	Type the IP address of SNMP server.
Port	Type 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. Click it 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. Type 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.

Applications

A-1 How to Add a User?


1. Open SYSTEM MENU>>User and choose User Management.
2. Click +Add.

 User >User Management

[+ Add](#) | [Delete](#)

	Username	Role	Status
<input type="radio"/>	root	System Administrator	Active

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

 User >User Management

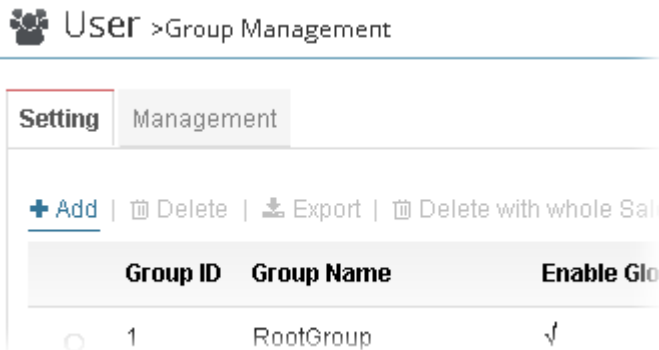
Add User Profile

Enable	<input checked="" type="checkbox"/>
Username	<input type="text" value="CNI"/>
Password	<input type="password" value="*****"/>
Role	<input type="text" value="Operator"/> ▼
SMS Notify	<input checked="" type="checkbox"/>
Telephone	<input type="text" value="0917555681"/>
Email Notify	<input checked="" type="checkbox"/>
Email	<input type="text" value="carrie@draytek.com"/>
Description	<input type="text" value="Router_owner"/>

4. Click Save.

A-2 How to Add a Group?

1. Open SYSTEM MENU>>User and choose Group Management.
2. Click +Add.



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

The screenshot shows the 'Add Group' form in the 'User > Group Management' interface. The form has the following fields and controls:

- Group name:** Text input field containing 'yfnfsui'.
- Nodes:** Text input field containing '-1'.
- Enable Global Mail Server:** Toggle switch, currently turned on.
- Enable Global SNMP Server:** Toggle switch, currently turned off.
- Enable Expire Date:** Toggle switch, currently turned on.
- Expire Date:** Date input field containing '2017/02/24'.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'.

1. **Group Name** - Type a new name of the user group.
 2. **Nodes** - Define number of node.
 3. **Enable Global Mail Server** - Click it to enable /disable global mail server.
 4. **Enable Global SNMP Server** - Click it to enable /disable global SNMP server.
 5. **Enable Expire Date** - Click it to enable/disable the expire date.
 6. **Expire Date** - Choose the expire date for such user group.
4. Click Save.

Setting		Management	
+ Add Delete Export Delete with whole Sale			
<input type="radio"/>	8	ACMEUK	√ - No Limit Nodes √ 2017/01/31 0
<input type="radio"/>	9	nobody group	- - No Limit Nodes - 2016/12/21 0
<input type="radio"/>	10	tim group	- - 7 √ 2017/01/26 2
<input type="radio"/>	15	one user account group	- - No Limit Nodes - 0
<input type="radio"/>	30	henry group	√ √ No Limit Nodes - 2
<input type="radio"/>	35	ttt	- - 18 - 0
<input type="radio"/>	39	r-group	- - No Limit Nodes - 0
<input type="radio"/>	41	lk1	- - No Limit Nodes - 0
<input type="radio"/>	42	alvaco	- - No Limit Nodes - 0
<input type="radio"/>	43	brinet	- - No Limit Nodes - 0
<input type="radio"/>	44	ScanAccess	- - No Limit Nodes - 2
<input type="radio"/>	46	Migrax	- - No Limit Nodes - 0
<input checked="" type="radio"/>	48	yfntsui	√ - No Limit Nodes √ 2017/02/24 0

Part III SYSTEM MENU, General Settings for Managing CPE

Chapter 6 Network Management

DrayTek VigorACS 2

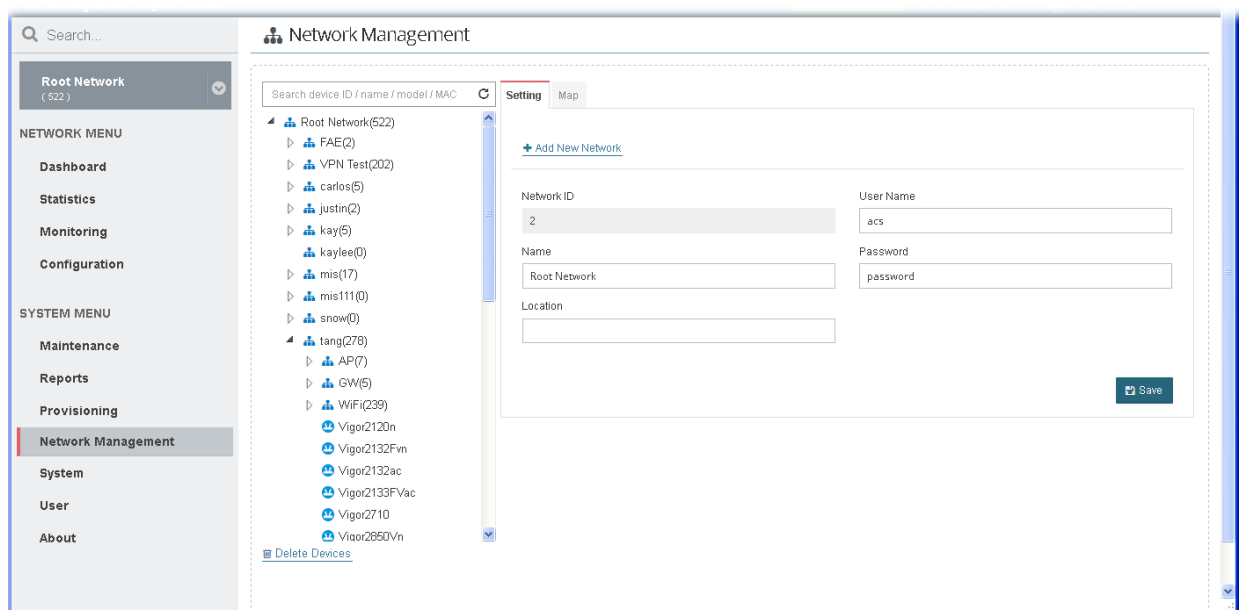
Network Management allows you to modify the information for Networks and Devices.

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.

6.1 Settings for Network

To add, change or delete a network, please open **SYSTEM MENU >> Network Management**. Click **Root Network** or sub-network to get the following web page.



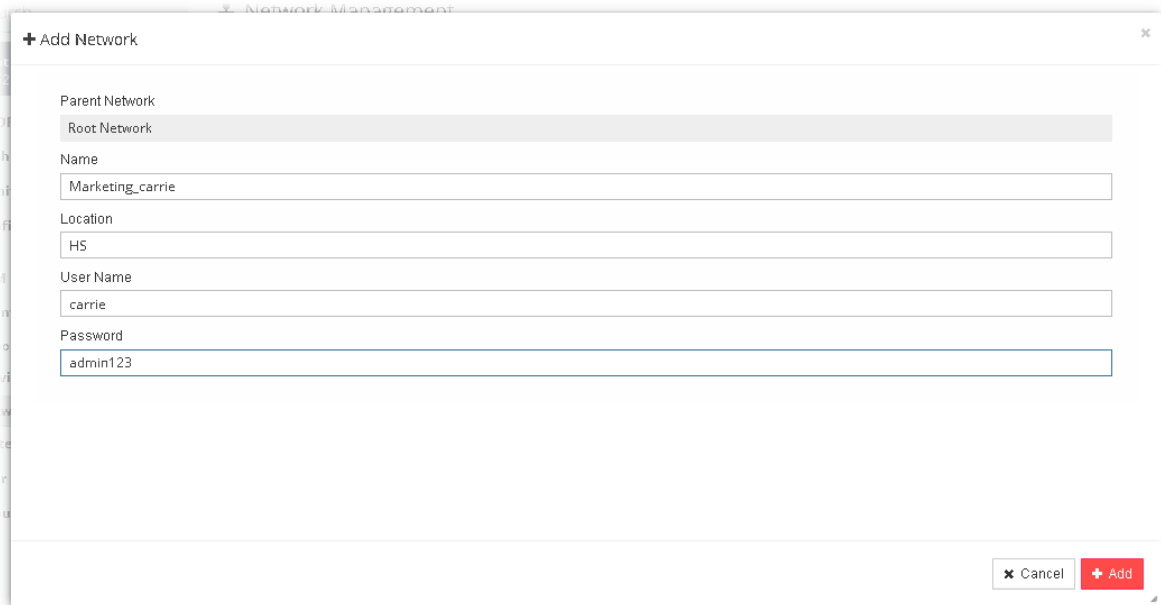
These parameters are explained as follows:

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 it to add a new network.
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 it to save the change.

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



The screenshot shows a web-based dialog box titled '+ Add Network'. It features a dropdown menu for 'Parent Network' with 'Root Network' selected. Below are text input fields for 'Name' (Marketing_carrie), 'Location' (HS), 'User Name' (carrie), and 'Password' (admin123). At the bottom right, there are 'Cancel' and 'Add' buttons.

Available settings are listed 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. In default, Root Network is the parent network for any new created network.
Name	Type a name for the new network.
Location	Type the location for the new network. Later, you can locate such network on the web page of SYSTEM MENU >> Network Management>>Map .
User Name	Type a login name (e.g., carrie) for the new network which will be used for communication between Vigor device and VigorACS.
Password	Type 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 <i>carrie</i> and <i>admin123</i>) in the corresponding fields.
Cancel	Discard current settings.
Save	Save the current settings and exit the page.

After finished the above settings, click Save to save the change.

6.2 Settings for Device

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

Open **SYSTEM MENU >> 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.

The screenshot displays the 'Network Management' interface. On the left is a navigation menu with 'Network Management' selected. The main area shows a tree view of networks under 'Root Network (353)'. A specific device is selected, and its settings are shown in a form. The form includes fields for Device ID (154), Network ID (134), Model Name (Vigor2920Vn), Device Name (2920Vn_00507FCC3E50), Serial number (29202920), MAC Address (00507FCC3E50), Location, IP (192.168.105.142), and Port (8069). There are also buttons for 'Delete This Device' and 'Change Network', and a 'Status' section with 'Disable' and 'Enable' options.

These parameters are explained as follows:

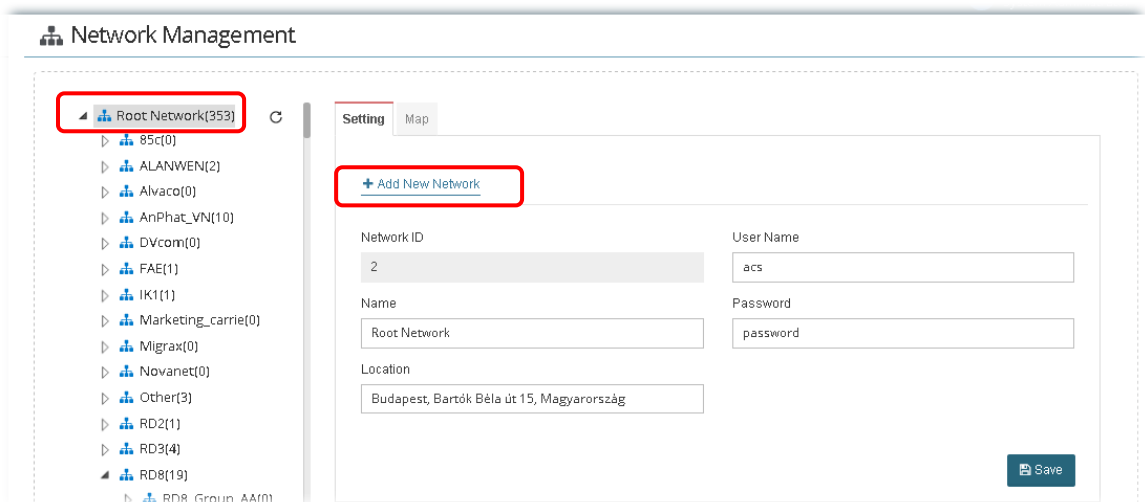
Item	Description
Delete This Device	Click it to remove the selected CPE from current group.
Change Network	Click it to change the network / group for the selected CPE.

	 <p>Move the mouse cursor on the network you want and click Apply.</p>
Status	<p>Disable - The selected device will be hidden on the tree view. Enable - The selected device can be displayed on the tree view.</p>
Known Device	<p>Known - The selected CPE is known (👤) to VigorACS 2. Unknown - If the selected CPE is new added device, it will be identified as Unknown (❓).</p>
Device ID / Network ID	<p>Device ID - Display the number of that device which is given by VigorACS 2 randomly. Network ID- Display the ID number of the network that selected device is grouped under.</p>
Model Name / Device Name	<p>Model Name - Display the model name of the selected device. Model name cannot be changed. Device Name - Display the name of the device for identification. It can be changed if required.</p>
Note 1 / Note 2	<p>Note 1 - Display brief description for the selected device. Note 2 - Display brief description for the network.</p>
Serial number / MAC Address	<p>Serial number - Type a number for identification of the device. MAC Address - Display the MAC address of the device.</p>
Location	<p>Display the position of the device.</p>
Phone No.	<p>It is optional and is used to offer additional information for reference. If required, type a phone number for such device.</p>
Domain Name	<p>Type a domain name for a CPE. Later, simply click the domain name to access into the CPE.</p>
Management Port	<p>Type a port number which will be used for accessing into web user interface of the CPE.</p>
Management Protocol	<p>Choose HTTPS or HTTP.</p>
IP / Port / URI	<p>Display the IP address, port number and URI.</p>
User Name / Password	<p>Display the username and password that VigorACS 2 can use to access into such CPE.</p>

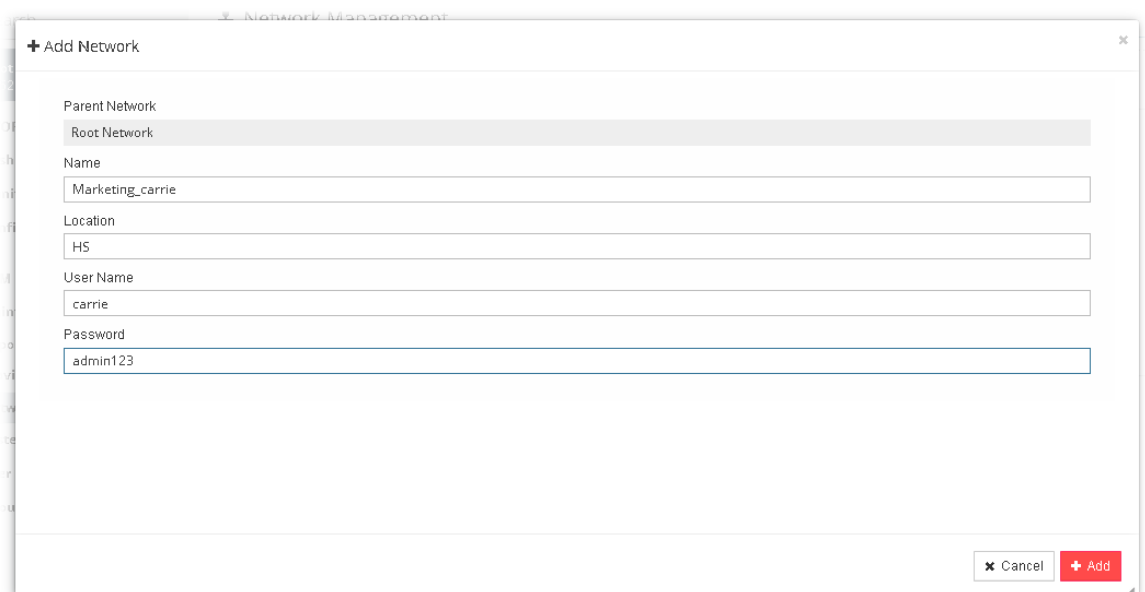
Applications

A.1 How to Create a Network for Managing Devices?

1. Open SYSTEM MENU>>Network Management and click Root Network.
2. Click +Add New Network on the Setting page.

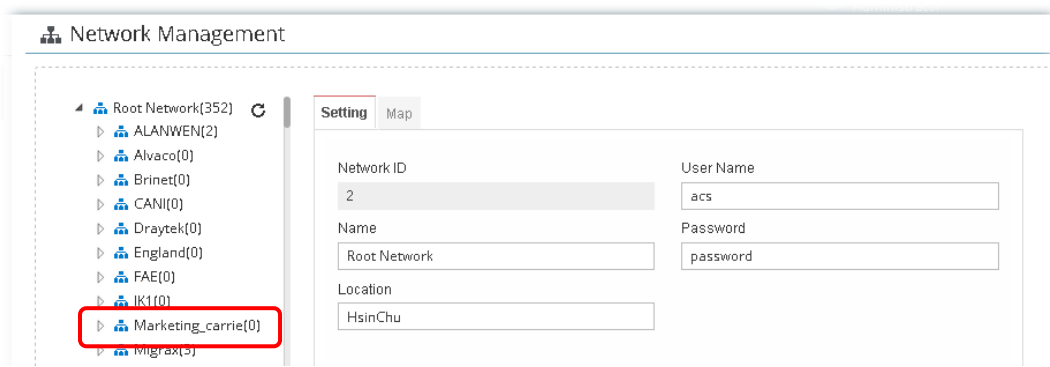


3. In the following page, type required information for the new network.



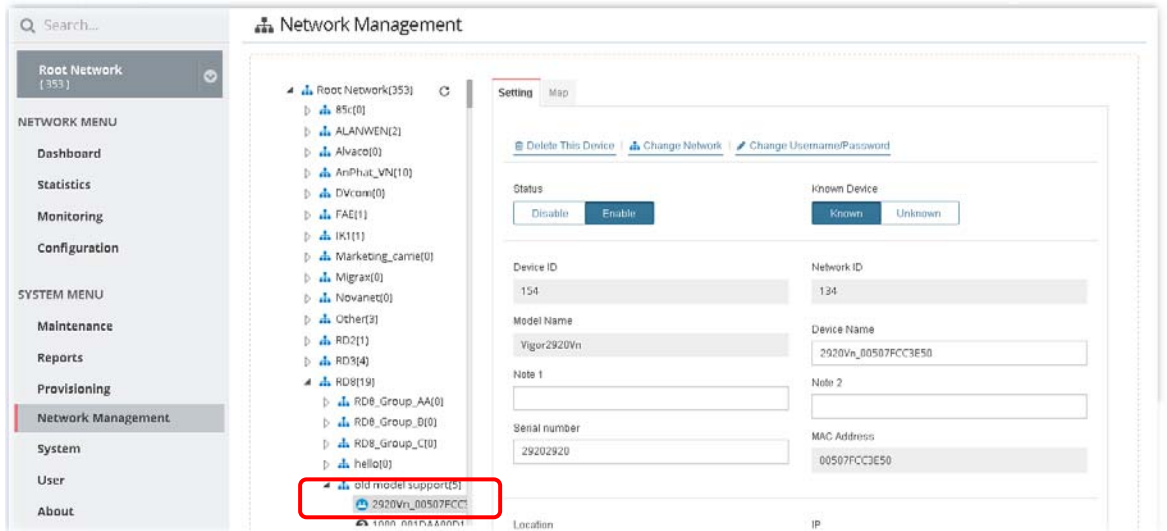
4. Click Add.

5. The new network has been created and displayed on the tree view.

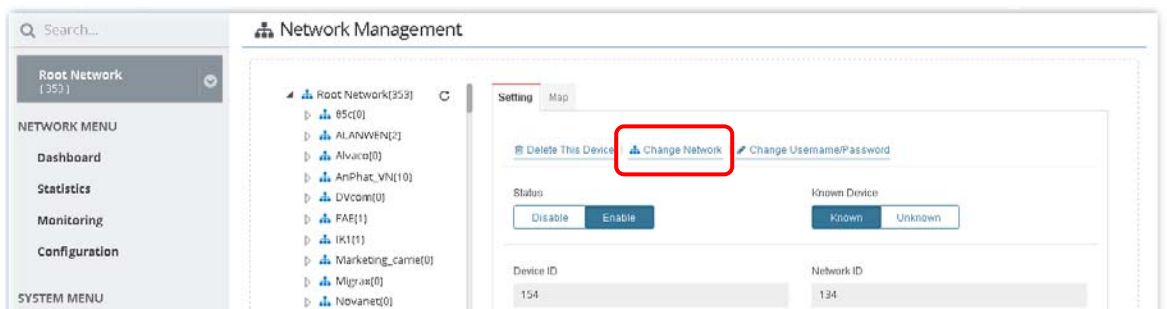


A.2 How to Change the Network of a Device?

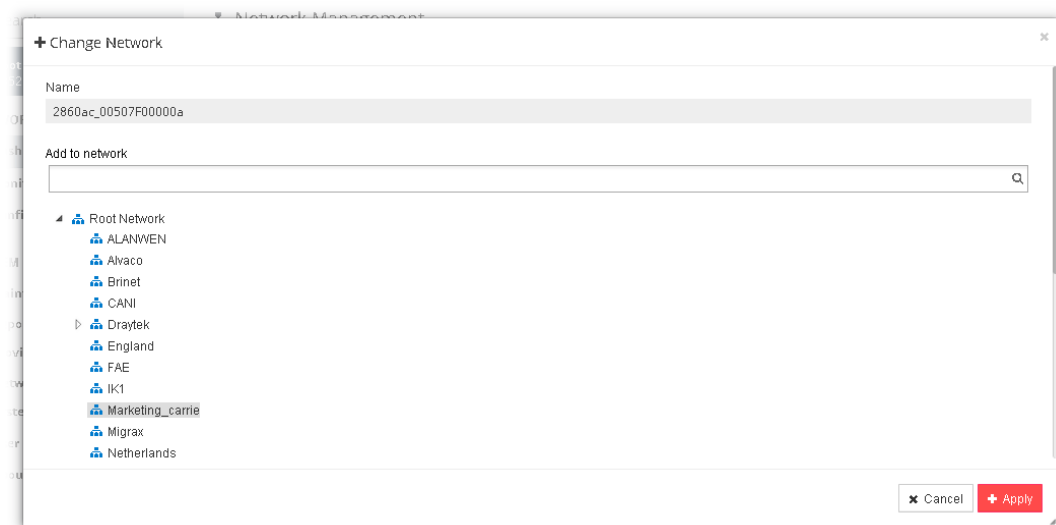
1. Open SYSTEM MENU>>Network Management.
2. Choose and click a CPE displayed on Root Network tree view.



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 (Marketing_carrie, in this case).

Network Management

- Root Network(352)
- ALANWEN(2)
- Alvaco(0)
- Brinet(0)
- CANI(0)
- Draytek(0)
- England(0)
- FAE(0)
- IK1(0)
- Marketing_carrie(1)
 - 2920Vn_00507FCC:
- Migrax(3)

Setting | Map

Status

Device ID

154

Model Name

Vigor2920Vn

Note 1

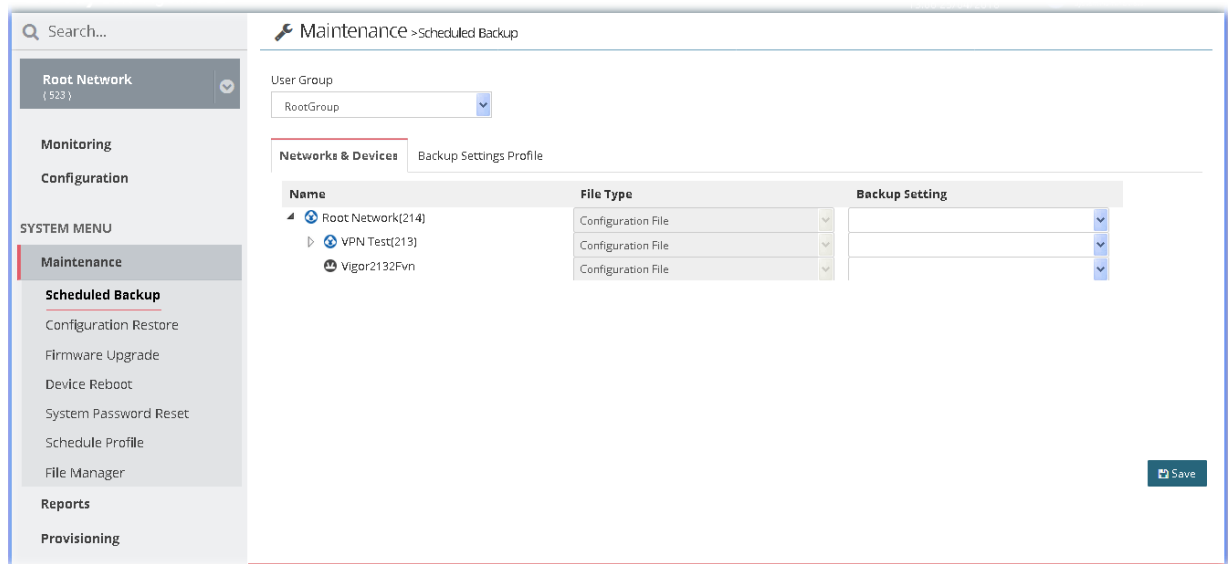
Chapter 7 Maintenance

Options in Maintenance are configured and applied onto numerous TR-069 CPEs instead of configuring settings for each CPE one by one.

7.1 Scheduled Backup

7.1.1 Networks & Devices

Such 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. Each user group can be configured with different backup settings profiles.
File Type	Display the file type used for the device.

Backup Setting	<p>Choose a profile defined in Backup Settings Profile for applying onto the selected CPE.</p> <div data-bbox="655 293 1305 600"><p>Backup Setting</p><p>Disabled ▼</p><p>As Parent ▼</p><p>As Parent</p><p>Disabled</p><p>Default</p><p>wifi</p></div>
Save	Save the current settings.

7.1.2 Backup Settings Profile

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

The screenshot shows the 'Maintenance > Scheduled Backup' page. On the left is a navigation menu with 'Maintenance' selected, and 'Scheduled Backup' highlighted. The main area shows a 'User Group' dropdown set to 'RootGroup' and a 'Backup Settings Profile' tab. Below is a table with columns: Name, Period(Days), Type, Time Interval, and Action. The table lists several profiles like BK_711, Default, 555, Nini, once a day, once in two days, once in three days, kd52, and Elena backup, each with edit and delete links.

Name	Period(Days)	Type	Time Interval	Action
BK_711	1	The Last 20	Any	Edit Delete
Default	1	The Last 20	00:00-00:00	Edit Delete
555	1	The Last 20	Any	Edit Delete
Nini	1	The Last 20	Any	Edit Delete
once a day	1	The Last 20	Any	Edit Delete
once in two days	2	The Last 20	Any	Edit Delete
once in three days	3	The Last 20	Any	Edit Delete
kd52	10	All	11:36-24:00	Edit Delete
Elena backup	1	The Last 20	Any	Edit Delete

These parameters are explained as follows:

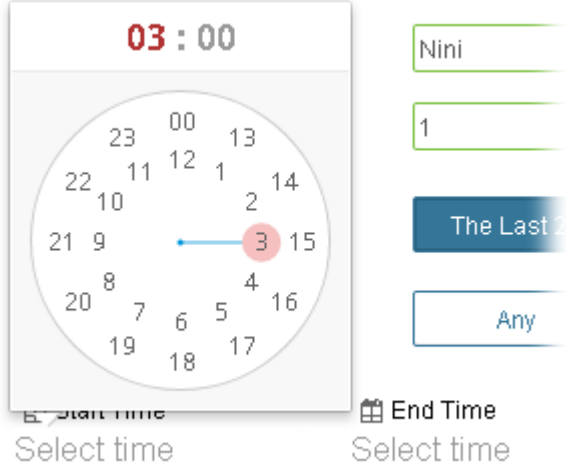
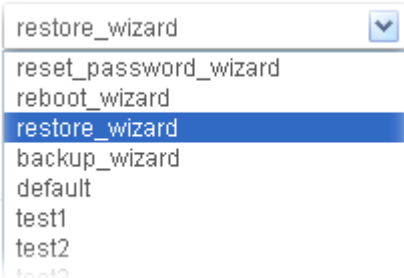
Item	Description
User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.
+Add	Click it to create a new profile.
Edit	Click it to modify, change the selected profile.
Delete	Click it to delete the selected profile.

The following setting page appears when +Add is clicked.

The screenshot shows the configuration form for a new backup settings profile. It includes fields for 'User Group' (RootGroup), 'Name' (Nini), 'Backup Period(days)' (1), 'Keep Files' (The Last 20), 'Time Interval' (Any), and 'Schedule Profile' (restore_wizard). There are 'Cancel' and 'Save' buttons at the bottom right.

Available settings are listed as follows:

Item	Description
------	-------------

User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.
Name	Type 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	<p>Set a time interval for executing the backup work for networks and devices.</p> <ul style="list-style-type: none"> ● Now ● Scheduled ● Schedule Profile
Scheduled	<p>Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date - Click it to enable the time setting. Date - Click it to pop up a calendar to choose a date as the starting date.</p>
Schedule Profile	<p>Choose a trigger profile from the drop down list. In which, VigorACS offers default schedule profile.</p> 

7.2 Configuration Restore

7.2.1 Apply to Devices

Such 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.

The screenshot shows the 'Configuration Restore' page in the VigorACS interface. The left sidebar contains a 'NETWORK MENU' with 'Configuration' selected, and a 'SYSTEM MENU' with 'Maintenance' > 'Configuration Restore' selected. The main content area shows a 'User Group' dropdown set to 'RootGroup'. Below this, there are two tabs: 'Apply to Devices' (active) and 'Restore Settings Profile'. The 'Apply to Devices' tab displays a tree view of the network structure. The tree shows 'Root Network(312)' expanded to 'Other(3)', which is expanded to 'vigor2910(1)'. Under 'vigor2910(1)', there are three devices: '2910V_00507FC26824', '2860n_01DAAF7A900', and '3900_00507F7FFCE8'. Each device has a toggle switch in the 'Apply' column, a dropdown menu in the 'File List' column, and another dropdown menu in the 'Restore Profile' column. The '2910V_00507FC26824' device has its toggle switch turned on. A 'Save' button is located at the bottom right of the table.

These parameters are explained as follows:

Item	Description
User Group	Specify a user group for applying the restore settings profile. Each user group can be configured with different restore settings profiles.
Apply	Click the icon to enable configuration restoration for the selected CPE.
File List	Use the drop down list to choose one of the files (with the date of the configuration file created) to be applied for the file restoration of the selected CPE.
Restore Profile	Choose a profile defined in Restore Settings Profile to be applied to the selected CPE.
Save	Save the current settings.

7.2.2 Restore Settings Profile

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

The screenshot shows the 'Maintenance > Configuration Restore' page. On the left is a navigation menu with 'Maintenance' selected. The main area shows a 'User Group' dropdown set to 'RootGroup' and a 'Restore Settings Profile' tab. Below this is a table with the following data:

Name	Trigger Profile	Time Interval	Action
restore_wizard	restore_wizard	05:12-05:17	Edit Delete
Default	default	00:00-00:00	Edit Delete
^RD8TestTestTest	-	06:12 AM-06:17 AM	Edit Delete
1111	-	Any	Edit Delete
2222	-	Any	Edit Delete
3.333	-	Any	Edit Delete

These parameters are explained as follows:

Item	Description
User Group	Specify a user group for applying the configuration restore settings profile. Each user group can be configured with different configuration restore settings profiles.
+Add	Click it to create a new profile.
Edit	Click it to modify, change the selected profile.
Delete	Click it to delete the selected profile.

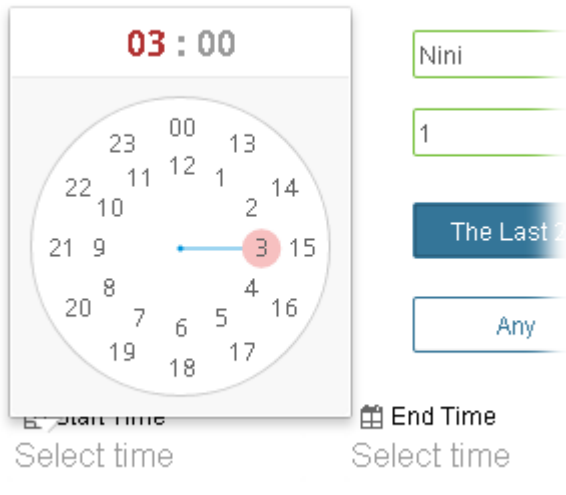
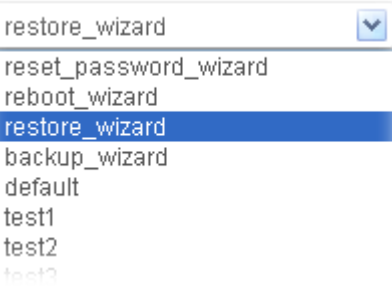
The following setting page appears when +Add is clicked.

The screenshot shows the 'Restore Settings Profile' configuration form. It includes a 'User Group' dropdown set to 'RootGroup'. The form has two tabs: 'Apply to Devices' and 'Restore Settings Profile'. The 'Restore Settings Profile' tab is active and contains the following fields:

- Name:** A text input field containing 'Monday' with a green checkmark to its right.
- Time Interval:** A set of three buttons: 'Any' (selected), 'Specify a Time', and 'Schedule Profile'.
- Specify Start Date:** A toggle switch that is currently turned off.
- Start date:** A text input field containing '2017-02-27'.

At the bottom right of the form are 'Cancel' and 'Save' buttons.

Available settings are listed as follows:

Item	Description
User Group	Specify a user group for applying the restore settings profile. Each user group can be configured with different restore settings profiles.
Name	Type a name of the restore setting profile.
Restore Time	Set a time interval for executing the backup work for networks and devices. <ul style="list-style-type: none"> ● Now ● Scheduled ● Schedule Profile
Any	Specify Start Date - Click it to enable the time setting. Start date - Click it to pop up a calendar to choose a date as the starting date.
Scheduled	<p>Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date - Click it to enable the time setting. Date - Click it to pop up a calendar to choose a date as the starting date.</p>
Schedule Profile	<p>Trigger Profile - Choosing a trigger profile from the drop down list. In which, VigorACS offers default schedule profile.</p> 

7.3 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.



Info

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.

Name	File Path	Schedule	Device Count	Status	Result	Action
3881	./kay/SharedFirmware/V2862 3.8.8.1 STD/v2862_3881_STD.all	13:00-14:00	1	Complete	Success:1 Fail:0	Edit Delete
389RC2	./kay/SharedFirmware/V2862 3.8.9 RC2/v2862_std_001.all	13:20-14:00	1	Complete	Success:1 Fail:0	Edit Delete

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 New Job	Click it to create a new job profile.
Delete All Complete Jobs	Click it to delete all profile.
Edit	Click it to edit / modify the settings for the selected profile.
Delete	Click it to delete the selected profile.

The following setting page appears when +Add is clicked.

Maintenance > Firmware Upgrade

Firmware Upgrade Job Settings

Name ✓

File Path ✓

Upgrade Time

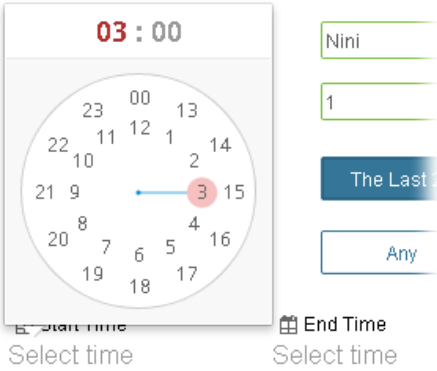
Start Time **End Time**

Date

Device to Upgrade

Name	Model Name	Firmware Version	Modem Version
Root Network(214)			
VPN Test(213)			
<input type="checkbox"/> Vigor2132Fvn	Vigor2132Fvn	3.7.9.1_RC1	No DSL

Available settings are listed as follows:

Item	Description
Name	Type a name of the job profile.
File Path	Available file paths from the computer's server will be displayed in this field. They will be different depending on the user groups.
Upgrade Time	Set a time interval for executing the backup work for networks and devices. <ul style="list-style-type: none"> ● Now ● Scheduled
Scheduled	<p>Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>The screenshot shows a circular clock interface with the time 03:00. The hour hand is on 3 and the minute hand is on 00. To the right of the clock are two input fields: the first contains 'Nini' and the second contains '1'. Below the clock are two buttons labeled 'The Last' and 'Any'. At the bottom, there are labels for 'Start time' and 'End Time' with 'Select time' text below them.</p>

	Date - Click it to pop up a calendar to choose a date as the starting date.
Device to Upgrade	Select one device or more devices to apply such firmware upgrade provision. Model Name - Display the model name for identification. 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.

7.4 Device Reboot

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

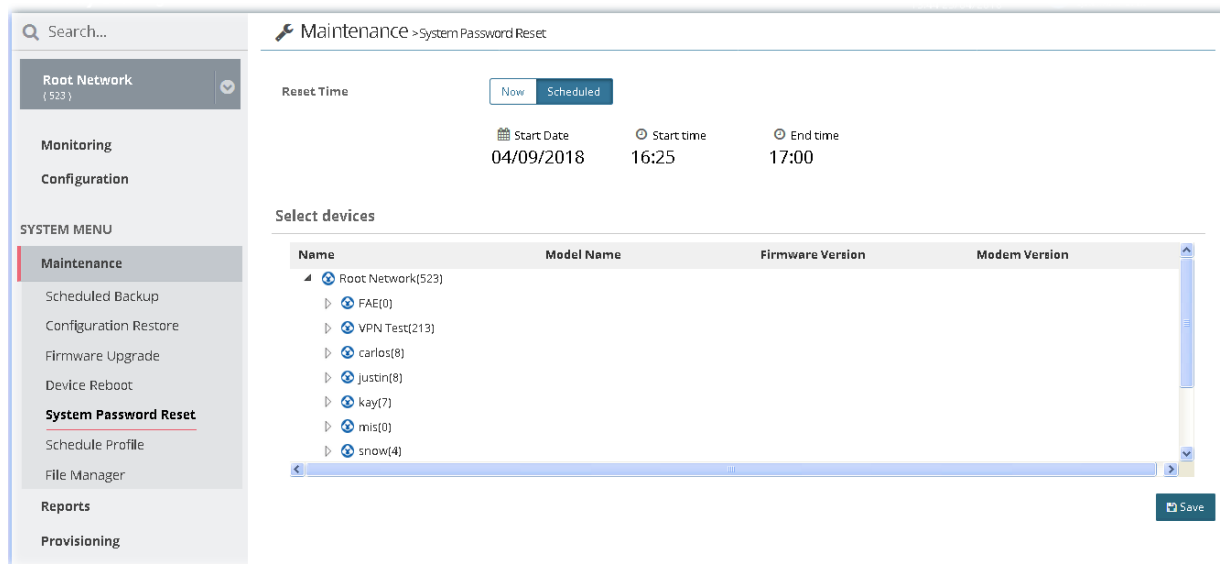
These parameters are explained as follows:

Item	Description
Period(days)	Determine the frequency for the CPE reboot by VigorACS. The default value is 1 day.
Reboot Time	<p>Now - Reboot the selected device(s) immediately.</p> <p>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.</p> <ul style="list-style-type: none"> ● Start day - Use the drop down calendar to specify the day you want to start the operation. ● 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.
Select devices	Choose the device that you want to do device reboot.

Save	Save the current settings.
------	----------------------------

7.5 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	<p>Now - Reset the password for the selected device(s) immediately.</p> <p>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.</p> <ul style="list-style-type: none"> ● Start day - Use the drop down calendar to specify the day you want to start the operation. ● 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.
Select devices	Choose the device that you want to do device reset.
Save	Save the current settings.

7.6 Schedule Profile

Schedule profiles can be set to apply to devices managed by VigorACS 2. 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 2.

The screenshot shows the 'Maintenance > Schedule Profile' page. On the left is a navigation menu with categories like Monitoring, Configuration, SYSTEM MENU, Maintenance (selected), Reports, Provisioning, Network Management, and System. The main content area features a 'User Group' dropdown set to 'RootGroup' and a '+ Add' button. Below is a table with the following data:

Name	Start Day	End Day	Start Time	End Time	Action
reset_password_wizard	2017-04-27		07:08	07:13	Edit Delete
reboot_wizard	2017-06-20		08:21	20:11	Edit Delete
restore_wizard	2016-12-14		05:12	05:17	Edit Delete
backup_wizard	2016-12-07		03:05	03:25	Edit Delete
default	2016-10-08	2016-10-09	00:00	00:00	Edit Delete
test1	2017-04-19	2017-04-11	00:00		Edit Delete
test2					Edit Delete
test3					Edit Delete
test4					Edit Delete
test5					Edit Delete

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 it to create a new schedule profile.
Edit	Click it to modify, change the selected profile.
Delete	Click it to delete the selected profile.

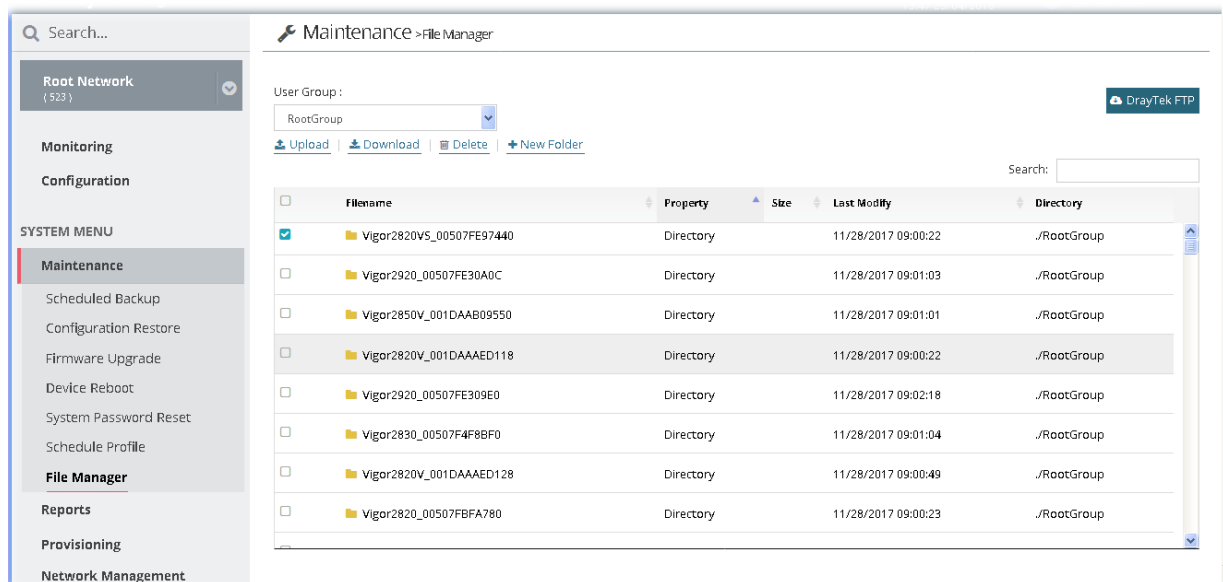
The following setting page appears when +Add is clicked.

Available settings are listed as follows:

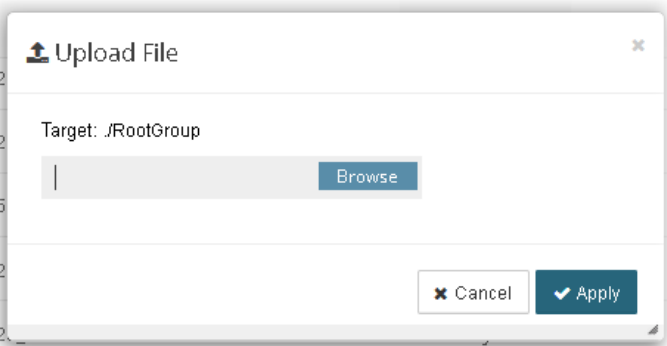
Item	Description
Profile Name	Type a name of the schedule profile.
Day Type	VigorACS 2 will perform the job for the selected CPE (s) according to the schedule set here. Any - When CPE meets settings configured in FWUpgradeFailInterval, the job (e.g., upgrade) for the CPE will be performed. Schedule - 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.
End Day	Use the drop down calendar to specify the day you want to end the operation.
Check End Day	Click it to check 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.
Time Type	Any - When CPE meets settings configured in FWUpgradeFailInterval, the job (e.g., upgrade) for the CPE will be performed. 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.

7.7 File Manager

Firmware driver for CPE device can be managed or classified with different folders.

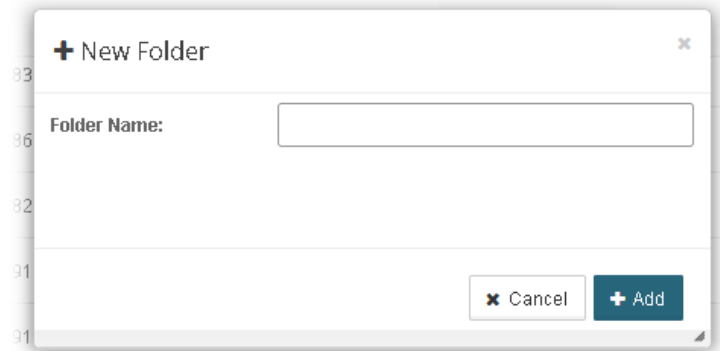


These parameters are explained as follows:

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 it to upload the file to VigorACS 2 server. 
Download	Download a driver (*.all, *.rst and etc.) related to CPE device from VigorACS 2 server.
Delete	Click it to delete the selected profile.

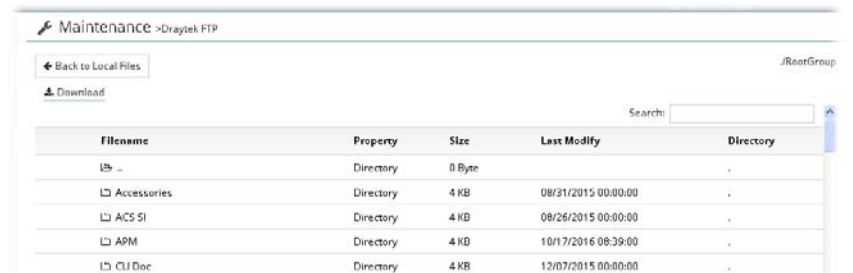
+New Folder

Create folders for files classification/management.



DrayTek FTP

After clicking the link, the following page will appear for you to download file from DrayTek FTP directly.



Chapter 8 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.

8.1 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.



Info


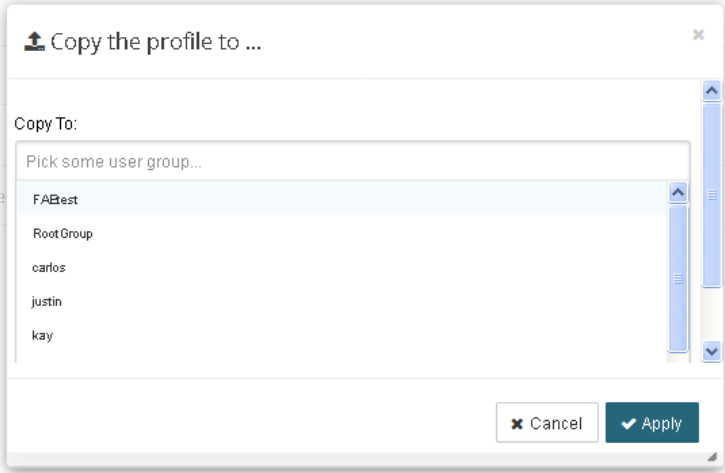
It is suitable and convenient when there are several CPE (with the same model) devices required to be configured with the same settings and values.

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

Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action
Empty	Web UI View		No	0		Edit Delete Copy To View Log
vpn_IPsec	Web UI View	General	No	2	2018/04/13 11:00:33 AM	Edit Delete Copy To View Log
vpn_change server IP	Web UI View	General	No	3	2018/05/28 01:52:40 PM	Edit Delete Copy To View Log
ping_from_wan	Web UI View	General	No	5	2018/04/18 09:37:56 AM	Edit Delete Copy To View Log
VPN	Web UI View	General	No	0	2018/08/29 11:52:13 AM	Edit Delete Copy To View Log
Login_Root	Web UI View	General	Yes	7	2018/10/05 12:27:46 PM	Edit Delete Copy To View Log
disable	Web UI View	General	Yes	1	2018/10/08 10:05:46 AM	Edit Delete Copy To View Log

These parameters are explained as follows:

Item	Description
+Add	Click it to create a new provision profile.
+Import XML	Click it to import an existed provision profile.

	
Profile Name	Display the name of the profile.
Model	Display the model name of the device.
Always Keep	Yes - Such profile is kept always. No - Such profile is not kept always.
Revision	Display the time for last modification.
Last Modification At	Display the time and date of the last modification of the provision.
Action	<p>Edit - Click it to configure settings for the selected profile.</p> <p>Delete - Click it to delete the profile.</p> <p>Copy To - If the administrator wants to apply the provision to certain user group, such action shall be used.</p>  <p>View Log - Click it to review detailed information for the selected profile.</p>

The screenshot shows the 'Provisioning > Global Parameters' page. On the left, under 'Profile Information', the following details are listed: Profile ID: 1, Profile Name: Empty, Model: General, Always Keep: No, Revision: 198, and Last Modified: 2017/05/05 05:37:45 PM. On the right, under 'Result Overview', there is a donut chart labeled 'Status' with a legend for 'Not yet applied' (blue), 'Failed' (orange), and 'Complete' (green). Below the chart is a table with the following data:

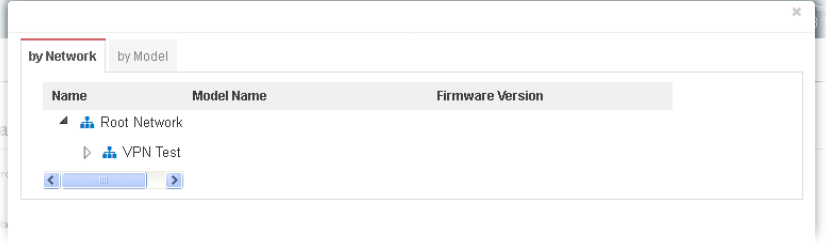
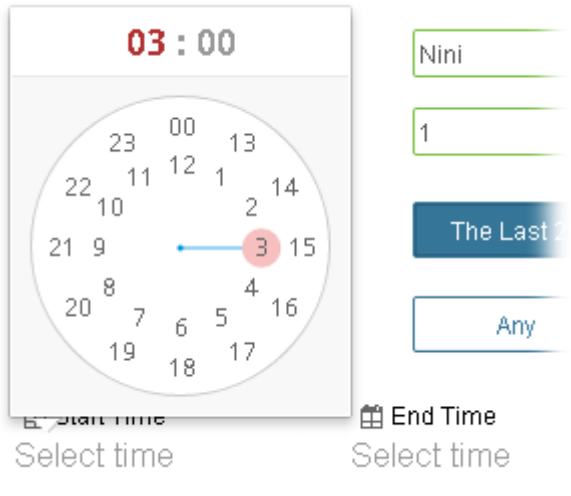
Device ID	Device Name	MAC Address	Network (ID)	Result	Status
114	2860ac_00507F000050	00507F000050	Root Network (2)	0 %	Not yet applied.
115	123123	00507F000051	Root Network (2)	0 %	Not yet applied.
120	2860ac_00507F00004F	00507F00004F	Root Network (2)	0 %	Not yet applied.
121	2860ac_00507F000054	00507F000054	Root Network (2)	0 %	Not yet applied.

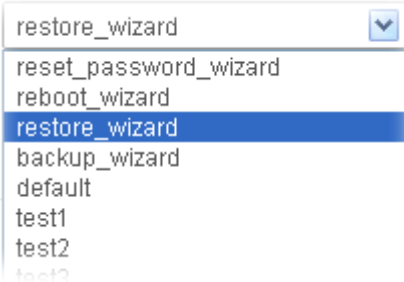
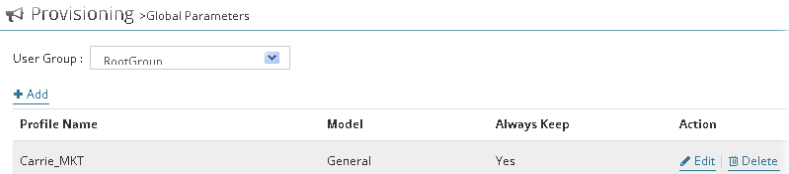
The following setting page appears when +Add is clicked.

The screenshot shows the 'Add a Profile' configuration page. It includes a note: 'Note: After applying the parameters, ACS will check the CPE responses and ask the CPE to reboot if needed.' The configuration options are: Profile Name (text input), Always Keep (toggle switch, currently off), Reboot after Provisioning (toggle switch, currently on), and Provisioning Time (radio buttons for 'Now', 'Scheduled', and 'Schedule Profile', with 'Now' selected). At the bottom right, there are 'Cancel' and 'Add' buttons.

Available settings are listed as follows:

Item	Description
Create Profile by	
Profile Name	It is available when Sampling from an Online Device / Creating a New Parameter List is specified on "Create Profile by". Type a name for the parameter profile.

Select Device	<p>It is available when Sampling from an Online Device is specified on "Create Profile by" .</p> 
Select XML file	<p>It is available when Sampling from an XML file is specified on "Create Profile by" .</p>
Always Keep	<p>Some ISPs do not wish CPE client changing the parameters of CPE device, therefore make the profile being kept is required.</p>
Reboot after provisioning	<p>Enable it to reboot the CPE after the provisioning is applied by certain CPE.</p>
Provisioning Time	<p>Set a time interval for executing the backup work for networks and devices.</p> <ul style="list-style-type: none"> ● Now ● Scheduled ● Schedule Profile
Scheduled	<p>Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date - Click it to enable the time setting. Start date - Click it to pop up a calendar to choose a date as the starting date.</p>

<p>Schedule Profile</p>	<p>Trigger Profile - Choose a trigger profile from the drop down list. In which, VigorACS offers default schedule profile.</p> 
<p>Cancel</p>	<p>Discard current settings and restore the default settings.</p>
<p>Add</p>	<p>Save and create the new profile.</p> 

Primary View

Global parameters (including Profile Setting, WAN, Multi-PVC, LAN, NAT, Object Settings, QoS, Firewall, System, VoIP, Routing, Wireless and Applications) for each provision profile can be seen and configured in Primary View.

Provisioning > Global Parameters

User Group:

[+ Add](#) | [Import XML](#)

Profile Name	Model	Always Keep	Revision	Last Modification At	Action
Empty	General	No	198	2017/05/05 05:37:45 PM	Edit Delete View Log
root_group_always_keep	General	Yes	558	2017/07/14 11:20:16 AM	Edit Delete View Log
globalparameter_test	General	No	320	2017/06/09 03:52:31 PM	Edit Delete View Log
Manoj	General	No	18	0001/01/01 12:00:00 AM	Edit Delete View Log
Stefan	General	No	2	2017/05/08 04:20:10 PM	Edit Delete View Log
mamie	General	No	2	0001/01/01 12:00:00 AM	Edit Delete View Log
Carrie_MKT	General	Yes	0	0001/01/01 12:00:00 AM	Edit Delete View Log

Click the Edit link for one of the created profile to get the primary view of the selected provision profile.

Provisioning > Global Parameters

Profile : Carrie_MKT

[Primary View](#) | [Parameter List](#)

Profile Setting

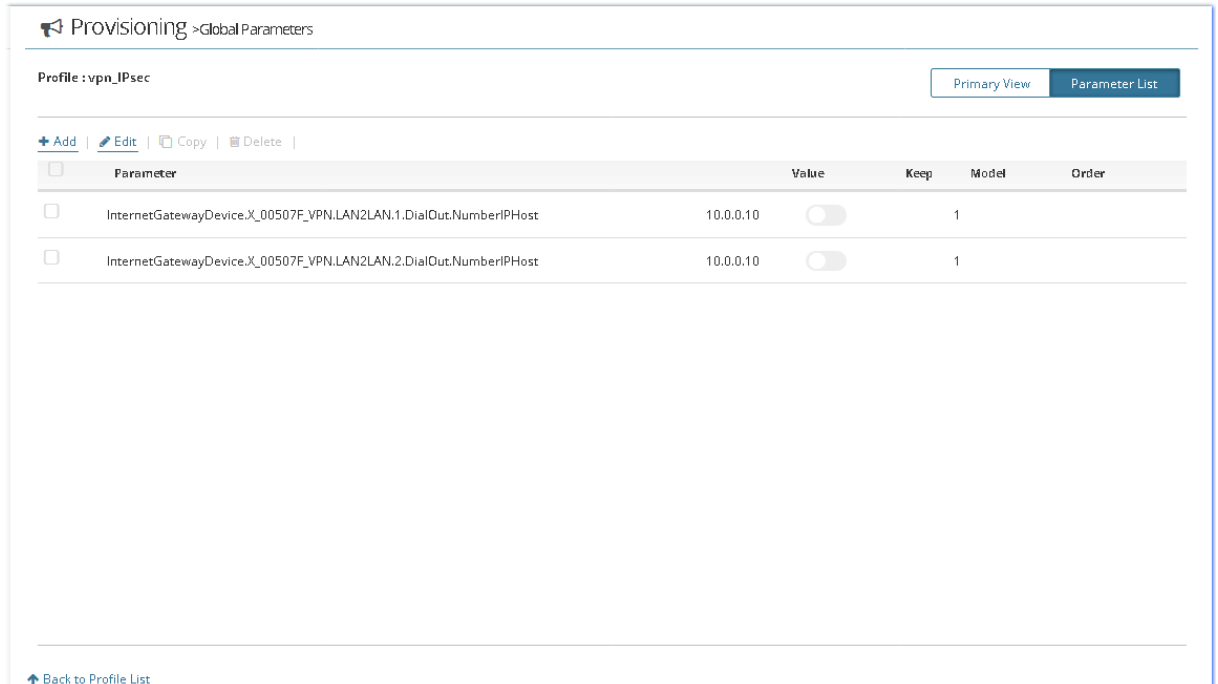
Select the parameters to be set

- WAN
- Multi-PVC
- LAN
- NAT
- Object Settings
- QoS
- Firewall
- System
- ...

[Back to Profile List](#)

Parameter List

This page displays an overview of settings configured in Primary View. Also, it allows the administrator to set different parameters with specific format.



Available settings are listed as follows:

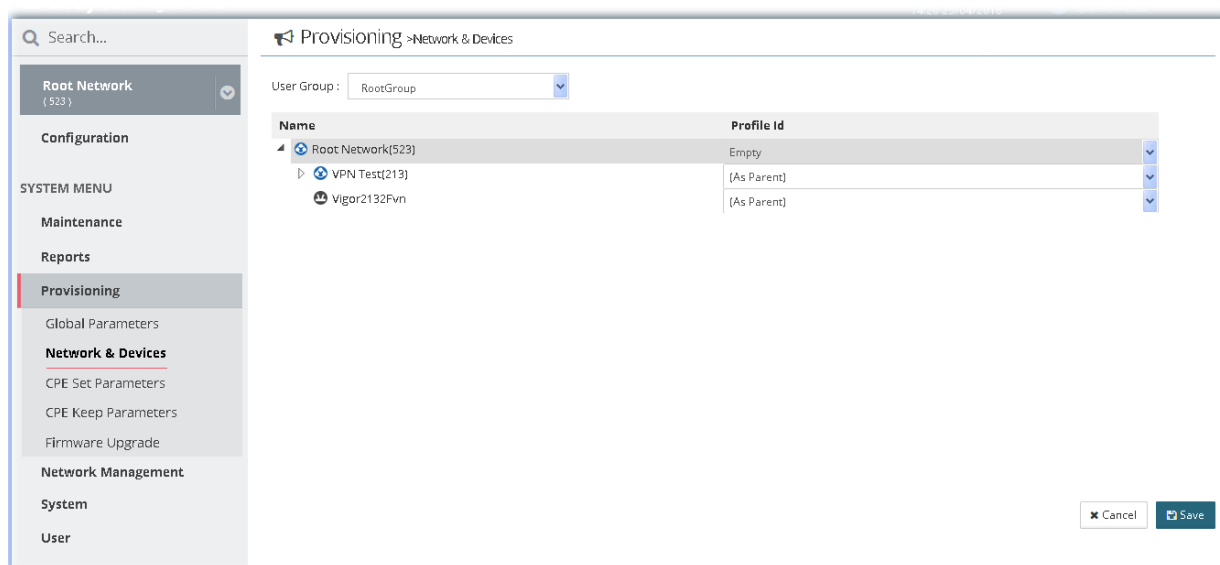
Item	Description
Add / Edit / Copy / Delete	<p>Add - Click it to create a new parameter.</p> <p>Edit - Modify the existed parameters for making modification.</p> <p>Copy - Duplicate the same settings for the selected parameter.</p> <p>Delete - Remove a selected parameter.</p>
Parameter	<p>After clicking Add/ Edit, type the script for the parameter you want in this field. For example, you would like to set the priority of the WAN1 interface, just type "InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.Priority". If you have no idea in typing the correct text, refer to the section "How to Modify Global Parameters for a Provision Profile?" for more detailed information.</p>
Value	<p>After clicking Add/ Edit, the number / text shall be typed according to the content of the parameters. If you have no idea in typing the</p>

	correct text, refer to the section “How to Modify Global Parameters for a Provision Profile?” for more detailed information.
Keep	Display if such parameter will be kept or not. Refer to the section “How to Modify Global Parameters for a Provision Profile?” for more detailed information.
Model	Display the model which applied with such provision.
Order	Display the priority of the parameter. After clicking Add/ Edit, you can change the priority of each parameter.
Back to Profile List	Return to the Profile List page.

8.2 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 Parameters) to be applied in such selected CPE/AP. (As Parent)- Use the same setting as the previous layer.

8.3 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.



Info

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.

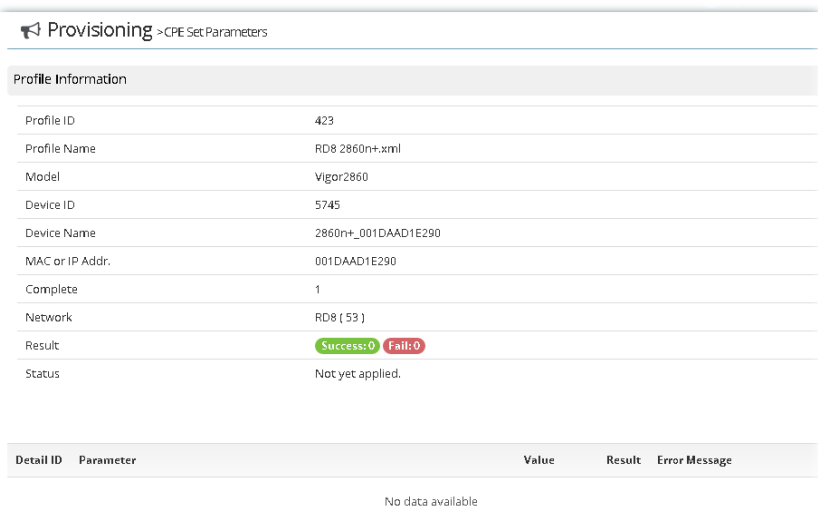
However, Global Parameters is suitable and convenient when there are several CPE (with the same model) devices required to be configured with the **same** settings and values.

Open Provisioning>>CPE Set Parameters, the profile list will be shown as follow:

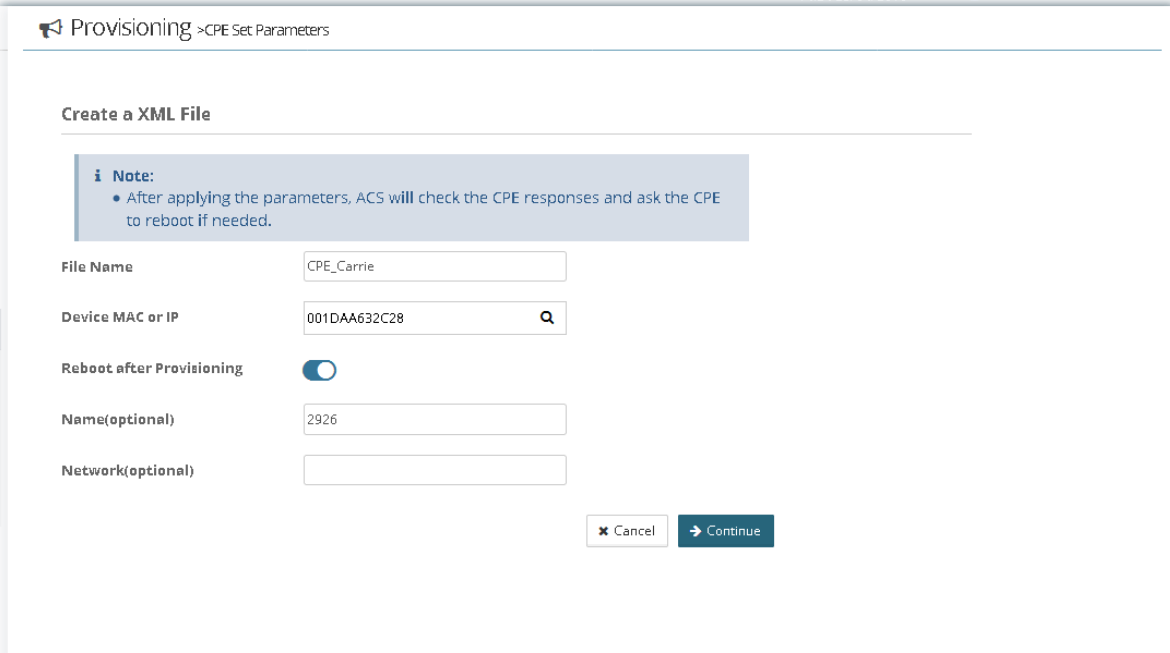
Id	Profile Name	Complete	Action
11	Carlos.xml	0	Edit Delete View Log

These parameters are explained as follows:

Item	Description
+Add	Click it to create a file saved with the file format of XML.

Action	<p>Edit - Click it to configure settings for the selected profile.</p> <p>Delete - Click it to delete the profile.</p> <p>View Log - Click it to review detailed information for the selected profile.</p> 
---------------	--

The following setting page appears when +Add is clicked.

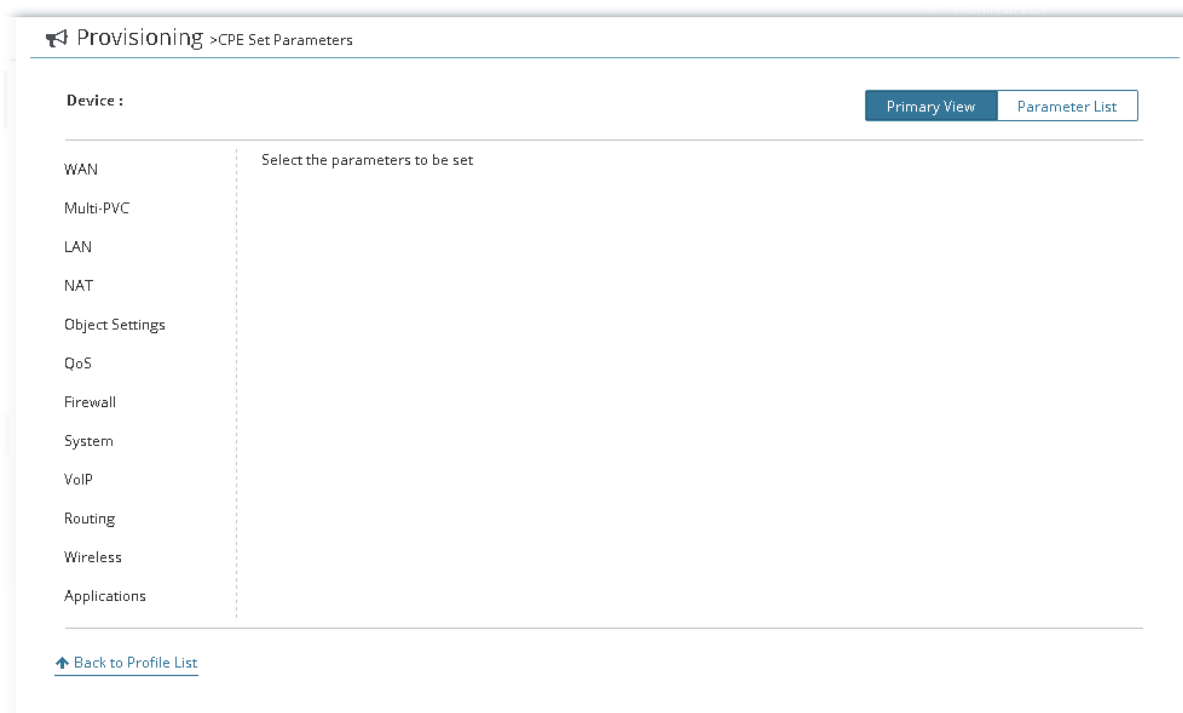


Available settings are listed as follows:

Item	Description
File Name	Type a name for the parameter profile.
Device MAC or IP	Type MAC address or IP address. After typing the address, VigorACS 2 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 settings.
Continue	Click it to get into next setting page.

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

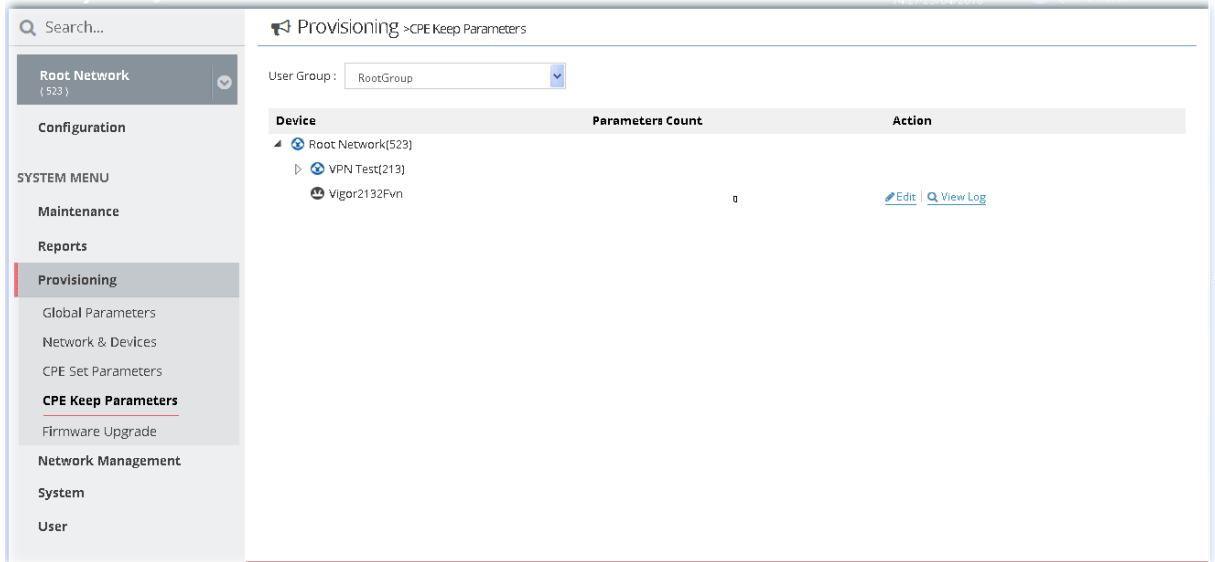


Available settings are listed as follows:

Item	Description
Device	Display the name of the device which will be applied with the parameters configured in this page.
Primary View	Parameters (including WAN, Multi-PVC, LAN, NAT, Object Settings, QoS, Firewall, System, VoIP, Routing, Wireless and Applications) ready for each CPE provision profile can be seen and configured in this page. 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 typing 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.

8.4 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	<p>Click it to open the configuration page.</p>

8.5 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.



Info

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.

8.5.1 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.

Name	Status	Model	FW Version	FW File	Schedule	Start Date	Action
BX2000	Disabled	VigorBX 2000	3.8.1.6_RC8	./RootGroup/SharedFirmware/vbx2k_3816RC8.all	14:00-14:30	2017-07-28	Edit Delete
sample	Disabled	Vigor2700 Series	3.1.1.1_RC6	v2k7v_a_3.1.1.1_RC6.all	Now	N/A	Edit Delete
V2860	Enabled	Vigor2860*	3.8.9_RC3_STD	./RootGroup/SharedFirmware/V2860 3.8.9 RC3/V2860_001.all	Now	N/A	Edit Delete
V2925	Enabled	Vigor2925*	3.8.9_RC3	./RootGroup/SharedFirmware/V2925 3.8.9 RC3/V2925_001.all	Now	N/A	Edit Delete

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 it to create a new job profile.
Edit	Click it to modify, change the selected profile.
Delete	Click it to delete the selected profile.

The following setting page appears when +Add is clicked.

Provisioning > Firmware Upgrade

Firmware Upgrade Job Settings

Name: ✓

Job Type: Normal Auth Key Check

Model: ▼

Note:

- Type full model name, e.g. Vigor2860Ln, or use wildcard for the whole series, e.g. Vigor2860* for Vigor2860 series.

Modem Version: ▼

Firmware Version: ▼

File Path: ✓

Status: Disable Enable

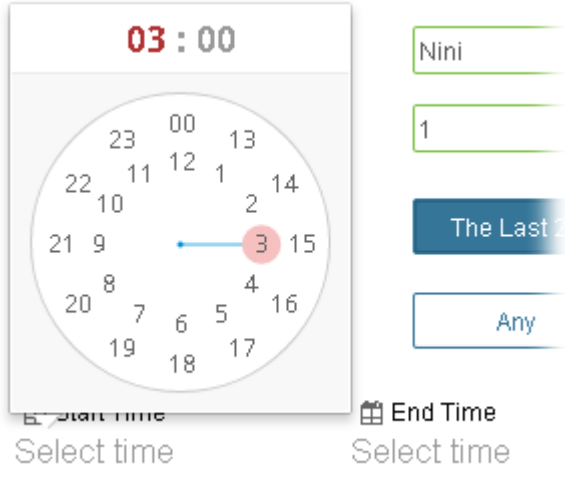
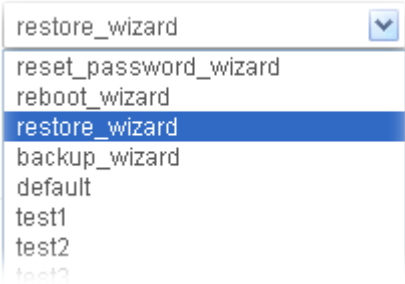
Upgrade Time: Now Scheduled Schedule Profile

Apply to Network

Name	Model Name	Firmware Version	Modem Version	Apply
Root Network(214)				NO ▼
└─ VPN Test(213)				▼

Available settings are listed as follows:

Item	Description
Name	Type a name of the job profile.
Job Type	<p>Normal - VigorACS 2 performs firmware upgrade without using any authentication key.</p> <p>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 2. That is, VigorACS 2 will verify all of the Vigor devices via authentication key issued by DrayTek to ensure the network security.</p>
Model	Choose a model for firmware upgrade.
Modem Version	<p>Available versions from VigorACS 2 database will be displayed in this field.</p> <p>Choose the correct modem version of the device, e.g., Annex A, Annex B and etc.</p> <p>Note: Before performing firmware upgrade for the CPE, VigorACS 2 will check if the received model name, modem firmware version, and software version match with the information recorded in VigorACS 2 server or not. If you type "*" in this field, the modem version will not be regarded as a comparison condition in the process of firmware upgrade. It will be ignored.</p>

Firmware Version	Available versions from VigorACS 2 database will be displayed in this field. Type the firmware version of the device.
File Path	Available file paths from the computer's server will be displayed in this field. They will be different depending on the user groups.
Status	Disable - Firmware upgrade is not allowed for such job profile. Enable - Firmware upgrade is allowed for such job profile.
Upgrade Time	Set a time interval for executing the backup work for networks and devices. <ul style="list-style-type: none"> ● Now ● Scheduled ● Schedule Profile
Scheduled	<p>Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date - Click it to enable the time setting. Date - Click it to pop up a calendar to choose a date as the starting date.</p>
Schedule Profile	<p>Trigger Profile - Choosing a trigger profile from the drop down list. In which, VigorACS 2 offers default schedule profile.</p> 
Apply to Network	It is available when Normal is selected as Job Type. Model Name - Display the model name for identification. Firmware Version - Display the firmware version that the model used currently. Apply - Click YES to select the device. Firmware upgrade will be executed for the models with YES selected.

For Auth Key Check	<p>It is available when Auth Key Check is selected as Job Type.</p> <p>In general, newest released firmware for DrayTek device contains "Auth Key". Therefore, the network administrator shall determine which CPE device required to execute firmware upgrade for owing the "Auth Key".</p> <p>This area is used to specify which CPE device required to execute firmware upgrade for having Auth Key.</p> <p>Model Name - Display the model name for identification.</p> <p>Firmware Version - Display the firmware version that the model used currently.</p> <p>Apply - If the device does not have Auth key, choose YES to carry out firmware upgrade for that device automatically when it tries to communicate with VigorACS 2. If the device has Auth key, choose NO for it is not necessary to perform firmware upgrade.</p>
Cancel	Discard current settings and return to previous page.
Save	Save the current settings and exit the page.

8.5.2 Exclude Devices

Not all the CPEs controlled by VigorACS 2 need to upgrade firmware at any time. VigorACS 2 provides excluding mechanism for the CPEs that do not need to upgrade firmware. This web page allows you to set excluded CPEs for firmware upgrade. Simply type the MAC address of the CPE on MAC address field and click **Save**. The one will be shown on the list. Next time, if you want to make firmware upgrade for the specified CPE, simple open this page and remove the item.

These parameters are explained as follows:

Item	Description
+Add	Click it to create a new profile.
Edit	Click it to modify, change the selected profile.
Delete	Click it to delete the selected profile.

To exclude devices from firmware upgrade, click **+Add** under Exclude Devices field. An input box appears as listed below. Type the MAC address of the device and click **Save**.

Exclude Devices

[+ Add](#) / [✎ Edit](#) / [🗑 Delete](#)

11:11:11:11:11:11
11:22:33:44:55:99
1357924680
22:22:22:22:22:22
55:55:55:55:55:55
11:22:33:44:55:66
<input type="text" value="11:26:38:52:89:3"/>

Now, firmware upgrade for the devices with MAC addresses listed in the table of Exclude Devices will not be executed by VigorACS.

Applications

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

1. Open SYSTEM MENU>>Provisioning and choose Global Parameters.
2. Click Add.

Provisioning >Global Parameters

User Group :

[+ Add](#)

Profile Name	Model	Always Keep	Action
Empty	General	No	Edit Delete

3. From the following window, type the profile name, choose the suitable model and enable the function of keeping the parameters

Provisioning >Global Parameters

User Group :

Add a Profile

Profile Name

Model

Always Keep

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

Provisioning >Global Parameters

User Group :

[+ Add](#)

Profile Name	Model	Always Keep	Action
Empty	General	No	Edit Delete
root_group_always_keep	General	Yes	Edit Delete
Carrie_MKT	General	Yes	Edit Delete

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

1. Open SYSTEM MENU>>Provisioning and choose Global Parameters.
2. Choose the profile (e.g., Carrie_MKT) you want to modify and click Edit.

Provisioning >Global Parameters

User Group :

[+ Add](#)

Profile Name	Model	Always Keep	Action
Empty	General	No	Edit Delete
root_group_always_keep	General	Yes	Edit Delete
Carrie_MKT	General	Yes	Edit Delete

3. The following page displays available parameters for the profile.

Provisioning >Global Parameters

Profile : Carrie_MKT Primary View Parameter List

Profile Setting

WAN

Multi-PVC

LAN

NAT

Object Settings

QoS

Firewall

System

VoIP

Routing

Wireless

Select the parameters to be set

[Back to Profile List](#)

4. Here we take WAN as an example. Click WAN>>Internet Access. A setting table will be shown as follows. Click +Add.

Provisioning >Global Parameters

Profile : Carrie_MKT Primary View Parameter List

Profile Setting

WAN

Internet Access

DSL Modem Settings

WAN IPv6

[+ Add](#)

Index	Priority	VLAN ID	Port	VLAN Tag Insertion	IP/PPP Enable	Action
No data available in table						

- Available settings will be shown as below.

Provisioning > Global Parameters

Profile : Carrie_MKT Primary View Parameter List

Profile Setting

WAN

Internet Access

DSL Modem Settings

WAN IPv6

Multi-PVC

LAN

NAT

Object Settings

QoS

Firewall

System

Index: 1

VLAN ID:

Port: WAN3

VLAN Tag Insertion:

Tag Value:

Priority: 3

Connection Mode: IP Enable PPP Enable

Static/DHCP

Addressing Type: DHCP Static

IP: 172.16.3.182

Cancel Save

- After finished the settings, click Save. WAN configuration for the CPE parameters has been created.

Provisioning > Global Parameters

Profile : Carrie_MKT Primary View Parameter List

Profile Setting

WAN

Internet Access

DSL Modem Settings

+

Index	Priority	VLAN ID	Port	VLAN Tag Insertion	IP/PPP Enable	Action
1	3		WAN3	false	IPEnable	Edit Delete

- If required, click Parameter List to have an overview of settings (e.g., WAN) configured in Primary View.

Provisioning > Global Parameters

Profile : Carrie_MKT Primary View Parameter List

[+ Add](#) [Edit](#) [Copy](#) [Delete](#)

Parameter	Value	Keep	Model	Order
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.Priority	3	<input checked="" type="checkbox"/>		0
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.EnableVLANTagInsertion	false	<input checked="" type="checkbox"/>		1
InternetGatewayDevice.X_00507F_INTERFACE_V39.WAN.1.Port	WAN3	<input checked="" type="checkbox"/>		2
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DNSServers	168.95.1.1	<input checked="" type="checkbox"/>		3
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.SubnetMask	255.255.255.0	<input checked="" type="checkbox"/>		4
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.Enable	IPEnable	<input checked="" type="checkbox"/>		5
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DefaultGateway	172.16.3.1	<input checked="" type="checkbox"/>		6
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.AddressingType	Static	<input checked="" type="checkbox"/>		7

[Back to Profile List](#)

- Click the **Edit** link in this page to modify the **Value**, **Keep status**, **Model** and **Order** if you are not satisfied with the configuration above and want to make change. After finished the changes, click **Save**.

Provisioning > Global Parameters

Profile : Carrie_MKT

Primary View Parameter List

+ Add | Edit | Copy | Delete

Parameter	Value	Keep	Model	Order
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.Priority	3	<input checked="" type="checkbox"/>	<input type="text"/>	0
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.EnableVLANTagInsertion	false	<input checked="" type="checkbox"/>	<input type="text"/>	1
InternetGatewayDevice.X_00507F_INTERFACE_V39.WAN.1.Port	W7	<input checked="" type="checkbox"/>	<input type="text"/>	2
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DNSServers	16	<input checked="" type="checkbox"/>	<input type="text"/>	3
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.SubnetMask	25	<input checked="" type="checkbox"/>	<input type="text"/>	4
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.Enable	IPE	<input checked="" type="checkbox"/>	<input type="text"/>	5
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DefaultGateway	17	<input checked="" type="checkbox"/>	<input type="text"/>	6
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.AddressingType	Sta	<input checked="" type="checkbox"/>	<input type="text"/>	7

Cancel Save



Info

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

A.3 How to Modify Provision Profile with CPE Set Parameters?

Basically, parameters to be edited in CPE Set Parameters are the same as the settings in Vigor CPE/AP device. To the administrator, CPE Set Parameters is a convenient tool which can be used to add/edit settings for the devices without accessing into the web page of Vigor CPE/AP device directly.

Here we take WAN>>Internet Access as an example.

1. Click WAN>>Internet Access. A setting table will be shown as follows.

The screenshot shows the 'Provisioning > CPE Set Parameters' interface. On the left, a sidebar menu lists 'WAN' with sub-items: 'Internet Access', 'DSL Modem Settings', 'WAN IPv6', 'Multi-PVC', and 'LAN'. 'Internet Access' is highlighted. The main area shows a table with columns: Index, Priority, VLAN ID, Port, VLAN Tag Insertion, IP/PPP Enable, and Action. The table is currently empty with the message 'No data available in table'. There are '+ Add' and 'Primary View' buttons.

2. Click +Add.
3. Available settings will be shown as below.

The screenshot shows the configuration form for a new WAN profile. The left sidebar is the same as in the previous screenshot. The main area contains a form with the following fields: Index (1), VLAN ID (empty), Port (WAN2), VLAN Tag Insertion (toggle off), Tag Value (empty), Priority (3), Connection Mode (IP Enable, PPP Enable), Static/DHCP section with Addressing Type (DHCP, Static), and IP (172.16.3.221). There are 'Cancel' and 'Save' buttons at the bottom right.

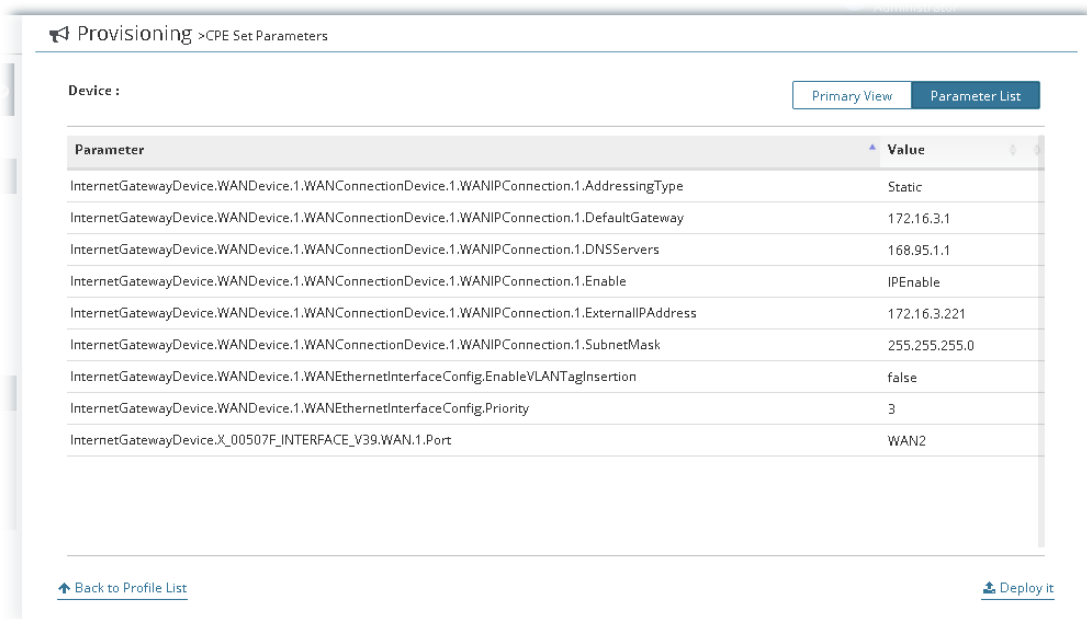
4. After finished the settings, click Save. WAN configuration for the CPE parameters has been created.

The screenshot shows the 'Provisioning > CPE Set Parameters' interface after saving. The table now contains one entry:

Index	Priority	VLAN ID	Port	VLAN Tag Insertion	IP/PPP Enable	Action
1	3		WAN2	false	IPEnable	Edit Delete

The '+ Add' button is still present, and the 'Primary View' button is active.

5. If required, click **Parameter List** to have an overview of settings (e.g., WAN) configured in Primary View. Click **Deploy it** to save the changes.



The screenshot shows the 'Provisioning > CPE Set Parameters' interface. At the top, there are two tabs: 'Primary View' and 'Parameter List', with 'Parameter List' selected. Below the tabs is a table with two columns: 'Parameter' and 'Value'. The table contains the following data:

Parameter	Value
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.AddressingType	Static
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DefaultGateway	172.16.3.1
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.DNSServers	168.95.1.1
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.Enable	IPEnable
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress	172.16.3.221
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.SubnetMask	255.255.255.0
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.EnableVLANTagInsertion	false
InternetGatewayDevice.WANDevice.1.WANEthernetInterfaceConfig.Priority	3
InternetGatewayDevice.X_00507F_INTERFACE_V39.WAN.1.Port	WAN2

At the bottom left, there is a link: [Back to Profile List](#). At the bottom right, there is a button: [Deploy it](#).



Info

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

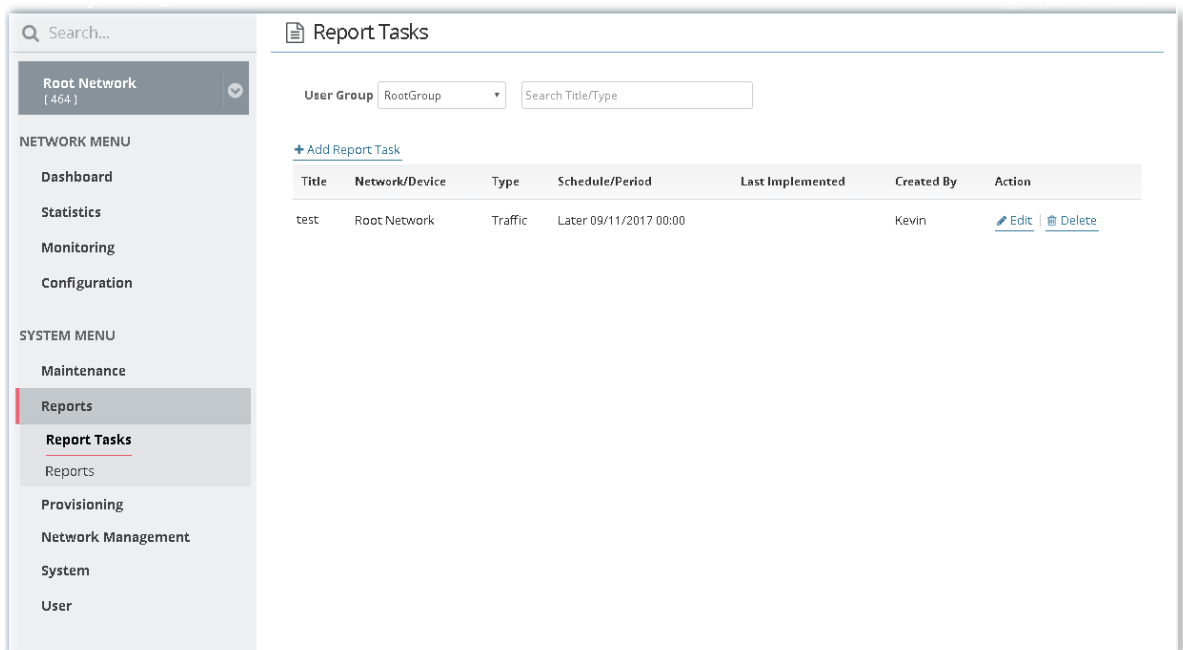
Chapter 9 Reports

VigorACS allows you to create reports with PDF files.

9.1 Report Tasks

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.

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

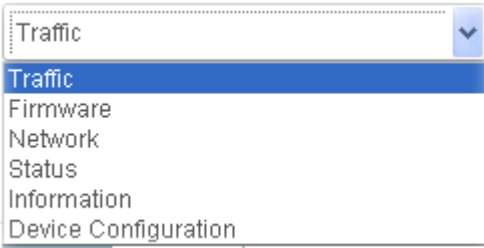


Available settings are listed as follows:

Item	Description
User Group	Use the drop down list to choose a group (e.g., RootGroup). 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 Report Task to create a new one.
+Add Report Task	Click it to create a new report task for specified CPE.
Action	Edit - Click it to modify an existing report task. Delete - Click it to remove the selected report task.

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

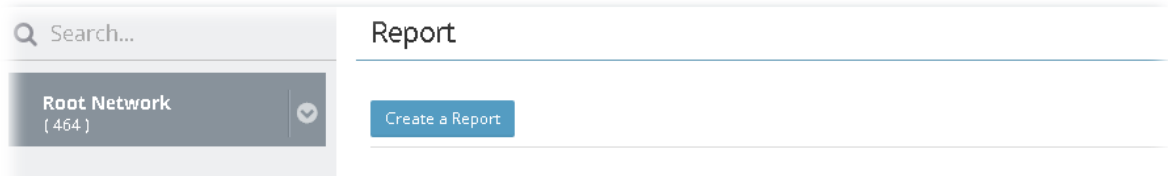
Available settings are listed as follows:

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	<p>At present, VigorACS offers five types of report, including traffic, firmware, network, status, information and device configuration.</p>  <p>Use the scroll bar to choose the type you want and select an option for that type. Select the way (statistic or graph) to show the report.</p>
File Type	<p>Such option is available when Device Configuration is selected as Report Content. Choose PDF or CSV as the file format for device configuration report.</p>

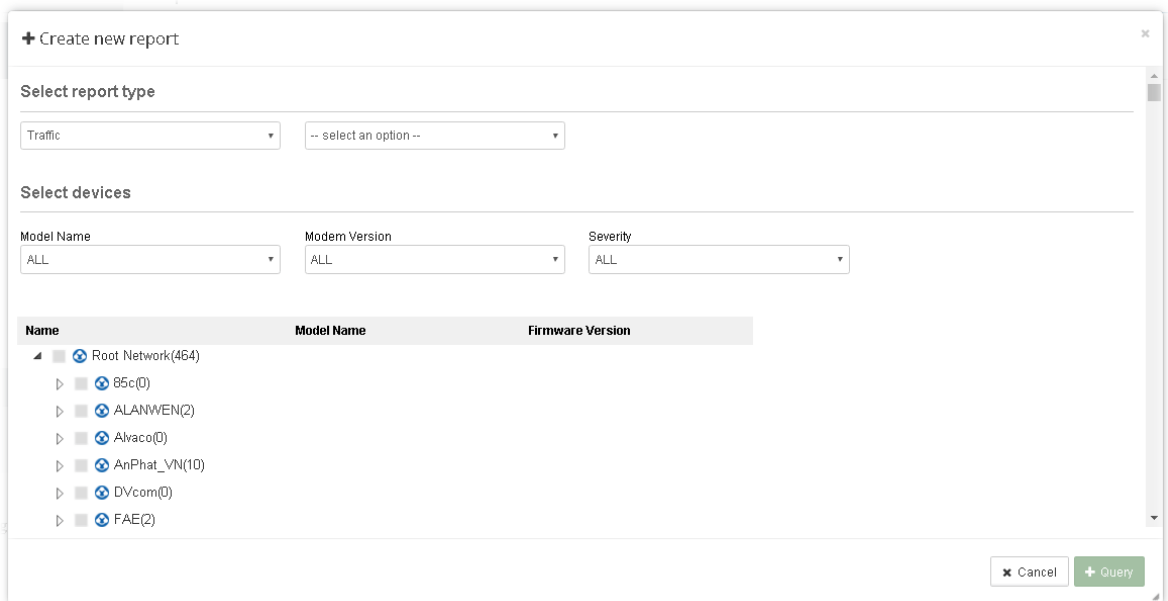
Parameter List	<p>Such option is available when Device Configuration is selected as Report Content.</p> <p>Enter the TR-069 parameter on the entry box and click +Add. Later, the report will be created with the configuration of the specified parameters listed in Parameter List.</p> <div data-bbox="671 398 1109 712"> <p>Parameter List</p> <hr/> <input type="text"/> <input type="text"/> <p>+ Add</p> </div>												
Run Report	<p>Once - The report will be made just for one time.</p> <p>Repeat - The report will be made repeatedly.</p>												
Email Subject	Specify the subject for the email.												
Email From	Enter the email address of the sender.												
Email Content	Enter the content of the email.												
Email To	<p>Enter the email address of the recipient.</p> <p>+Add recipient - If there is more than one recipient for adding, click such link to have more entry box(es) for adding more recipients.</p>												
Select devices	<p>Only the CPEs under the selected User Group (e.g., RootGroup in this case) will be shown in this field.</p> <p>Check the box to the left of the network group to select the device(s) you want to make report.</p> <div data-bbox="663 1272 1348 1624"> <p>Select devices</p> <hr/> <table border="1"> <thead> <tr> <th>Name</th> <th>Model Name</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Root Network(417)</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Other(3)</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> RDB(18)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> FAE(2)¹</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Marketing_carrie(0)</td> <td></td> </tr> </tbody> </table> </div>	Name	Model Name	<input type="checkbox"/> Root Network(417)		<input checked="" type="checkbox"/> Other(3)		<input checked="" type="checkbox"/> RDB(18)		<input type="checkbox"/> FAE(2)¹		<input type="checkbox"/> Marketing_carrie(0)	
Name	Model Name												
<input type="checkbox"/> Root Network(417)													
<input checked="" type="checkbox"/> Other(3)													
<input checked="" type="checkbox"/> RDB(18)													
<input type="checkbox"/> FAE(2)¹													
<input type="checkbox"/> Marketing_carrie(0)													
Save	Save the settings and return to previous page.												

9.2 Reports

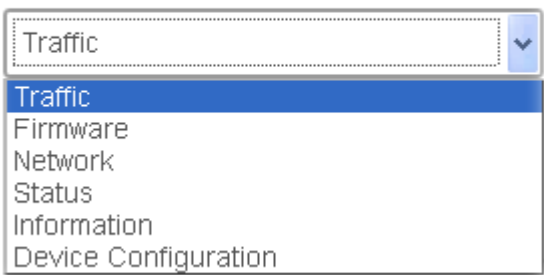
This function can print out VigorACS report based on the settings configured in this web page.




Simply click Create a Report to get the following page.



Available settings are listed as follows:

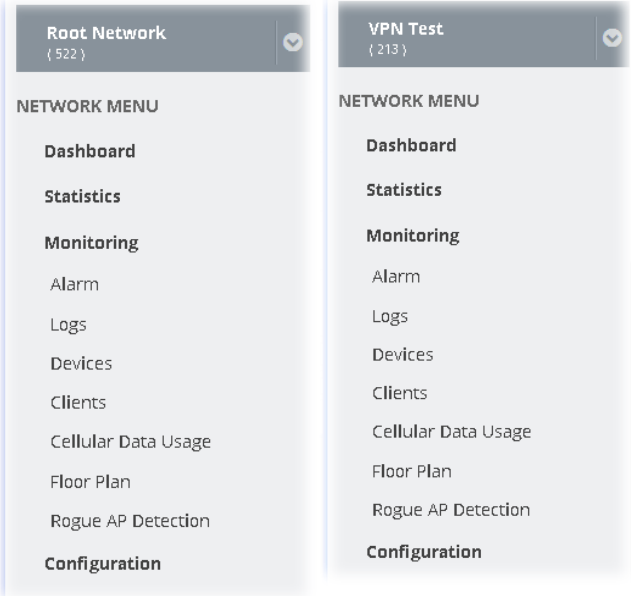
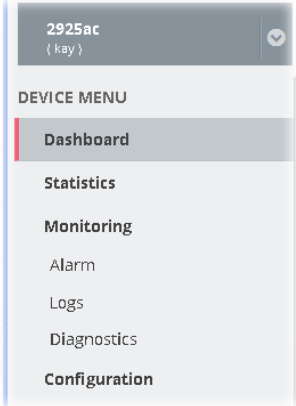
Item	Description
Select report type	<p>At present, VigorACS offers five types of report, including traffic, firmware, network, status, information and device configuration.</p> <p>Select report type</p>  <p>Use the scroll bar to choose the type you want and select an option for that type.</p>

<p>Select devices</p>	<p>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.</p> <p>Modem Version - The default is "All". However, some models do not have modem version, choose "No DSL" instead.</p> <p>Severity - Specify the severity of the selected device(s).</p>
<p>Name</p>	<p>The models displayed here depend on the conditions set in Select devices.</p>
<p>Query</p>	<p>After specifying the conditions (report type, device selection...), click Query to create a new report.</p>  <p>Create a Report - This button appears after the first report created. If required, click it to create more reports for reference.</p> <p>Report 1/ Report 2 ... - Each tab represents different reports created.</p>

Part IV NETWORK MENU for Root Network (VPN and AP Management)

Chapter 10 Monitoring for Network

Monitoring menu offers Alarm, Logs and Diagnostics for monitoring the normal and abnormal actions for CPE. Monitoring settings will vary for NETWORK MENU and DEVICE MENU.

Settings to be configured under Root Network / Group	Settings to be configured when a CPE is selected
 <p>The screenshot shows two side-by-side network menu panels. The left panel is for 'Root Network (522)' and the right is for 'VPN Test (213)'. Both panels show a 'NETWORK MENU' with the following items: Dashboard, Statistics, Monitoring, Alarm, Logs, Devices, Clients, Cellular Data Usage, Floor Plan, Rogue AP Detection, and Configuration.</p>	 <p>The screenshot shows a 'DEVICE MENU' for '2925ac (kay)'. The menu items are: Dashboard, Statistics, Monitoring, Alarm, Logs, Diagnostics, and Configuration.</p>

10.1 Alarm

Alarm message will be recorded on VigorACS 2 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.

No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type
6601	Not Ack	2017/09/13 03:45:26 PM	2860Vn+_00507F000330	00507F000330	Critical	Device Loss Connection	Device Loss Connection
6600	Not Ack	2017/09/13 03:32:14 PM	2925Ln_001DAAF00DAB	001DAAF00DAB	Critical	Device Loss Connection	Device Loss Connection
6570	Not Ack	2017/09/13 01:54:48 PM	2132Vac_001DAAD666F8	001DAAD666F8	Critical	Device Loss Connection	Device Loss Connection
6561	Not Ack	2017/09/13 12:03:37 PM	2120In+_001DAA662288	001DAA662288	Critical	Device Loss Connection	Device Loss Connection
6539	Not Ack	2017/09/13 10:50:31 AM	2050V_001DAA7D9CC0	001DAA7D9CC0	Critical	Device Loss Connection	Device Loss Connection
6529	Not Ack	2017/09/13 10:10:00 AM	2060V_001DAA625D0	001DAA625D0	Critical	Device Loss Connection	Device Loss Connection
6507	Not Ack	2017/09/13 09:00:54 AM	2960_001DAAB8B8C8	001DAAB8B8C8	Critical	Device Loss Connection	Device Loss Connection
6441	Not Ack	2017/09/13 01:17:23 AM	2860n+_001DABA6598	001DABA6598	Critical	Device Loss Connection	Device Loss Connection
6438	Not Ack	2017/09/12 11:33:45 PM	2926ac_001DAAF0FA20	001DAAF0FA20	Critical	Device Loss Connection	Device Loss Connection
6437	Not Ack	2017/09/12 11:33:43 PM	AP 902_001DAA802080	001DAA802080	Critical	Device Loss Connection	Device Loss Connection
6435	Not Ack	2017/09/12 11:33:20 PM	AP 902_001DAA3D9000	001DAA3D9000	Critical	Device Loss Connection	Device Loss Connection
6434	Not Ack	2017/09/12 11:33:20 PM	2132FVi+_001DAA8EFD00	001DAA8EFD00	Critical	Device Loss Connection	Device Loss Connection

These parameters are explained as follows:

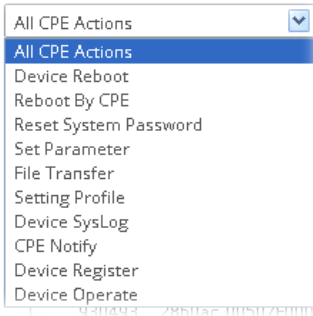
Item	Description
Alarm / History	Alarm - Display the alarm records recently. History - Display all the alarm records that have been solved and cleared.
Export All	Click this button to save alarm log as a XLS file.
Delete	Clear the alarm record which has been solved by VigorACS 2.
Delete All	Clear all of the alarm records which have been solved by VigorACS 2.
No.	Display the index number of the alarm. It is offered by VigorACS 2 automatically.
Ack Status	Display the status of the records with the type specified here (Not Ack or Acked).
MAC Address	Display the MAC address of the monitored device.
Alarm Level	Display the alarm message with the severity (e.g., Critical) specified.
Alarm Message	Display a brief explanation for the alarm sent by VigorACS 2 automatically.
Alarm Type	Display the alarm message with the type specified.

10.2 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.

ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
201795	V2860_234	3544	001DAAA8B7E8	172.17.1.234	Inform	...	2018/04/26 11:21:17 AM
201794	2820_00507FBFAA38	580	00507FBFAA38	172.17.1.82	Inform	...	2018/04/26 11:20:43 AM
201793	2960_00507FFF3900	3535	001DAA0D0246	172.17.6.63	Inform	...	2018/04/26 11:18:39 AM
201792	2820_00507FBFA6A8	513	00507FBFA6A8	172.17.1.73	Inform	...	2018/04/26 11:15:50 AM
201791	2960_00507FFF3900	3535	001DAA0D0246	172.17.6.63	Inform	...	2018/04/26 11:15:08 AM
201790	V2760	4962	001DAA822D08	172.17.6.69	Inform	...	2018/04/26 11:13:01 AM
201789	V2860_234	3544	001DAAA8B7E8	172.17.1.234	Inform	...	2018/04/26 11:12:51 AM
201788	2960_00507FFF3900	3535	001DAA0D0246	172.17.6.63	Inform	...	2018/04/26 11:11:28 AM
201787	V2760	4962	001DAA822D08	172.17.6.69	Inform	...	2018/04/26 11:10:08 AM

These parameters are explained as follows:

Item	Description
Log Type	Choose one of the conditions to display related log on this page. 
<input type="text" value="Search Device Name / IP / MAC"/>	Enter the condition for VigorACS to search and display relational information.
Export All	Click this button to save alarm log as a XLS file.
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.

10.3 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 on left side is the group to be monitored and information related to this selected network group will be shown on right side.

Simply open NETWORK MENU>>Monitoring>>Devices to get the following page.

Device	IP Address	MAC Address	Model	Network	Status	Up Time	F/W Version	Current Client	Current Traffic
2952n_001DAAE061E8	172.16.2.73	001DAAE061E8	Vigor2952n	ALANWEN	offline	0d:0h:0m:0s	r66400_beta	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0 Byte)
2960_00507FFF3900	172.16.2.69	00507FFF3900	Vigor2960	ALANWEN	offline	0d:0h:0m:0s	1.3.0_Beta	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0 Byte)
AP 910C_001DAA0FCC8C	192.168.11.3	001DAA0FCC8C	VigorAP 910C	AnPhat_VN	offline	0d:0h:0m:0s	1.2.3	0 (Local Wireless: 0)	...
AP 918C_001DAA0FD01C	192.168.11.2	001DAA0FD01C	VigorAP 910C	AnPhat_VN	offline	0d:0h:0m:0s	1.2.3	0 (Local Wireless: 0)	...
AP 919C_001DAA0FCD44	192.168.11.4	001DAA0FCD44	VigorAP 910C	AnPhat_VN	offline	0d:0h:0m:0s	1.2.3	0 (Local Wireless: 0)	...
AP 810_001DAA0F3320	192.168.11.5	001DAA0F3320	VigorAP 810	AnPhat_VN	offline	0d:10h:7m:52s	1.2.1RC1	7 (Local Wireless: 7)	...
2912_001DAA88040C	14.167.99.211	001DAA88040C	Vigor2912	AnPhat_VN	offline	0d:0h:0m:0s	3.8.4	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0 Byte)
2912_001DAA87F510	14.291.192.146	001DAA87F510	Vigor2912	AnPhat_VN	offline	0d:0h:0m:0s	3.8.4	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0 Byte)
2912_001DAA87FAE4	129.20.129.2	001DAA87FAE4	Vigor2912	AnPhat_VN	offline	0d:0h:0m:0s	3.8.4	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0 Byte)
2912Fr_001DAA8C0FDC	14.161.2.165	001DAA8C0FDC	Vigor2912Fr	AnPhat_VN	offline	0d:7h:9m:35s	3.8.4	0 (Local Wireless: 0)	374.13 KB (↑ 183.16 KB ↓ 19)

These parameters are explained as follows:

Item	Description
<input type="text" value="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. 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. Offline - This page displays information for the device which is offline currently. 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. Check All to display all of the devices; or check the name of the device to display the information related to the selected device. 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. Wireless - List only the wireless information for the CPE under the selected group.

Click the **Export** link to export information for monitored devices as “.xls” file.

10.4 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., Root Network in this case) selected on left side is the group to be monitored and information related to this selected network group will be shown on right side.

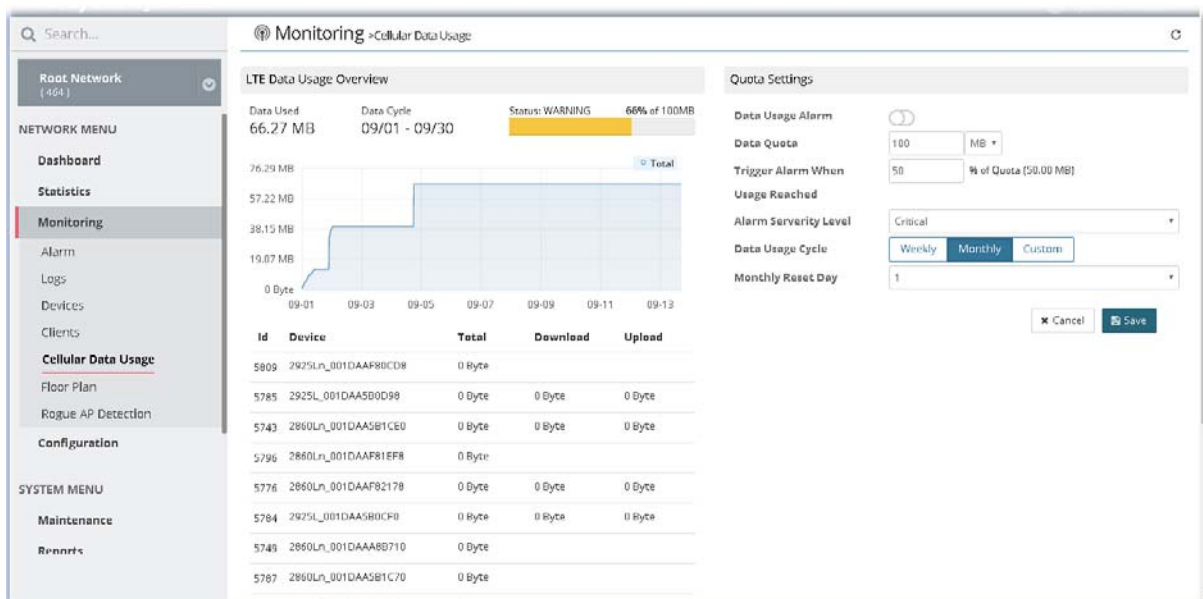
These parameters are explained as follows:

Item	Description
<p>Last 24 Hours / Last 7 Days / Last 30 Days / Custom</p>	<p>Display the clients detected within 24 hours, 7 days, 30 days or user defined days.</p>
<p>Search Device Name / IP / MAC</p>	<p>Enter the condition for VigorACS to search and display relational information.</p>
<p>Device</p>	<p>This area lists all of the devices (under the selected network group) that monitored by VigorACS.</p> <p>Check All selected to display information for all of the devices; or check the name of the device to display the information related to the selected device.</p>
<p>Type</p>	<p>Check All to display information for all of the devices (including wired and wireless devices).</p> <p>Wired - This page displays information for the device without wireless feature.</p> <p>Wireless_2.4g - This page displays information for the device with 2.4GHz wireless feature.</p> <p>Wireless_5g - This page displays information for the devices with 5GHz wireless feature.</p>
<p>SSID</p>	<p>This area lists information for CPE with wireless features monitored by VigorACS.</p> <p>Check All to display all of the devices; or check the name of the device to display the information related to the selected device.</p> <p>SSID - SSIDs for CPE with wireless features will be displayed in this</p>

drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.

10.5 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 (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:

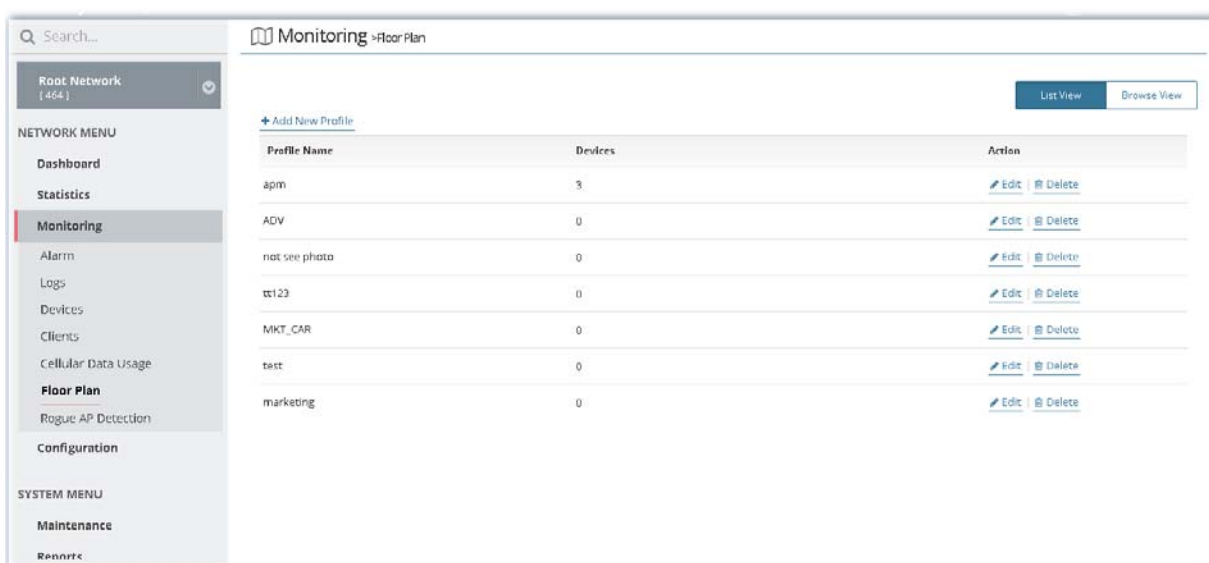
Item	Description
LTE Data Usage Overview	<p>Status - The bar chart displays the data usage in yellow, green and grey based on values defined in Quota Settings. If data usage for the LTE model exceeds the percentage of quota configured in the field of Trigger Alarm When Usage Reached in Quota Settings, 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.</p> <p>In addition, device name, throughput, downloaded data and uploaded data for each LTE can be seen on the table below this page.</p>
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	<p>Select one of the options (Weekly, Monthly, Custom) as data usage cycle.</p> <p>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.</p> <p>Cycle Starts On -When Custom is selected, specify one date as a starting point to reset the data quota for LTE model.</p> <p>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.</p> <p>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.</p>
-------------------------	---

10.6 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.

10.6.1 List View

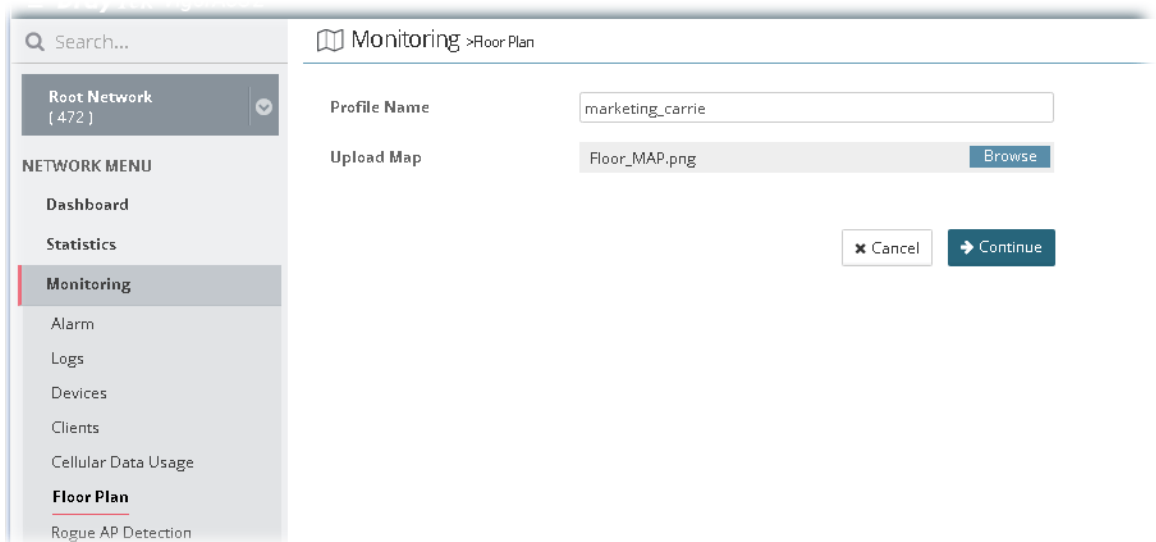


These parameters are explained as follows:

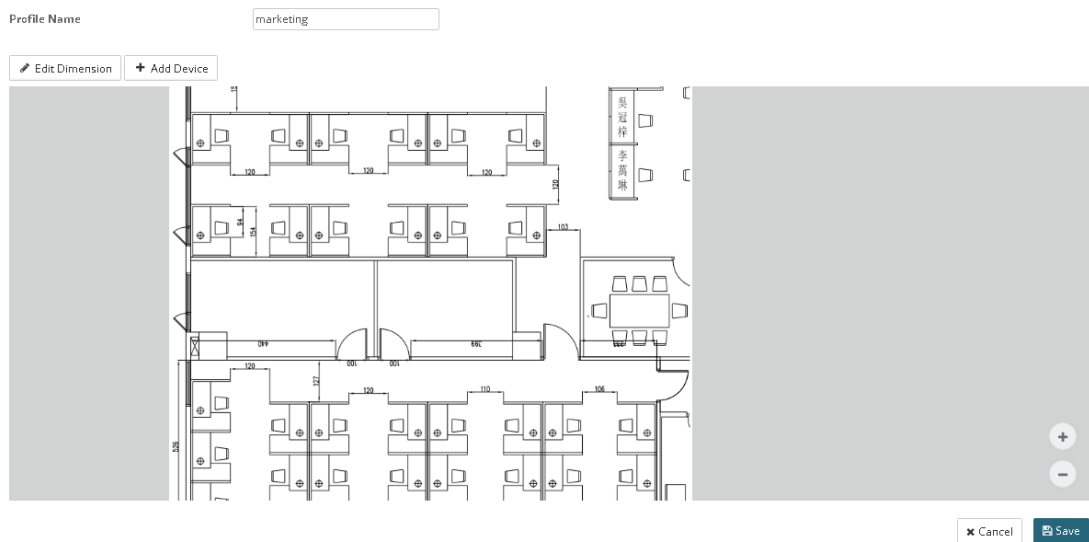
Item	Description
+Add New Profile	Create a new profile.
List View / Browse View	Display the profile with different views.

To create a new profile:

1. Click **Add New Profile**.
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**.



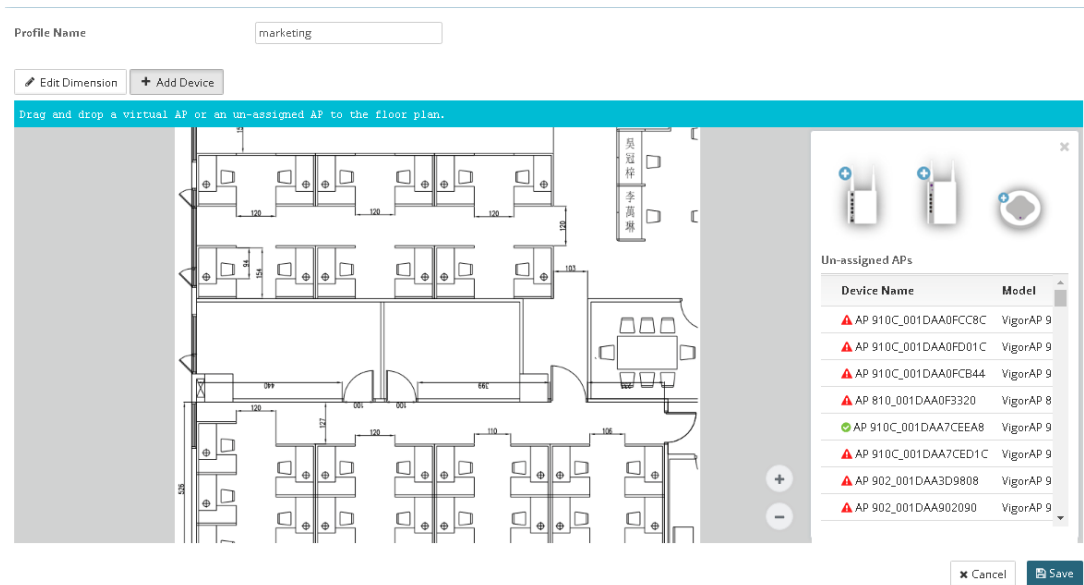
3. A floor map will be displayed on the screen.



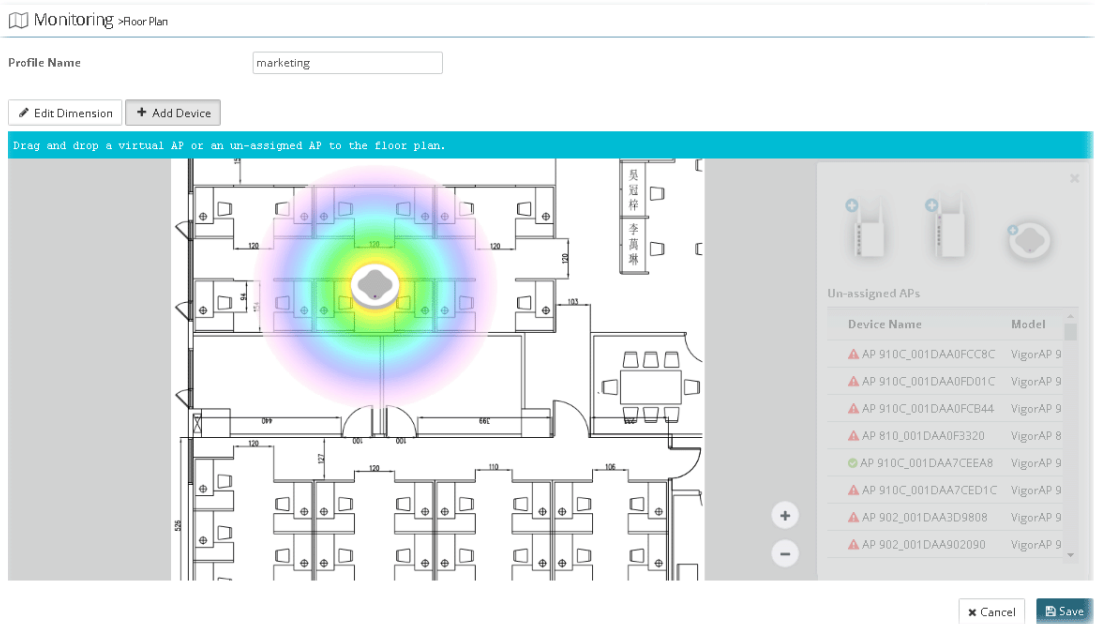
Edit Dimension - Draw a line and enter the distance of length / width of the map.

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

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



- 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.



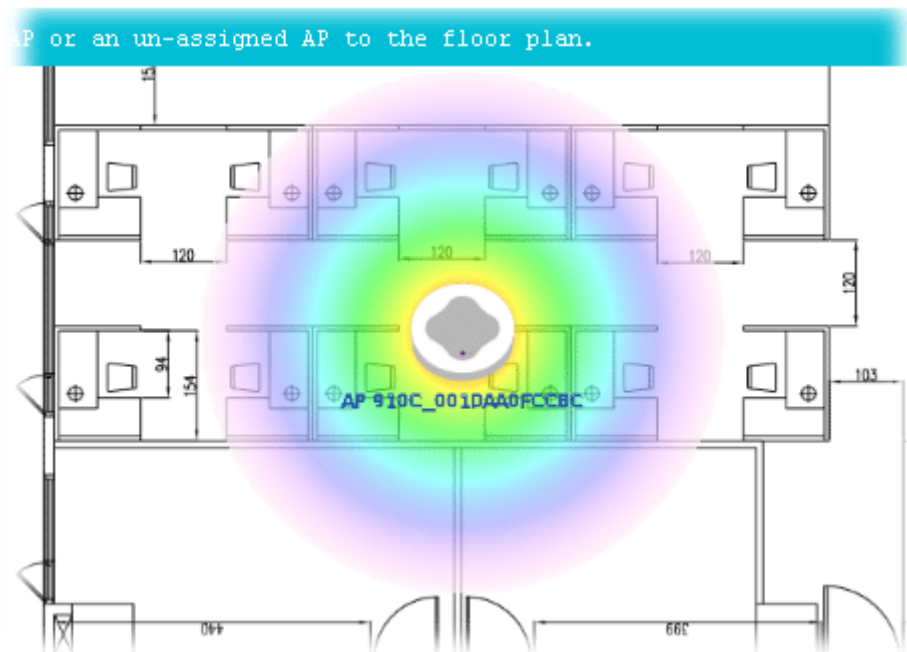
- Slightly click the AP icon on the map. Two links of **Link to an AP** and **Remove Device** will be shown on the right side.



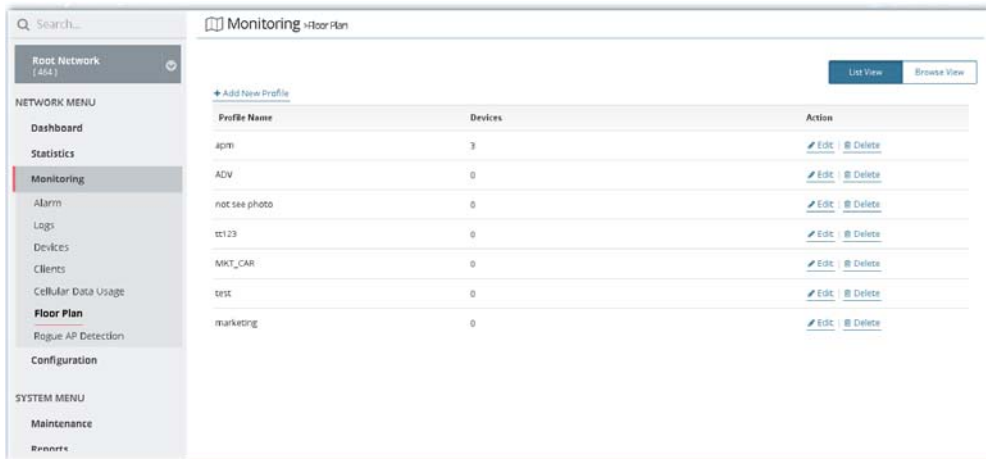
Remove Device - If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.

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.

- Click **Link to an AP** to select the AP you want. Then, the name of the VigorAP will be displayed below the icon on the map.

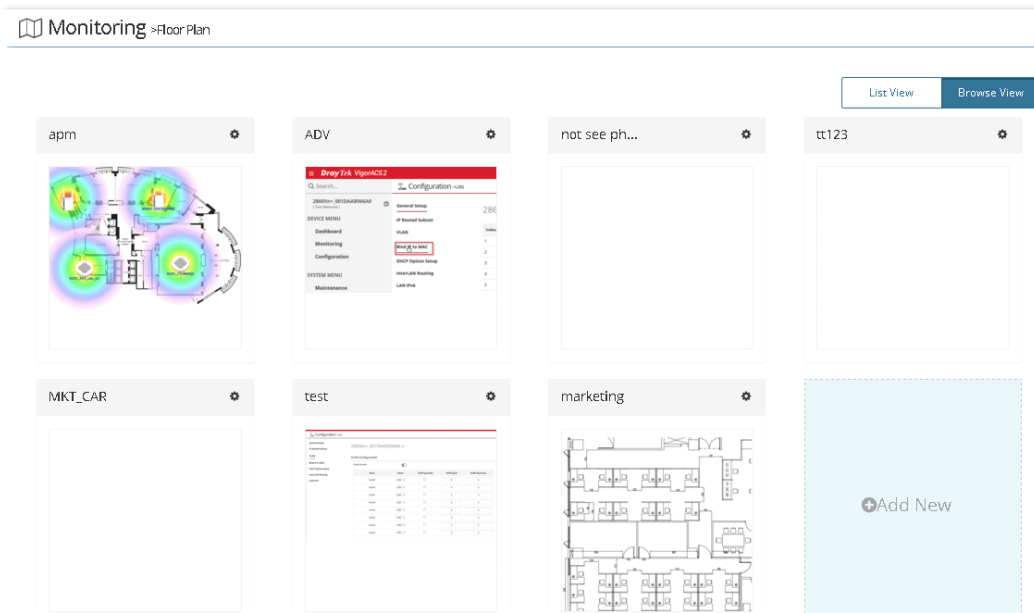


- Click **Save**. The new created profile will be shown on the page.

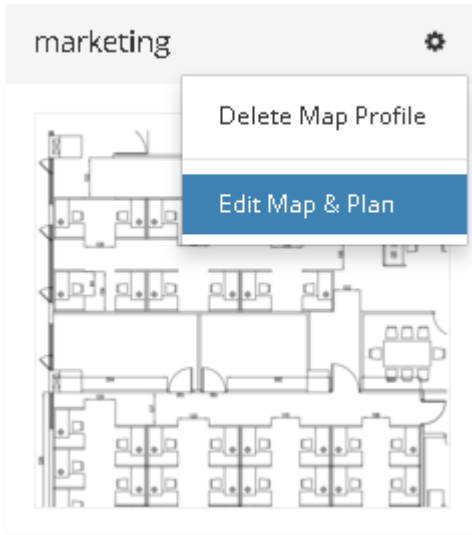


10.6.2 Browse View

This page displays all of the floor plan profiles with the map used.



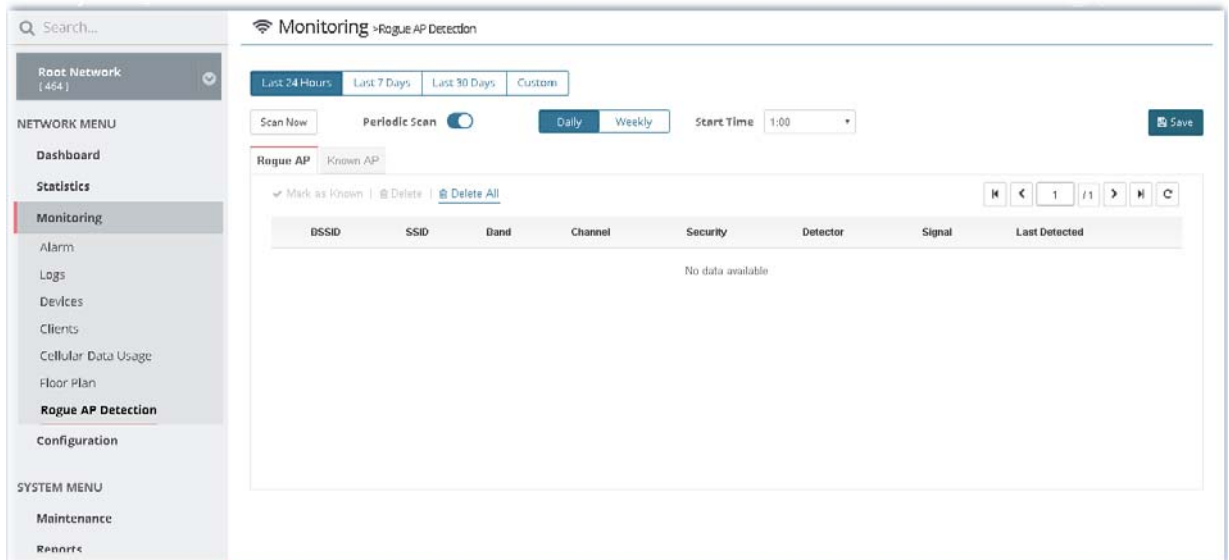
You can click **Add New** on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click **Edit Map & Plan** to perform the modification, or click **Delete Map Profile** to remove the selected floor plan profile.



10.7 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.

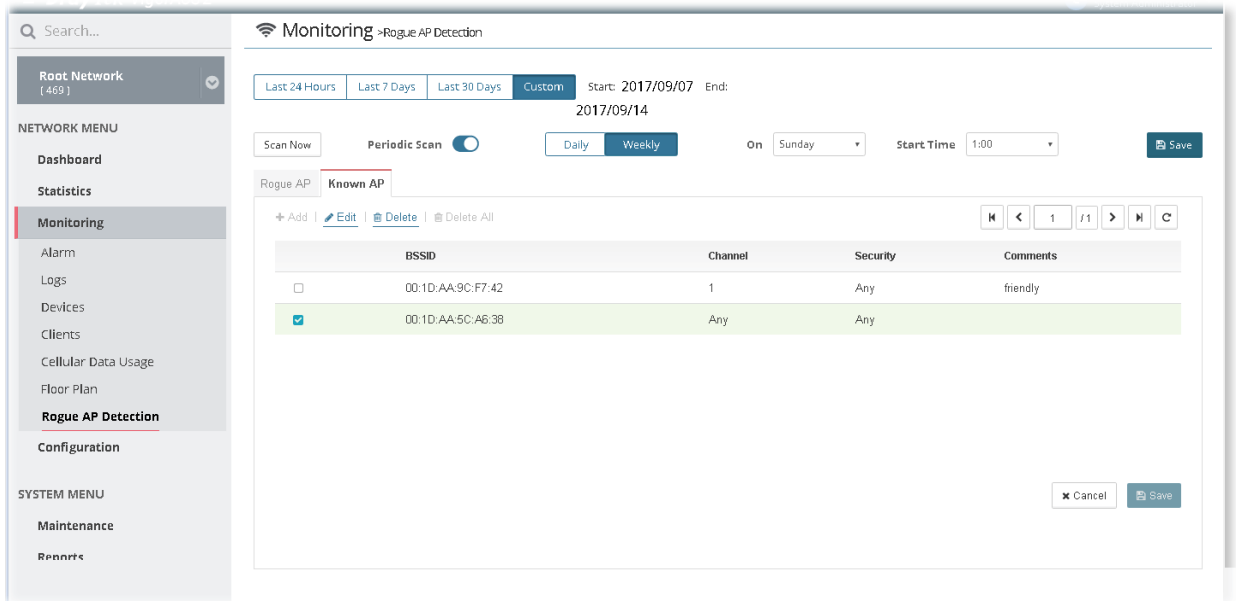
Click the **Rogue AP** tab to display the following page. All the APs detected will be treated as Rogue AP.

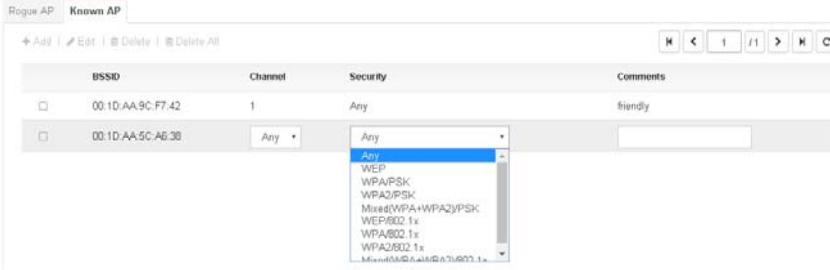


These parameters are explained as follows:

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	<p>After enabling this feature, access points will be detected periodically based on the setting configured here.</p> <p>Daily - VigorACS will detect access point on certain time every day.</p> <ul style="list-style-type: none"> ● Start Time - Specify a time point as starting time for device detection. <p>Weekly - VigorACS will detect access point on certain time every week.</p> <ul style="list-style-type: none"> ● On - Choose the day to perform device detection. ● 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.

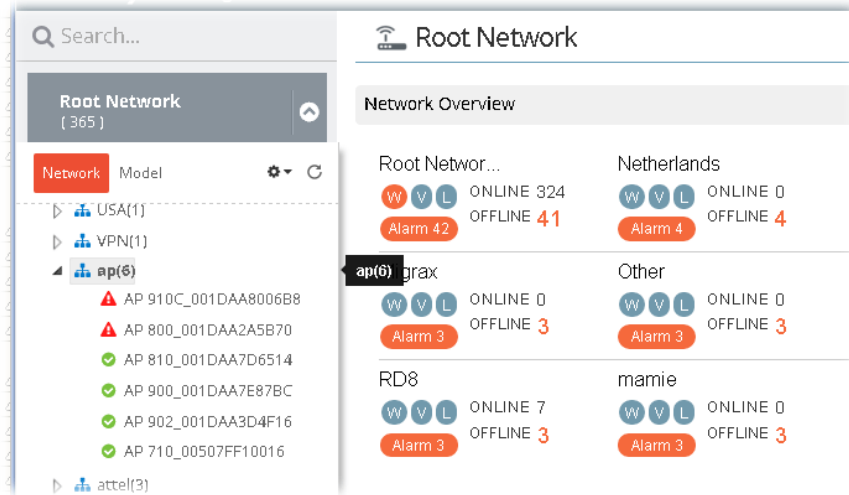


Item	Description
Add	Click it to create a new entry for entering information for access point.
Edit	<p>Change the settings for a selected access point.</p> <p>Select one of the access points. The Edit link will be available for clicking, then.</p> <p>After clicking it, channel, security and comments will be allowed to be modified with different values</p> 
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	<p>Display the channel used by the access point.</p> <p>Check the box of the selected access point and click Edit.</p>
Security	<p>Display the security mode used by the access point.</p> <p>It can be changed.</p>
Comments	<p>Display a brief explanation for the access point.</p> <p>It can be changed.</p>
Save	Save the settings.

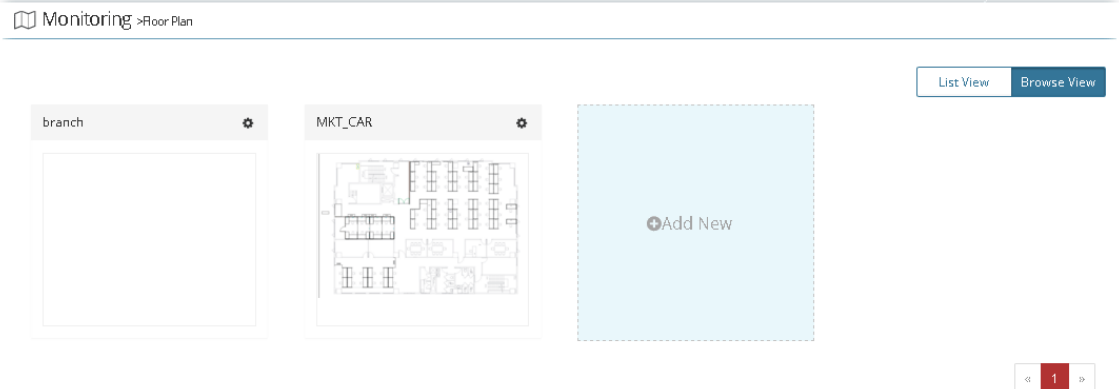
Applications

A.1 How to specify an AP device to an existed Floor Plan Profile?

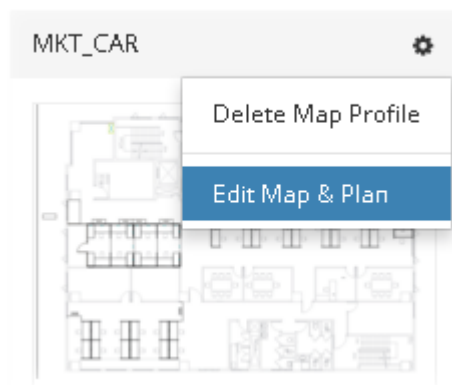
1. From the **Root Network**, locate the access point or the group with access points. In this case, we choose "ap" group.



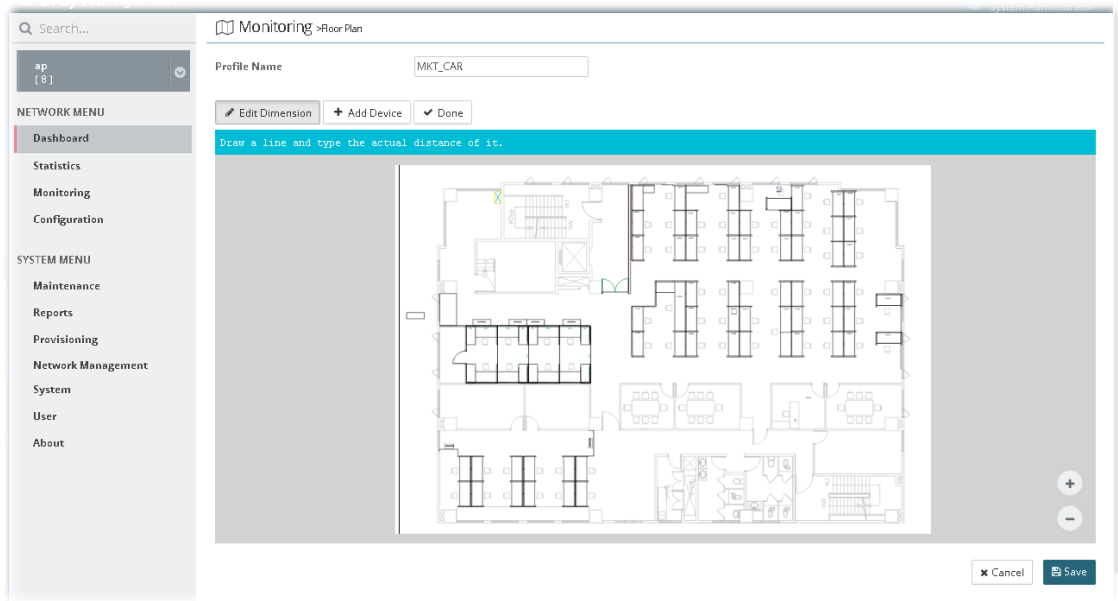
2. Open **NETWORK MENU >> Monitoring >> Floor Plan** and click **Browse View**. Choose one of the AP Map profiles. In this case, we choose "MKT_CAR" as an example.



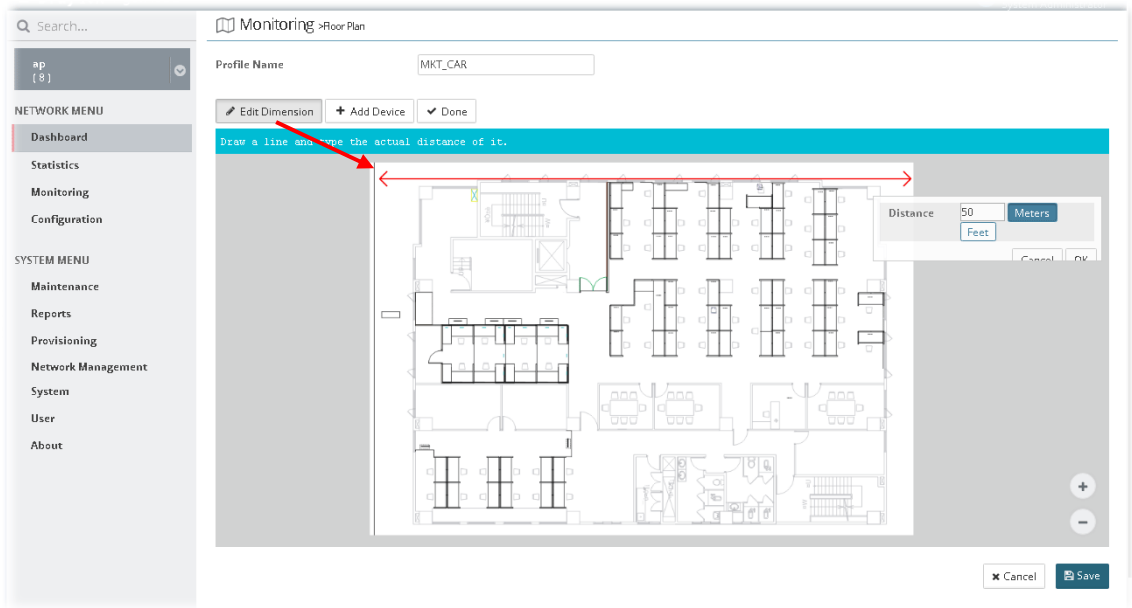
3. Click the button on the top-right to display a drop down menu. Choose **Edit Map & Plan**.



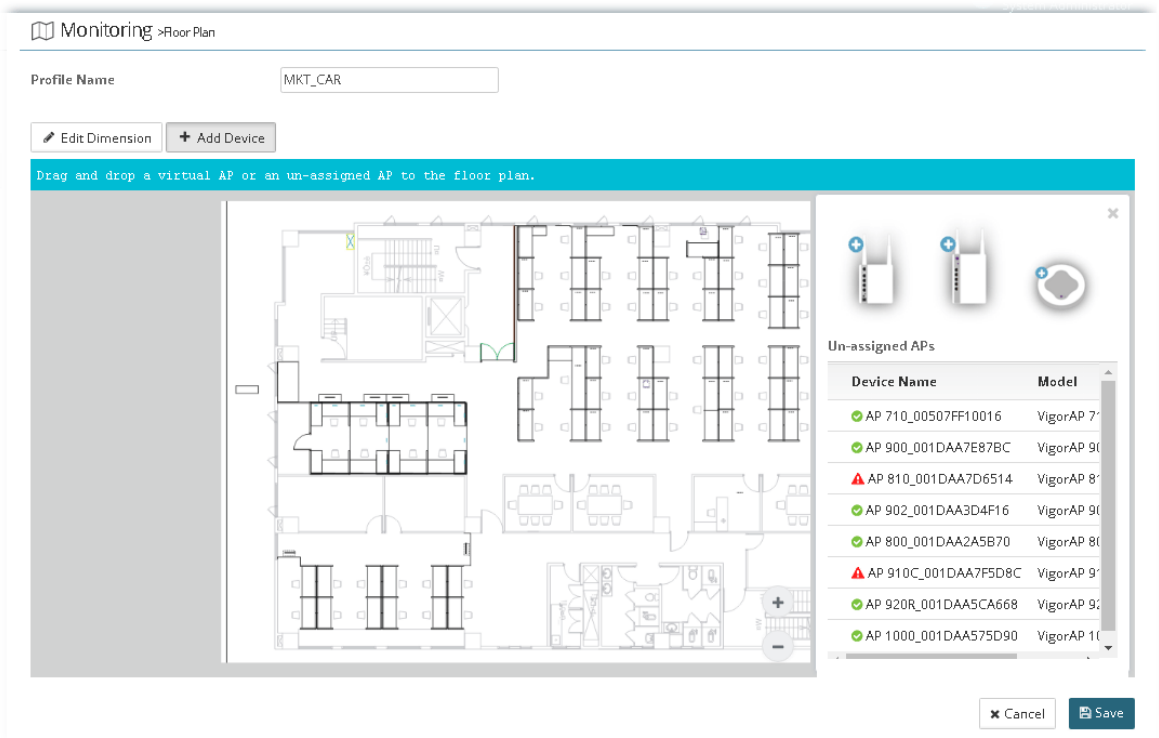
4. In the following web page, click **Edit Dimension** for setting dimension for the map.



5. Click **Edit Dimension** and drag the mouse on the map horizontally / vertically to draw a red line for width /length. Then, type the value on the pop up dialog to determine the real distance and click **OK**.



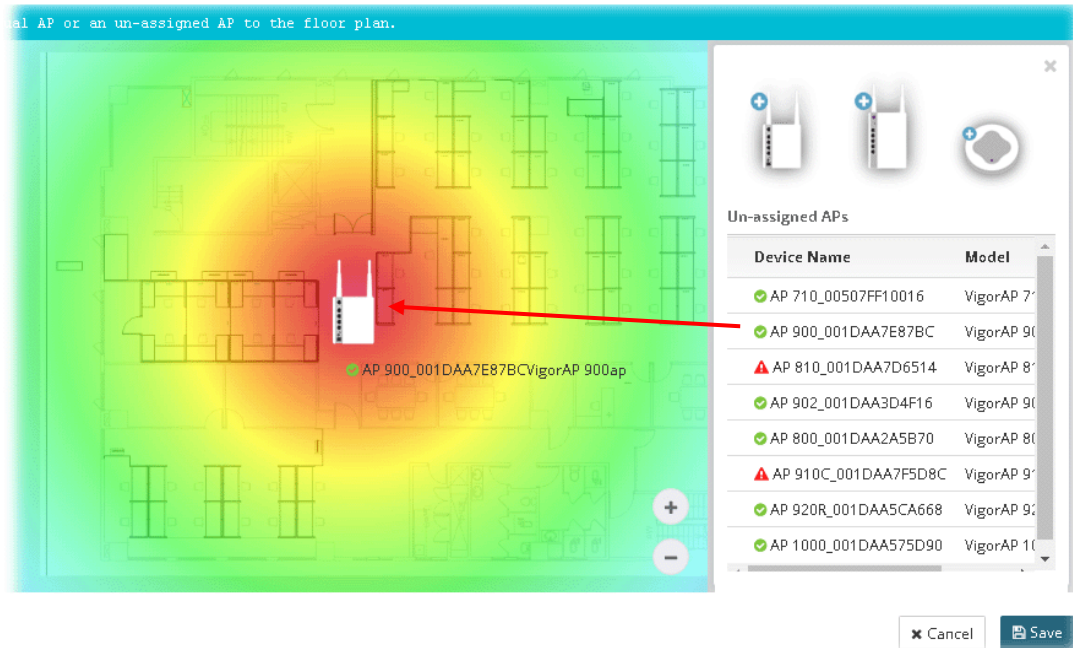
6. Click **Add Device** to display AP icons and available AP list (unassigned APs).



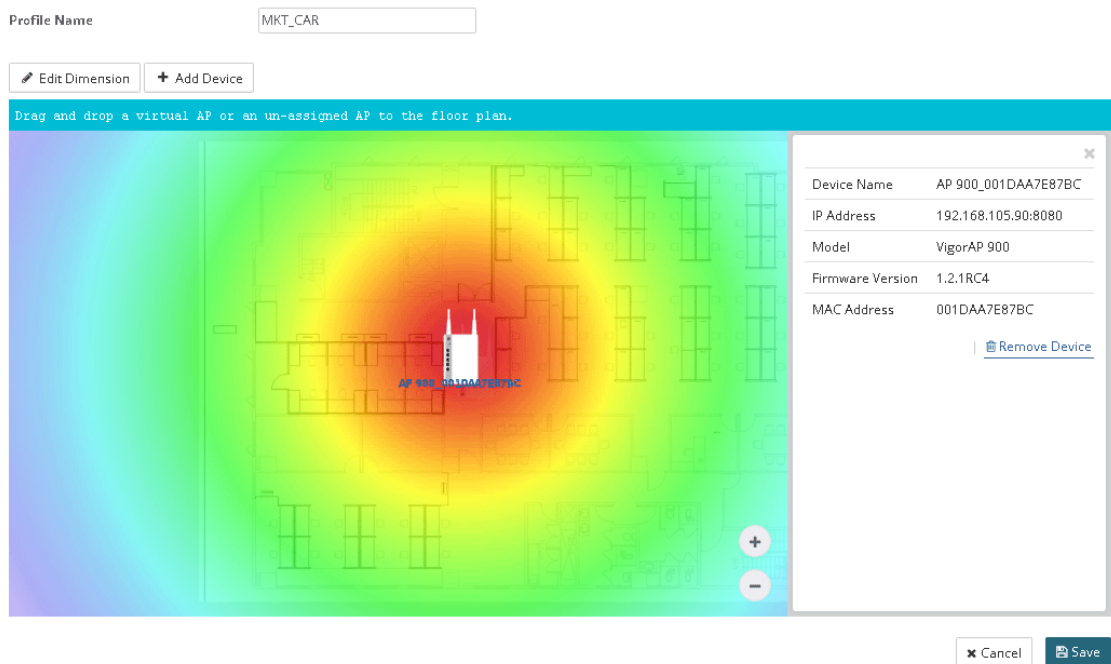
7. Drag an AP icon from right side to the point you want to place the selected AP and drop it.



8. Choose one of device names from the list of Un-assigned APs. Drag the device name to the icon on the left side.



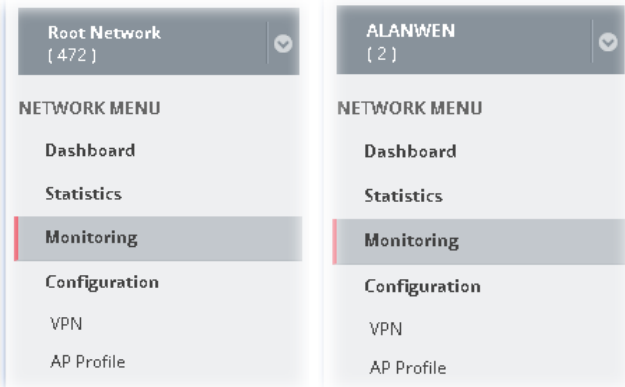
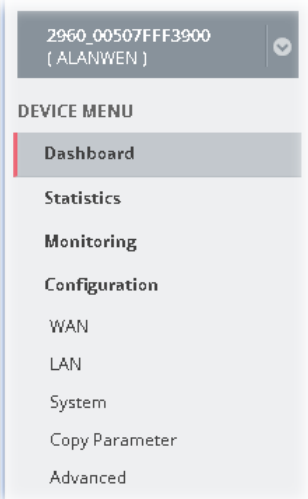
- Now, VigorAP with device name will be shown on this page. Slightly click the AP icon, brief description for such AP will be shown on the right side of this page.



- Click Save.

Chapter 11 Configuration for Network

Configuration settings will vary for NETWORK MENU and DEVICE MENU.

Settings to be configured under Root Network / Group	Settings to be configured when a CPE is selected
	

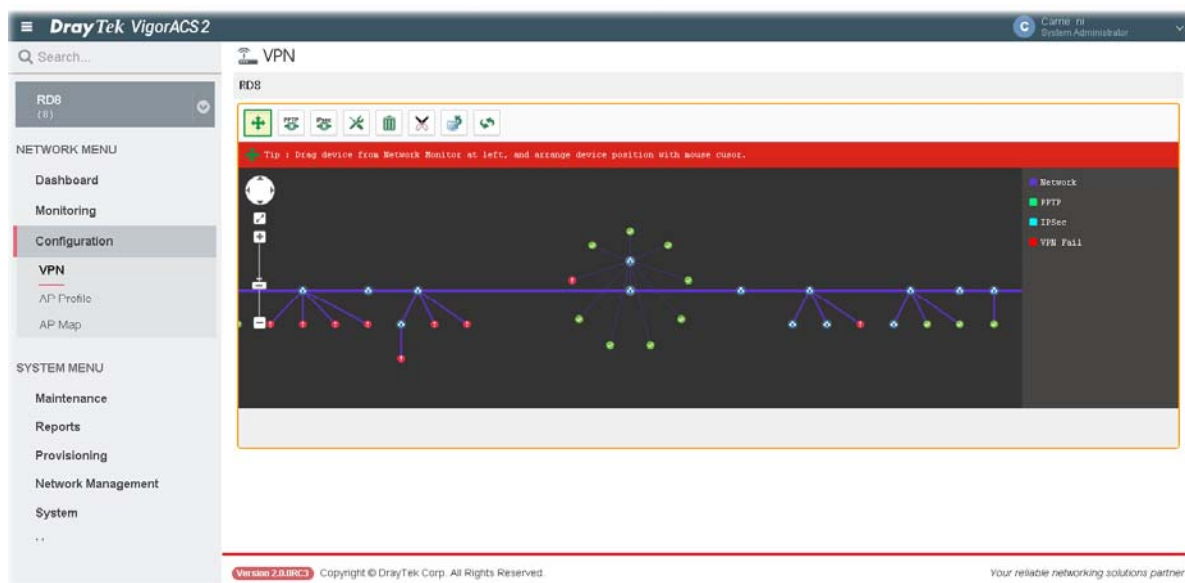
NETWORK MENU is available for Root Network and network group; however, DEVICE MENU is available when a device managed by VigorACS is selected. Configuration menu for root network/group contains VPN, AP Profile and AP MAP. Yet, the menu items for a selected device, basically, are the same as the settings on web user interface of the selected device (CPE, AP and etc.). In other words, 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.

11.1 VPN

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

11.1.1 VPN under NETWORK MENU

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

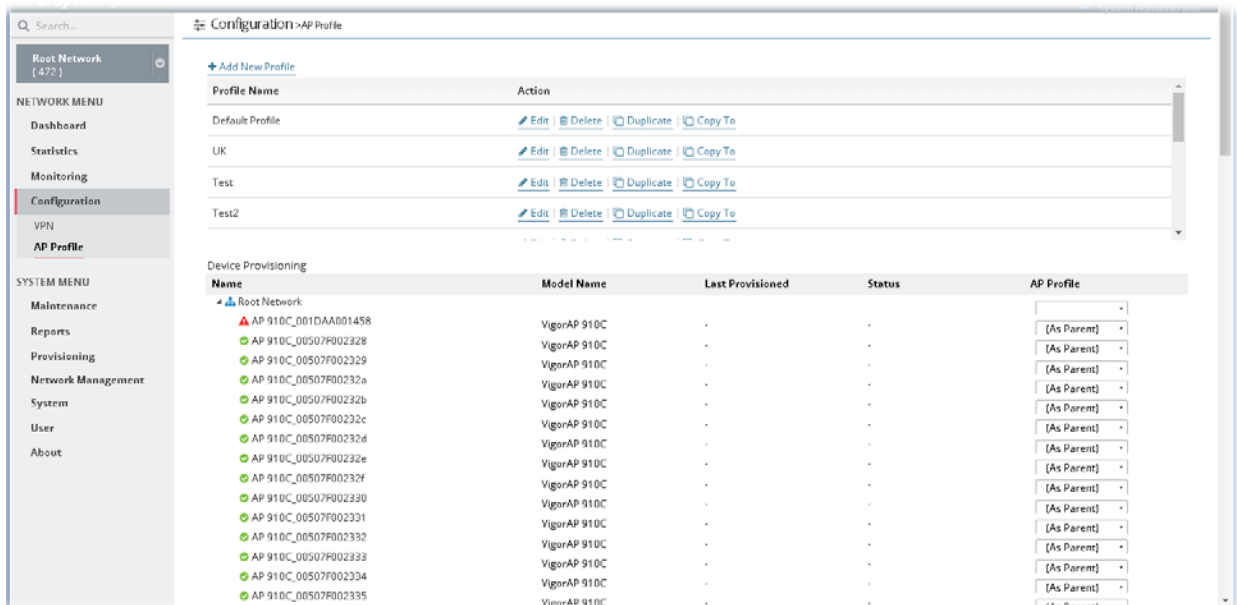


Different colors for arrows represent different protocols used in VPN connections. Purple means Network Group; Green means PPTP mode; Blue means IPSec mode; and Red means the VPN connection is failed.

11.2 AP Profile

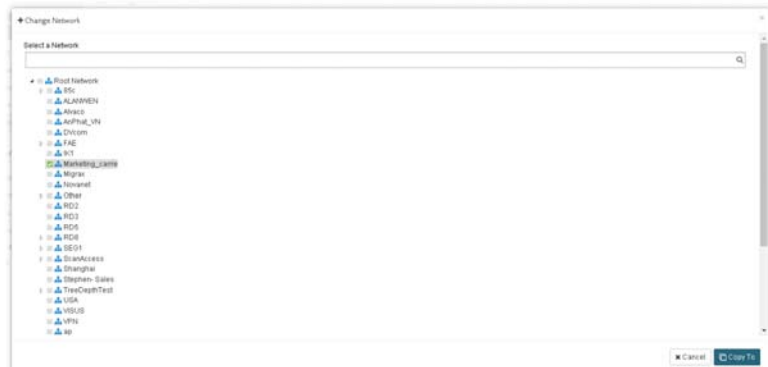
AP profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.

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 support will be overwritten by the selected AP profile.



These parameters are explained as follows:

Item	Description
+Add New Profile	Create a new AP profile with basic settings.
Profile	Display the name of AP profile.
Action	<p>Edit - Configure detailed settings for the selected AP profile.</p> <p>Delete -Delete the selected AP profile.</p> <p>Duplicate - Click it to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).</p> <p>Copy To - Click it 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).</p>



Device Provisioning	<p>Locate the access points for applying suitable AP profile.</p> <p>Name - Display a tree view for model managed by VigorACS.</p> <p>Model Name - Display the name of the model.</p> <p>Last Provisioned - Display the time that AP profile was applied to the selected device.</p> <p>Status - Display the status (updating, complete and "-") of the AP.</p> <p>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.</p>
Refresh	Refresh current page.
Save	Save the changes in this page.

11.2.1 Add New Profile

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

System Administrator

Configuration > AP Profile

Add a Profile

Profile Name: ✓

AP Login Username: ✓

AP Login Password: ✓

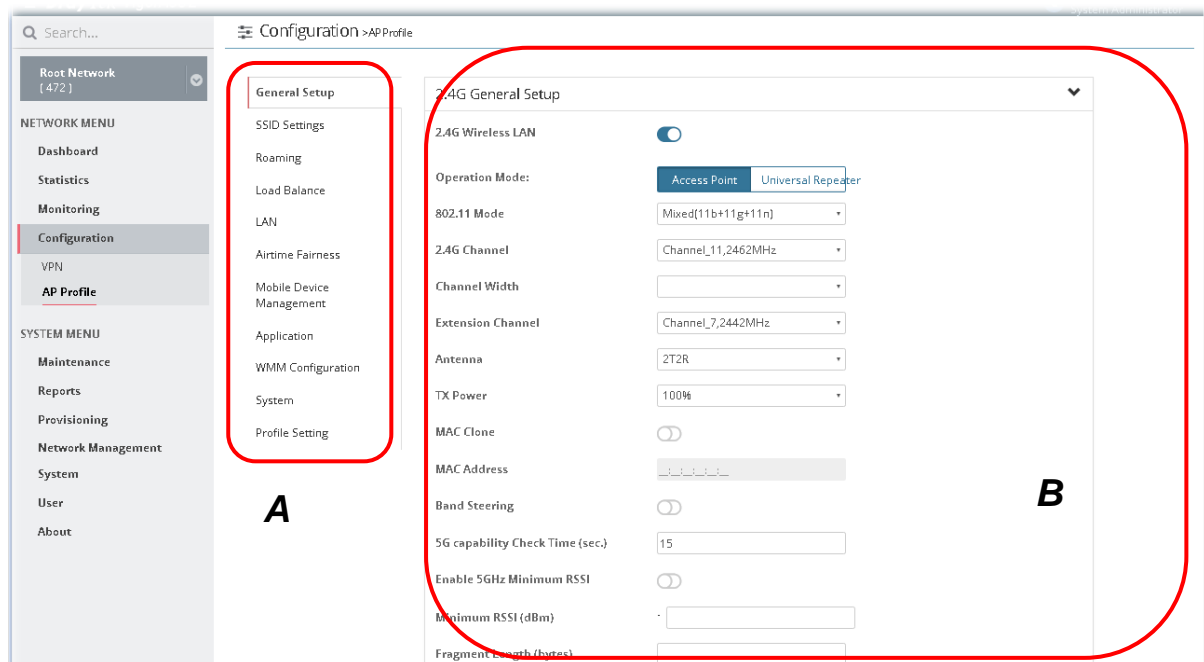
[Back to profile list](#) Save

Available settings are listed as follows:

Item	Description										
Profile Name	Type a name of the profile.										
AP Login Username	Type a username for login the access point.										
AP Login Password	Type a password for login the access point.										
Back to profile list	Return to previous page, AP profile list.										
Save	<p>Save the settings and display the new profile on the AP profile list.</p> <p>Add New Profile</p> <table border="1"> <tbody> <tr> <td>Test</td> <td>Edit Delete Duplicate Copy To</td> </tr> <tr> <td>Test2</td> <td>Edit Delete Duplicate Copy To</td> </tr> <tr> <td>ttt</td> <td>Edit Delete Duplicate Copy To</td> </tr> <tr> <td>redf</td> <td>Edit Delete Duplicate Copy To</td> </tr> <tr> <td>AP_Carrie</td> <td>Edit Delete Duplicate Copy To</td> </tr> </tbody> </table>	Test	Edit Delete Duplicate Copy To	Test2	Edit Delete Duplicate Copy To	ttt	Edit Delete Duplicate Copy To	redf	Edit Delete Duplicate Copy To	AP_Carrie	Edit Delete Duplicate Copy To
Test	Edit Delete Duplicate Copy To										
Test2	Edit Delete Duplicate Copy To										
ttt	Edit Delete Duplicate Copy To										
redf	Edit Delete Duplicate Copy To										
AP_Carrie	Edit Delete Duplicate Copy To										

11.2.2 Edit the AP Profile

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



Available settings are listed as follows:

Item	Description
Area A - Menu Item	At present, the available menu items contain, <ul style="list-style-type: none"> ● General Setup ● SSID Settings ● Roaming ● Load Balance ● LAN ● Airtime Fairness ● Mobile Device Management ● Application ● WMM Configuration ● System ● Profile Setting
Area B - Settings	Such area will vary according to the item selected in Area A - Menu Item.



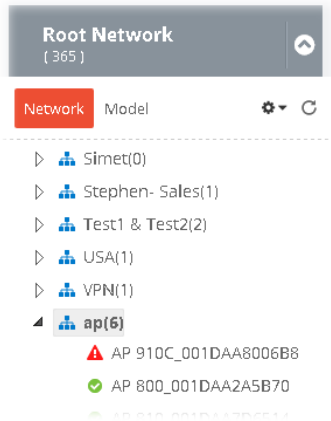
Info

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

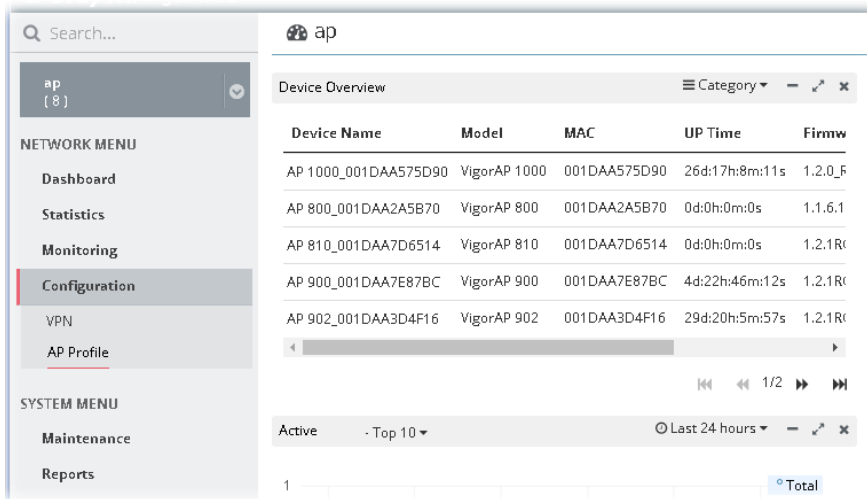
Applications

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

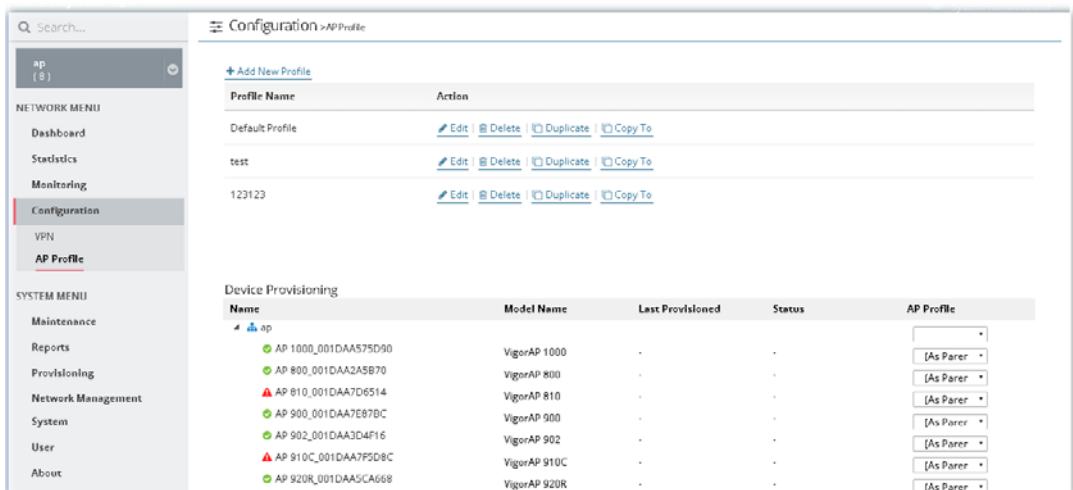
1. Choose a group containing with access points (e.g., “ap” in this case) from Root Network.



2. The dashboard of “ap” group appears as follows.



3. Open NETWORK MENU>>Configuration>>AP Profile.



In the **Device Provisioning**, all of the access points (e.g., AP 800/ AP810/ AP900 / AP902) grouped under “ap” are displayed under the field of Name.

4. Select the AP (e.g., AP 810 in this case) required to apply new AP profile; and use the drop down list of AP Profile to specify a profile (e.g., test in this case).



Info

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.

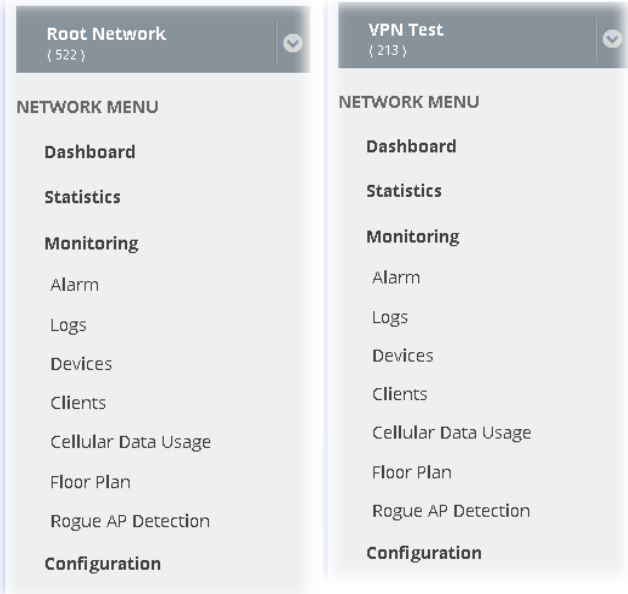
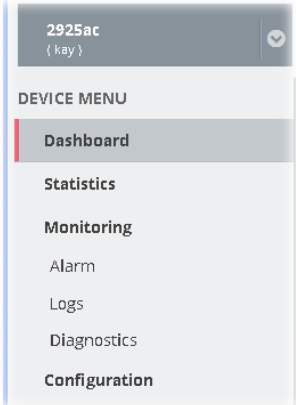
5. Click **Save**. The settings in web user interface of the selected VigorAP will be overwritten with the settings configured in AP profile immediately.

This page is left blank.

Part V DEVICE MENU for Specified CPE

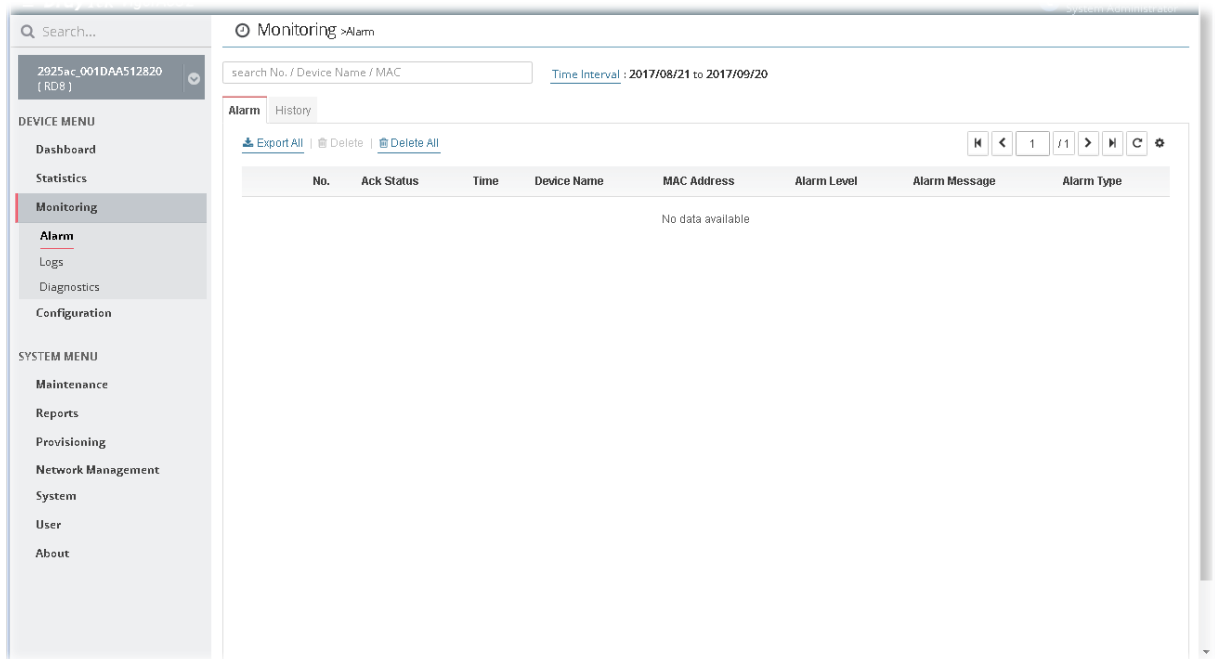
Chapter 12 Monitoring for CPE

Monitoring menu offers Alarm, Logs and Diagnostics for monitoring the normal and abnormal actions for the specified CPE.

Settings to be configured under Root Network / Group	Settings to be configured when a CPE is selected
 <p>The screenshot shows two side-by-side menu panels. The left panel is titled 'Root Network { 522 }' and contains a 'NETWORK MENU' with items: Dashboard, Statistics, Monitoring, Alarm, Logs, Devices, Clients, Cellular Data Usage, Floor Plan, Rogue AP Detection, and Configuration. The right panel is titled 'VPN Test { 213 }' and contains a 'NETWORK MENU' with items: Dashboard, Statistics, Monitoring, Alarm, Logs, Devices, Clients, Cellular Data Usage, Floor Plan, Rogue AP Detection, and Configuration.</p>	 <p>The screenshot shows a menu panel titled '2925ac { Ray }'. It contains a 'DEVICE MENU' with items: Dashboard, Statistics, Monitoring, Alarm, Logs, Diagnostics, and Configuration.</p>

12.1 Alarm

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



These parameters are explained as follows:

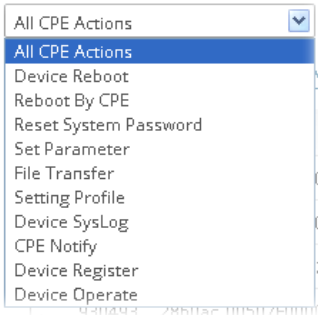
Item	Description
Alarm / History	Alarm - Display the alarm records recently. History - Display all the alarm records that have been solved and cleared.
Export All	Click this button to save alarm log as a XLS file.
Delete	Clear the alarm record which has been solved by VigorACS.
Delete All	Clear all of the alarm records which have been solved by VigorACS.
No.	Display the index number of the alarm. It is offered by VigorACS automatically.
Ack Status	Display the status of the records with the type specified here (Not Ack or Acked).
Time	Display the time that the alert occurred.
Device Name	Display the name of the device encountering the trouble.
MAC Address	Display the MAC address of the device.
Alarm Level	Display the alarm message with the severity specified.
Alarm Message	Display a brief explanation for the alarm sent by VigorACS automatically.
Alarm Type	Display the alarm message with the type specified.
Alarm Status	Display the status of the records with the type specified here (Alarm or Rearm).
Clear Status	Display the clear status for the alarm records. To view different clear status, use the drop down list to specify the one you want to see on the screen.

12.2 Logs

Log provides administrator records for action executed, device name, MAC address, Device ID, MAC Address, Device IP, Action, Action ID and Time for the selected CPE device.

The screenshot displays the 'Monitoring > Logs' page. On the left is a sidebar menu with 'Monitoring' highlighted. The main area shows a table of log entries with the following columns: ID, Device Name, Device ID, MAC Address, Device IP, Action, Action ID, and Time. The table contains 15 rows of data, with the first row having ID 388116 and the last row having ID 370955. Above the table are controls for 'Log Type' (set to 'All CPE Actions'), a search field, and a 'Time Interval' (set to '2017/08/21 to 2017/09/20'). There are also buttons for 'Export All', 'Delete', and 'Delete All'.

These parameters are explained as follows:

Item	Description
Log Type	Choose one of the conditions to display related log on this page. 
<input type="text" value="Search Device Name / IP / MAC"/>	Enter the condition for VigorACS to search and display relational information.
Time Interval	Specify the time interval to display information within that time period.

Export All	Click this button to save alarm log as a XLS file.
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.

12.3 Diagnostics

Menu item under Diagnostics will be different based on the specified CPE.

12.3.1 Ping

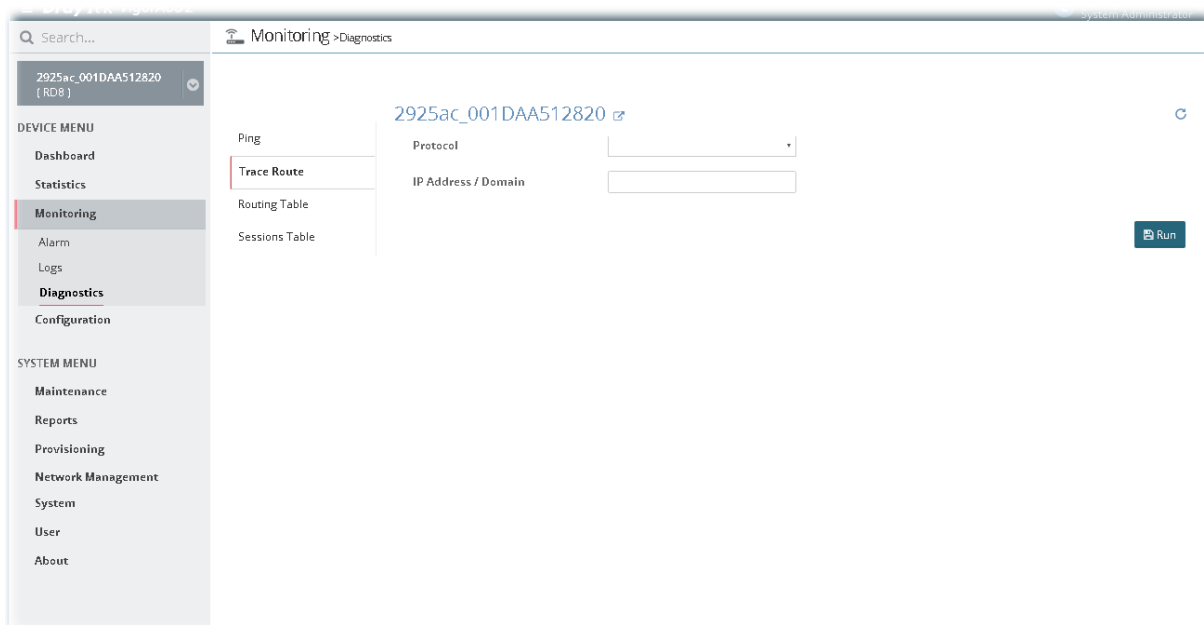
This page allows the system administrator / user to ping a LAN PC (IPv4 or IPv6) through specified WAN interface.

Index	Result
1	Pinging 192.168.1.1 with 64 bytes of Data through WAN1:
2	Request timed out !!!
3	Request timed out !!!
4	Request timed out !!!
5	Request timed out !!!
6	Request timed out !!!
7	Packets: Sent = 5, Received = 0, Lost = 5 (100% loss)

Click the Run button to start the ping work. The result will be displayed on the screen.

12.3.2 Trace Route

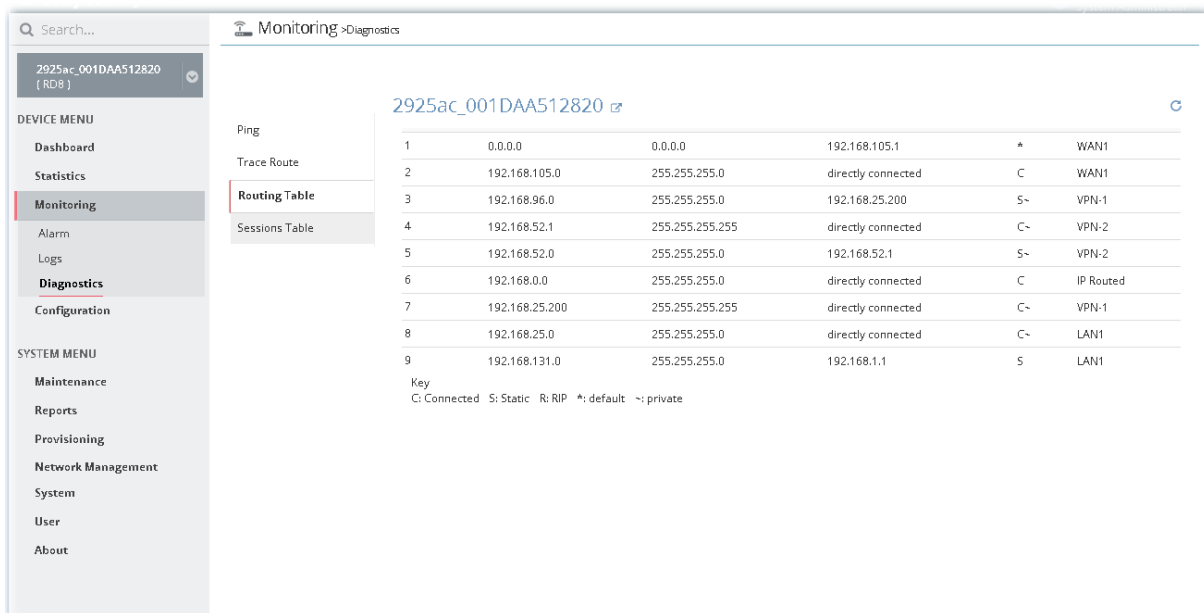
This page allows system administrator / user to trace the routes from router to the host.



Simply type the IP address of the host in the field of IP Address / Domain and click Run. The result of route trace will be shown on the screen.

12.3.3 Routing Table

This page displays a reference table for packets routing by Vigor router.



12.3.4 ARP Table

This page shows a list of LAN/WAN IP address sent by the CPE. The information detected in this page is the same as the data displayed on Diagnostics>>View ARP Cache Table of CPE WUI.

The screenshot shows the WUI interface for a Vigor2926Vac device. The left sidebar contains a navigation menu with sections for DEVICE MENU, SYSTEM MENU, and various sub-menus like Dashboard, Statistics, Monitoring, Diagnostics, Configuration, Maintenance, Reports, Provisioning, Network Management, and System. The main content area is titled 'Monitoring > Diagnostics' and 'Vigor2926Vac'. A sub-menu on the left lists various diagnostic tools, with 'ARP Table' selected. The main display shows a table with the following data:

Index	IP	MAC Address	NetBIOS	Interface	VLAN	Port	Device	Description	Comment
1	172.17.6.73	1C-65-9D-95-77-34		WAN2	---	--			
2	172.17.6.77	00-1D-AA-D0-EE-B1		WAN2	---	--			
3	172.17.6.95	00-1D-AA-5D-CB-21		WAN2	---	--			
4	172.17.6.111	00-1D-AA-FE-F9-62		WAN2	---	--			
5	172.17.6.132	00-1D-AA-66-E0-31		WAN2	---	--			
6	172.17.6.144	00-50-7F-E3-0A-91		WAN2	---	--			
7	172.17.6.152	00-1D-AA-66-E0-11		WAN2	---	--			
8	172.17.6.169	00-1D-AA-64-DD-D9		WAN2	---	--			
9	172.17.6.170	00-1D-AA-FE-F9-59		WAN2	---	--			
10	172.17.6.173	00-1D-AA-E0-62-2A		WAN2	---	--			
11	172.17.6.176	00-1D-AA-7F-9C-F1		WAN2	---	--			
12	192.168.1.10	08-60-6E-4B-FF-D5		LAN1	---	--			
13	172.17.6.179	00-1D-AA-1B-1C-71		WAN2	---	--			

12.3.5 DHCP Table

This page shows a list of DHCP server quantity sent by the CPE. The information detected in this page is the same as the data displayed on Diagnostics>> View DHCP Assigned IP Addresses.

The screenshot shows the WUI interface for a Vigor2926Vac device. The left sidebar contains a navigation menu with sections for DEVICE MENU, SYSTEM MENU, and various sub-menus like Dashboard, Statistics, Monitoring, Diagnostics, Configuration, Maintenance, Reports, Provisioning, Network Management, and System. The main content area is titled 'Monitoring > Diagnostics' and 'Vigor2926Vac'. A sub-menu on the left lists various diagnostic tools, with 'DHCP Table' selected. The main display shows a table with the following data:

Index	Name	IP	Mask	Start IP	End IP	DHCP Server
1	LAN1	192.168.1.1	255.255.255.0	192.168.1.10	192.168.1.209	On

12.3.6 Sessions Table

This page displays a reference table for NAT sessions detected by Vigor router.

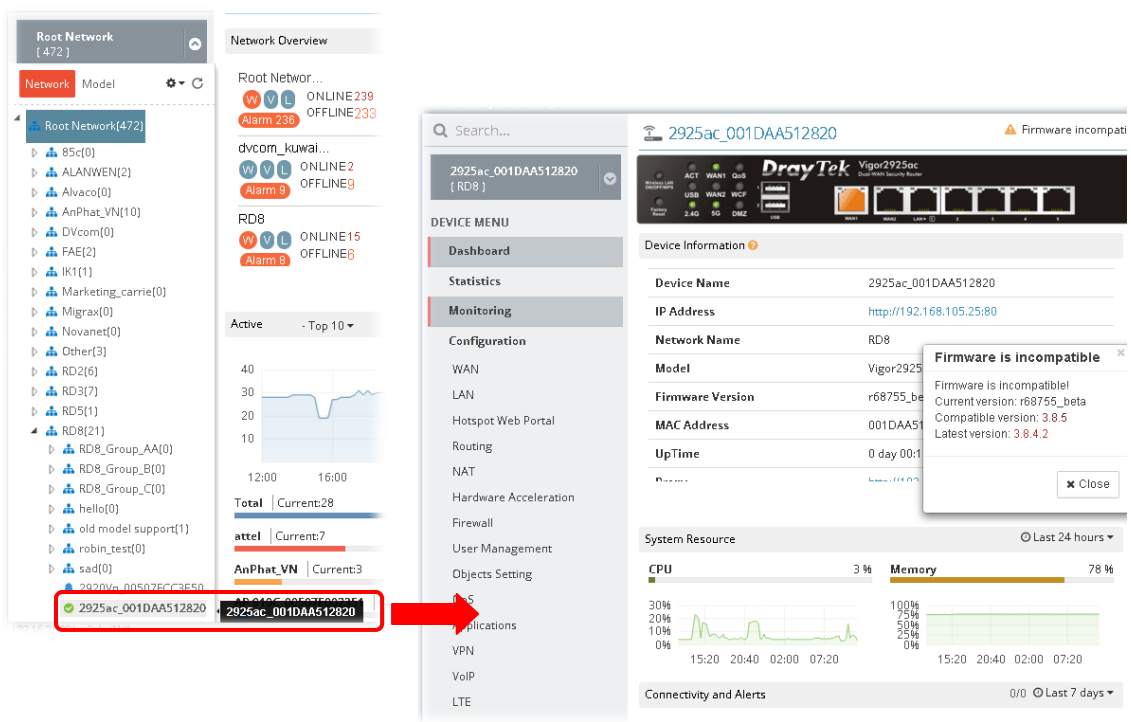
The screenshot shows the Vigor router web interface. At the top, there is a search bar and the breadcrumb "Monitoring >Diagnostics". Below the search bar, the device ID "2925ac_001DAA512820 [RD8]" is displayed. The left sidebar contains a "DEVICE MENU" with options: Dashboard, Statistics, Monitoring (highlighted), Alarm, Logs, Diagnostics, and Configuration. Below this is a "SYSTEM MENU" with options: Maintenance, Reports, Provisioning, Network Management, System, User, and About. In the main content area, a dropdown menu is open, showing options: Ping, Trace Route, Routing Table, and Sessions Table (highlighted). The main content area displays the URL "2925ac_001DAA512820" with a refresh icon. Below the URL, the text "No data available" is shown.

Chapter 13 Configuration for CPE

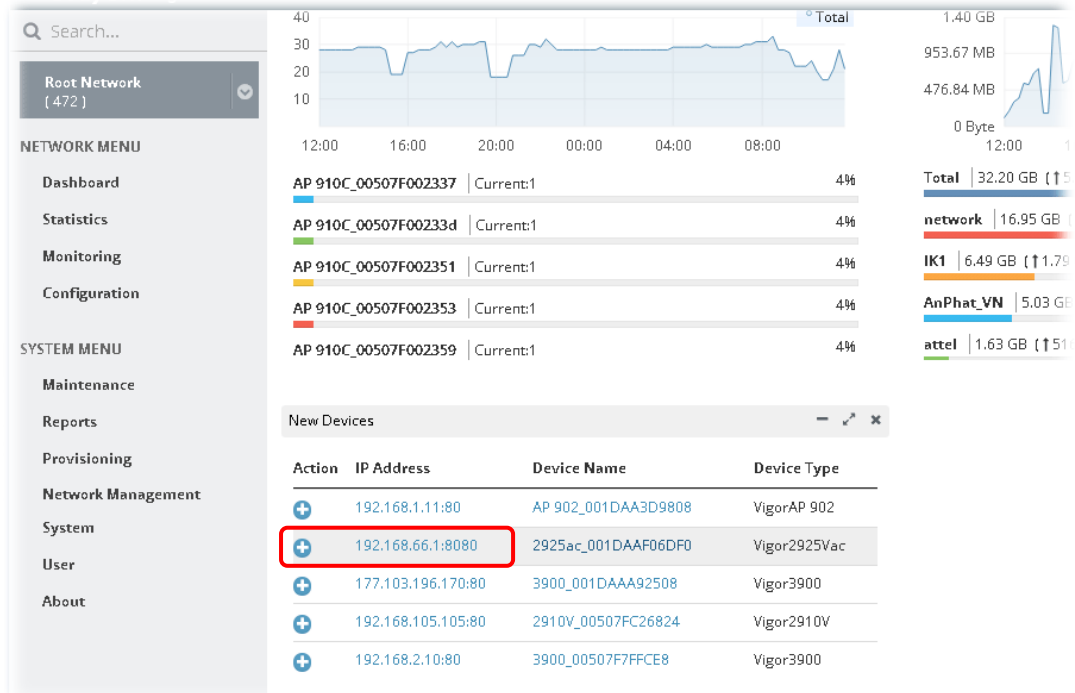
DrayTek VigorACS 2

There are two methods to modify CPE settings via VigorACS, changing the settings from **DEVICE MENU**>>**Configuration** on VigorACS or click the IP address link of the selected CPE to access into the web user interface of that CPE.

How to select a CPE? On the left side of the home page of VigorACS 2, open Root Network and find out the CPE you want. Then, click the CPE. A page view with settings related to the selected CPE will be shown on the screen.



Or, access into the web user interface of that CPE by clicking IP address link of the selected CPE:



Configuration settings will vary for NETWORK MENU (for network/group) and DEVICE MENU (for CPE).

Settings to be configured under Root Network / Group	Settings to be configured when a CPE (e.g, Vigor2862Lac) is selected

NETWORK MENU is available for Root Network and network group; however, DEVICE MENU is available when a device managed by VigorACS 2 is selected.

The menu items for a selected device, basically, are the same as the settings on web user interface of the selected device (CPE, AP and etc.). If required, the administrator can modify the settings for the selected device through the options displayed via VigorACS 2. The modifications will be applied to the selected device immediately.



Info

The menu items listed under Configuration will be changed based on the CPE device / AP device selected. The explanation and usage of the menu items are totally the same as the descriptions stated on User's Guide of each device.

In this chapter, Vigor2862VBn / Vigor2860Vac is selected as an example. That is, the menu items displayed under Configuration are based on the menu items used by Vigor2862VBn /Vigor2860Vac.

13.1 Modifying WAN Settings for CPE

WAN settings relate to access Internet for CPEs. If you want to change WAN settings for specified CPE(s), please choose the device. And, open **DEVICE MENU>>Configuration>>WAN**.

13.1.1 Internet Access – Check WAN Status

Internet Access is convenient for checking WAN status for the selected CPE/group.

Alarm Enable	Index	MAC Address	Up Time	IP	Addressing Type
disable	1	00:1D:AA:C6:4C:51	0d 00h 00m	...	
disable	2	00:1D:AA:C6:4C:52	3d 20h 39m	192.168.105.69	Static
disable	3	00:1D:AA:C6:4C:53		...	
disable	4	00:1D:AA:C6:4C:54		...	

To edit the parameters settings of the selected CPE, move the mouse cursor on the table and click the index number (index 1 ~ index 4 represent WAN 1 ~ WAN 4) to get the following page.

2860Vac_001DAAC64C50 [↗](#)

Internet Access

Connection Detection

Multi-PVC/VLAN

WAN IPv6

WAN Budget

DSL

Alarm

Enable

Active Mode Always On | Failover

Physical Type(Ethernet) Auto negotiation ▾

VLAN Tag Insertion

Connection Mode Static or Dynamic IP | PPPoE

MTU

MAC Address Default MAC | Specify MAC

Show alarm message when this WAN interface disconnects.

Static or Dynamic IP

Connection Type DHCP | Static

IP Address

Subnet Mask

Gateway IP Address

Primary DNS Server

Secondary DNS Server

WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool	Action
1	<input checked="" type="checkbox"/>	192.168.105.69	<input checked="" type="checkbox"/>	
2	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	+ Add

✕ Cancel 💾 Save

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.1.2 Connection Detection

It allows you to verify whether network connection for the specified CPE is alive or not through ARP Detect or Ping Detect.

Index	Mode	Primary Ping IP	Secondary Ping IP	Ping Gateway IP	TTL
1	ARP Detect	0.0.0.0	0.0.0.0	false	255
2	ARP Detect	0.0.0.0	0.0.0.0	false	255
3	ARP Detect	0.0.0.0	0.0.0.0	false	255
4	ARP Detect	0.0.0.0	0.0.0.0	false	255

To edit the parameters settings of the selected CPE, move the mouse cursor on the table and click the index number (index 1 ~ index 4 represent WAN 1 ~ WAN 4) to get the following page.

Configuration > WAN

2860Vac_001DAAC64C50

Connection Detection

Index: 1

Mode: Ping Detect

Primary Ping IP: 0.0.0.0

Secondary Ping IP: 0.0.0.0

Ping Gateway IP:

TTL: 255

Ping Interval: 1

Ping Retry: 10

Cancel Save

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.1.3 Multi-PVC/VLAN

This page allows you to create multi-PVC for different data transferring for using.

Channel	General Enable	WAN Type	VPI	VCI	QoS Type	Protocol	Encapsulation
5	false	ADSL	1	45	UBR	PPPoA	VC_MUX
6	false	ADSL	1	46	UBR	PPPoA	VC_MUX
7	false	ADSL	1	47	UBR	PPPoA	VC_MUX
8	false	ADSL	1	48	UBR	PPPoA	VC_MUX
9	false	ADSL	1	49	UBR	PPPoA	VC_MUX
10	false	ADSL	1	50	UBR	PPPoA	VC_MUX

To edit the parameters settings for each channel (5 to 10), move the mouse cursor on the table and click the channel number to get the following page.

Configuration > WAN

2860Vac_001DAAC64C50

Internet Access

Connection Detection

Multi-PVC/VLAN

WAN IPv6

WAN Budget

DSL

Channel: 5

Enable:

WAN Type: ADSL ✓

General Settings

VPI: 1

VCI: 45

Protocol: PPPoA

Encapsulation: VC MUX

Add VLAN Header:

VLAN Tag: 0

Wan Count: 1

ATM QoS

QoS Type: UBR

PCR: 0

SCR: 0

MBS: 0

Port-based Bridge

Open Port-based Bridge:

Connection

Physical Members: P2 P3 P4 P5 P6

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.1.4 WAN IPv6

All WAN interfaces can be configured with IPv6 addresses.

Configuration > WAN

2860Vac_001DAAC64C50

Internet Access

Connection Detection

Multi-PVC/VLAN

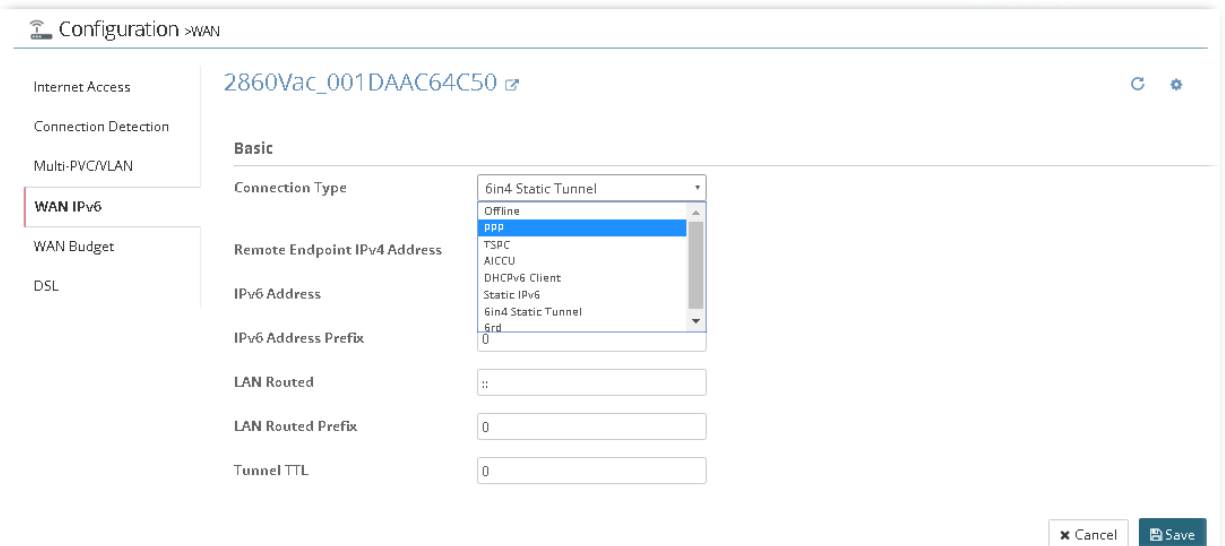
WAN IPv6

WAN Budget

DSL

Index	Connection Type	TSPC : Username	TSPC : Password	TSPC : Tunnel Broker	AICCU : Always On
1	Offline				false
2	Offline				false
3	Offline				false
4	Offline				false

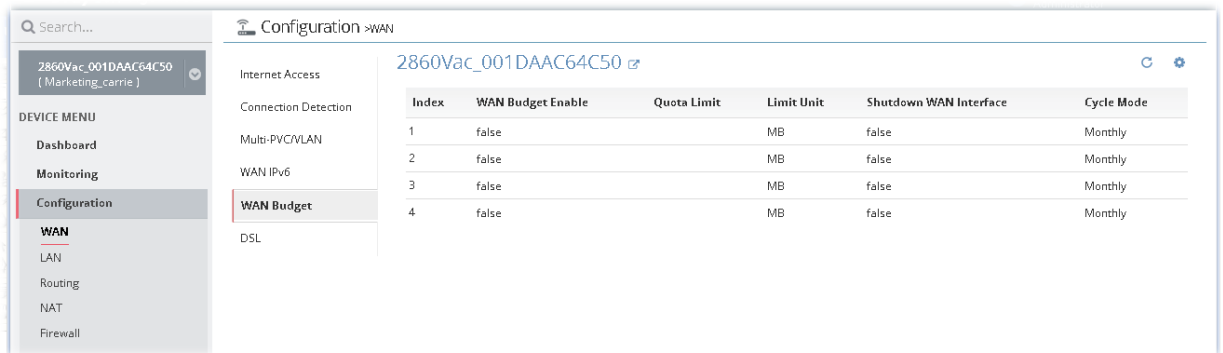
To edit the parameters settings for each WAN interface, move the mouse cursor on the table and click the index number (index 1 ~ index 4 represent WAN 1 ~ WAN 4) to get the following page.



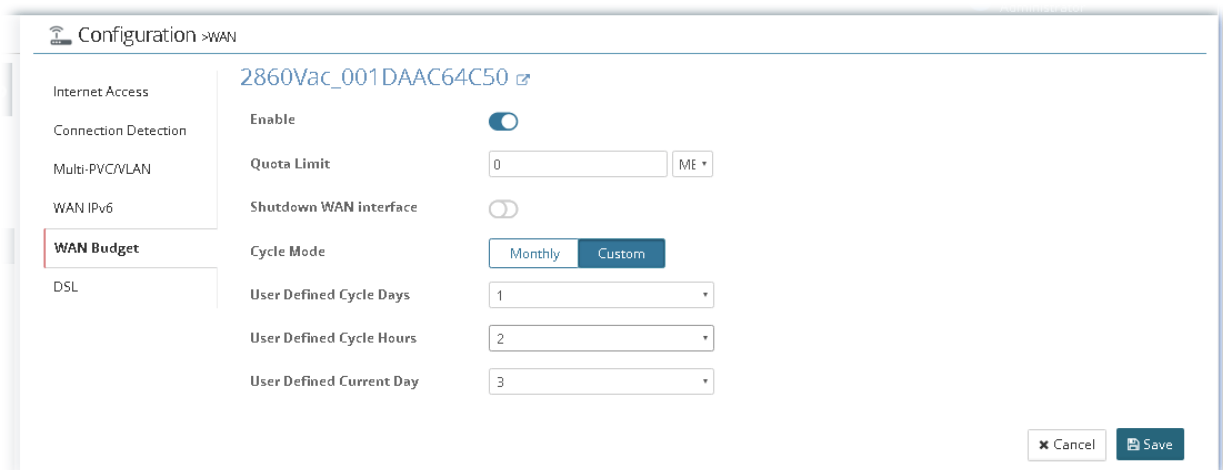
After finished the settings, click **Save**. The modification for the CPE will take effect immediately.

13.1.5 WAN Budget

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



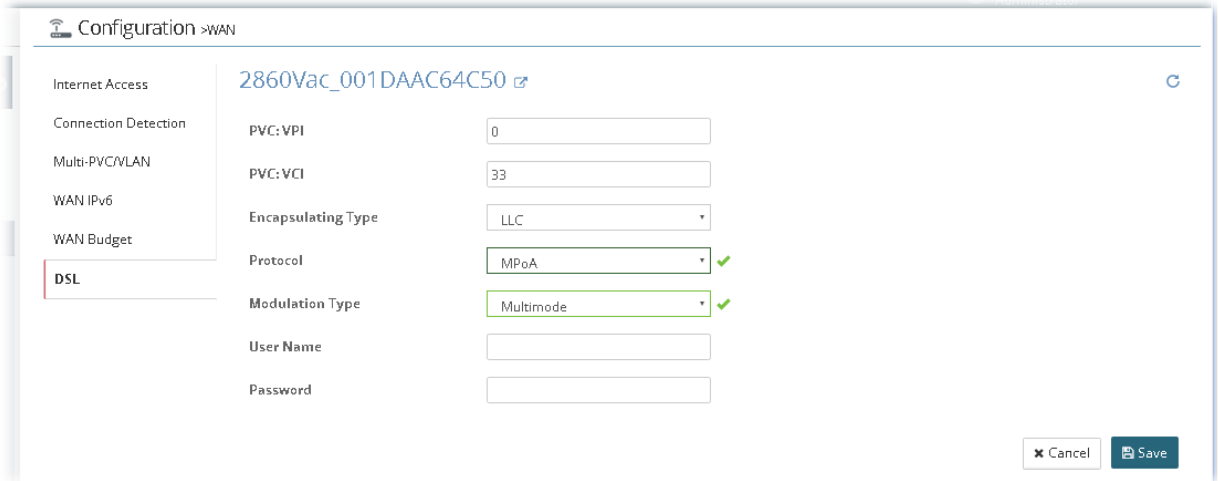
To edit the parameters settings for each WAN interface, move the mouse cursor on the table and click the index number (index 1 ~ index 4 represent WAN 1 ~ WAN 4) to get the following page.



After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.1.6 DSL

This page allows you to set up the DSL parameters required by your ISP.



After finished the settings, click Save. The modification for the CPE will take effect immediately.

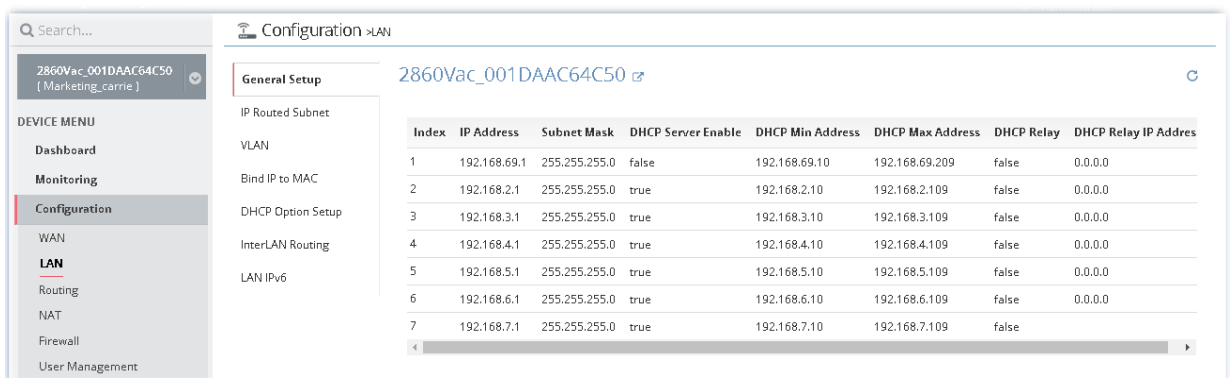
13.2 Modifying LAN Setting for CPE

The administrator can check and edit LAN settings for the selected CPE if necessary.

Click **DEVICE MENU>>Configuration>>LAN**. The following screen will appear with all of the LAN settings for the selected CPE.

13.2.1 General Setup

This page provides you the general settings for LAN. There are six subnets provided by the router which allow users to divide groups into different subnets (LAN 1 - LAN 7). At present, LAN1 setting is fixed with NAT mode only. LAN 2 - LAN 7 can be operated under NAT or Route mode. IP Routed Subnet can be operated under Route mode.



To edit the parameters settings for each LAN interface, move the mouse cursor on the table and click the index number (index 1 ~ index 7 represent LAN interfaces) to get the following page.

Index 1 represents LAN1:

Configuration > LAN

2860Vac_001DAAC64C50

General Setup

IP Routed Subnet
VLAN
Bind IP to MAC
DHCP Option Setup
InterLAN Routing
LAN IPv6

General Setup

Index: 1

Enable:

IP Address: 192.168.69.1

Subnet Mask: 255.255.255.0

DHCP Server Setup

DHCP Server Enable:

DHCP Relay:

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Cancel Save

Index 2 to Index 7 represents LAN 2 to LAN 6 and DMZ:

Configuration > LAN

2860Vac_001DAAC64C50

General Setup

IP Routed Subnet
VLAN
Bind IP to MAC
DHCP Option Setup
InterLAN Routing
LAN IPv6

General Setup

Index: 2

Enable:

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Usage: NAT Routing

DHCP Server Setup

DHCP Server Enable:

IP Pool Start: 192.168.2.10

IP Pool End: 192.168.2.109

Gateway IP Address: 192.168.2.1

DHCP Lease Time: 259200

DHCP Relay:

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Cancel Save

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.2.2 IP Routed Subnet

Configuration > LAN

2860Vac_001DAAC64C50

General Setup

IP Routed Subnet

VLAN

Bind IP to MAC

DHCP Option Setup

InterLAN Routing

LAN IPv6

General Setup

Enable

IP Address

Subnet Mask

DHCP Server Setup

IP Pool Start

IP Pool Counts

(max. 32)

Use LAN Port

Use LAN Port1

Use LAN Port2

Use MAC Address

MAC Address Table

Index	Matched MAC Address	Given IP Address	Action
1	<input type="text"/>	<input type="text"/>	+ Add

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.2.3 VLAN

With the 6-port Gigabit switch on the LAN side, Vigor router provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. Gigabit LAN ports can be isolated from each other. On the Wireless-equipped models, each of the wireless SSIDs can also be grouped within one of the VLANs.

Search... Configuration >LAN 2860Vac_001DAAC64C50

2860Vac_001DAAC64C50 (Marketing_carrie)

DEVICE MENU

- Dashboard
- Monitoring
- Configuration

SYSTEM MENU

- Maintenance
- Reports
- Provisioning
- Network Management
- System
- User
- About

General Setup

IP Routed Subnet

VLAN

Bind IP to MAC

DHCP Option Setup

InterLAN Routing

LAN IPv6

VLAN Configuration

VLAN Enable

Name	Subnet	VLAN Tag Enable	VLAN Tag ID	VLAN Tag Priority
VLAN0	LAN1	<input type="checkbox"/>	0	0
VLAN1	LAN1	<input type="checkbox"/>	0	0
VLAN2	LAN1	<input type="checkbox"/>	0	0
VLAN3	LAN1	<input type="checkbox"/>	0	0
VLAN4	LAN1	<input type="checkbox"/>	0	0
VLAN5	LAN1	<input type="checkbox"/>	0	0
VLAN6	LAN1	<input type="checkbox"/>	0	0
VLAN7	LAN1	<input type="checkbox"/>	0	0

VLAN Member(LAN)

Name	P1	P2	P3	P4	P5	P6
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VLAN Member(Wireless 2.4G)

Name	SSID1	SSID2	SSID3	SSID4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VLAN Member(Wireless 5G)

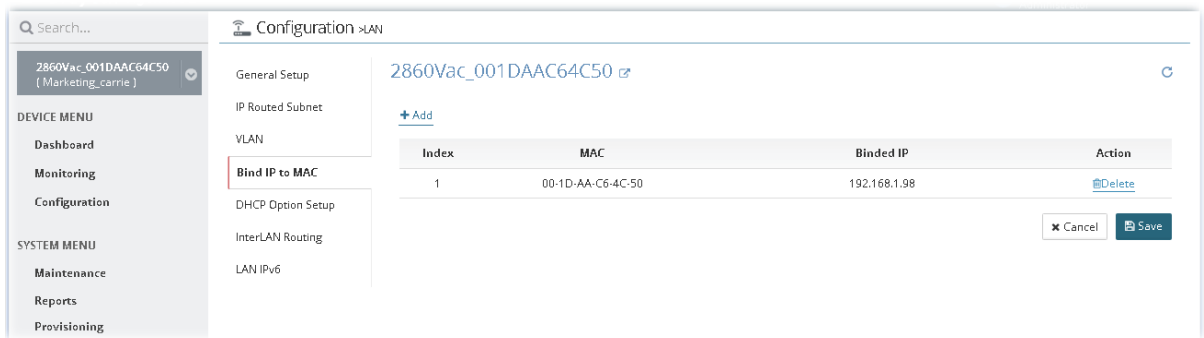
Name	SSID1_5G	SSID2_5G	SSID3_5G	SSID4_5G
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Clear VLAN setup](#)

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

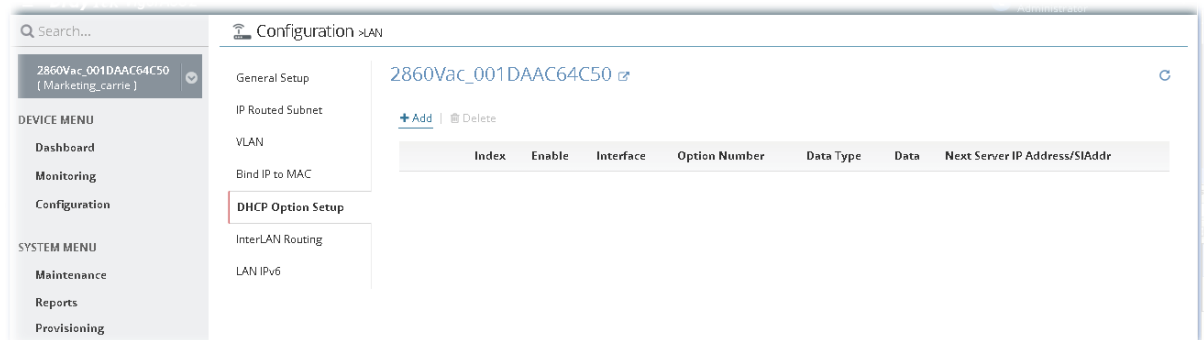


To add the parameters settings for DHCP server, click **+Add** to type the MAC address and an IP address for binding.

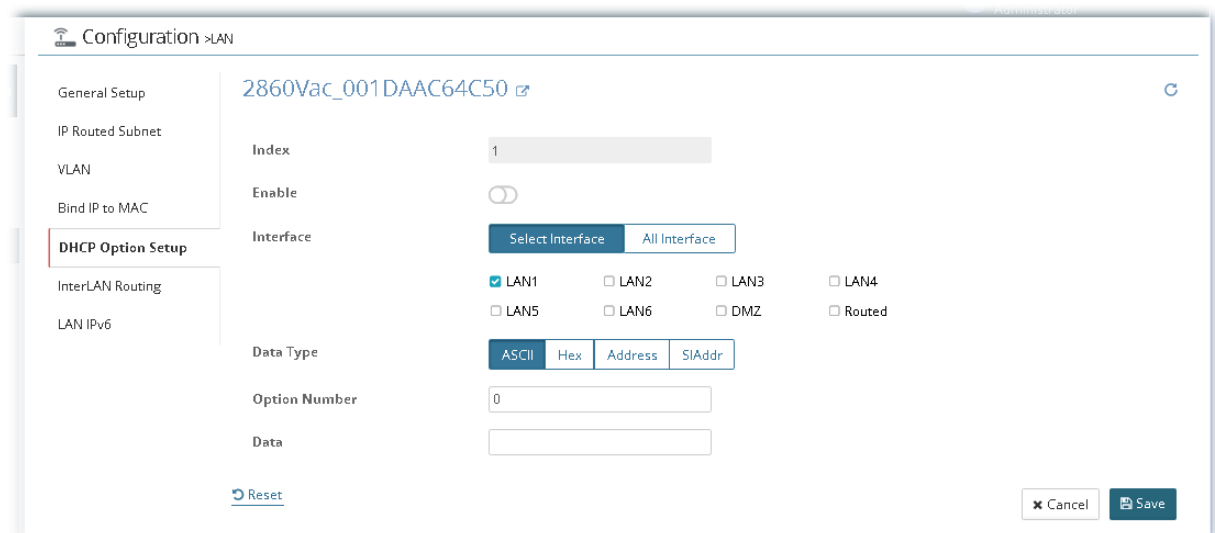
After finished the settings, click **Save**. The modification for the CPE will take effect immediately.

13.2.5 DHCP Option Setup

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



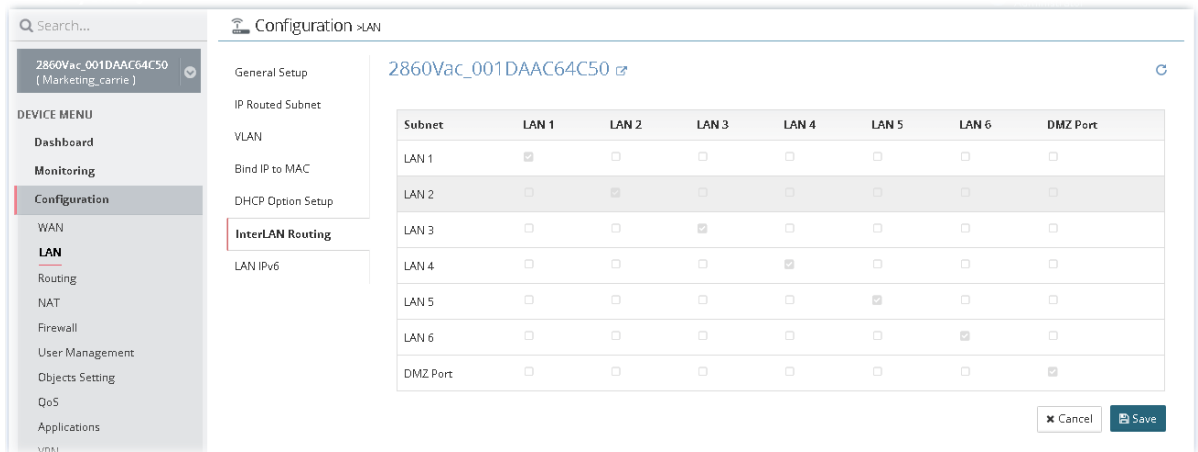
To add the parameters settings for DHCP server, click **+Add** to get the following page.



After finished the settings, click **Save**. The modification for the CPE will take effect immediately.

13.2.6 InterLAN Routing

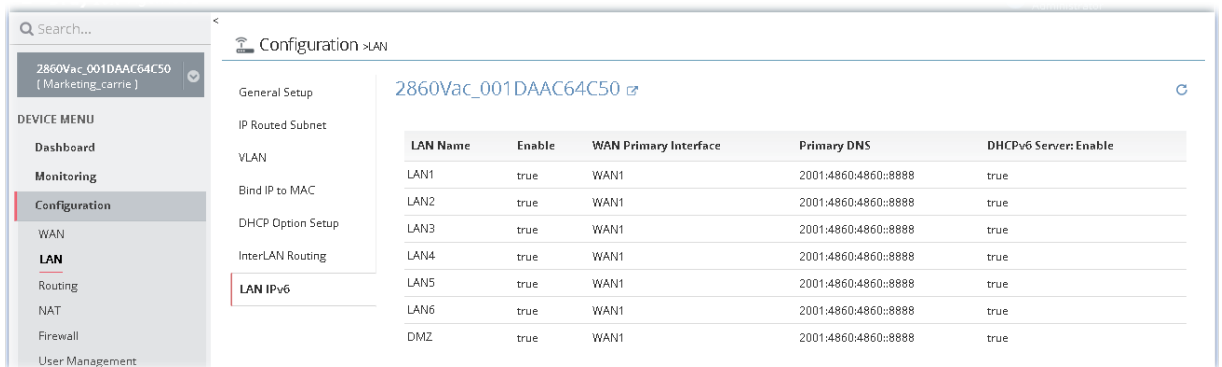
This page is used for linking two or more different subnets (LAN and LAN).



After finished the settings, click **Save**. The modification for the CPE will take effect immediately.

13.2.7 LAN IPv6

There are two configuration pages for LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/DMZ Port, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. This page shows configuration for IPv6.



To edit the parameters settings for each LAN interface and DMZ, move the mouse cursor on the table and click any one of the LAN names to get the following page.

Configuration > LAN

2860Vac_001DAAC64C50

General Setup
IP Routed Subnet
VLAN
Bind IP to MAC
DHCP Option Setup
InterLAN Routing
LAN IPv6

Basic Setup

LAN Name: LAN1

Enable:

WAN Primary Interface: WAN1

Static IPv6

ULA Config: Off

ULA Config Address: ::

Prefix Length: 64

IPv6 Address Table

Index	IPv6 Address	Prefix Length	Action
1	FE80::21D:AFF:FE6:4C50	64	Delete
2	<input type="text"/>	<input type="text"/>	+Add

DNS Server IPv6

DNS Enable: Deploy_when_WAN_is_up

Primary DNS: 2001:4860:4860::8888

Secondary DNS: 2001:4860:4860::8844

Management

Management: SLAAC(stateless)

Other Option(O-bit):

DHCPv6 Server

DHCPv6 Server Enable:

Auto IPv6 Range:

Start Address: ::

End Address: ::

Router Advertisement Configuration

Enable:

Hop Limit: 64

Min Interval Time(sec): 200

Max Interval Time(sec): 600

Default Lifetime(sec): 1800

[High Availability secondary is 0]

Default Preference: Medium

MTU Auto:

0

RIPng Protocol

Enable:

Extension WAN

Selected WAN: WAN2 WAN3 WAN4

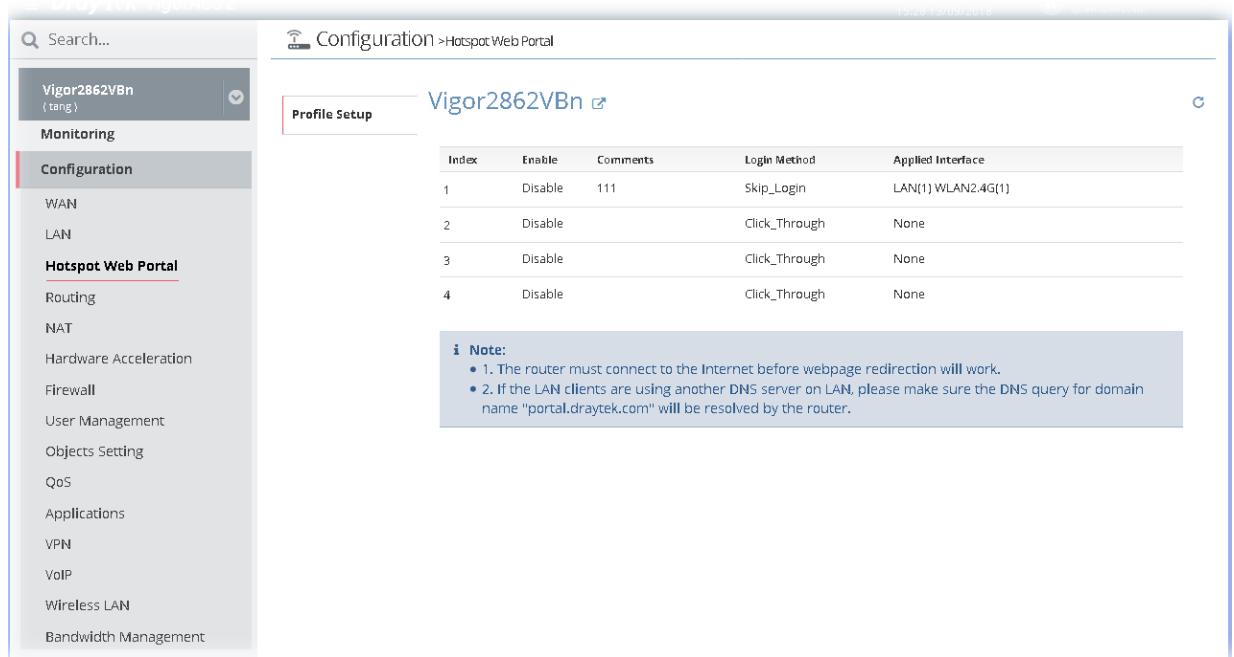
After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.3 Hotspot Web Portal for CPE

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.

13.3.1 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.



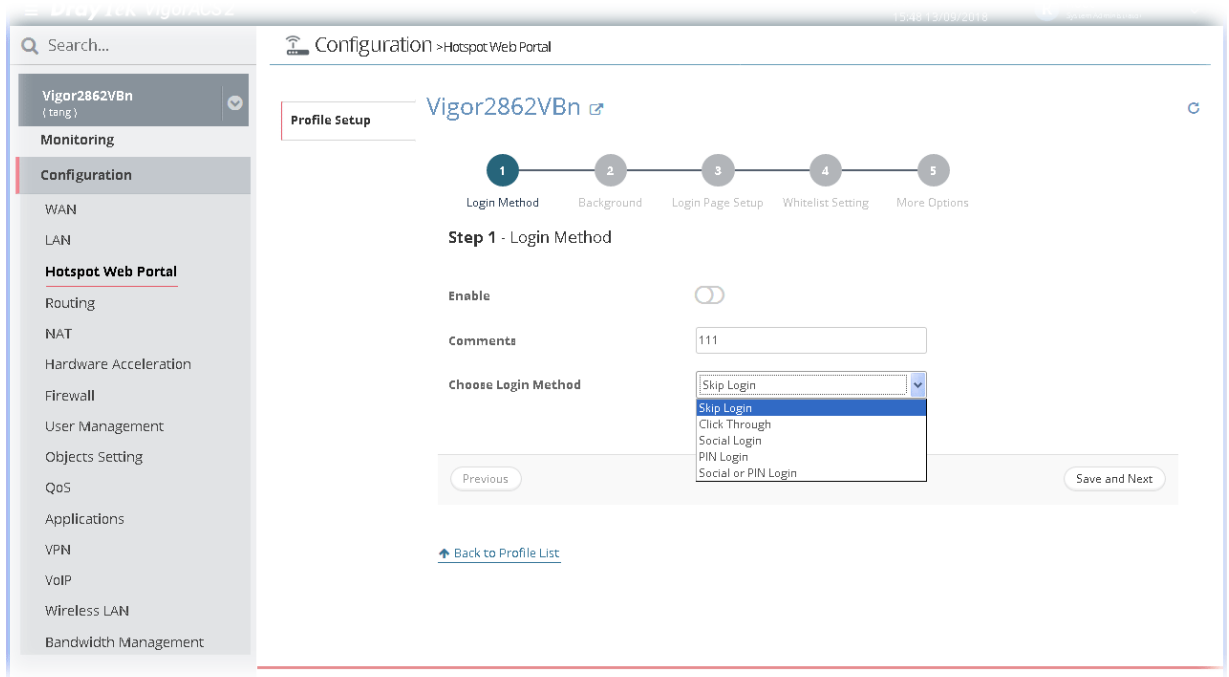
The screenshot shows the configuration page for the Hotspot Web Portal on a Vigor2862VBn router. The page is titled "Profile Setup" and displays a table with four profiles. The first profile is enabled, while the others are disabled. A note is provided below the table regarding Internet connectivity and DNS resolution.

Index	Enable	Comments	Login Method	Applied Interface
1	Disable	111	Skip_Login	LAN(1) WLAN2.4G(1)
2	Disable		Click_Through	None
3	Disable		Click_Through	None
4	Disable		Click_Through	None

Note:

- 1. The router must connect to the Internet before webpage redirection will work.
- 2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

To edit the parameters settings for each profile, move the mouse cursor on the table and click any one of the indexes to get the following page.

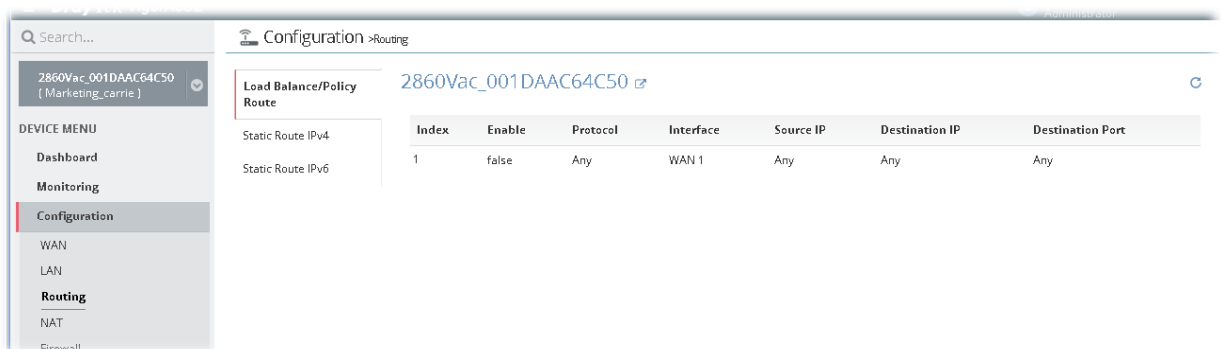


There are five login modes to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

Please follow the on-screen steps for configuring a Web Portal Profile.

13.4 Routing Settings for CPE

13.4.1 Load Balance/Policy Route



To add a new route policy profile, move the mouse cursor on the table and click the index number #1 to get the following page.

Configuration > Routing

2860Vac_001DAAC64C50

Load Balance/Policy Route

Static Route IPv4

Static Route IPv6

Index: 1

Enable:

Criteria

Protocol: ICMP ✓

Source IP: Range ✓

Source IP Start: 192.168.2.56 ✓

Source IP End: 192.168.2.100 ✓

Destination IP: Any

Destination Port: Range ✓

Destination Port Start: 250 ✓

Destination Port End: 500 ✓

Send via if Criteria Matched

Interface: WAN 1

Gateway IP: Default_Gateway

Packet Forwarding Via: Force_NAT

More Options

Enable Failover:

Failover to: Default_WAN

Failover to Gateway IP: Default_Gateway

Failover to Specific Gateway: 0.0.0.0

Failback:

Cancel Save

After finished the settings, click Save. A new policy route has been created. And, the modification for the CPE will take effect immediately.

Configuration > Routing

2860Vac_001DAAC64C50

Load Balance/Policy Route

Static Route IPv4

Static Route IPv6

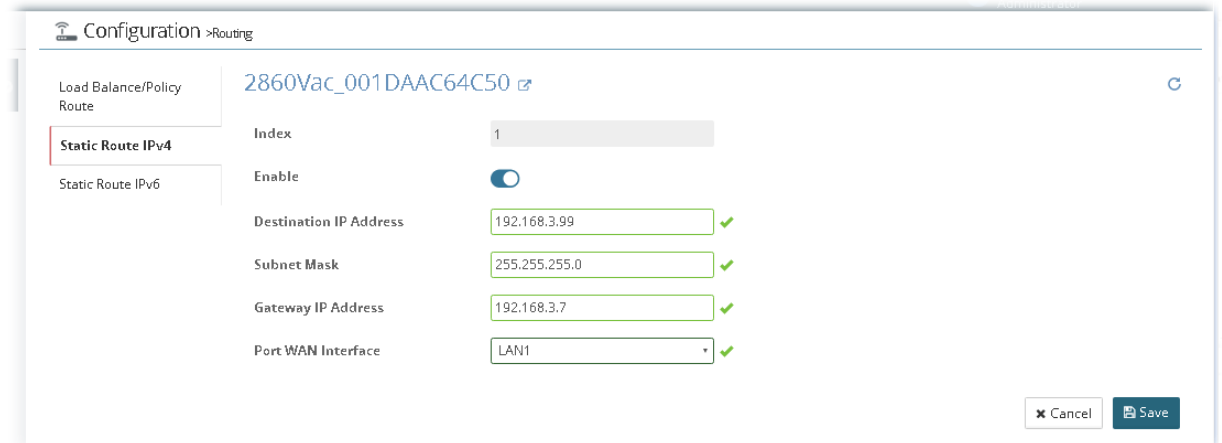
Index	Enable	Protocol	Interface	Source IP	Destination IP	Destination Port
1	true	ICMP	WAN 1	Range	Any	Range
2	false	Any	WAN 1	Any	Any	Any

13.4.2 Static Route IPv4 / IPv6

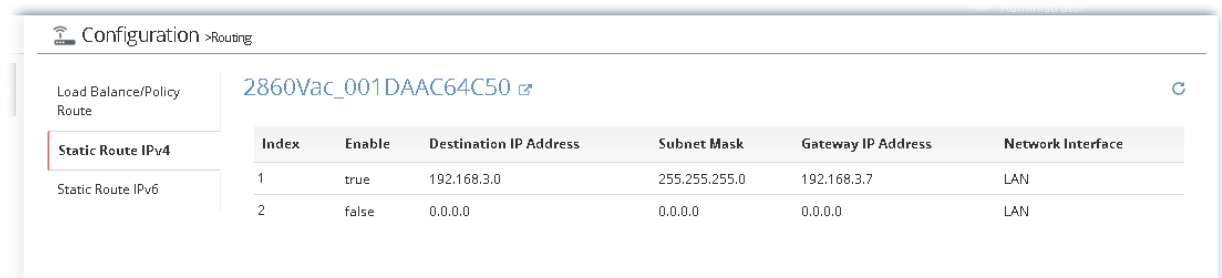
The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.



To add a new static route profile, move the mouse cursor on the table and click the index number #1 (default blank profile) to get the following page.



After finished the settings, click Save. A new static route has been created. And, the modification for the CPE will take effect immediately.

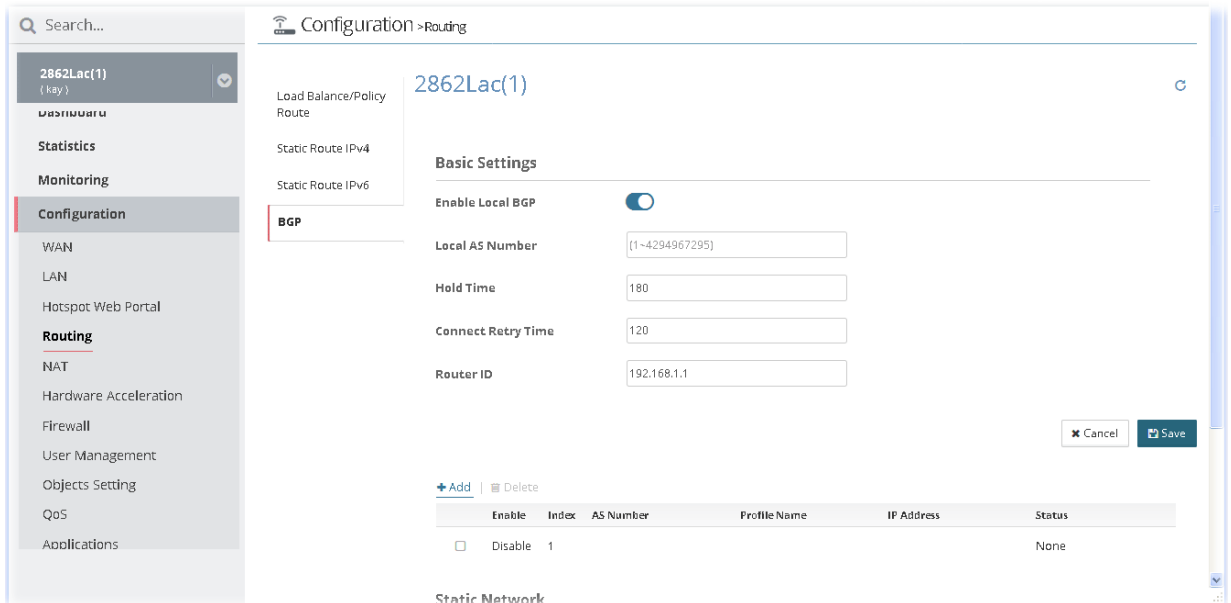


Info

New added profile will be displayed on the top side (index #1) of the page. The default blank profile (index #2) will be moved to the bottom.

13.4.3 BGP

Border Gateway Protocol (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
Basic Settings	<p>Set general settings for for local router and neighboring routers.</p> <p>Enable Local BGP - Switch the button to enable the function.</p> <p>Local AS Number - Display the local AS number.</p> <p>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.</p> <p>Connect Retry Time - If the router fails to connect to neighboring router, it requires a period of time to reconnect.</p> <p>Router ID - Specify the LAN subnet for the router.</p> <p>+Add - Add a new neighbor profile.</p>
Cancel	Discard current settings.
Save	Save the current settings and exit the page.

Static Network

+Add - Add a new static network profile by giving IP address and subnet mask.

The screenshot shows the 'Configuration > Routing' page for a device named '2862Lac(1)'. On the left, there is a sidebar menu with options: 'Load Balance/Policy Route', 'Static Route IPv4', 'Static Route IPv6', and 'BGP'. The 'Static Route IPv4' option is selected. The main area contains a form with the following fields: 'Index' (value: 1), 'IP Address' (empty), and 'Subnet Mask' (empty). At the bottom right, there are 'Cancel' and 'Save' buttons.

Save - Click it to save the configuration.

13.5 NAT Settings for CPE

13.5.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. It can only apply to incoming traffic.

The screenshot shows the 'Configuration > NAT' page for a device named '2860Vac_001DAAC64C50'. The 'Port Redirection' option is selected. Below the title, there is a table with the following columns: 'Index', 'Enabled', 'Port Redirection Mode', 'Service Name', 'Protocol', 'Public Port Start', 'Public Port End', 'Private IP Start', and 'Private IP End'. The table contains one row with the following values: Index: 1, Enabled: false, Port Redirection Mode: Single, Service Name: ---, Protocol: ---, Public Port Start: 0, Public Port End: 0, Private IP Start: 0. At the bottom right, there are 'Cancel' and 'Save' buttons.

To add a new port redirection profile, move the mouse cursor on the table and click the index number #1 (default blank profile) to get the following page.

The screenshot shows the 'Configuration > NAT' page for a device named '2860Vac_001DAAC64C50'. The 'Port Redirection' option is selected. The main area contains a form with the following fields: 'Index' (value: 1), 'Enabled' (checkbox checked), 'Port Redirection Mode' (radio buttons: 'Single' selected, 'Range'), 'Service Name' (text input: 'test_1'), 'Protocol' (radio buttons: 'TCP' selected, 'UDP'), 'WAN Interface' (dropdown menu: 'ALL'), 'Public Port Start' (text input: '200'), 'Source IP' (dropdown menu: 'Any'), 'Private IP Start' (text input: '192.168.13.69'), and 'Private Port' (text input: '100'). At the bottom left, there is a 'Clear' button. At the bottom right, there are 'Cancel' and 'Save' buttons.

After finished the settings, click **Save**. A new port redirection profile has been created. And, the modification for the CPE will take effect immediately.



Info

New added profile will be displayed on the top side (index #1) of the page. The default blank profile (index #2) will be moved to the bottom.

13.5.2 DMZ Host

Port Redirection can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Use this function to configure DMZ host for the specified CPE device.

The screenshot shows the 'DMZ Host' configuration page for profile '2860Vac_001DAAC64C50'. The left sidebar contains a 'DEVICE MENU' with 'Configuration' selected. The main content area is titled 'DMZ Host Setup WAN1' and includes the following settings:

- Enable:**
- LAN Host:** ✓
- Private IP:** ✓

Below this are sections for 'DMZ Host Setup WAN2', 'DMZ Host Setup WAN3', and 'DMZ Host Setup WAN4', each with an 'Enable' toggle and a 'Private IP' field set to '0.0.0.0'. A 'Save' button is located at the bottom right.

After finished the settings, click **Save**. And, the modification for the CPE will take effect immediately.

13.5.3 Open Ports

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

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

The screenshot shows the 'Open Ports' configuration page for profile '2860Vac_001DAAC64C50'. The left sidebar contains a 'SYSTEM MENU' with 'Maintenance' selected. The main content area is titled 'Open Ports' and displays a table with the following data:

Index	Enable Open Ports	Comment	WAN Interface	WAN IP	Local IP Address	Source IP
1	false		WAN1	WAN1_IP_Alias[1]	0.0.0.0	Any

To add a new open ports profile, move the mouse cursor on the table and click the index number #1 (default blank profile) to get the following page.

Configuration > NAT

2860Vac_001DAAC64C50

Port Redirection

DMZ Host

Open Ports

Index: 1

Enable:

Comment: test_33

WAN Interface: WAN1

Source IP: Any

Local IP Address: 0.0.0.0

Open Port List

Index	Protocol	Start Port	End Port
1	UDP	0	0
2		0	0
3	TCP	0	0
4	UDP	0	0
5	TCP/UDP	0	0
6		0	0
7		0	0
8		0	0
9		0	0
10		0	0

Clear Cancel Save

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

Configuration > NAT

2860Vac_001DAAC64C50

Port Redirection

DMZ Host

Open Ports

Index	Enable Open Ports	Comment	WAN Interface	WAN IP	Local IP Address	Source IP
1	true	test_33	WAN1	WAN1_IP_Alias[1]	0.0.0.0	Any
2	false		WAN1	WAN1_IP_Alias[1]	0.0.0.0	Any

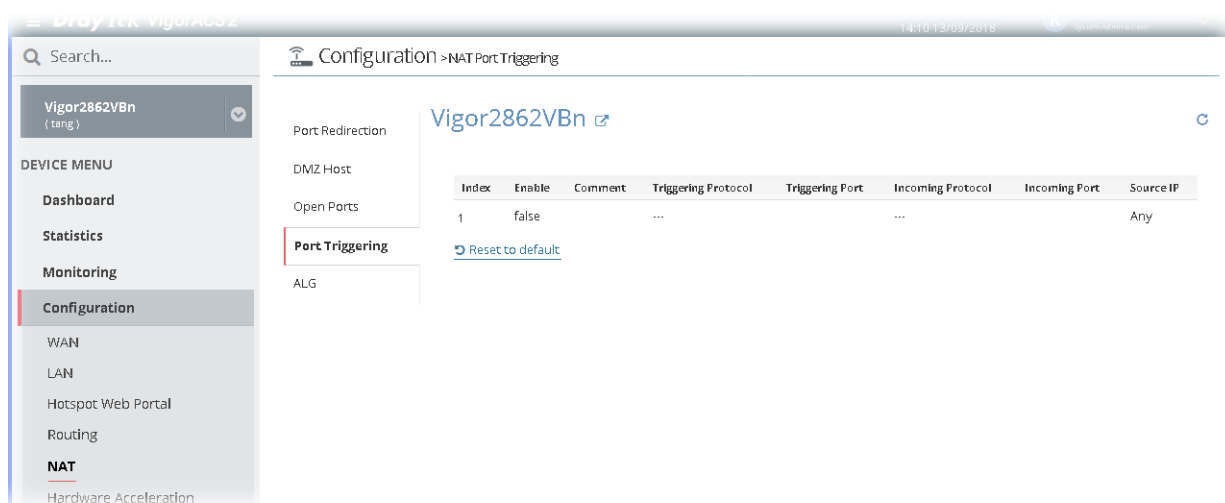


Info

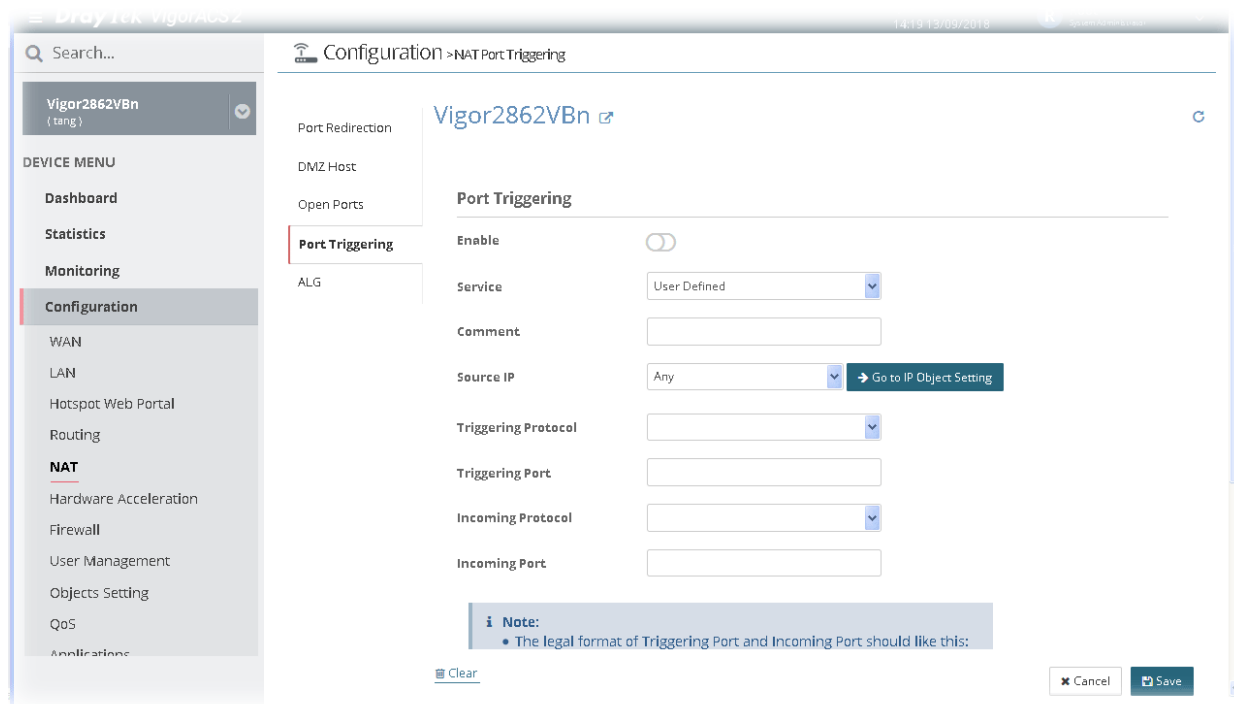
New added profile will be displayed on the top side (index #1) of the page. The default blank profile (index #2) will be moved to the bottom.

13.5.4 Port Triggering

It is a variation of open ports function.



To add a new port triggering profile, move the mouse cursor on the table and click the index number #1 (default blank profile) to get the following page.



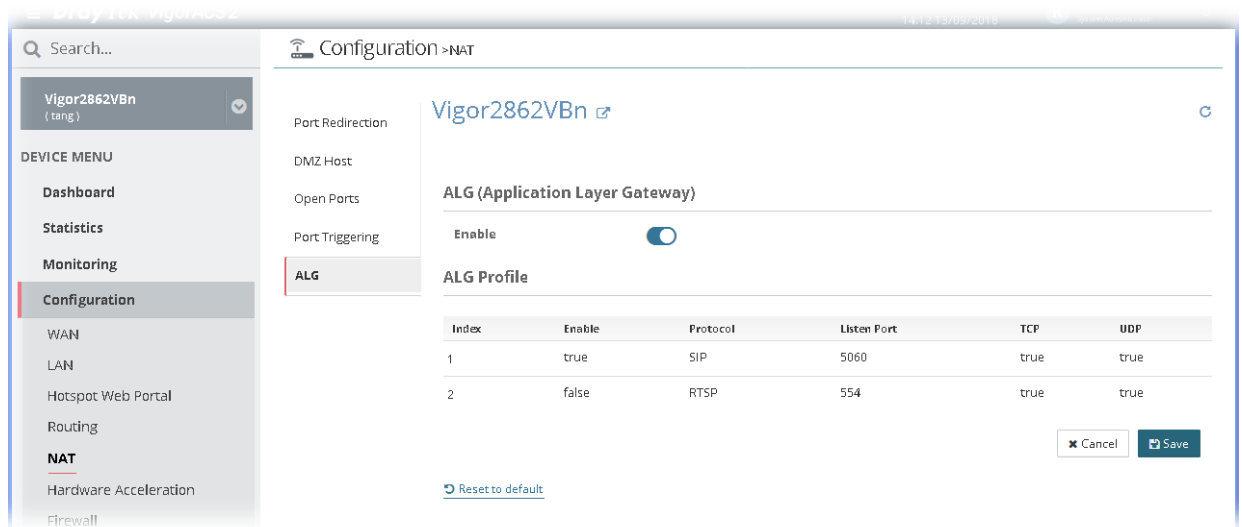
After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

13.5.5 ALG

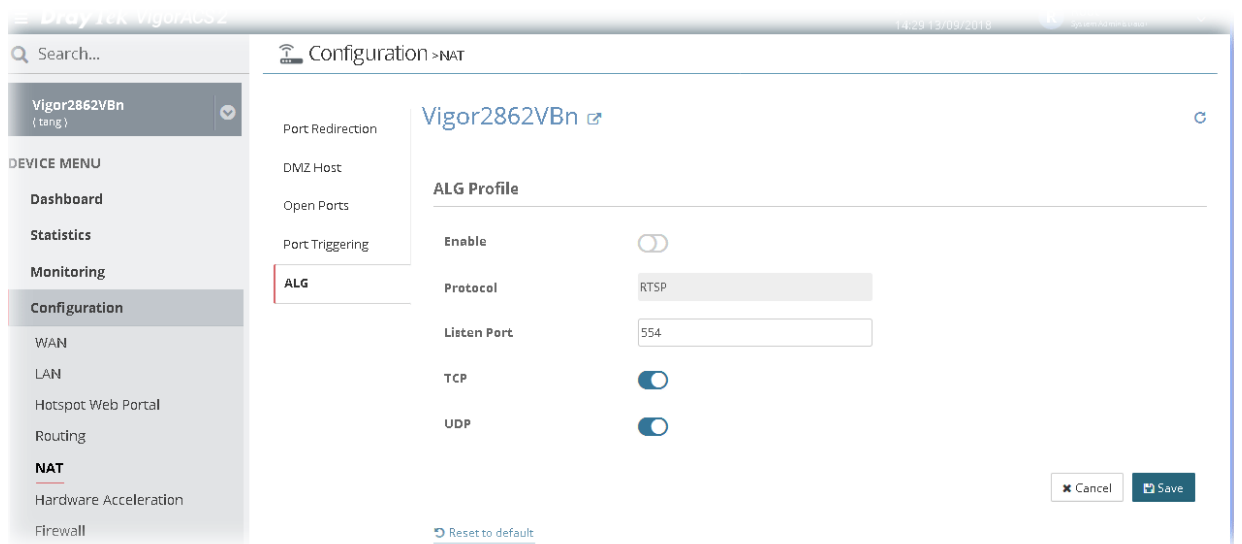
There are two methods provided by Vigor router, RTSP (Real Time Streaming Protocol) ALG and SIP (Session Initiation Protocol) ALG, for processing the packets of voice and video.

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

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



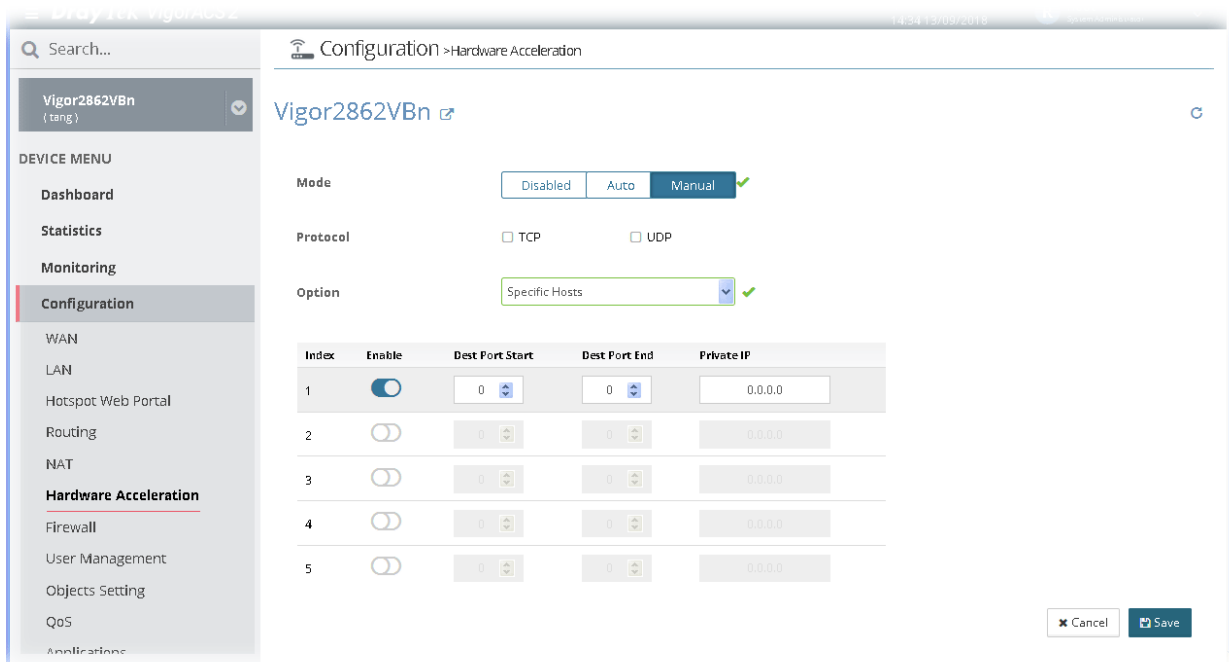
To edit ALG profile, move the mouse cursor on the table and click the index number #1 or 2 to get the following page.



After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.6 Hardware Acceleration Settings for CPE

In such section, Vigor2862VBn is selected as an example for displaying hardware acceleration settings. Hardware Acceleration is also called PPA in DrayTek for it is based on Protocol Processing Engine (PPE) of Infineon. It can only support 128 sessions for network traffic (IN & OUT) with implementing three kinds of modes - Disable, Auto and Manual.



These parameters are explained as follows:

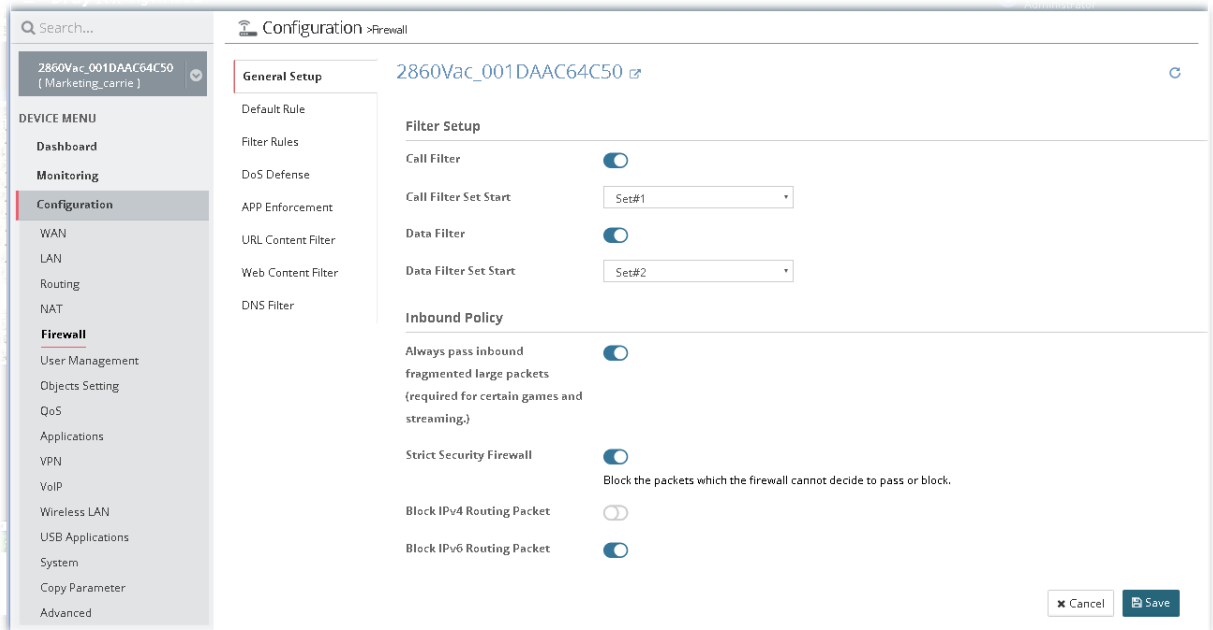
Item	Description
Mode	<p>Disable - The default setting.</p> <p>Auto - When the hardware acceleration is configured with the Auto mode, the sessions with the heaviest loading and the lower latency traffic will be added into PPA. However, the Auto mode does not support UDP protocol by designed.</p> <p>Manual - The Manual mode implements three sub-items-- <i>Accelerate most heavy traffic sessions</i>, <i>Apply the Class Rule in Quality of Service</i>, and <i>Specific Hosts</i>. Each of these sub-items can support TCP and UDP protocol.</p>
Protocol	There are two types supported by this function, TCP and UDP.
Option	<p>Accelerate heaviest traffic sessions - Such option is available in Auto Mode, too. But the UDP protocol is only supported in this sub-item.</p> <p>Apply the Class Rule in Quality of Service - Users can apply the information provided by QoS in this sub-item.</p> <p>Specific Hosts - This sub-item provides 5 hosts for adding NAT sessions into the PPA. For the PPA only supports 128 sessions, these hosts will share these sessions. Therefore, the performance will be lower than only one host.</p> <p>Choose this option to specify certain PCs on LAN to apply the hardware acceleration.</p> <ul style="list-style-type: none"> ● Enable - Check the box to make PC(s) specified in the selected index entry to be applied. ● Dest Port Start - Type the starting port for the PC(s) in LAN. ● Dest Port End - Type the ending port for the PC(s) in LAN. ● Private IP/Choose PC - Type the IP address as the selected host. Or click the Choose PC button to specify one IP address from the pop-up window.

After finished the settings, click **Save**. The modification for the CPE will take effect immediately.

13.7 Firewall Settings for CPE

13.7.1 General Setup

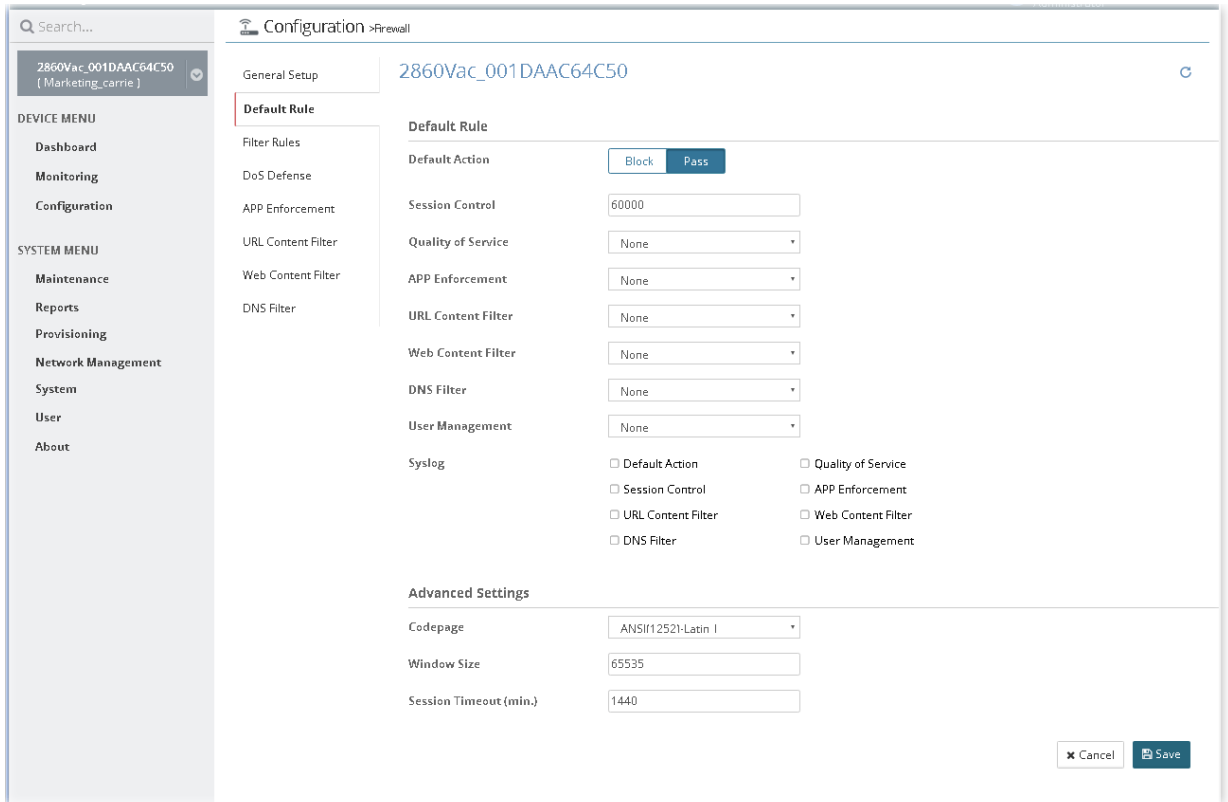
General Setup allows you to adjust settings of IP Filter and common options.



After finished the settings, click Save. And, the modification for the CPE will take effect immediately.

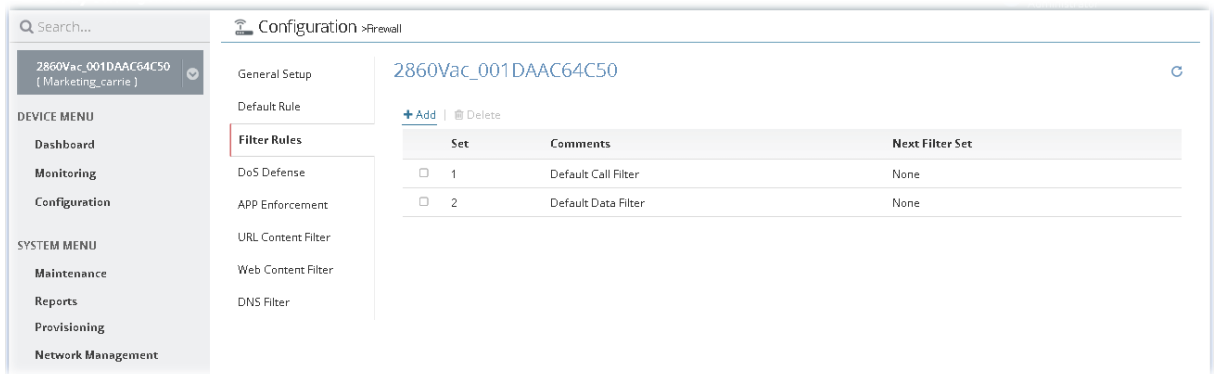
13.7.2 Default Rule

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

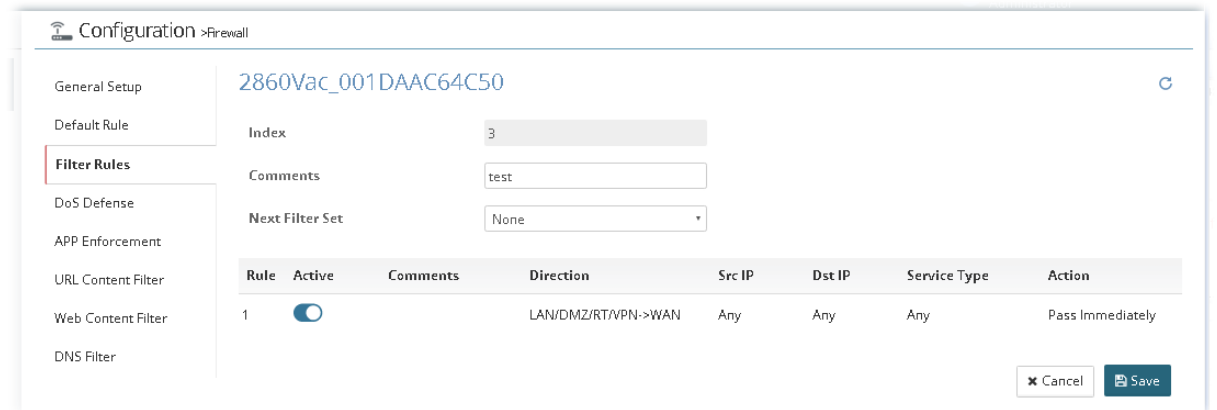


After finished the settings, click Save. And, the modification for the CPE will take effect immediately.

13.7.3 Filter Rules



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



Then, move the mouse cursor on the rule table and click index number #1 to access into next configuration page.

Configuration > Firewall

2860Vac_001DAAC64C50

General Setup
Default Rule
Filter Rules
DoS Defense
APP Enforcement
URL Content Filter
Web Content Filter
DNS Filter

General Settings

Filter Rule: 1

Comments: test_only

Active:

Filter Conditions

Direction: LAN/DMZ/RT/VPN->WAN ✓

Source IP: Subnet Address ✓

Source Start IP: 192.168.2.56 ✓

Source Subnet Mask: 255.255.255.0 ✓

Source Invert Selection:

Destination IP: Subnet Address ✓

Destination Start IP: 192.168.2.100 ✓

Destination Subnet Mask: 255.255.255.0 ✓

Destination Invert Selection:

After finished the settings, click Save.

Configuration > Firewall

2860Vac_001DAAC64C50

General Setup
Default Rule
Filter Rules
DoS Defense
APP Enforcement
URL Content Filter
Web Content Filter
DNS Filter

Index: 3

Comments: test

Next Filter Set: None

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action
1	<input checked="" type="checkbox"/>	test_only	LAN/DMZ/RT/VPN->WAN	192.168.2.56/ 255.255.255.0	192.168.2.100/ 255.255.255.0	Any	Pass Immediat
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN->WAN	Any	Any	Any	Pass Immediat

Cancel Save

And, the modification for the CPE will take effect immediately.

13.7.4 DoS Defense

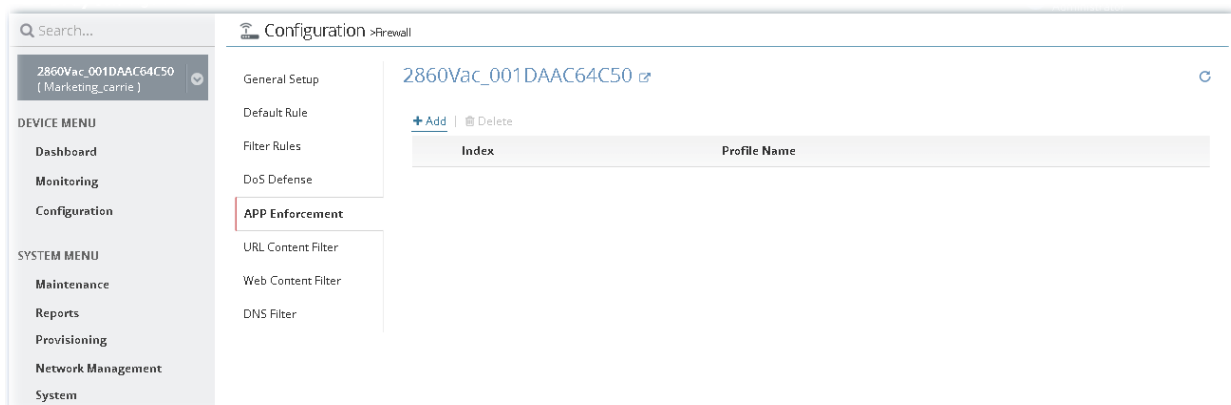
As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the DoS Defense setup. In default, the DoS Defense functionality is disabled.

The screenshot displays the configuration page for DoS Defense on a VigorACS 2 device. The interface includes a search bar at the top left, a breadcrumb trail 'Configuration > Firewall', and a device identifier '2860Vac_001DAAC64C50'. A left-hand navigation menu lists 'DEVICE MENU' (Dashboard, Monitoring, Configuration) and 'SYSTEM MENU' (Maintenance, Reports, Provisioning, Network Management, System, User, About). The main content area is divided into sections: 'General Setup' (DoS Defense:) and 'Flood Defense' (SYN Flood Defense: , SYN Flood Threshold (pkts/sec): 2000, Session Time-Out (sec): 10). Below this is 'Port Scan Detection' (Port Scan Detection: , Port Scan Threshold (pkts/sec): 2000). The 'Others' section contains a 'Select All' button and six individual toggle switches: Block IP Options, Block Land, Block Smurf, Block TCP Flag Scan, Block Tear Drop, and Block Ping of Death.

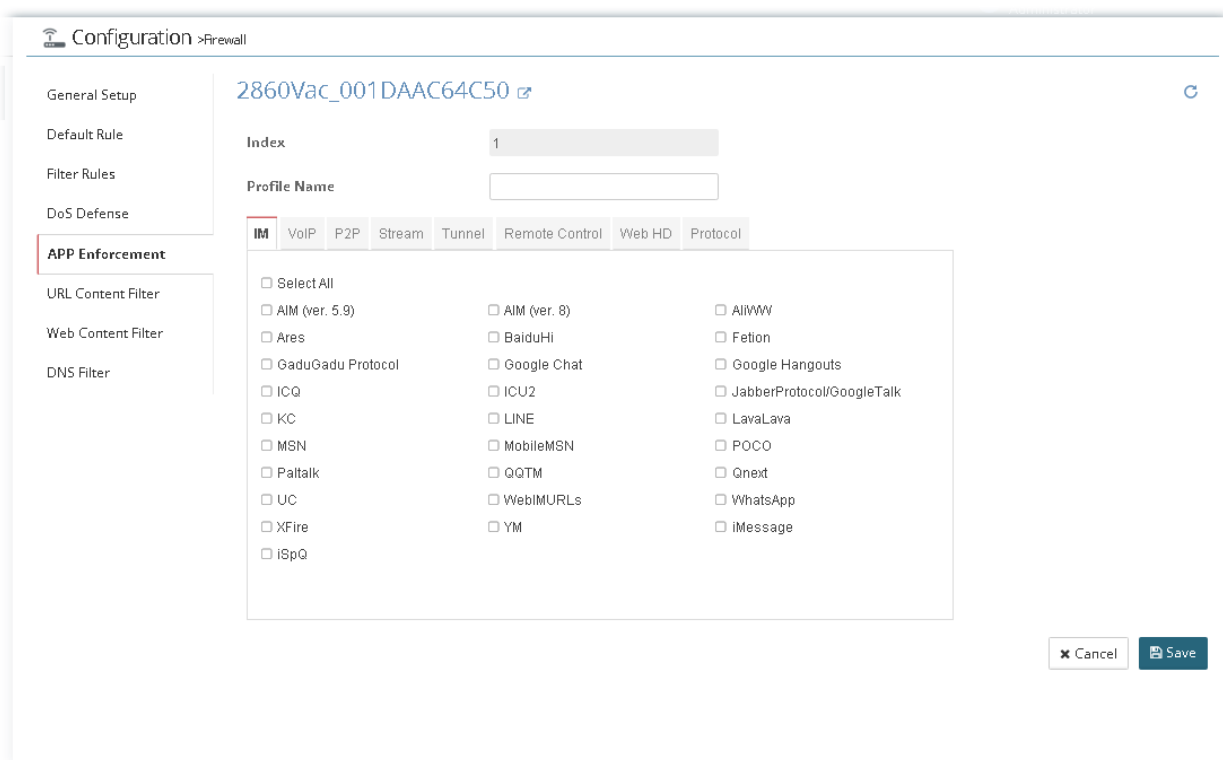
After finished the settings, click Save. And, the modification for the CPE will take effect immediately.

13.7.5 APP Enforcement

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application.



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



After finished the settings, click Save. And, the modification for the CPE will take effect immediately.

13.7.6 URL Content Filter

URL Content Filter not only limits illegal traffic from/to the inappropriate web sites but also prohibits other web feature where malicious code may conceal.

The screenshot shows the configuration page for a URL Content Filter. The left sidebar contains a navigation menu with 'URL Content Filter' highlighted. The main content area shows the configuration for profile '2860Vac_001DAAC64C50'. A table lists the filter rules:

Index	Profile Name	URL Access Control	URL Access Control Action	Web Feature	Web Feature Action
1		false	Pass	false	Pass

Below the table, there is an 'Administration Message' field containing the following text:


```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

 At the bottom right, there are buttons for 'Default Message' and 'Save'.

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

The screenshot shows the configuration page for adding a new filter rule profile. The left sidebar contains a navigation menu with 'URL Content Filter' highlighted. The main content area shows the configuration for profile '2860Vac_001DAAC64C50'. The 'Add' form includes the following fields:

- Index: 1
- Profile Name: URL_Game
- Priority: Either : URL Access Control Fir
- Log: None

The 'URL Access Control' section is expanded, showing:

- URL Access Control:
- Prevent web access from IP address:
- Action: Block (selected), Pass

Below the form, there are two tables for adding keyword objects and groups:

Index	Keyword Object	Action
1	None	+Add

Index	Keyword Group	Action
1	None	+Add

The 'Web Feature' section is also visible at the bottom.

After finished the settings, click Save. And, the modification for the CPE will take effect immediately.

Configuration > Firewall

2860Vac_001DAAC64C50

+ Add | Delete

Index	Profile Name	URL Access Control	URL Access Control Action	Web Feature	Web Feature Action	
<input checked="" type="checkbox"/>	1	URL_Game	true	Pass	false	Pass

Administration Message

```
<body><center><br><br><p>The requested Web page has been blocked by URL Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

Default Message Save

13.7.7 Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats.

Search...

Configuration > Firewall

2860Vac_001DAAC64C50 (Marketing_carrie)

General Setup

Default Rule

Filter Rules

DoS Defense

APP Enforcement

URL Content Filter

Web Content Filter

DNS Filter

2860Vac_001DAAC64C50

+ Add | Delete

Index	Profile Name	Log	Action	Black/White List:Action	
<input type="checkbox"/>	1	Default	Block	Block	Block

Administration Message

```
<body><center><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

Legend:
 %SIP% - Source IP, %DIP% - Destination IP, %URL% - URL
 %CL% - Category, %RNAME% - Router Name

Default Message Save

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

Configuration > Firewall

2860Vac_001DAAC64C50

General Setup
Default Rule
Filter Rules
DoS Defense
APP Enforcement
URL Content Filter
Web Content Filter
DNS Filter

Index: 2

Profile Name: For_children ✓

Syslog: Block

Action: Block Pass

White/Black List

Black/White List:

Action: Block Pass

Index	Keyword Object	Action
1	None	+Add

Index	Keyword Group	Action
1	None	+Add

Category Selection Select / Clear All

Child Protection Alcohol & Tobacco Criminal Activity
 Gambling Hate & Intolerance
 Illegal Drug Nudity

After finished the settings, click **Save**. And, the modification for the CPE will take effect immediately.

2860Vac_001DAAC64C50

+Add | Delete

Index	Profile Name	Log	Action	Black/White List:Action
<input type="checkbox"/>	1	Default	Block	Block
<input type="checkbox"/>	2	For_children	Block	Block

Administration Message

<body><center>

<p>The requested Web page
 from %SIP%
to %URL%
that is categorized with %CL%
has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>

Legend:
 %SIP% - Source IP, %DIP% - Destination IP, %URL% - URL
 %CL% - Category, %RNAME% - Router Name

Default Message Save

13.7.8 DNS Filter

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

The screenshot shows the 'DNS Filter Local Setting' configuration page for device 2860Vac_001DAAC64C50. The page is divided into a left sidebar with navigation options and a main content area. The main content area includes a table of DNS filter rules, a 'DNS Filter Local Setting' section with toggle and dropdown menus, and an 'Administration Message' section with a text editor and a legend.

Index	Profile Name	DNS Syslog	DNS WCF	DNS UCF
1		None	None	None

DNS Filter Local Setting

DNS Filter:

Syslog:

UCF:

WCF:

Administration Message

```
<body><center><br><br><p>The requested Web page <br> from %SIP% <br> to %URL% <br> that is categorized with %CL% <br> has been blocked by %RNAME% DNS Filter.<p>Please contact your system administrator for further information.</center></body>
```

Legend:
 %SIP% - Source IP, %URL% - URL
 %CL% - Category, %RNAME% - Router Name

Buttons: Default Message, Save

DNS Filter Local Setting will be applied to DNS query from clients on LAN when router's DNS server is used.

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

The screenshot shows the 'Add New DNS Filter Rule' configuration page. The 'Profile Name' field is set to 'DNS_Market' and has a green checkmark. The 'Syslog' dropdown is set to 'ALL', 'UCF' is set to 'UCF-1 URL Game', and 'WCF' is set to 'WCF-2 For children'.

Buttons: Cancel, Save

After finished the settings, click **Save**. And, the modification for the CPE will take effect immediately.

The screenshot shows the DNS Filter configuration page after saving the new rule. The table now includes the 'DNS_Market' profile.

Index	Profile Name	DNS Syslog	DNS WCF	DNS UCF
1	DNS_Market	ALL	WCF-2 For_children	UCF-1 URL_Game

DNS Filter Local Setting

DNS Filter:

13.8 User Management Settings for CPE

User Management is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password. Instead of managing with IP address/MAC address, User Management function manages hosts with user account. Network administrator can give different firewall policies or rules for different hosts with different User Management accounts. This is more flexible and convenient for network management. Not only offering the basic checking for Internet access, User Management also provides additional firewall rules, e.g. CSM checking for protecting hosts.

13.8.1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.

The screenshot shows the 'General Setup' page for a user profile named '2860Vac_001DAAC64C50'. The 'Mode Selection' section has 'Rule-Based' selected. The 'Authentication page' section includes 'Web Authentication' (HTTP and HTTPS), 'Login Page Logo' (Default and Blank), 'Login Page Greeting', and 'Display IP Enable' (disabled). The 'Landing page' section contains a JavaScript snippet for displaying the IP address on the dialog box after a successful login. Buttons for 'Cancel' and 'Save' are visible at the bottom right.

After finished the settings, click **Save**. And, the modification for the CPE will take effect immediately.

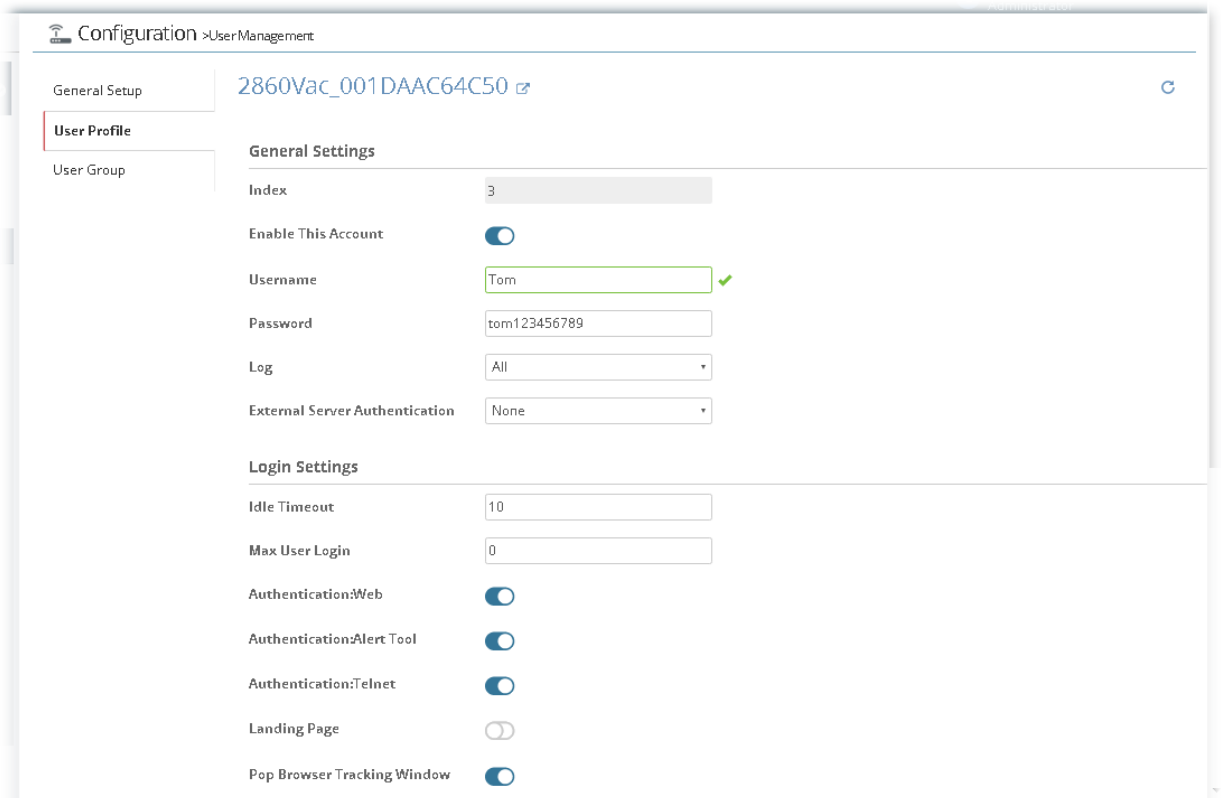
13.8.2 User Profile

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under User Management.

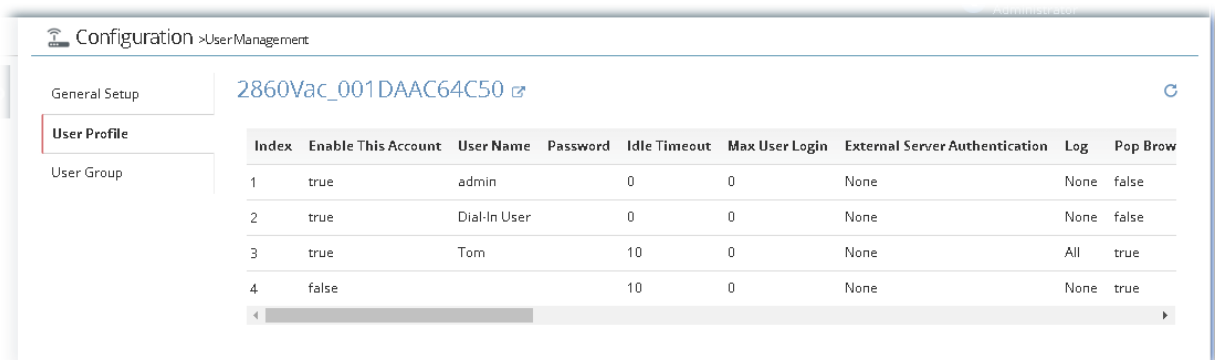
The screenshot shows the 'User Profile' page for the same user profile. It displays a table with the following data:

Index	Enable This Account	User Name	Password	Idle Timeout	Max User Login	External Server Authentication	Log	Pop Brow
1	true	admin		0	0	None	None	false
2	true	Dial-In User		0	0	None	None	false
3	false			10	0	None	None	true

To add a new profile, move the mouse cursor on the table and click the index number #3 (index #1 and index #2 are factory default settings) to get the following page.

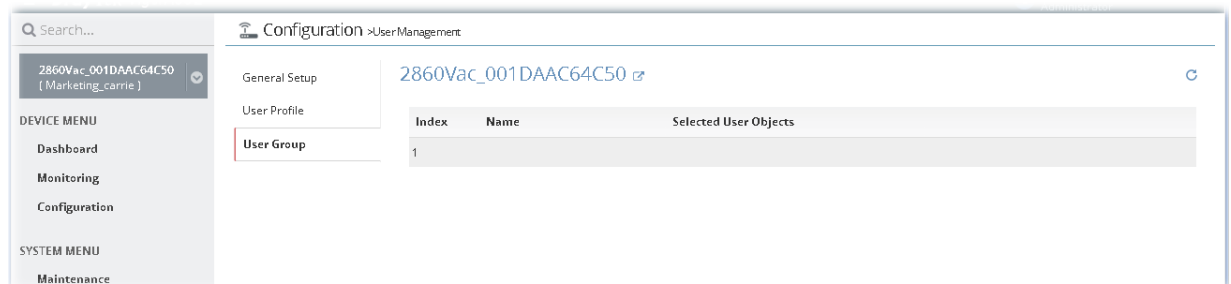


After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

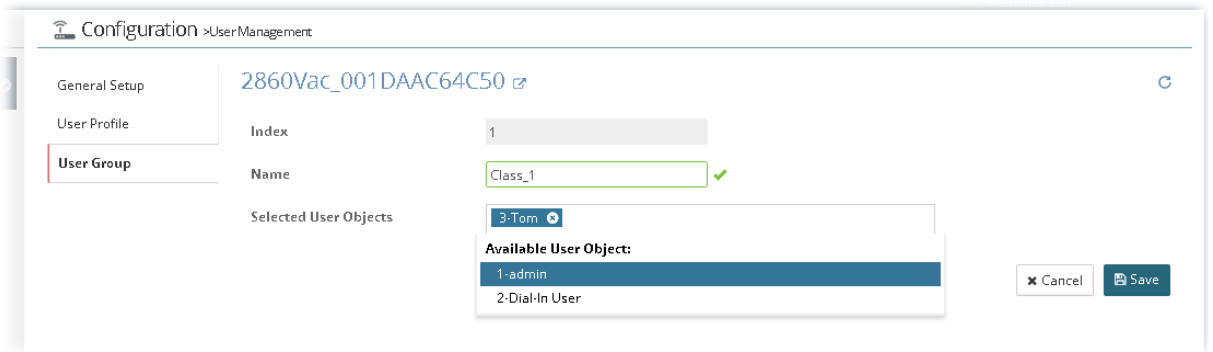


13.8.3 User Group

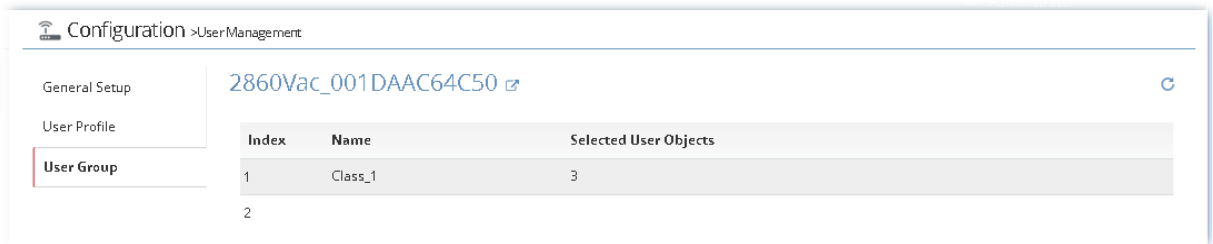
This page allows you to bind several user profiles into one group.



To add a new profile, move the mouse cursor on the table and click the index number #1 to get the following page.



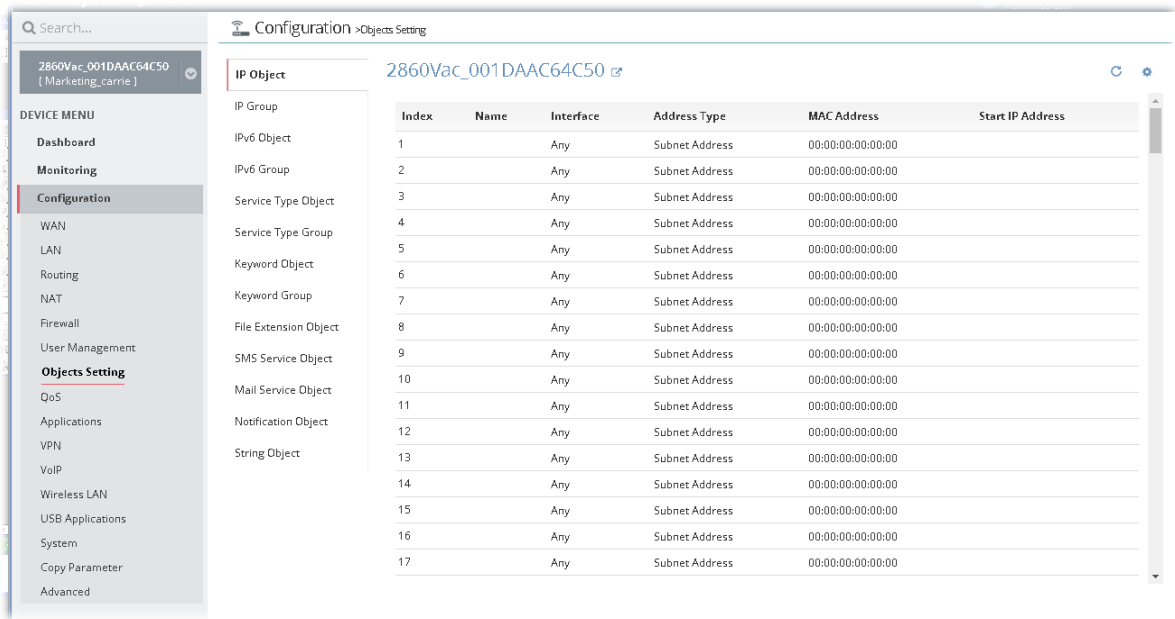
After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.



13.9 Modifying Objects Settings for CPE

13.9.1 Create / Edit an IP Object Profile

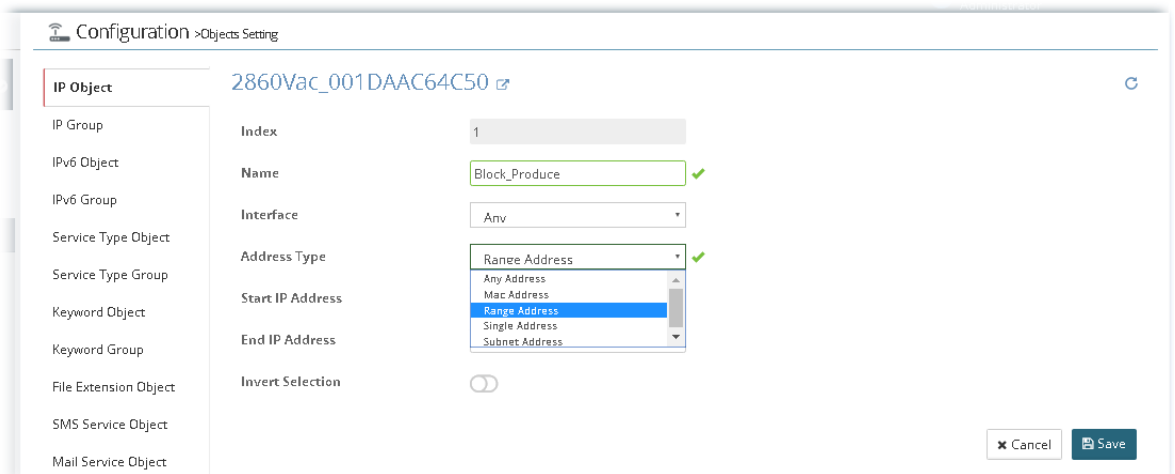
For IPs in a range in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* for using conveniently. Later, we can select that object that can apply it.



The screenshot shows the 'IP Object' configuration page for the object '2860Vac_001DAAC64C50'. A table lists 17 existing objects with their respective settings.

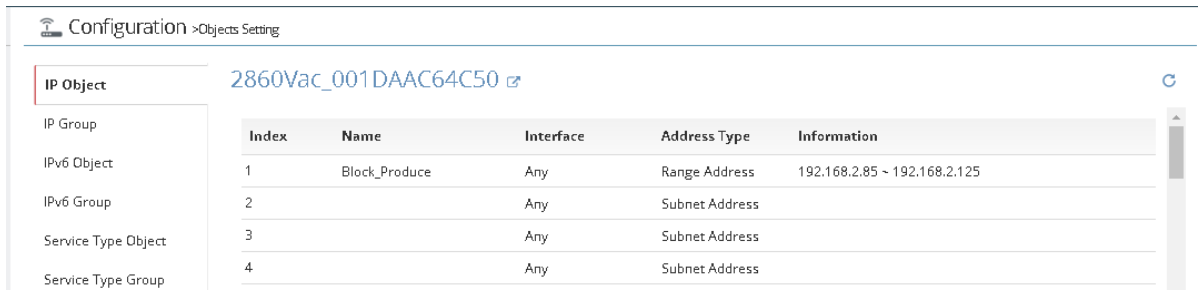
Index	Name	Interface	Address Type	MAC Address	Start IP Address
1		Any	Subnet Address	00:00:00:00:00:00	
2		Any	Subnet Address	00:00:00:00:00:00	
3		Any	Subnet Address	00:00:00:00:00:00	
4		Any	Subnet Address	00:00:00:00:00:00	
5		Any	Subnet Address	00:00:00:00:00:00	
6		Any	Subnet Address	00:00:00:00:00:00	
7		Any	Subnet Address	00:00:00:00:00:00	
8		Any	Subnet Address	00:00:00:00:00:00	
9		Any	Subnet Address	00:00:00:00:00:00	
10		Any	Subnet Address	00:00:00:00:00:00	
11		Any	Subnet Address	00:00:00:00:00:00	
12		Any	Subnet Address	00:00:00:00:00:00	
13		Any	Subnet Address	00:00:00:00:00:00	
14		Any	Subnet Address	00:00:00:00:00:00	
15		Any	Subnet Address	00:00:00:00:00:00	
16		Any	Subnet Address	00:00:00:00:00:00	
17		Any	Subnet Address	00:00:00:00:00:00	

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.



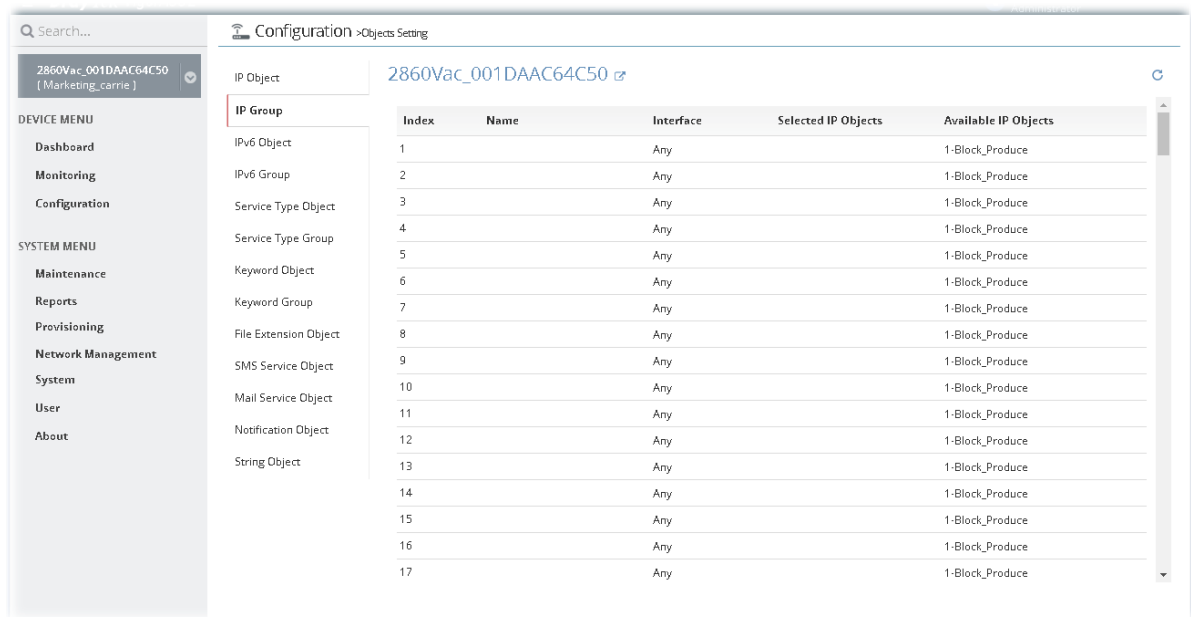
The screenshot shows the edit form for the IP Object profile at index 1. The form includes fields for Name, Interface, Address Type, Start IP Address, End IP Address, and Invert Selection. The 'Name' field is set to 'Block_Produce', the 'Interface' is 'Any', and the 'Address Type' is 'Range Address'. The 'Start IP Address' and 'End IP Address' fields are empty. The 'Invert Selection' checkbox is unchecked. There are 'Cancel' and 'Save' buttons at the bottom right.

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

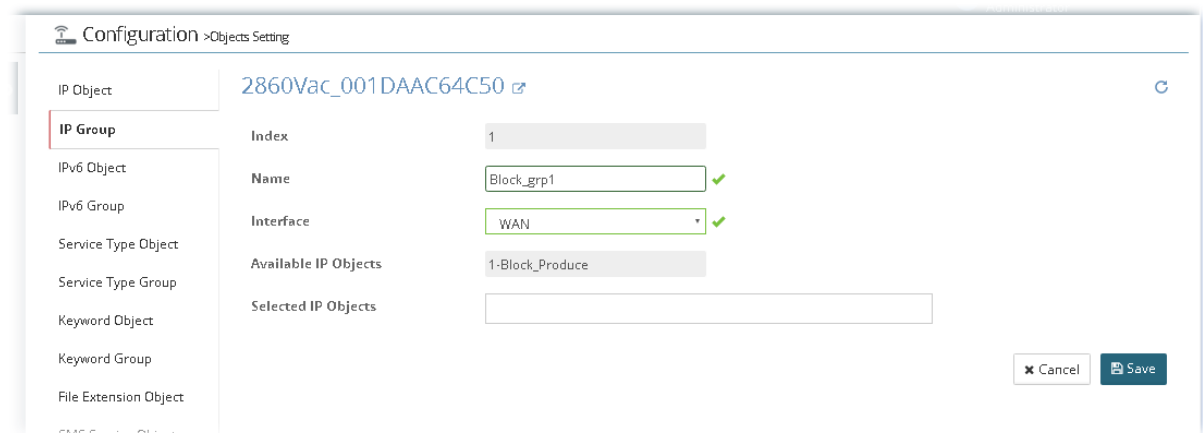


13.9.2 Create / Edit an IP Group Profile

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. Later, we can select that object/group for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

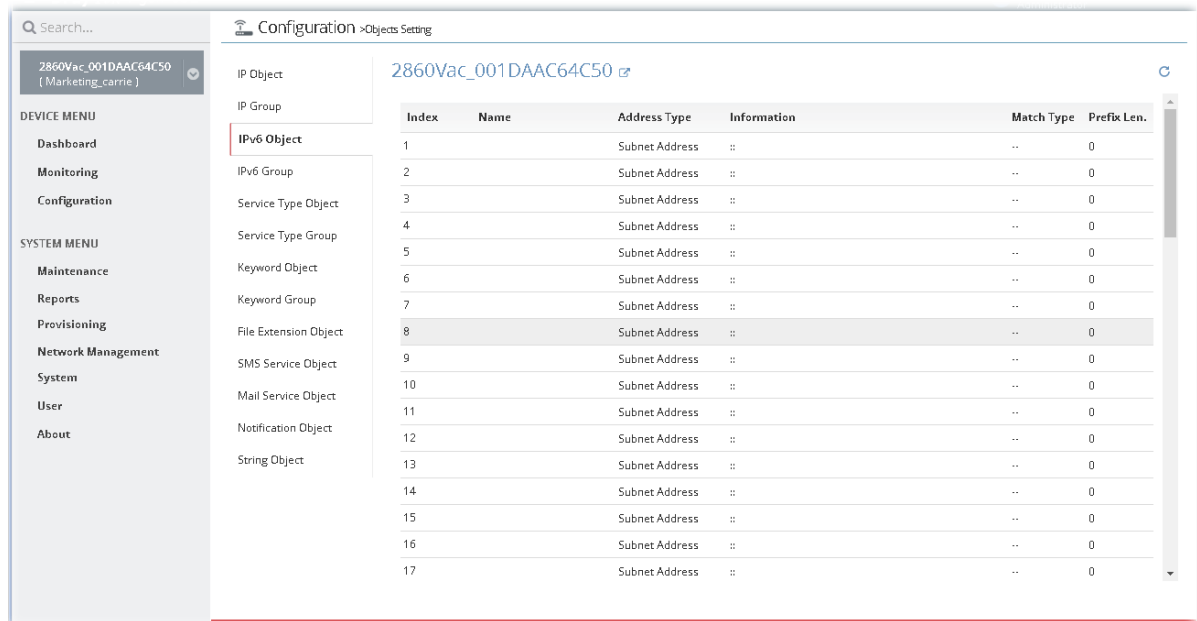


To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

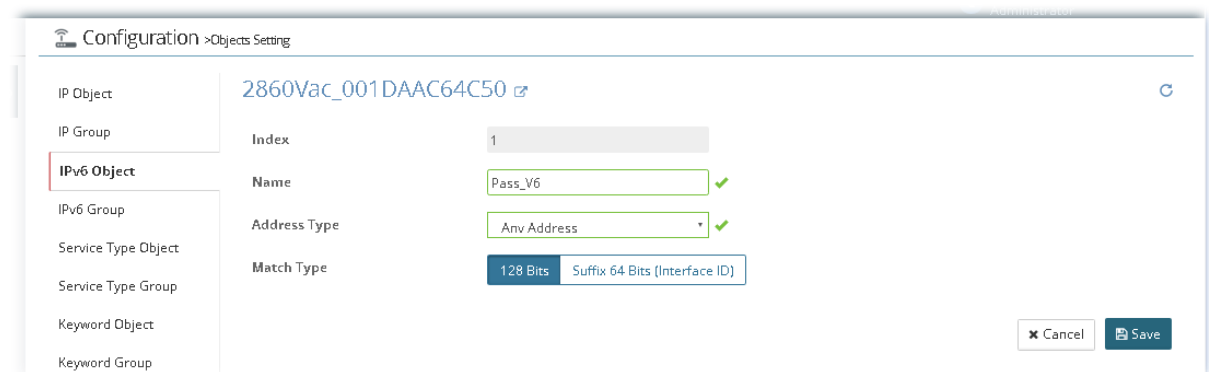


After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

13.9.3 Create / Edit an IPv6 Object Profile

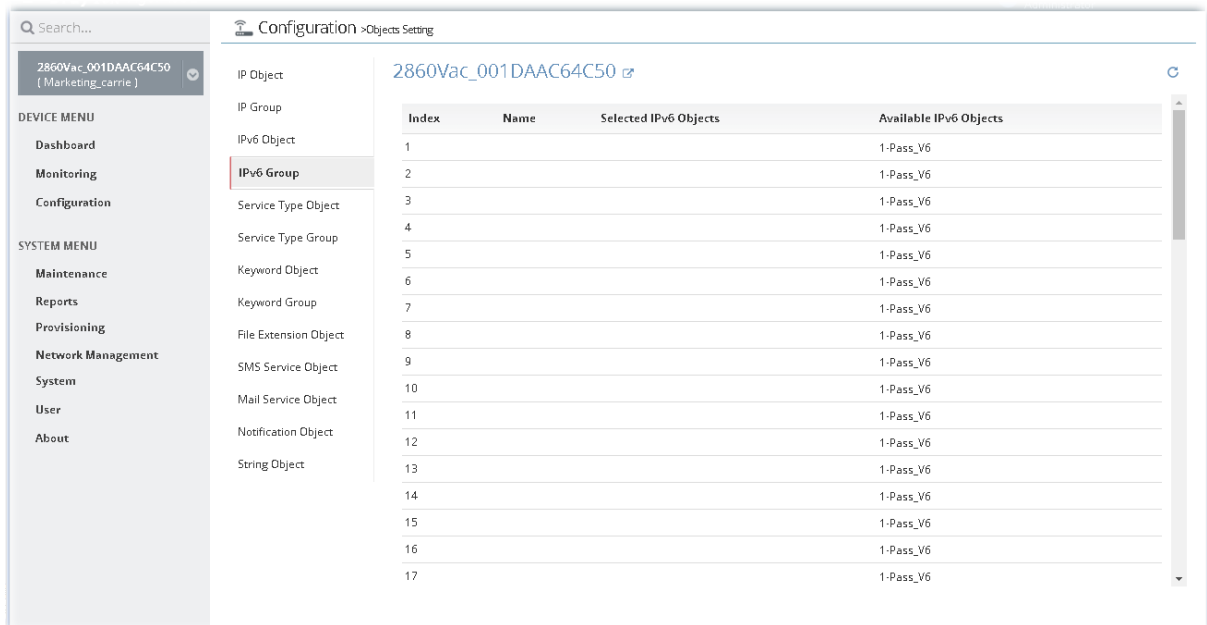


To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.



After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

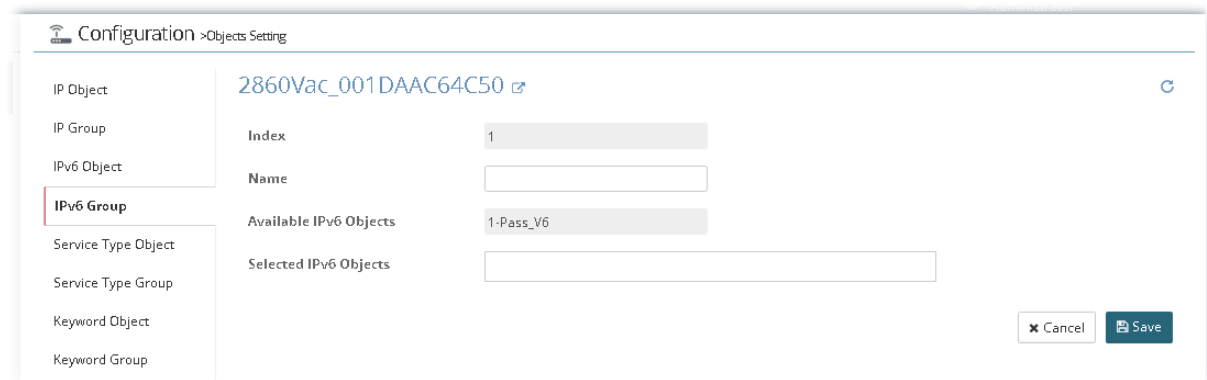
13.9.4 Create / Edit an IPv6 Group Profile



The screenshot shows the configuration page for an IPv6 Group. The breadcrumb is Configuration > Objects Setting. The page title is 2860Vac_001DAAC64C50. The left sidebar contains a menu with sections: DEVICE MENU (Dashboard, Monitoring, Configuration), SYSTEM MENU (Maintenance, Reports, Provisioning, Network Management, System, User, About), and a search bar. The main content area shows a table with the following data:

Index	Name	Selected IPv6 Objects	Available IPv6 Objects
1			1-Pass_V6
2			1-Pass_V6
3			1-Pass_V6
4			1-Pass_V6
5			1-Pass_V6
6			1-Pass_V6
7			1-Pass_V6
8			1-Pass_V6
9			1-Pass_V6
10			1-Pass_V6
11			1-Pass_V6
12			1-Pass_V6
13			1-Pass_V6
14			1-Pass_V6
15			1-Pass_V6
16			1-Pass_V6
17			1-Pass_V6

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.



The screenshot shows the configuration page for an IPv6 Group in edit mode. The breadcrumb is Configuration > Objects Setting. The page title is 2860Vac_001DAAC64C50. The left sidebar contains a menu with sections: DEVICE MENU (Dashboard, Monitoring, Configuration), SYSTEM MENU (Maintenance, Reports, Provisioning, Network Management, System, User, About), and a search bar. The main content area shows the following form:

Index:

Name:

Available IPv6 Objects:

Selected IPv6 Objects:

Buttons:

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

13.9.5 Create / Edit a Service Type Object Profile

Configuration > Objects Setting

2860Vac_001DAAC64C50 [Marketing_carrie]

DEVICE MENU

- Dashboard
- Monitoring
- Configuration

SYSTEM MENU

- Maintenance
- Reports
- Provisioning
- Network Management
- System
- User
- About

IP Object

- IP Group
- IPv6 Object
- IPv6 Group
- Service Type Object**
- Service Type Group
- Keyword Object
- Keyword Group
- File Extension Object
- SMS Service Object
- Mail Service Object
- Notification Object
- String Object

2860Vac_001DAAC64C50

Index	Name	Protocol	Protocol Number	Source Port Option	Source Port From
1		Any	0	=	0
2		Any	0	=	0
3		Any	0	=	0
4		Any	0	=	0
5		Any	0	=	0
6		Any	0	=	0
7		Any	0	=	0
8		Any	0	=	0
9		Any	0	=	0
10		Any	0	=	0
11		Any	0	=	0
12		Any	0	=	0
13		Any	0	=	0
14		Any	0	=	0
15		Any	0	=	0
16		Any	0	=	0
17		Any	0	=	0

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

Configuration > Objects Setting

2860Vac_001DAAC64C50

IP Object

- IP Group
- IPv6 Object
- IPv6 Group
- Service Type Object**
- Service Type Group
- Keyword Object
- Keyword Group
- File Extension Object
- SMS Service Object
- Mail Service Object
- Notification Object
- String Object

Index: 1

Name: RD1_2 ✓

Protocol: TCP/UDP ✓

Source Port Option: =

Source Port From: 0

Source Port To: 0

Destination Port Option: =

Destination Port From: 0

Destination Port To: 0

Cancel Save

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

Configuration > Objects Setting

2860Vac_001DAAC64C50

IP Object

- IP Group
- IPv6 Object
- IPv6 Group
- Service Type Object**
- Service Type Group

Index	Name	Protocol	Protocol Number	Source Port Option	Source Port From
1	RD1_2	TCP/UDP	255	=	50
2		Any	0	=	0
3		Any	0	=	0
4		Any	0	=	0

13.9.6 Create / Edit a Service Type Group Profile

The screenshot shows the 'Configuration > Objects Setting' page. On the left, there is a sidebar with 'DEVICE MENU' and 'SYSTEM MENU'. The main content area shows a list of object types on the left and a table of 'Service Type Group' profiles on the right. The table has the following data:

Index	Name	Available Service Type Objects	Selected Service Type Objects
1		1-RD1_2	
2		1-RD1_2	
3		1-RD1_2	
4		1-RD1_2	
5		1-RD1_2	
6		1-RD1_2	
7		1-RD1_2	
8		1-RD1_2	
9		1-RD1_2	
10		1-RD1_2	
11		1-RD1_2	
12		1-RD1_2	
13		1-RD1_2	
14		1-RD1_2	
15		1-RD1_2	
16		1-RD1_2	
17		1-RD1_2	

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

The screenshot shows the 'Configuration > Objects Setting' page with the edit form for a Service Type Group profile. The form fields are:

- Index: 1
- Name: Development (with a green checkmark)
- Available Service Type Objects: 1-RD1_2
- Selected Service Type Objects: 1-RD1_2 (with a dropdown arrow)

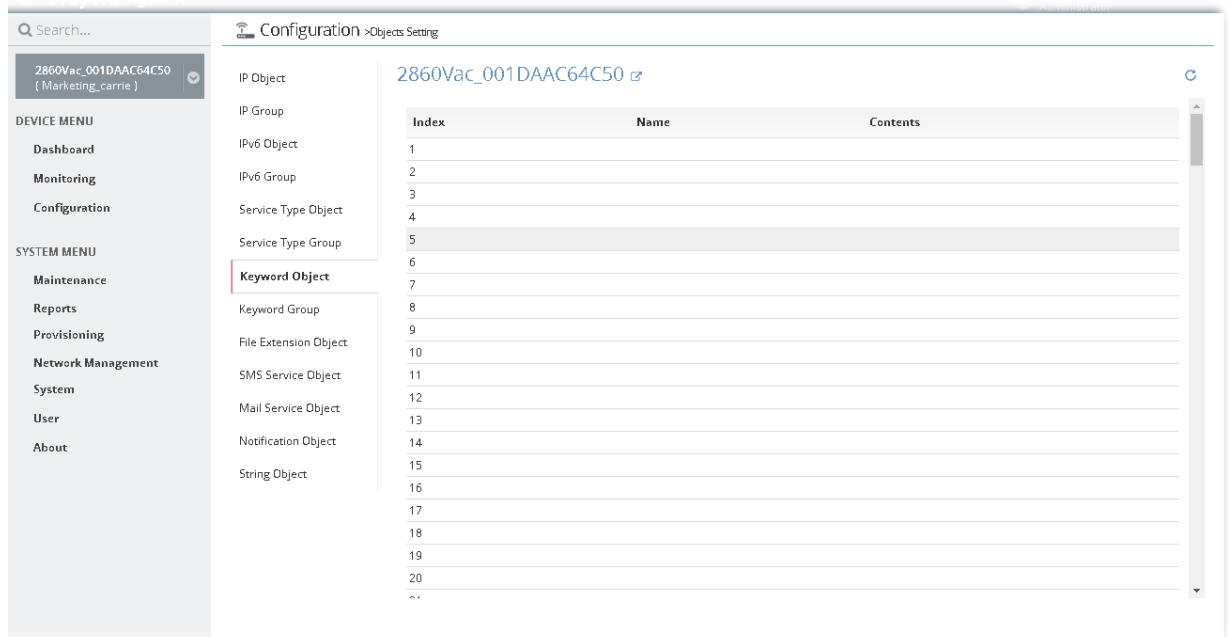
At the bottom right, there are 'Cancel' and 'Save' buttons.

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

The screenshot shows the 'Configuration > Objects Setting' page with the updated table of Service Type Group profiles. The table now includes the newly created profile:

Index	Name	Available Service Type Objects	Selected Service Type Objects
1	Development	1-RD1_2	1
2		1-RD1_2	
3		1-RD1_2	
4		1-RD1_2	

13.9.7 Create / Edit a Keyword Object Profile



Configuration > Objects Setting

2860Vac_001DAAC64C50 (Marketing_carrie)

DEVICE MENU

- Dashboard
- Monitoring
- Configuration

SYSTEM MENU

- Maintenance
- Reports
- Provisioning
- Network Management
- System
- User
- About

IP Object

IP Group

IPv6 Object

IPv6 Group

Service Type Object

Service Type Group

Keyword Object

Keyword Group

File Extension Object

SMS Service Object

Mail Service Object

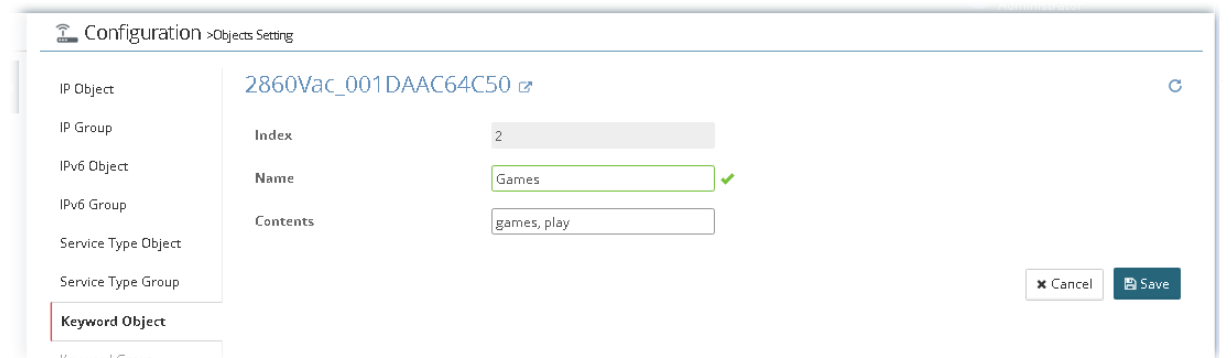
Notification Object

String Object

2860Vac_001DAAC64C50

Index	Name	Contents
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
~		

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.



Configuration > Objects Setting

2860Vac_001DAAC64C50

IP Object

IP Group

IPv6 Object

IPv6 Group

Service Type Object

Service Type Group

Keyword Object

Keyword Group

Index: 2

Name: Games ✓

Contents: games, play

Cancel Save

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.



Configuration > Objects Setting

2860Vac_001DAAC64C50

IP Object

IP Group

IPv6 Object

IPv6 Group

Service Type Object

Service Type Group

Index	Name	Contents
1		
2	Games	games, play
3		
4		
5		

13.9.8 Create / Edit a Keyword Group Profile

The screenshot shows the configuration page for profile 2860Vac_001DAAC64C50. On the left is a navigation menu with sections for DEVICE MENU (Dashboard, Monitoring, Configuration), SYSTEM MENU (Maintenance, Reports, Provisioning, Network Management, System), User, and About. The main area shows a list of object types on the left and a table of objects on the right.

Index	Name	Available Keyword Objects	Selected Keyword Objects
1		2-Games	
2		2-Games	
3		2-Games	
4		2-Games	
5		2-Games	
6		2-Games	
7		2-Games	
8		2-Games	
9		2-Games	
10		2-Games	
11		2-Games	
12		2-Games	
13		2-Games	
14		2-Games	
15		2-Games	
16		2-Games	
17		2-Games	

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

The screenshot shows the edit form for profile 2860Vac_001DAAC64C50. The left navigation menu is visible, with 'Keyword Group' selected. The form fields are:

- Index: 1
- Name: Children_1_18 (with a green checkmark)
- Available Keyword Objects: 2-Games
- Selected Keyword Objects: 2-Games (with a dropdown arrow)

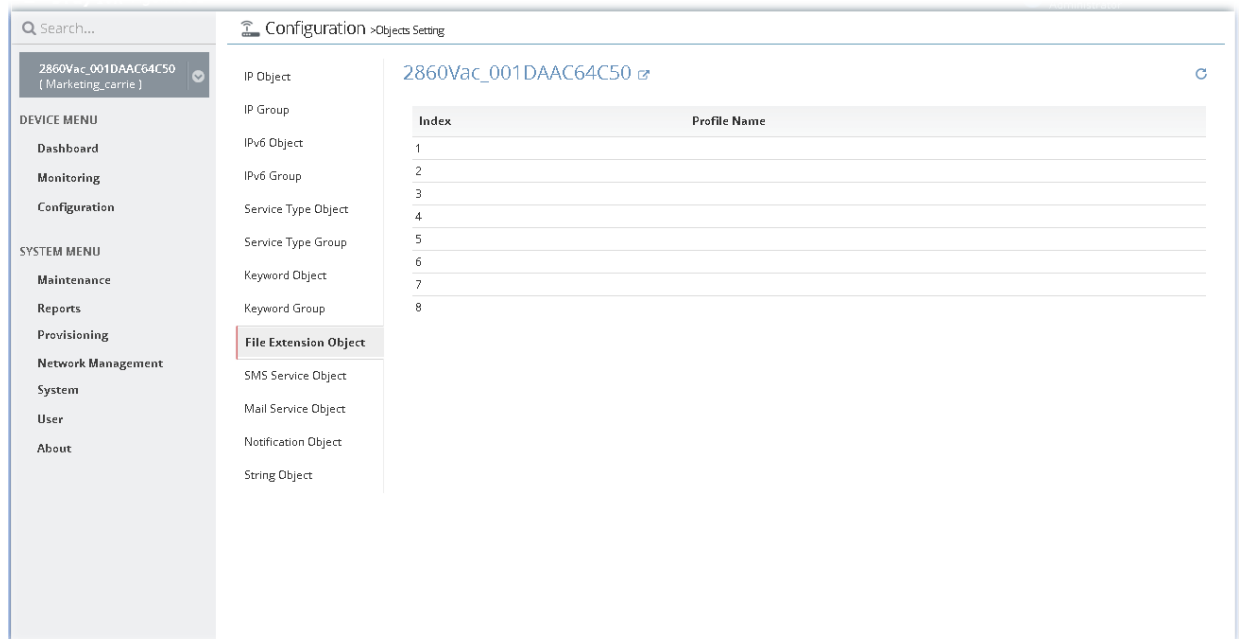
Buttons for 'Cancel' and 'Save' are located at the bottom right of the form.

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

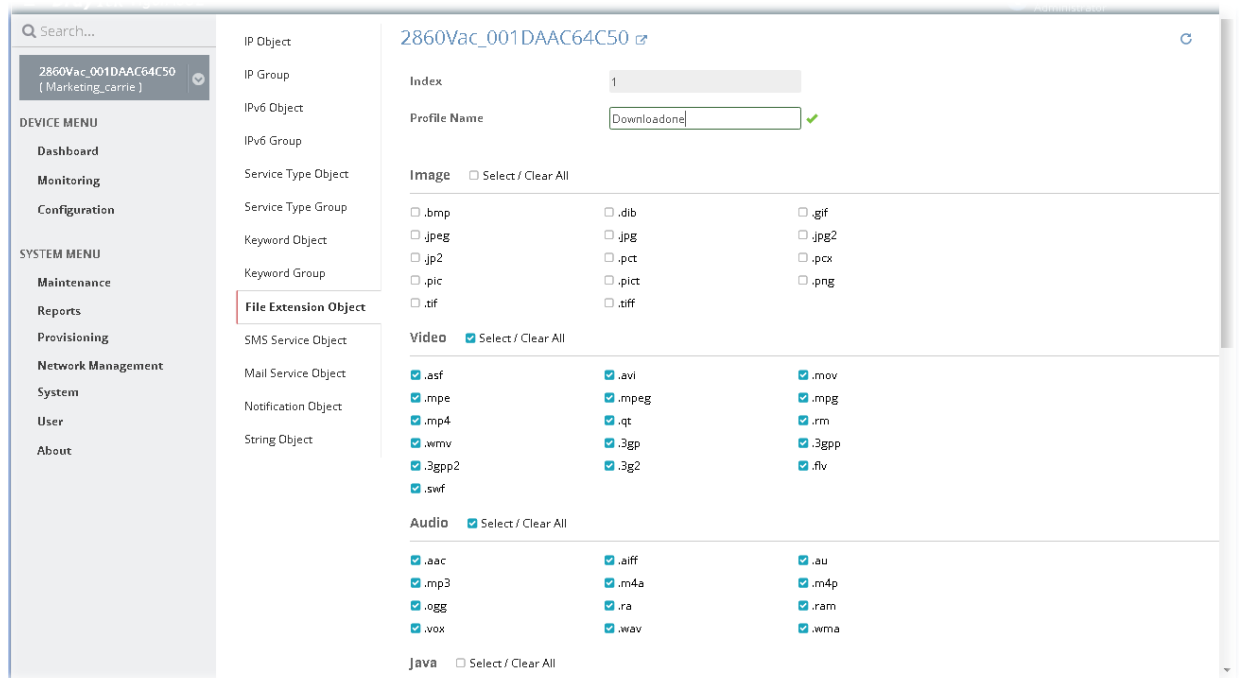
The screenshot shows the updated configuration page for profile 2860Vac_001DAAC64C50. The table now shows the new profile configuration:

Index	Name	Available Keyword Objects	Selected Keyword Objects
1	Children_1_18	2-Games	2
2		2-Games	
3		2-Games	
4		2-Games	

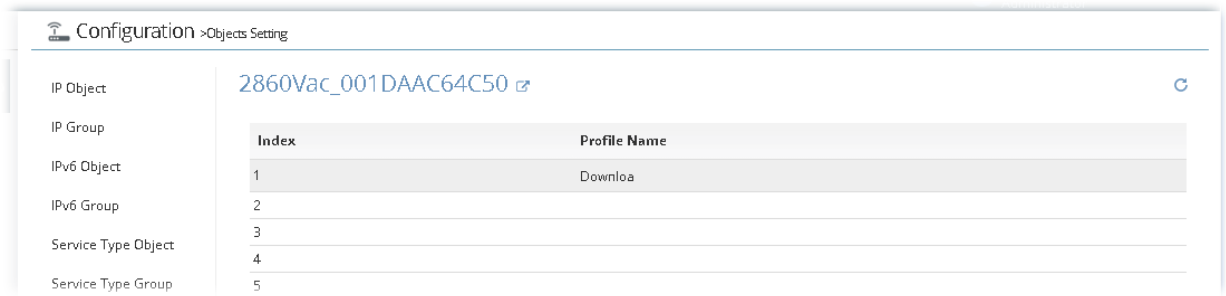
13.9.9 Create / Edit a File Extension Object Profile



To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

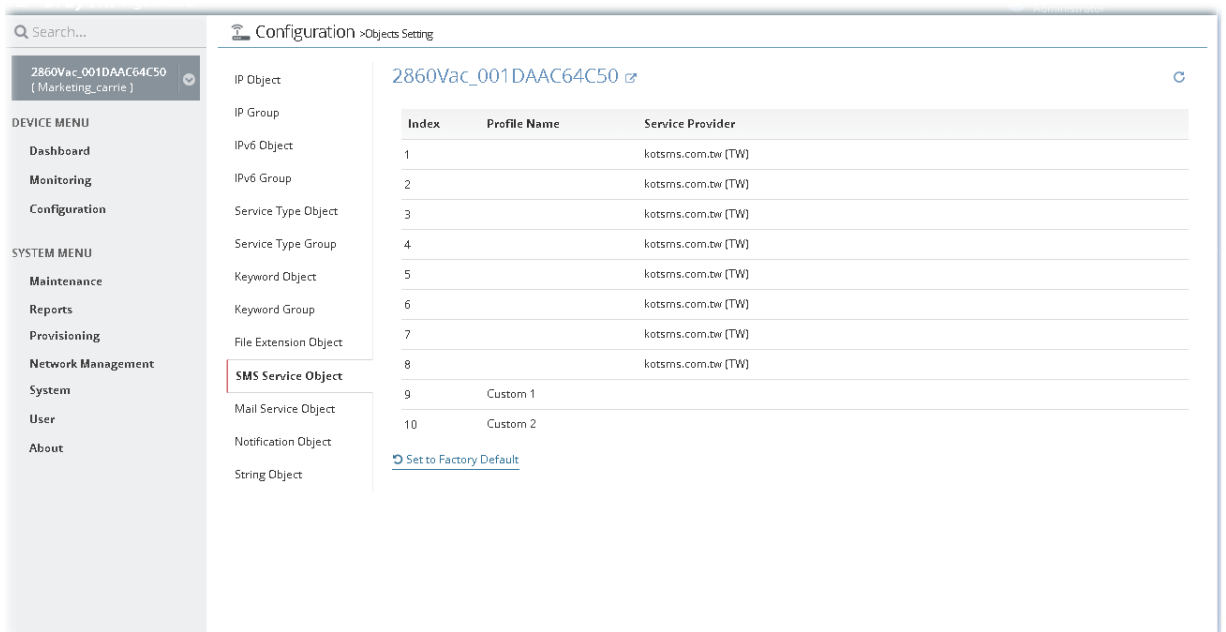


After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.



13.9.10 Create / Edit a SMS Service Object Profile

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.



To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

Configuration > Objects Setting

2860Vac_001DAAC64C50

Index: 2

Profile Name: school ✓

Service Provider: kotsms.com.tw (TW)

Username: adminadmin

Password: 12345admin

Quota: 10

Sending Interval: 3

Note:

- Only one message can be sent during the "Sending Interval" time.
- If the "Sending Interval" was set to 0, there will be no limitation.

Clear Cancel Save

After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

Configuration > Objects Setting

2860Vac_001DAAC64C50

Index	Profile Name	Service Provider
1		kotsms.com.tw (TW)
2	school	kotsms.com.tw (TW)
3		kotsms.com.tw (TW)
4		kotsms.com.tw (TW)

13.9.11 Create / Edit a Mail Service Object Profile

Configuration > Objects Setting

2860Vac_001DAAC64C50

Mail Service Object

Index	Profile Name	SMTP Service	SMTP Port	Sender Address
1			0	
2			0	
3			0	
4			0	
5			0	
6			0	
7			0	
8			0	
9			0	
10			0	

Set to Factory Default

To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

Configuration > Objects Setting

2860Vac_001DAAC64C50

IP Object

IP Group

IPv6 Object

IPv6 Group

Service Type Object

Service Type Group

Keyword Object

Keyword Group

File Extension Object

SMS Service Object

Mail Service Object

Notification Object

String Object

Index: 1

Profile Name: marketing18 ✓

SMTP Service: 172.16.3.8

SMTP Port: 100 ✓

Sender Address: carrie_ni@draytek.com

Use SSL:

Authentication:

Username: mail12345

Password: pass112233

Sending Interval: 10 ✓

Note:

- Only one mail can be sent during the "Sending Interval" time.
- If the "Sending Interval" was set to 0, there will be no limitation.

Clear

Cancel Save

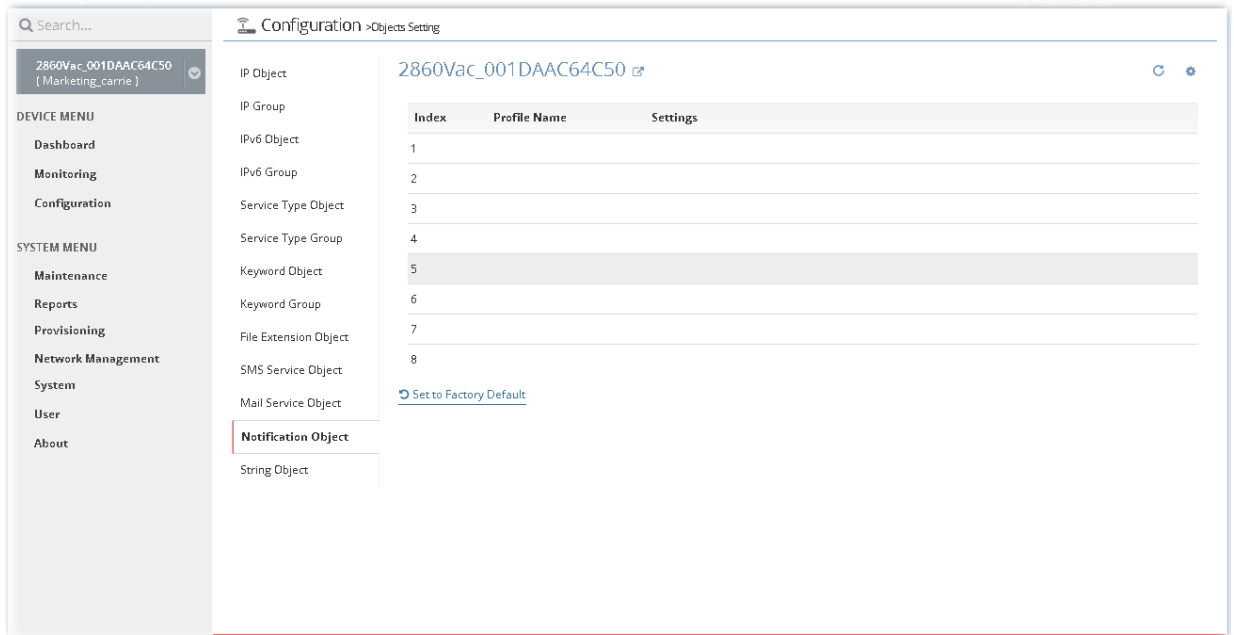
After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

Configuration > Objects Setting

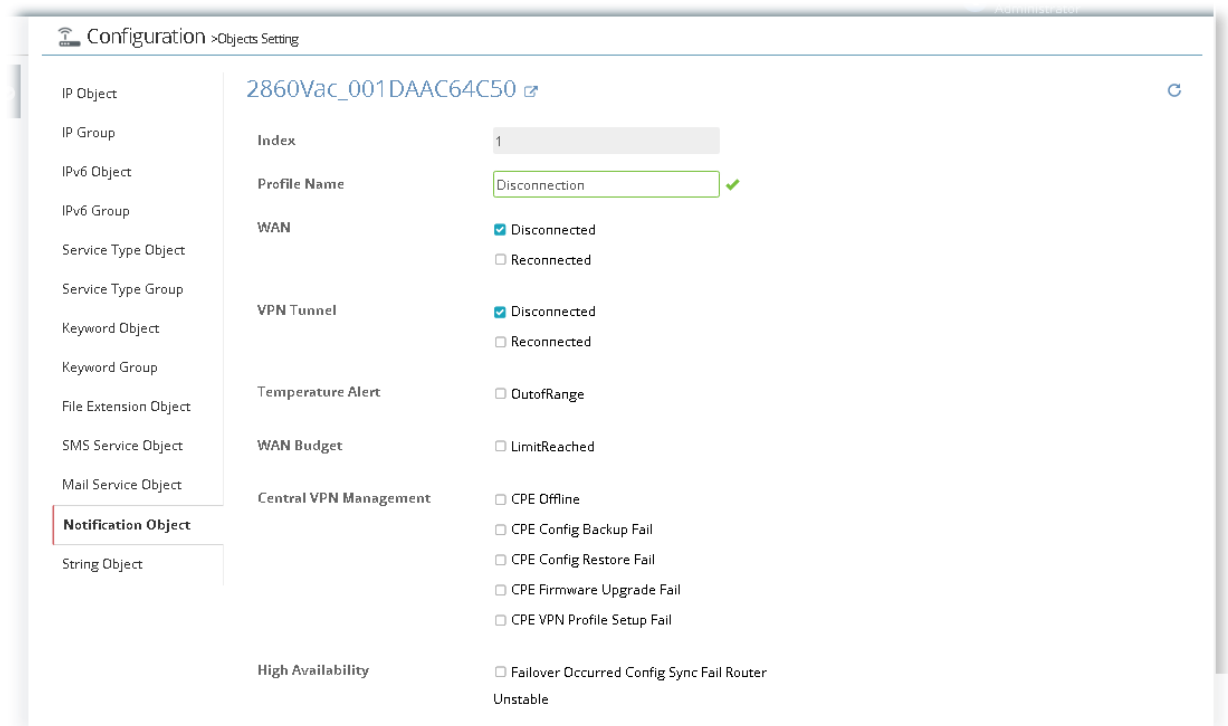
2860Vac_001DAAC64C50

Index	Profile Name	SMTP Service	SMTP Port	Sender Address
1	marketing18	172.16.3.8	100	carrie_ni@draytek.com
2			0	
3			0	
4			0	

13.9.12 Create / Edit a Notification Object Profile

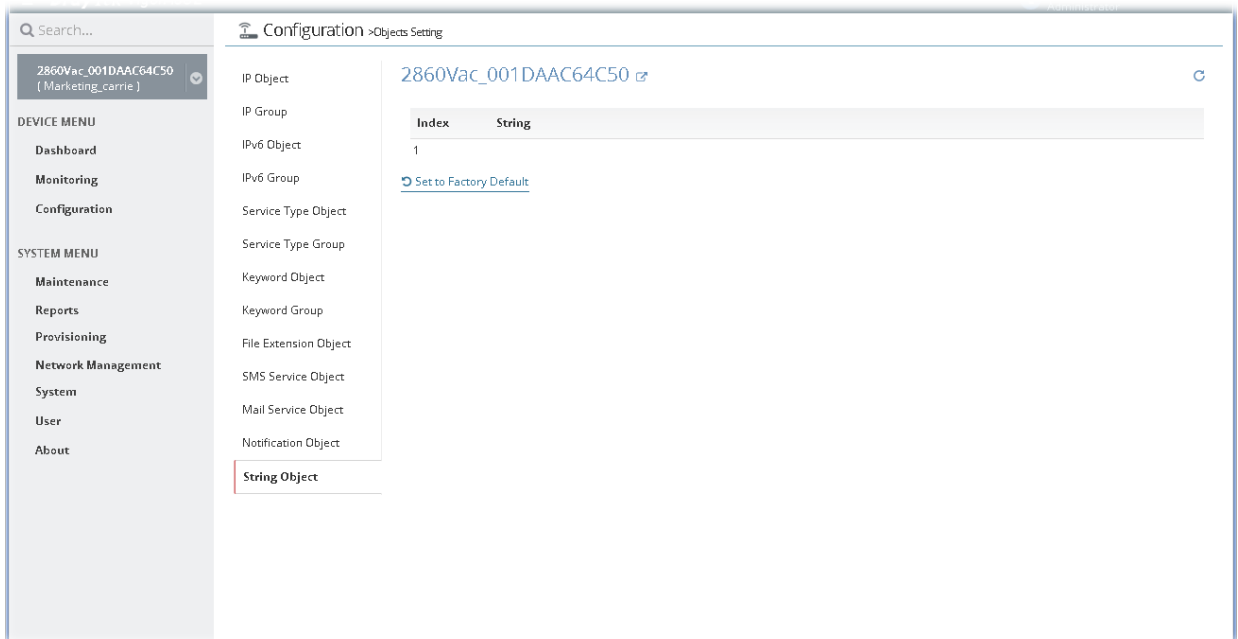


To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.

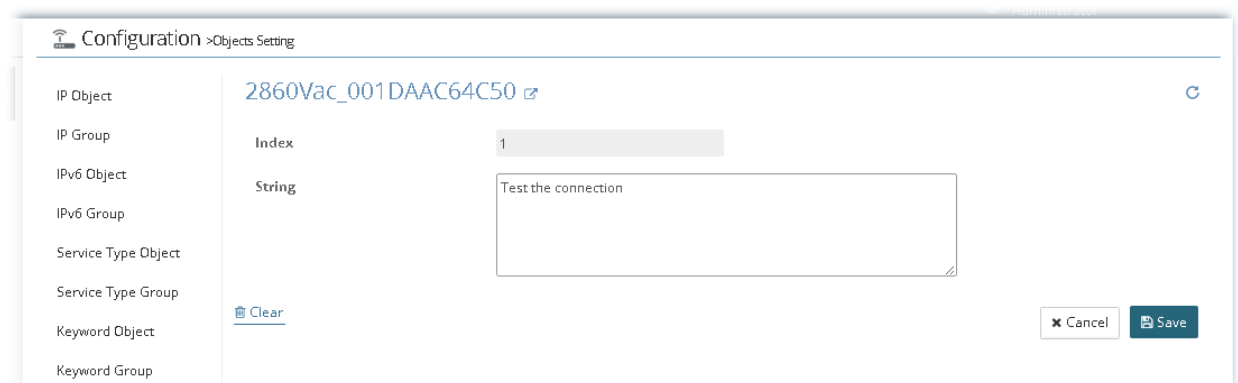


After finished the settings, click **Save**. A new profile has been created. And, the modification for the CPE will take effect immediately.

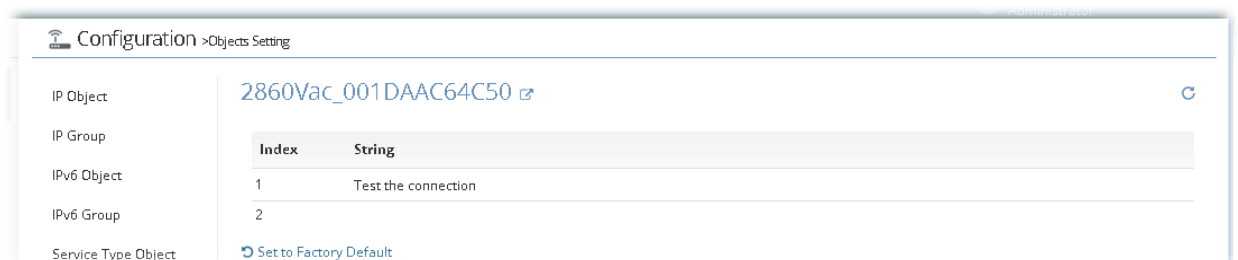
13.9.13 Create / Edit a String Object



To add a new profile or edit an existing profile, move the mouse cursor on the table and click the index number to get the following page.



After finished the settings, click Save. A new profile has been created. And, the modification for the CPE will take effect immediately.

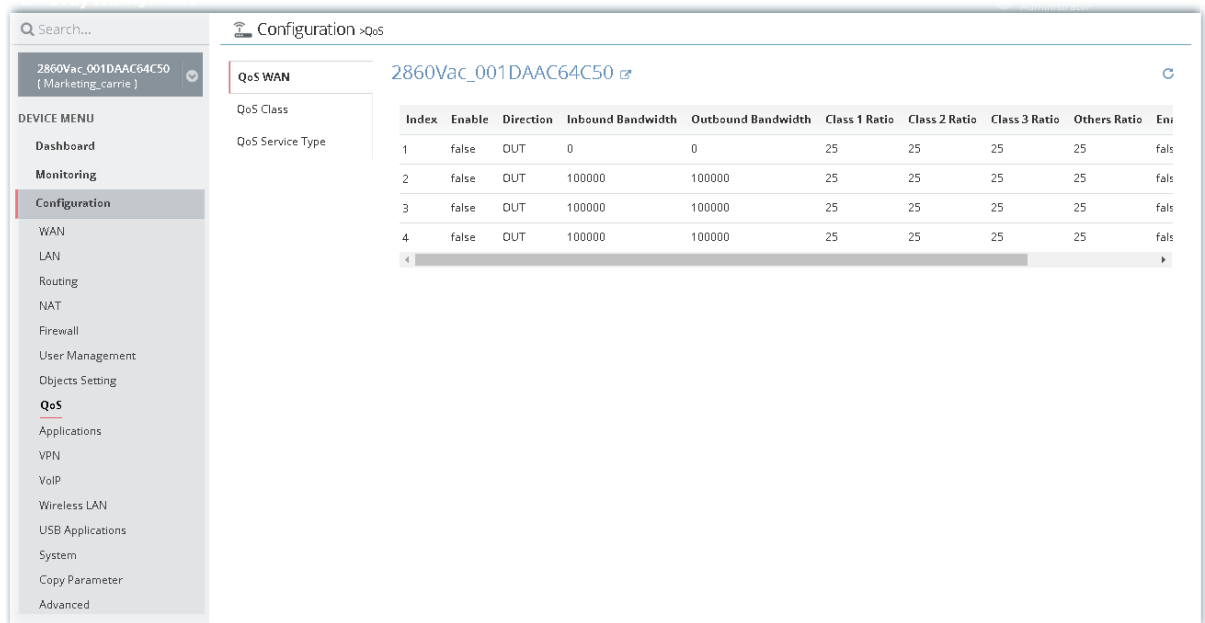


13.10 QoS Settings for CPE

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

13.10.1 QoS WAN

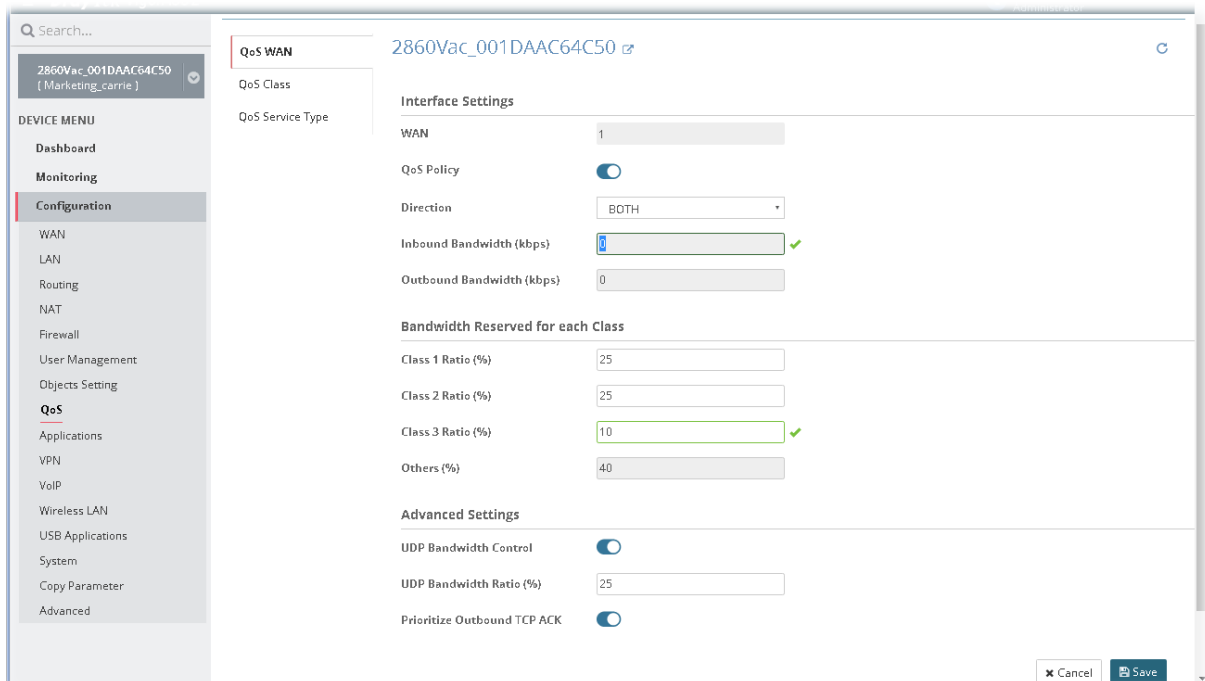
This page allows you to configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control.



The screenshot shows the configuration page for QoS WAN on a device. The left sidebar contains a 'DEVICE MENU' with options like Dashboard, Monitoring, Configuration, WAN, LAN, Routing, NAT, Firewall, User Management, Objects Setting, QoS, Applications, VPN, VoIP, Wireless LAN, USB Applications, System, Copy Parameter, and Advanced. The main content area is titled 'Configuration > qos' and '2860Vac_001DAAC64C50'. It displays a table of QoS classes with the following data:

Index	Enable	Direction	Inbound Bandwidth	Outbound Bandwidth	Class 1 Ratio	Class 2 Ratio	Class 3 Ratio	Others Ratio	Eni
1	false	OUT	0	0	25	25	25	25	fals
2	false	OUT	100000	100000	25	25	25	25	fals
3	false	OUT	100000	100000	25	25	25	25	fals
4	false	OUT	100000	100000	25	25	25	25	fals

To edit the parameters settings for each WAN (index #1 to 4), move the mouse cursor on the table and click the index number to get the following page.



The screenshot shows the detailed configuration page for QoS WAN on a device. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Configuration > qos' and '2860Vac_001DAAC64C50'. It displays the following settings:

Interface Settings

- WAN: 1
- QoS Policy:
- Direction: BOTH
- Inbound Bandwidth (kbps): 0
- Outbound Bandwidth (kbps): 0

Bandwidth Reserved for each Class

- Class 1 Ratio (%): 25
- Class 2 Ratio (%): 25
- Class 3 Ratio (%): 10
- Others (%): 40

Advanced Settings

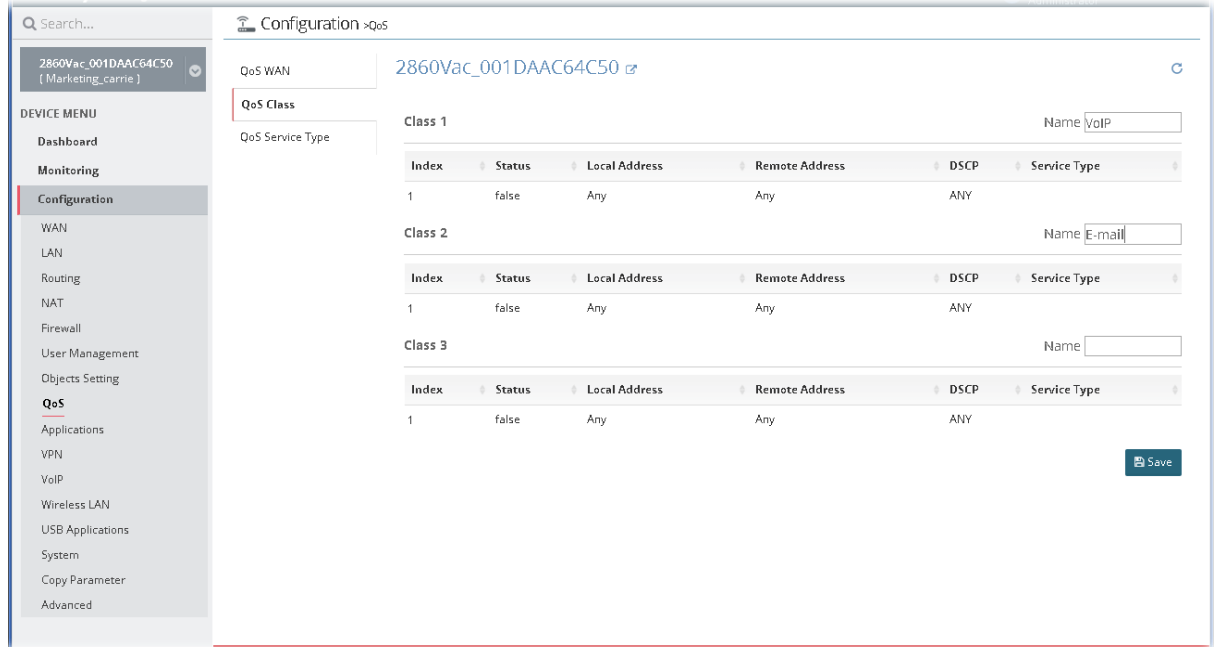
- UDP Bandwidth Control:
- UDP Bandwidth Ratio (%): 25
- Prioritize Outbound TCP ACK:

Buttons: Cancel, Save

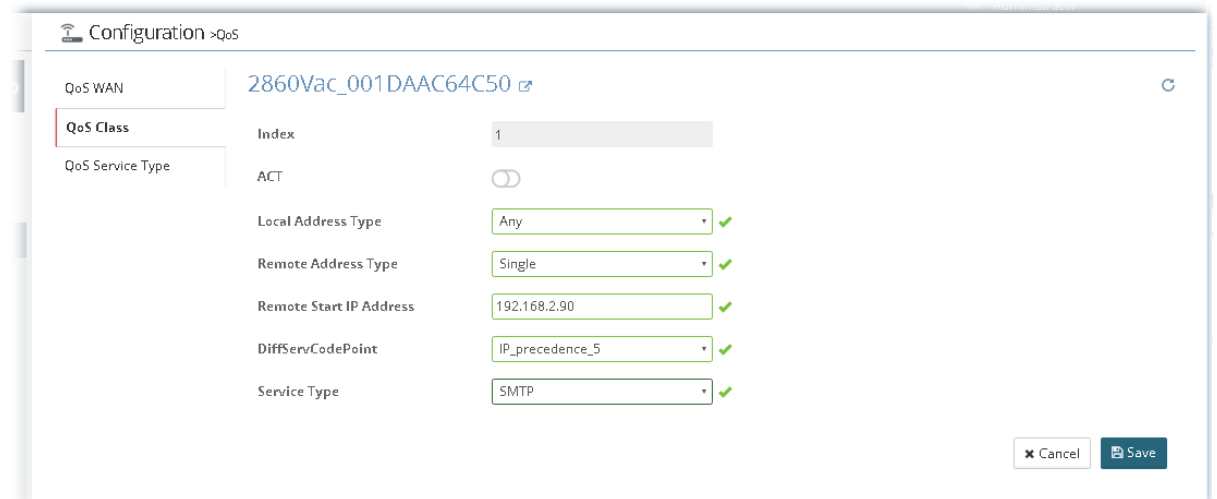
After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.10.2 QoS Class

Class rules can be adjusted for your necessity.



To edit the parameters settings for class rules, move the mouse cursor on the table and click any one of the class rules to get the following page.



After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.10.3 QoS Service Type

The screenshot shows a web interface for configuring QoS. On the left is a 'DEVICE MENU' with options like Dashboard, Monitoring, Configuration, WAN, LAN, Routing, NAT, Firewall, User Management, Objects Setting, QoS, Applications, VPN, VoIP, Wireless LAN, USB Applications, System, Copy Parameter, and Advanced. The 'Configuration > QoS' page is active, showing 'QoS WAN' and '2860Vac_001DAAC64C50'. Under 'QoS Class', 'QoS Service Type' is selected. A table lists service types:

Index	Name	Protocol Type	Port Type	Port Number From	Port Number To
1				0	0

To add / edit the parameters settings for service type, move the mouse cursor on the table and click any index number to get the following page.

The screenshot shows the configuration form for 'QoS Service Type' (Index 1). The form includes the following fields:

- Index: 1
- Name: Good
- Service Type: TCP/UDP
- Port Type: Single (selected), Range (checked)
- Port Number Start: 100 (checked)
- Port Number End: 500 (checked)

Buttons for 'Cancel' and 'Save' are located at the bottom right.

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.10.4 Others

Such feature is available for certain CPE (e.g., Vigor2133 series) only. It is used for enabling the first priority for VoIP SIP/RTP and configuring port number for SIP UDP.

The screenshot shows the configuration page for QoS settings on a Vigor2133FVAc device. The breadcrumb navigation is "Configuration > qos". On the left, there is a sidebar menu with options: "QoS WAN", "QoS Class", "QoS Service Type", and "Others" (which is currently selected). The main content area is titled "Vigor2133FVAc" and contains two settings:

- Enable the First Priority for VoIP SIP/RTP:** A toggle switch that is currently turned on.
- SIP UDP Port:** A text input field containing the value "5060".

At the bottom right of the configuration area, there are two buttons: "Cancel" and "Save".

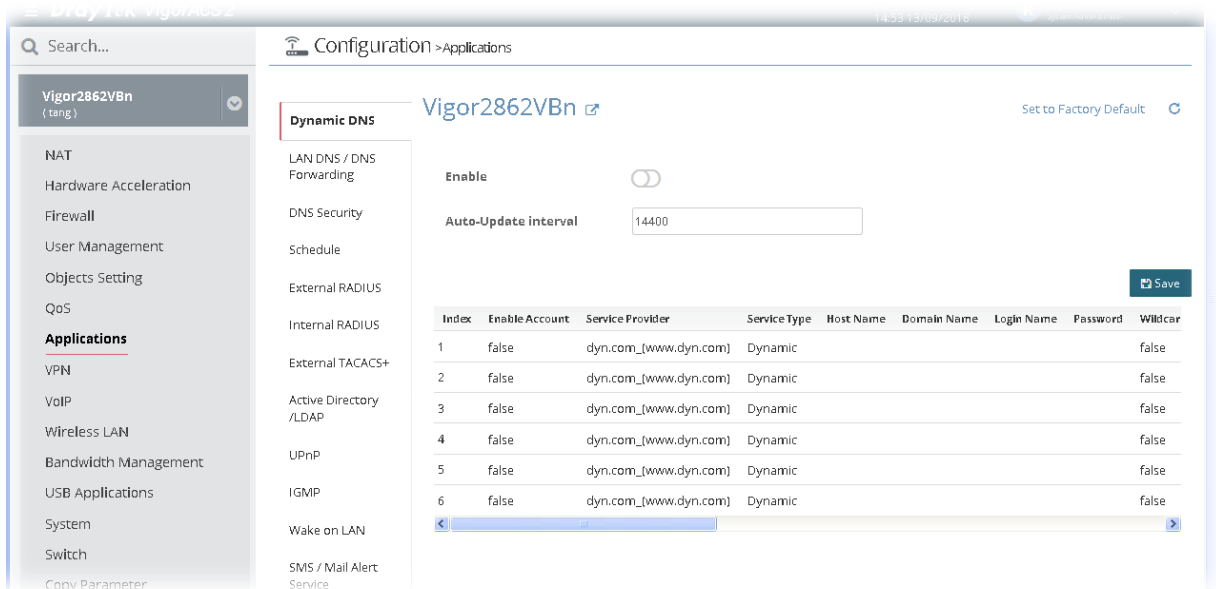
13.11 Applications Settings for CPE

In such section, Vigor2862VBn is selected as an example for displaying Applications settings.

13.11.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

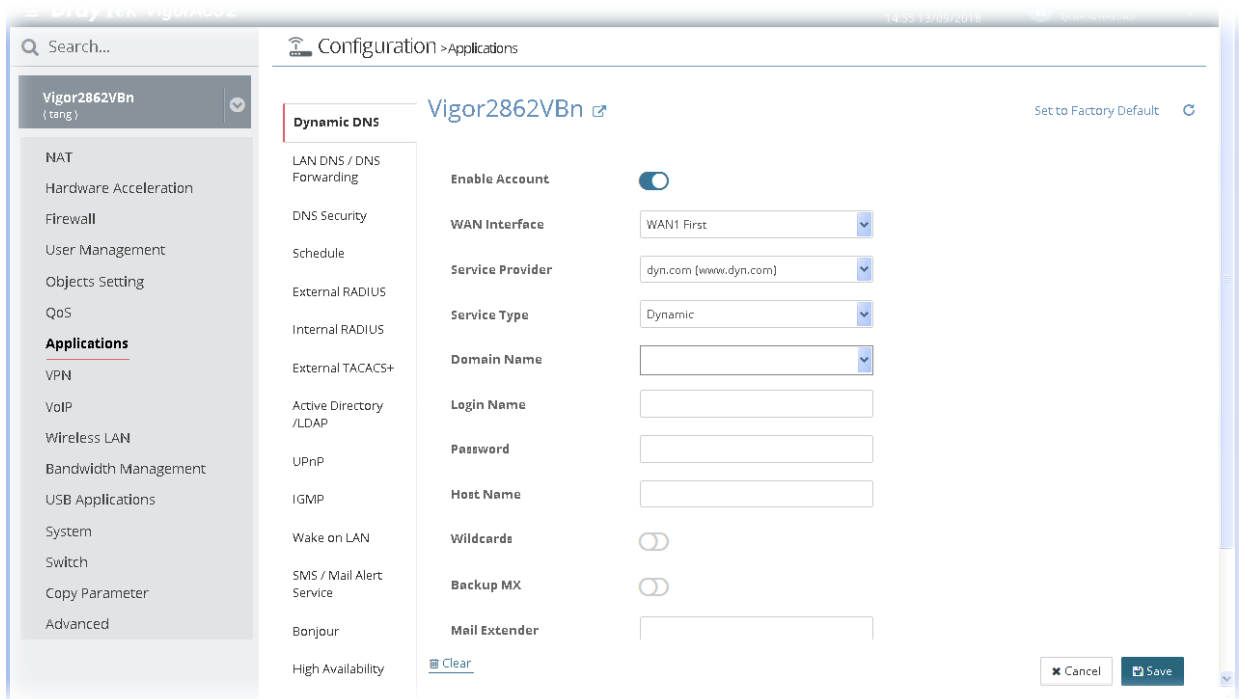
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers.



The screenshot shows the web interface for configuring the Dynamic DNS service on a Vigor2862VBn router. The interface includes a search bar, a navigation sidebar, and a main configuration area. The 'Dynamic DNS' section is active, showing the 'Enable' toggle set to 'Off' and the 'Auto-Update interval' set to 14400. Below this is a table of service providers.

Index	Enable Account	Service Provider	Service Type	Host Name	Domain Name	Login Name	Password	Wildcard
1	false	dyn.com_(www.dyn.com)	Dynamic					false
2	false	dyn.com_(www.dyn.com)	Dynamic					false
3	false	dyn.com_(www.dyn.com)	Dynamic					false
4	false	dyn.com_(www.dyn.com)	Dynamic					false
5	false	dyn.com_(www.dyn.com)	Dynamic					false
6	false	dyn.com_(www.dyn.com)	Dynamic					false

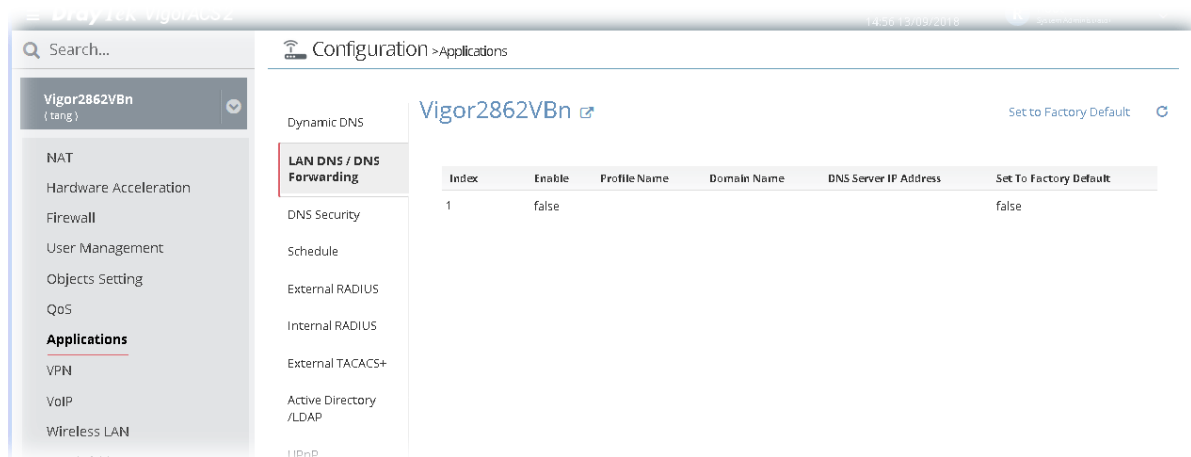
To edit the parameters settings for DDNS service, move the mouse cursor on the table and click any index number to get the following page.



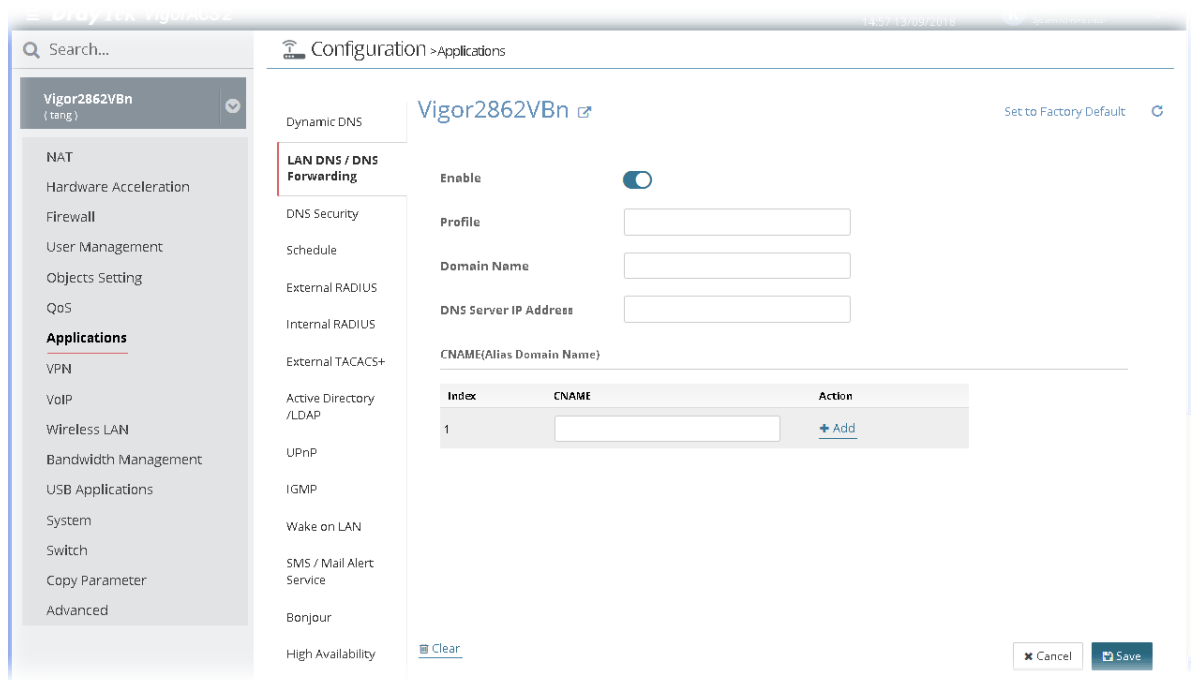
After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.11.2 LAN DNS / DNS Forwarding

LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor router will respond the specified private IP address.

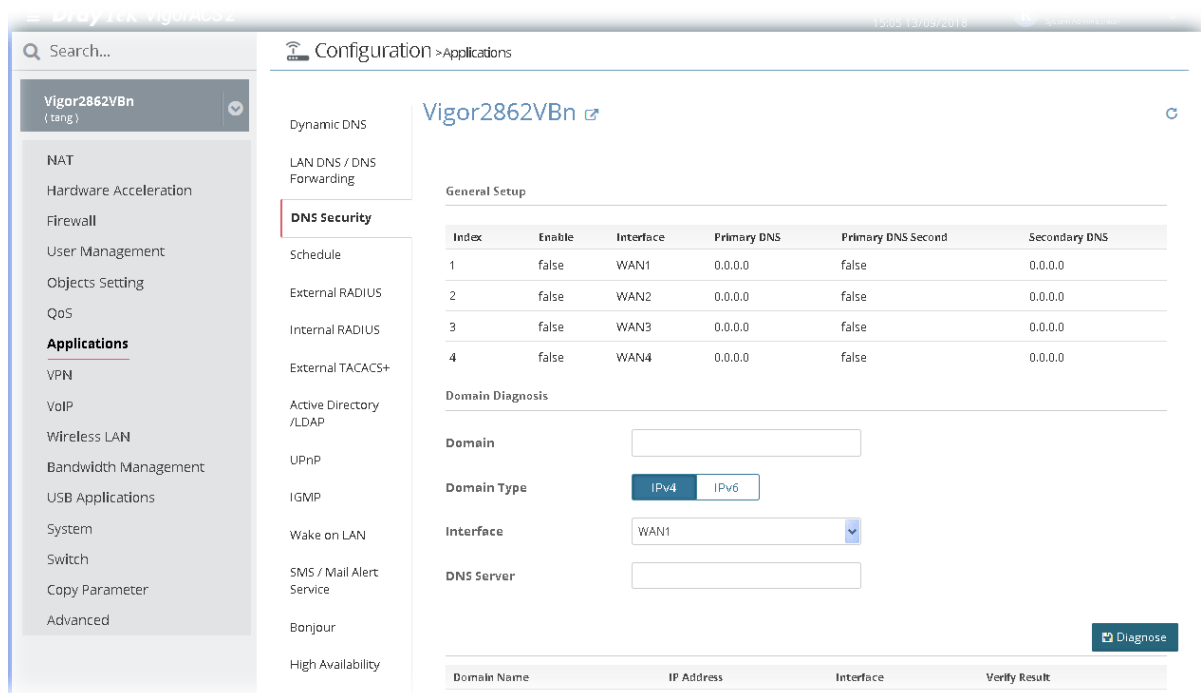


To edit the parameters settings for LAN DNS profile, move the mouse cursor on the table and click any index number to get the following page.

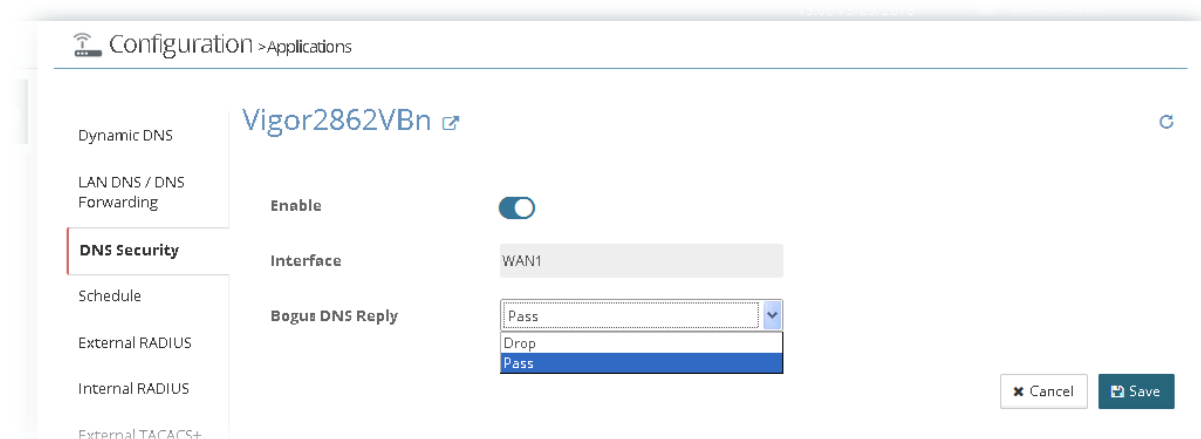


13.11.3 DNS Security

DNS security is able to ensure that the incoming data is not falsified and the source of the data is secure and correct to prevent from DNS attack by someone.



All of WAN interfaces of Vigor router can be configured with DNS Security enabled respectively. To edit the parameters settings for DDNS security, move the mouse cursor on the table and click any index number to get the following page.

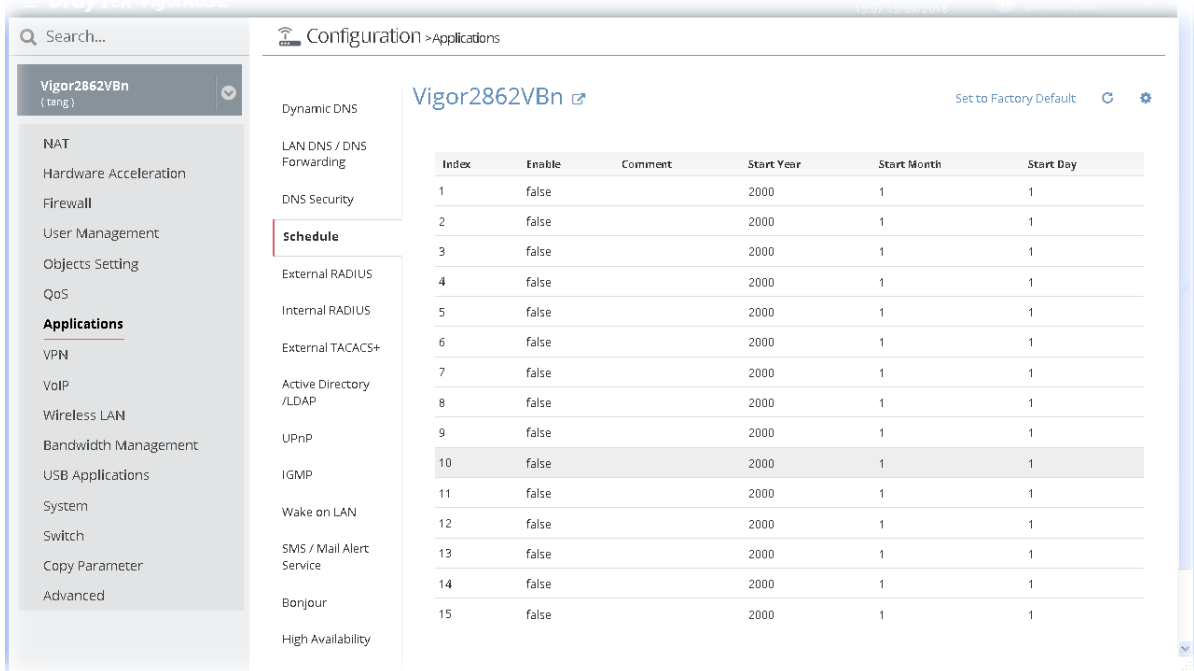


After finished the settings, click Save. The modification for the CPE will take effect immediately.

In addition, the button of Diagnose is a simple way to manually detect if the domain used for the specified CPE is secure not.

13.11.4 Schedule

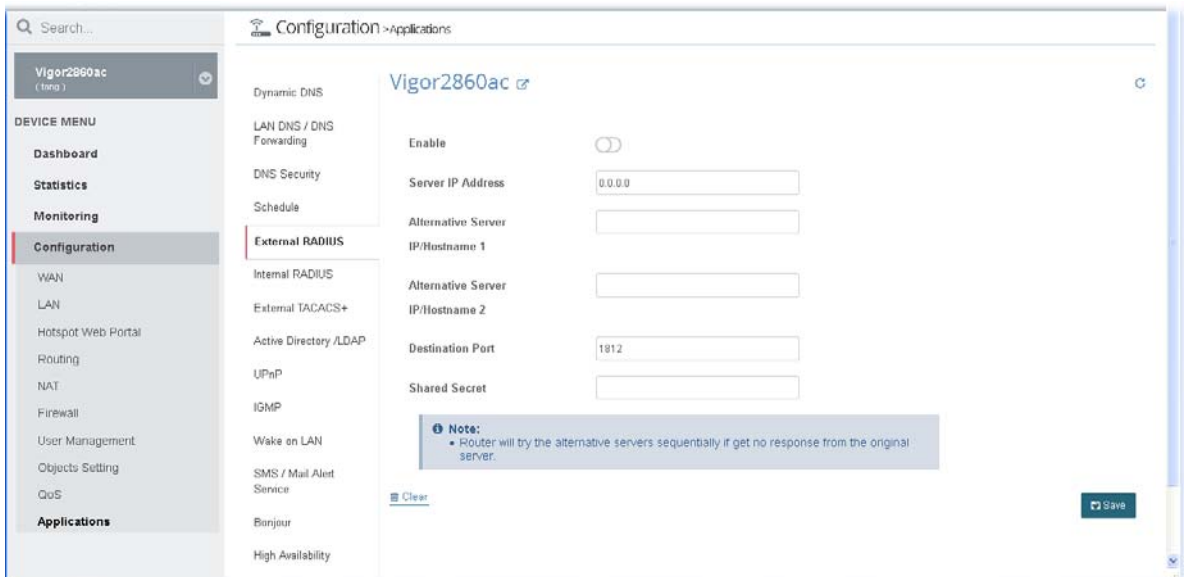
The Vigor router has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect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



13.11.5 External RADIUS

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

Vigor router can be operated as a RADIUS client. Therefore, this page is used to configure settings for external RADIUS server. Then LAN user of Vigor router will be authenticated by such server for network application.

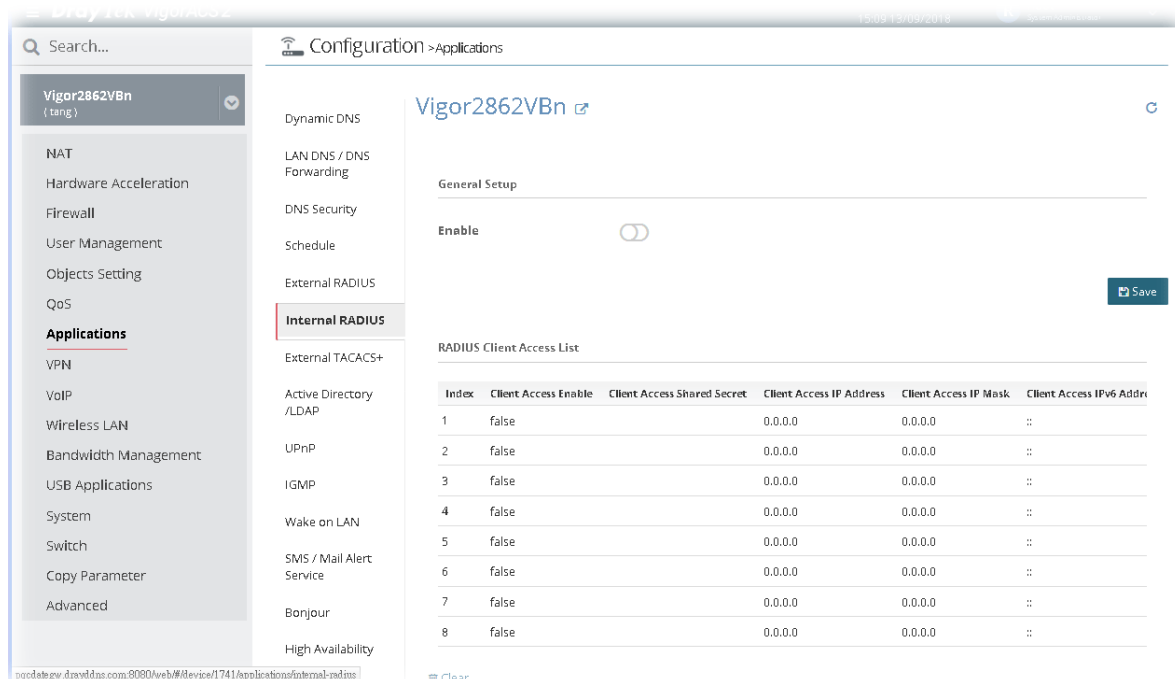


The option of Alternative Server is available for some CPE (e.g., Vigor2860ac).

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.11.6 Internal RADIUS

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



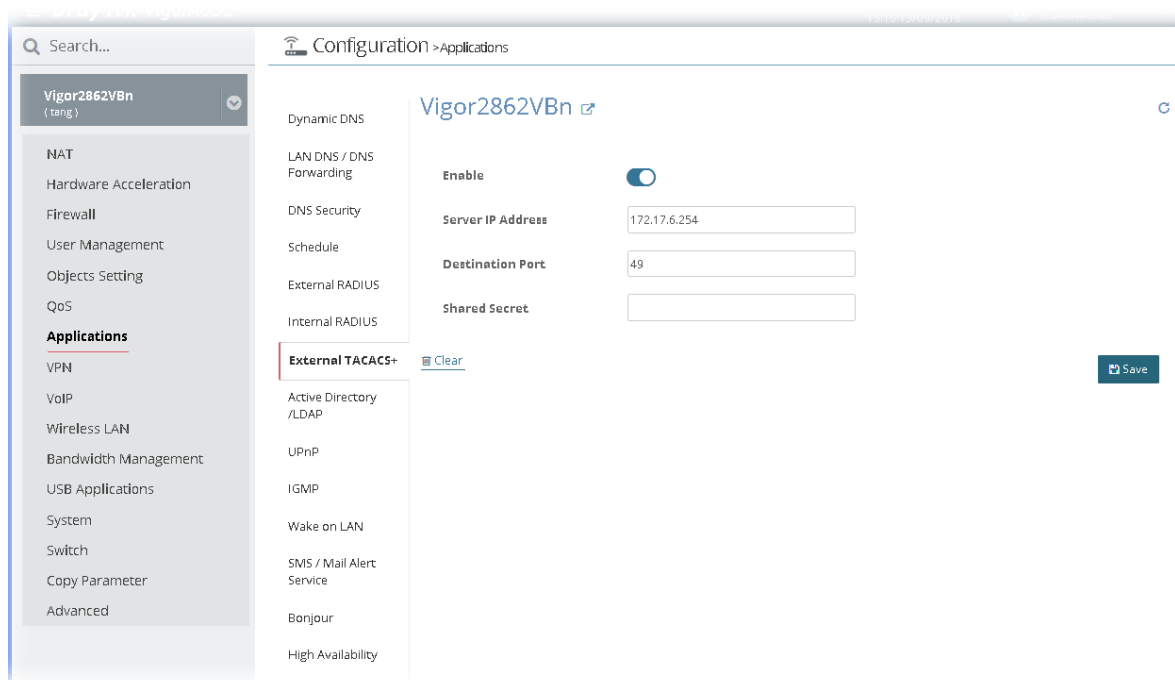
The screenshot shows the configuration page for the Vigor2862VBn router, specifically the 'Internal RADIUS' section. The 'Enable' toggle is turned on. Below it is a table for the RADIUS Client Access List.

Index	Client Access Enable	Client Access Shared Secret	Client Access IP Address	Client Access IP Mask	Client Access IPv6 Address
1	false		0.0.0.0	0.0.0.0	::
2	false		0.0.0.0	0.0.0.0	::
3	false		0.0.0.0	0.0.0.0	::
4	false		0.0.0.0	0.0.0.0	::
5	false		0.0.0.0	0.0.0.0	::
6	false		0.0.0.0	0.0.0.0	::
7	false		0.0.0.0	0.0.0.0	::
8	false		0.0.0.0	0.0.0.0	::

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.11.7 External TACACS+

TACACS+ means Terminal Access Controller Access-Control System Plus. It works like RADIUS does. The TACACS+ 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.



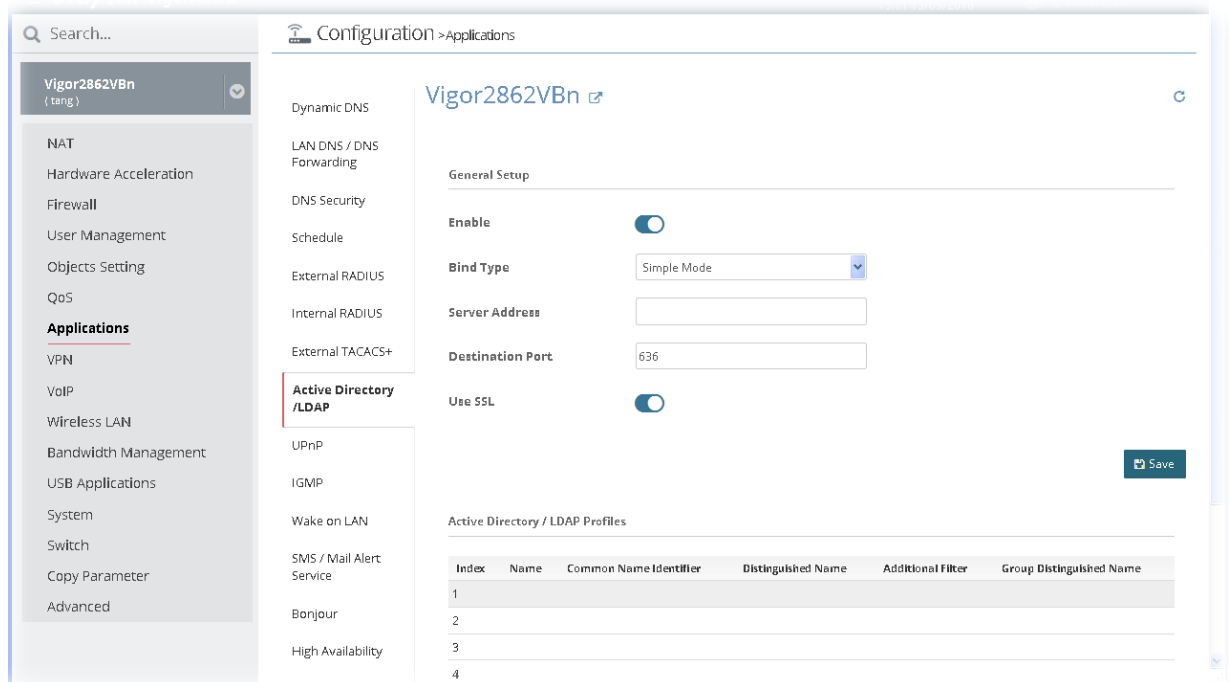
The screenshot shows the configuration page for the Vigor2862VBn router, specifically the 'External TACACS+' section. The 'Enable' toggle is turned on. Below it are input fields for 'Server IP Address' (172.17.6.254), 'Destination Port' (49), and 'Shared Secret'.

After finished the settings, click Save. The modification for the CPE will take effect immediately.

13.11.8 Active Directory/LDAP

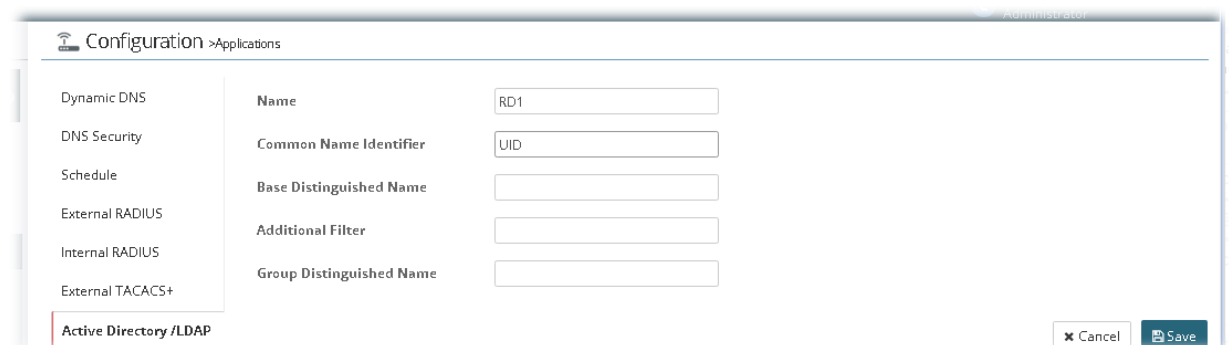
Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.



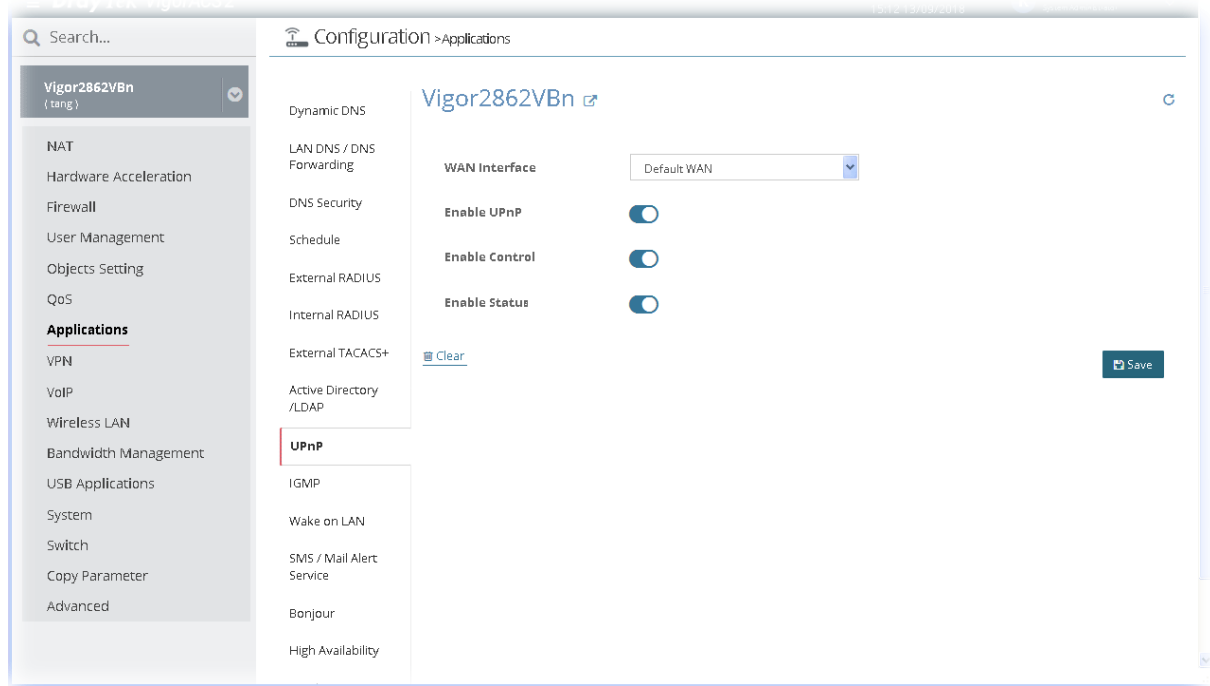
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

In addition, you can configure eight AD/LDAP profiles. These profiles would be used with User Management for different purposes in management. To edit the parameters settings for AD/LDAP, move the mouse cursor on the table and click any index number (e.g., index number 4) to get the following page.



13.11.9 UPnP

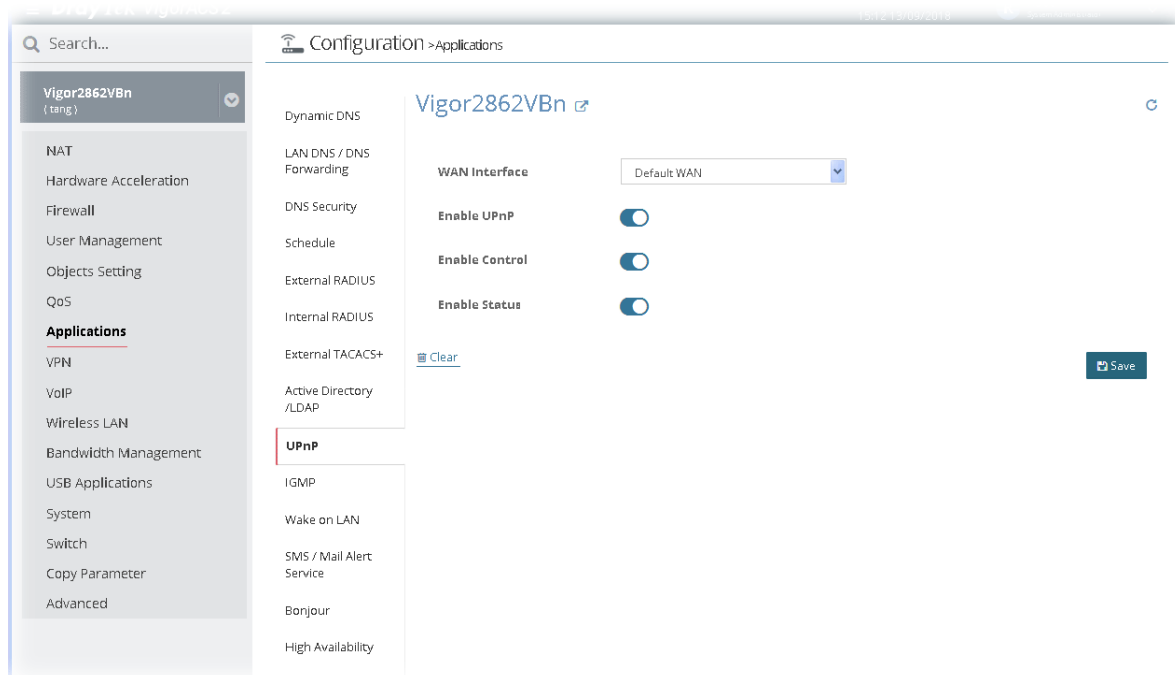
The UPnP (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.11.10 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

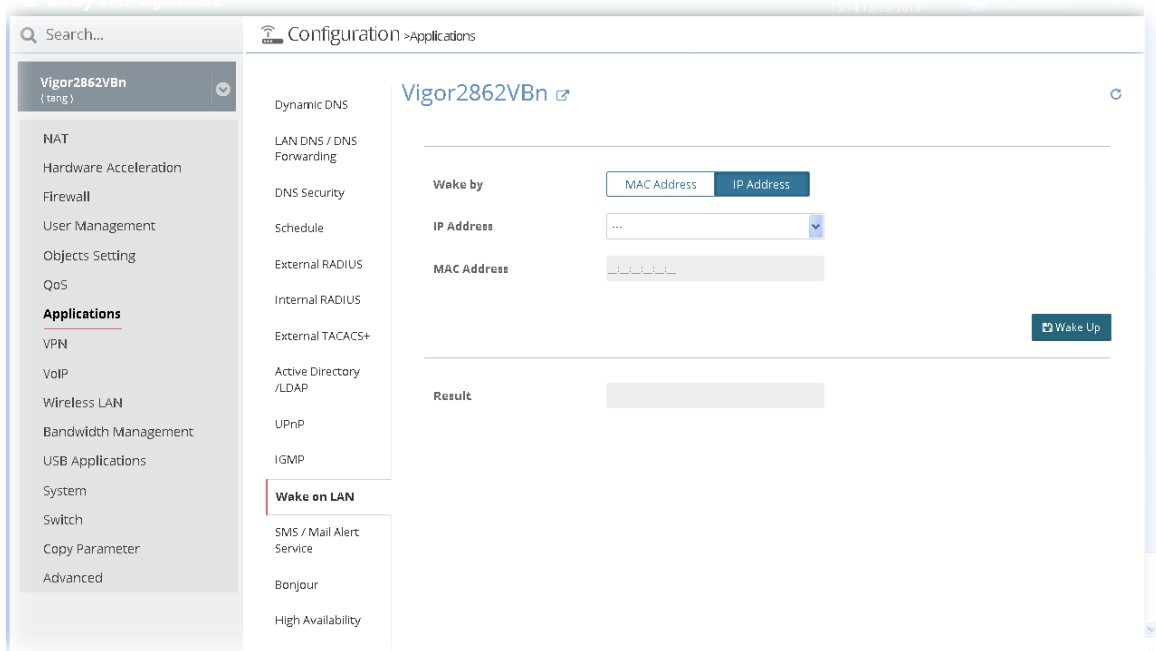


After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.11.11 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN (WOL)** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.



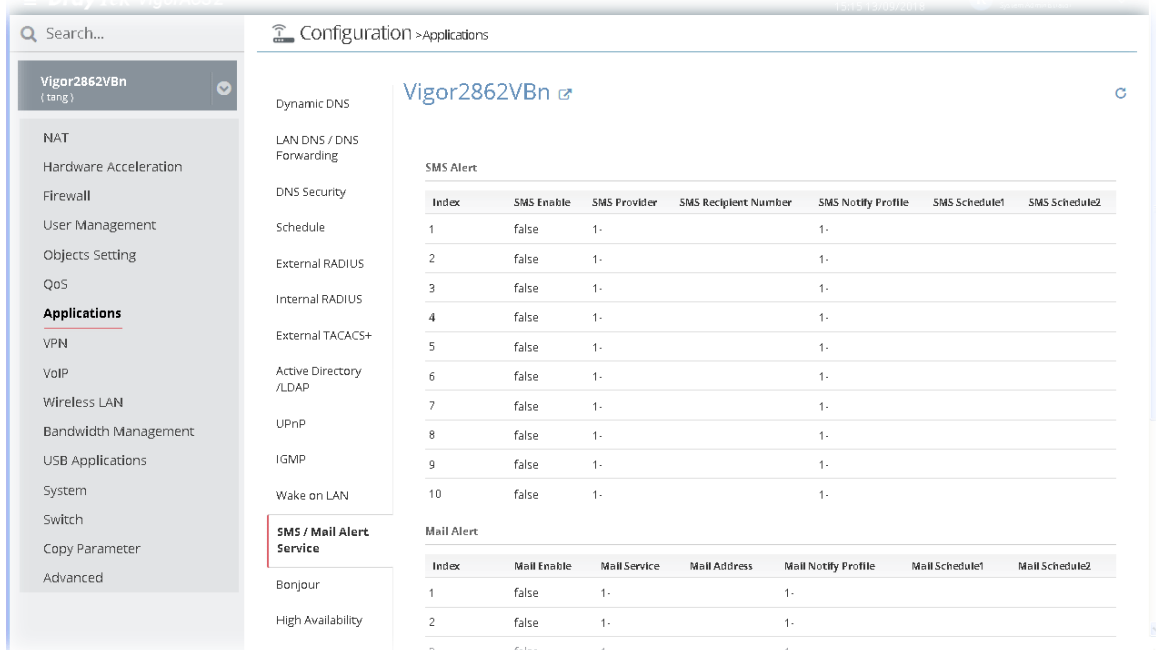
Click **Wake Up** to wake up the selected IP. The result will be shown on the field of Result.

13.11.12 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.

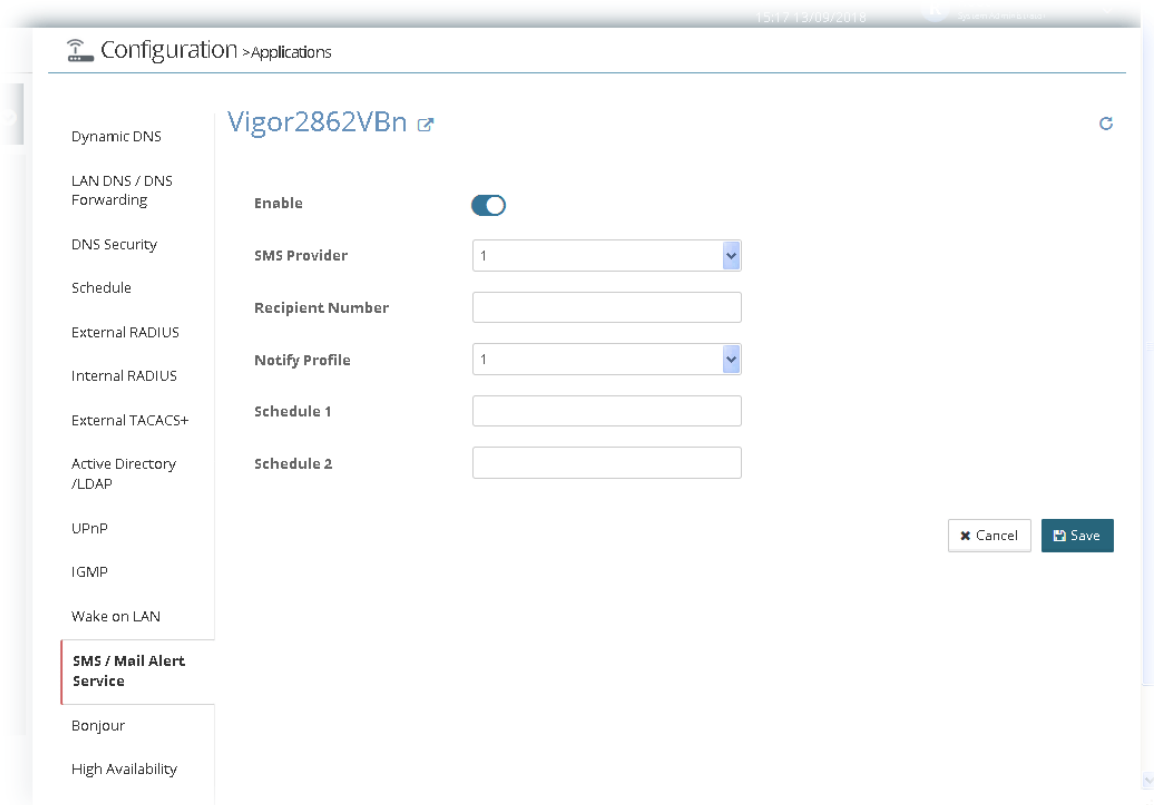
SMS Alert

Vigor router allows you to set up to 10 SMS profiles which will be sent out according to different conditions.



SMS Alert allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

To edit the parameters settings for SMS alert service, move the mouse cursor on the table and click any index number to get the following page.

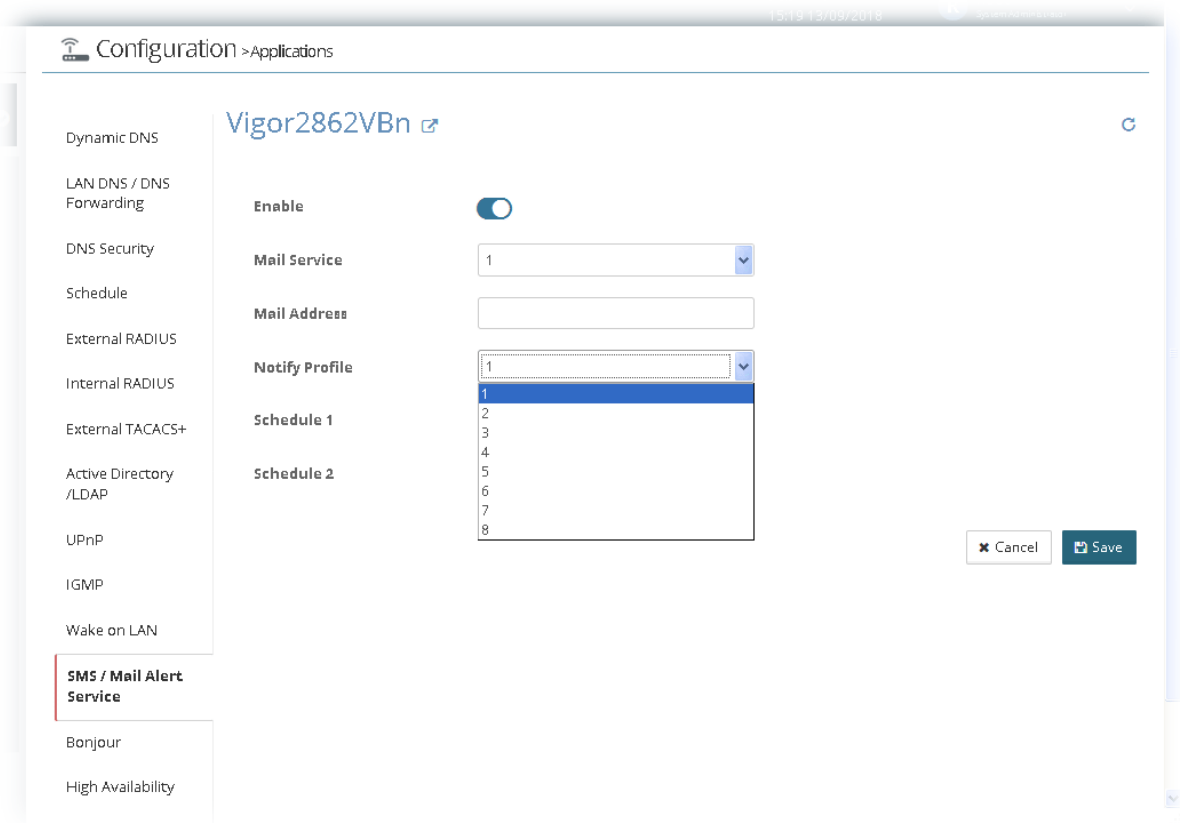


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

Mail Alert

Mail Alert 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 edit the parameters settings for mail alert service, move the mouse cursor on the table and click any index number to get the following page.

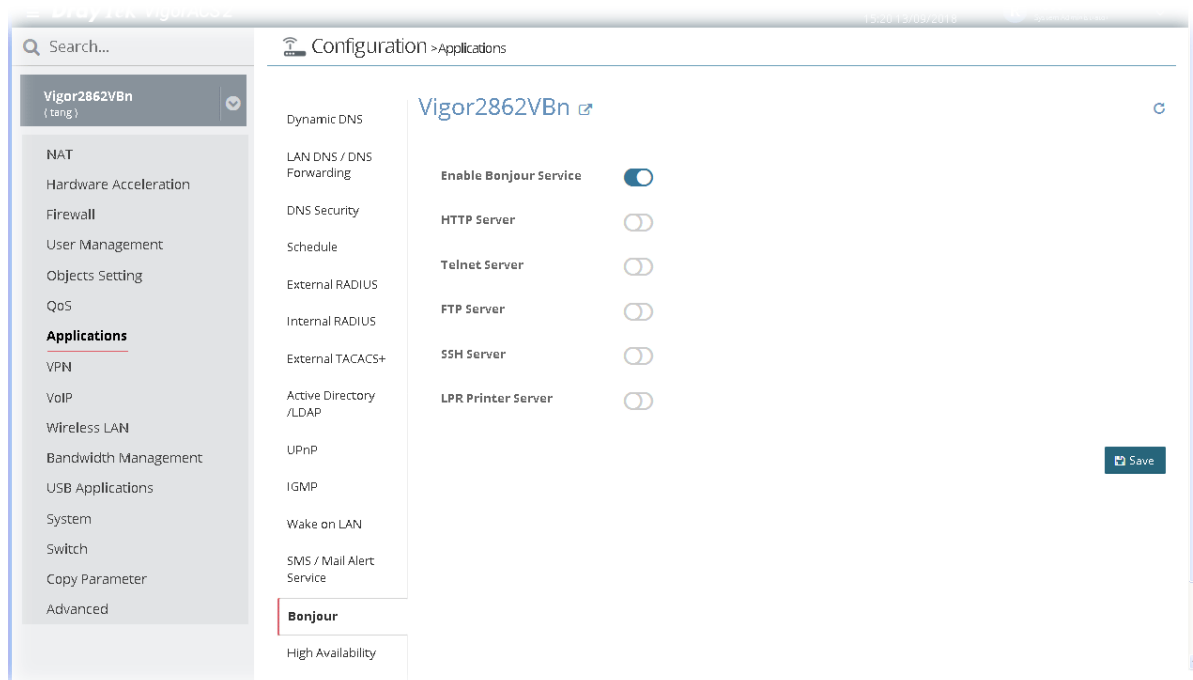


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.11.13 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.

Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer have the plug-in Bonjour driver install, they can utilize the service offered by the router by clicking the router name icon. In short, what the Clients/users need to know is the name of the router only.

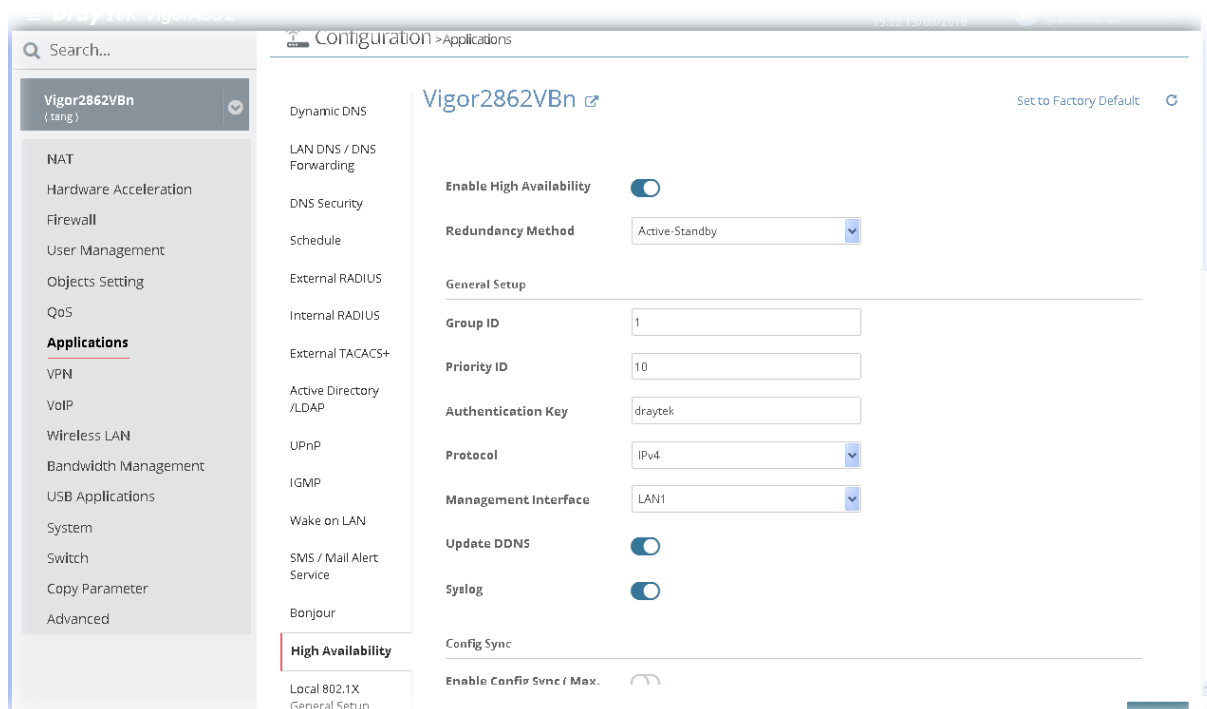


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.11.14 High Availability

The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, providing nearly full-time availability, typically have redundant hardware and software that make the system available despite failures.

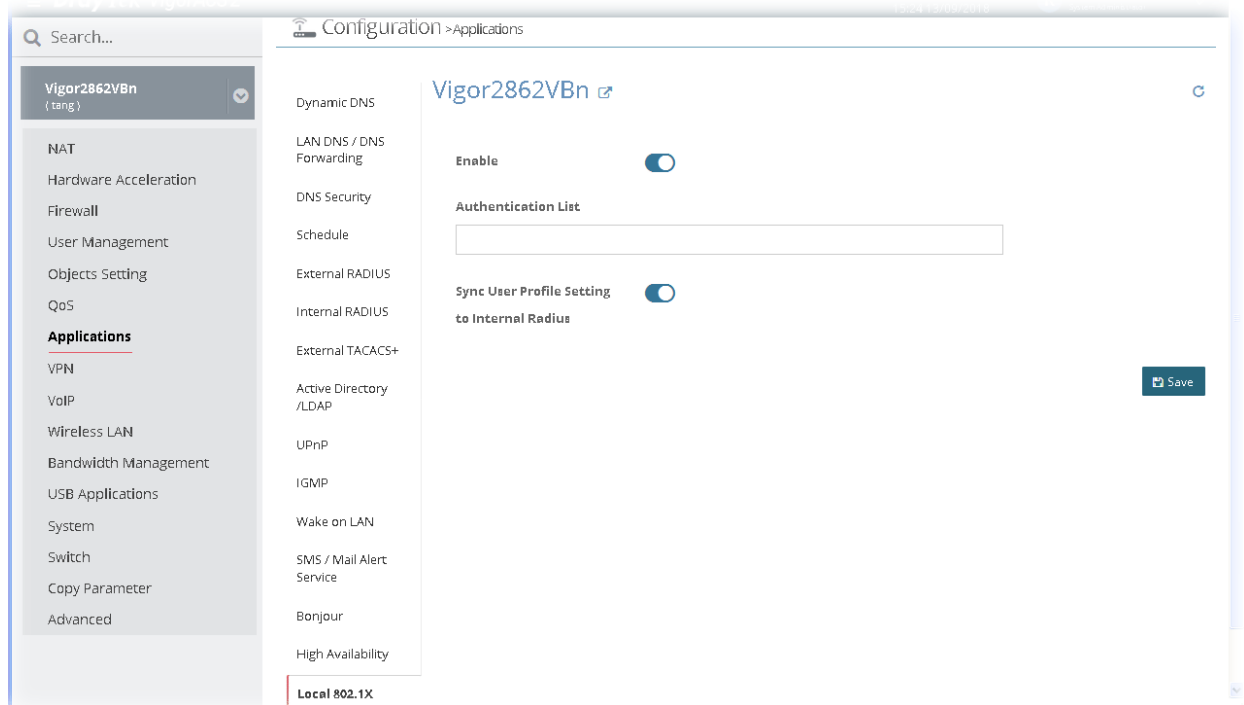
The high availability of the Vigor router is designed to avoid single points-of-failure. When failures occur, the failover process moves processing performed by the failed component (the “primary”) to the backup component (the “secondary”). This process remains system-wide resources, recovers partial of failed transactions, and restores the system to normal within a few seconds.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.11.15 Local 802.1X General Setup

It allows you to configure general settings for Local 802.1X server built in Vigor router.



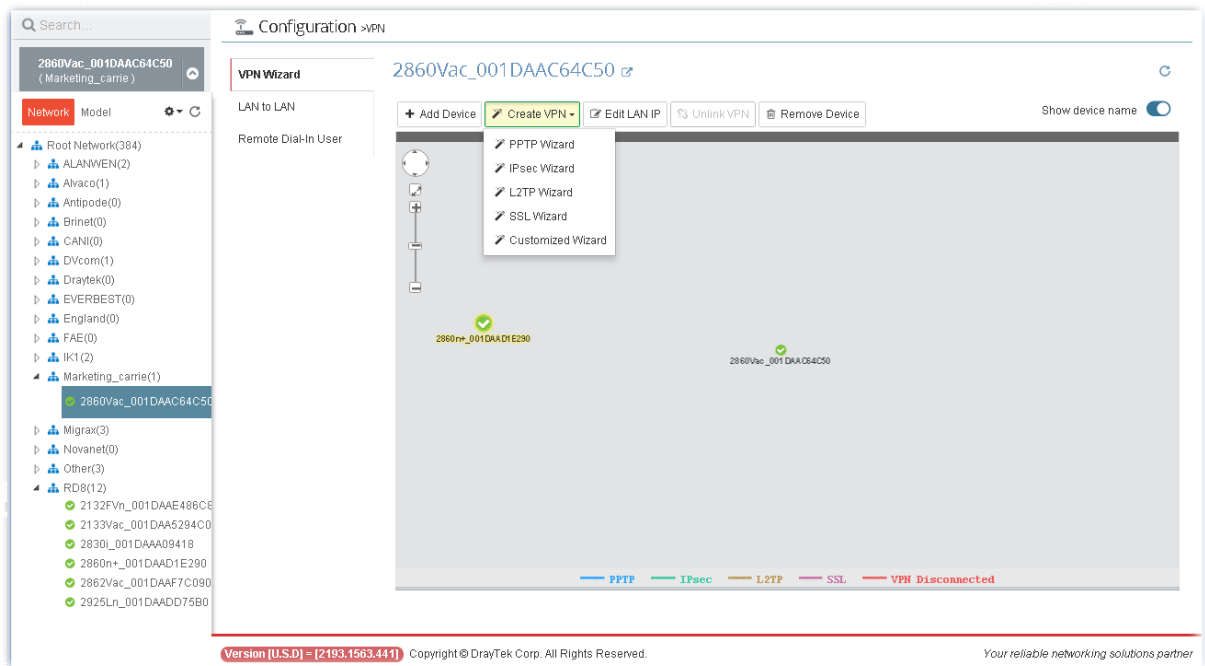
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.12 VPN Settings for CPE

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.

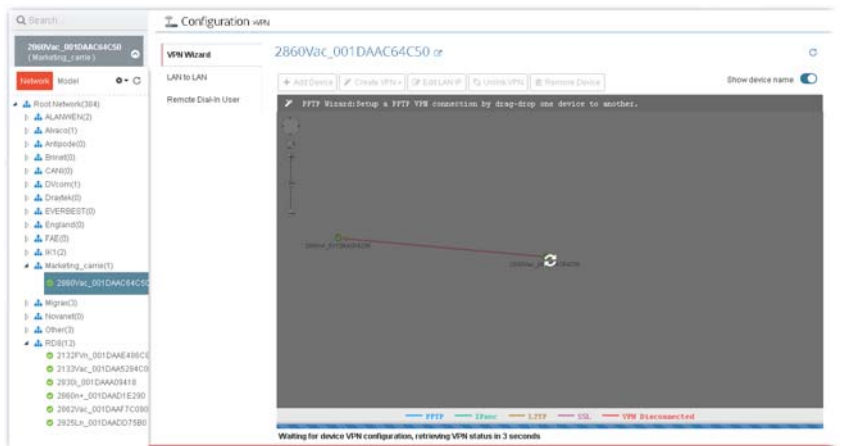
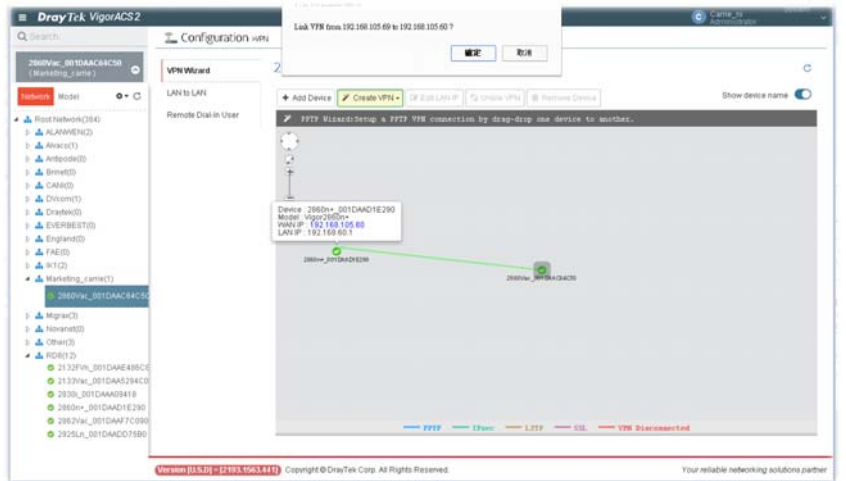
13.12.1 VPN Wizard

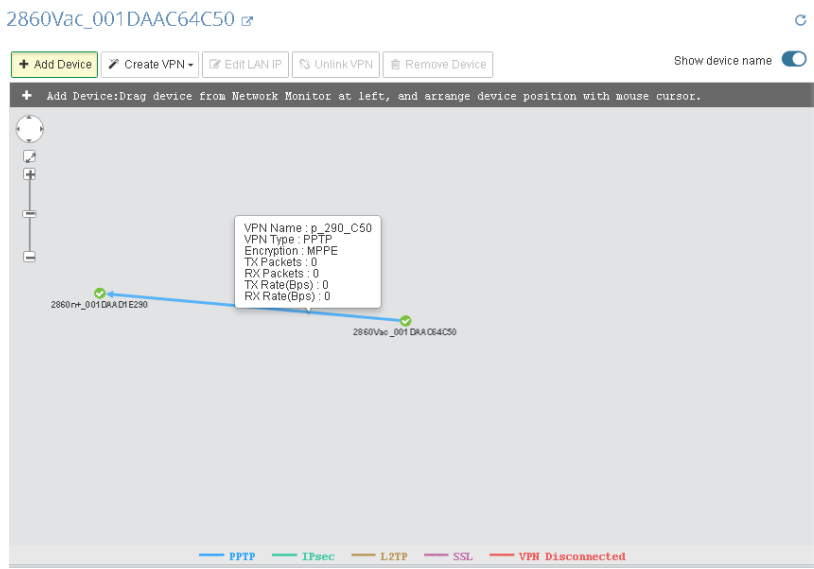
This page displays the VPN status related to the specified device.



These parameters are explained as follows:

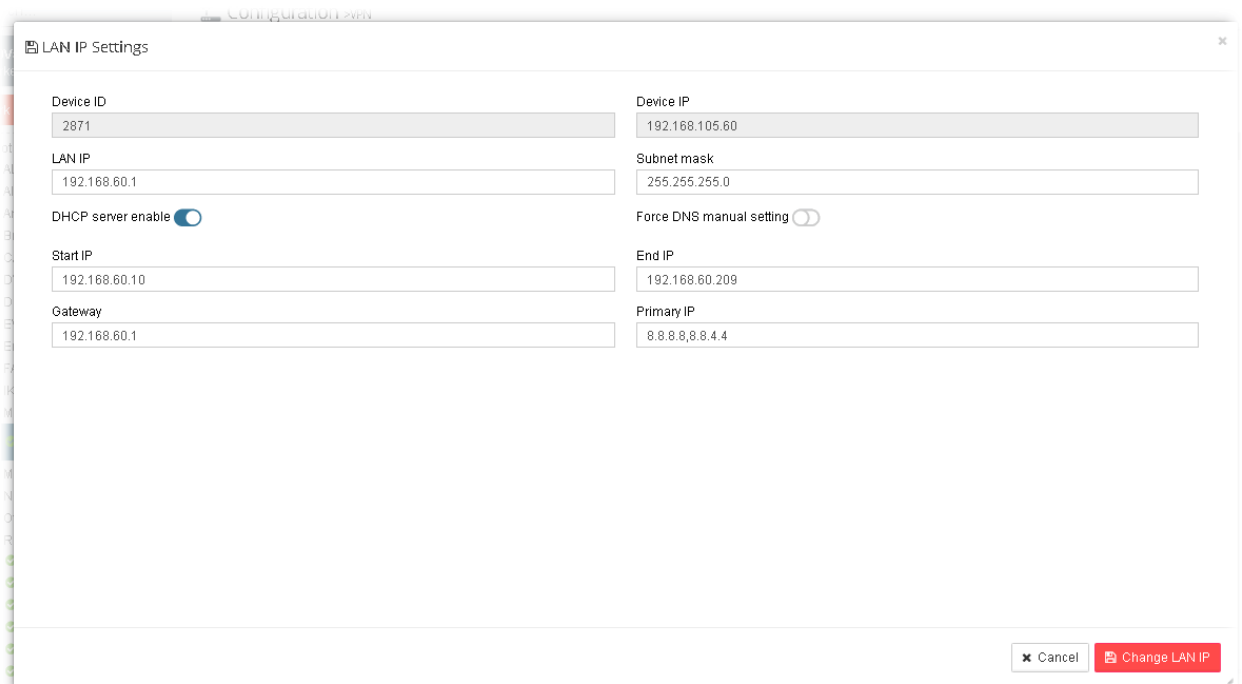
Item	Description
Add Device	Click this button to add a device for building VPN connection. If you do not click this button first, you can not drag any device from Network view.
Create VPN	To build a quick VPN connection with PPTP/IPsec/L2TP/SSL/customized settings , simply click this button and choose one of the wizards for establishing VPN. Then, drag and drop one device to another.



	
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 this button to remove the selected device without VPN connection.
Show device name	Click it to display / hide the name of the device.

Change LAN IP for Selected Device

If there is LAN IP segment conflict in VPN connection, you can change the LAN IP setting for the device and avoid the conflict. Choose the device on the screen and click **Edit LAN IP**. The following dialog will appear.

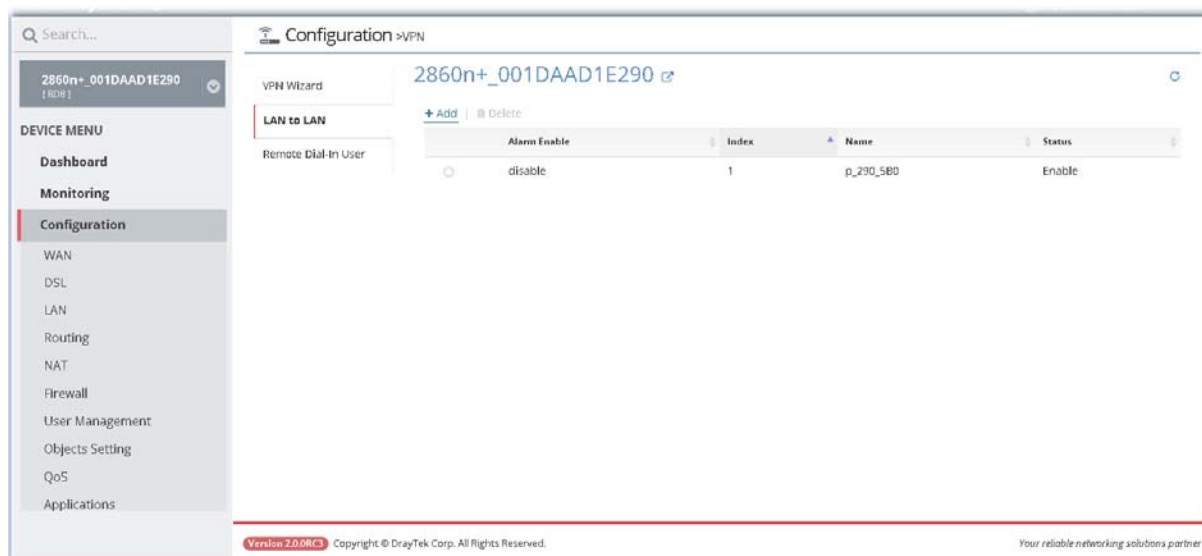


These parameters are explained as follows:

Item	Description
Device ID	Display the identification number of the selected device (CPE).
Device IP	Display the WAN IP address of the selected device (CPE).
LAN IP	Display the LAN IP address of the selected device. You can change it with another IP address to avoid the conflict.
Subnet mask	Display the subnet mask of the selected device. You can change it if required.
DHCP server enable	DHCP server has been activated. If you uncheck this box, you have to specify static IP address for the selected device.
Start IP	Type the starting IP address for the range that DHCP server can utilize.
End IP	Type the ending IP address for the range that DHCP server can utilize.
Gateway	Type the gateway address of the selected device.
Primary IP	Specify a DNS server IP address here for the ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

13.12.2 Create LAN to LAN Profile for VPN Connection

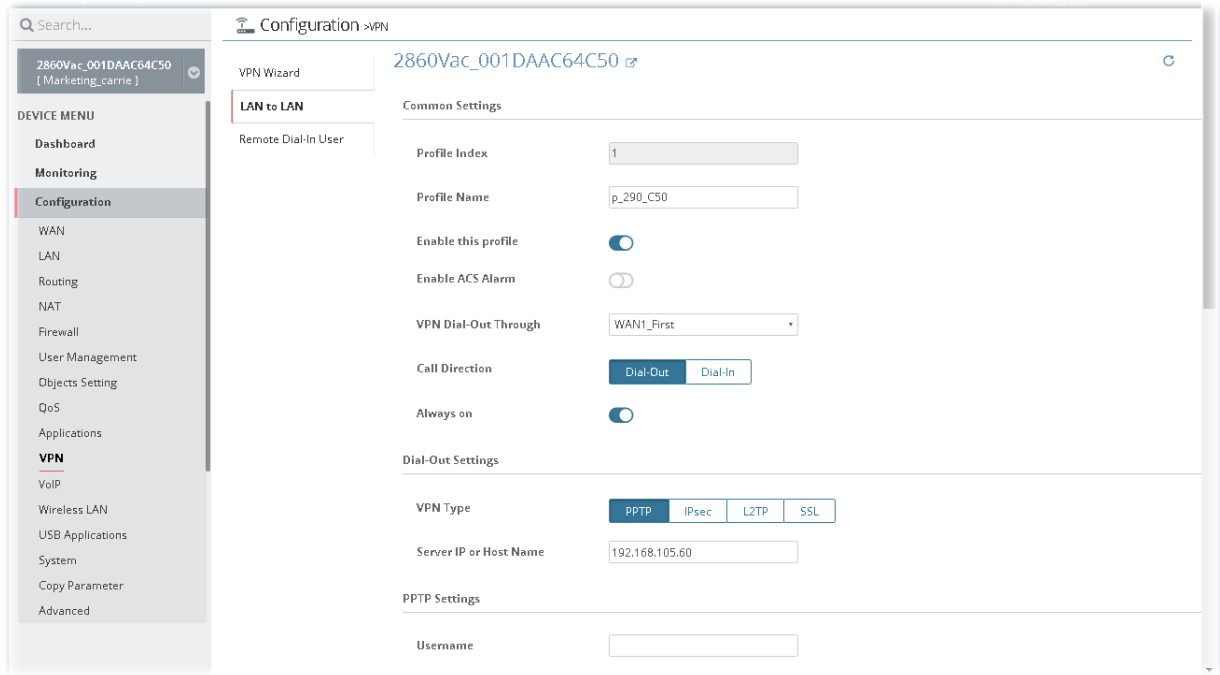
To create a LAN to LAN connection for the selected CPE, choose **LAN to LAN**. You can create up to 32 profiles for such CPE.



These parameters are explained as follows:

Item	Description
Alarm Enable	Display the activation status for alarm mechanism.
Index	VigorACS allows you to create up to 32 index numbers (profiles).
Name	Display the name of the LAN-to-LAN profile.
Status	Display if such profile is enabled or disabled for such CPE.
+Add	Create a new LAN to LAN profile.

The following setting page appears when +Add is clicked.



These parameters are explained as follows:

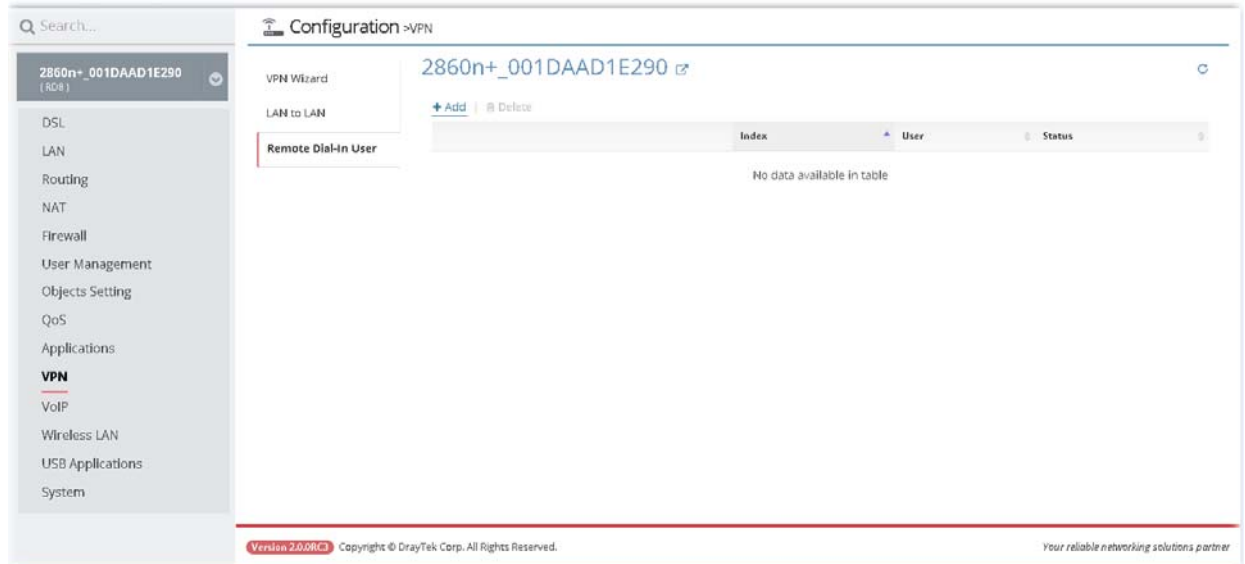
Item	Description
Common Settings	
Profile Name	Display the profile name. Modify it if it is required.
Enable this profile	Click it to enable such profile.
Enable ACS Alarm	Click it to enable the ACS alarm function.
VPN Dial-Out Through	Use the drop down list to choose one way for VPN connection.
Call Direction	Specify which direction that such profile will use Dial-In or Dial-Out.
Dial-Out Settings	
VPN Type	<p>When PPTP is selected, you have to fill the username and password, choose PPP Authentication and specify if VJ compression should be on or off for such connection.</p> <ul style="list-style-type: none"> ● Server IP or Host Name - Type the IP address for the server / client or the host name. ● Username ● Password ● PPP Authentication ● VJ Compression <p>When IPsec is selected, you have to type IKE Pre-Shared Key, and choose IPsec Security Method for such connection.</p> <ul style="list-style-type: none"> ● IPsec Tunnel with ● Server IP or Host Name - Type the IP address for the server / client or the host name. ● IKE Pre-Shared Key ● IPsec Security Method

	<p>When L2TP is selected, you have to type required information for the following options.</p> <ul style="list-style-type: none"> ● L2TP with IPsec Policy ● Server IP or Host Name - Type the IP address for the server / client or the host name. ● Username ● Password ● PPP Authentication ● VJ Compression <p>When SSL is selected, you have to type required information for the following options.</p> <ul style="list-style-type: none"> ● Server IP or Host Name - Type the IP address for the server / client or the host name. ● Server Port (for SSL Tunnel) ● Username ● Password ● PPP Authentication ● VJ Compression
TCP IP Network Settings	<p>My WAN IP - Specify the WAN IP address for the selected CPE. Remote Gateway IP - Specify the IP address for the remote client. Remote Network IP - Specify the IP address for the remote server. Remote Network Mask - Specify the network mask for the remote server.</p>
Save	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

13.12.3 Create Remote Dial-in User Profile for VPN Connection

The administrator can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. The administrator may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

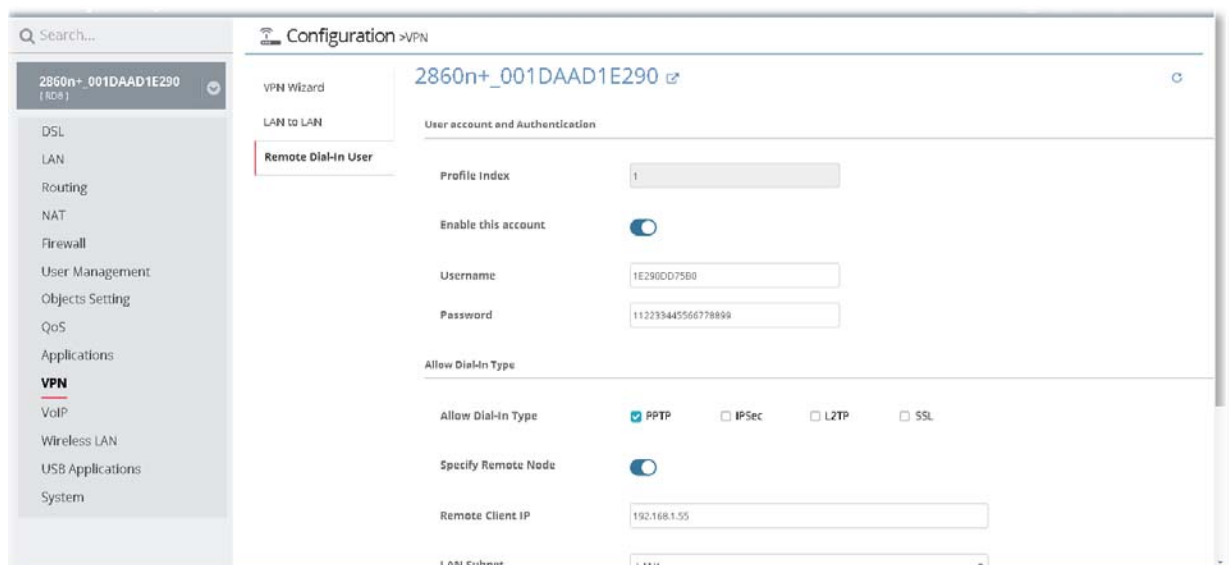
To create a remote dial-in user profile for the selected CPE, click **Remote Dial-in User**, the following screen will appear.



These parameters are explained as follows:

Item	Description
+Add	Create a new LAN to LAN profile.
Index	VigorACS allows you to create up to 32 index numbers (profiles).
User	Display the name of the remote dial-in profile.
Status	Display if such profile is enabled or disabled for such CPE.

The following setting page appears when +Add is clicked.



These parameters are explained as follows:

Item	Description
Enable this account	Click it to enable such account.
Username	Type a username for such account which will be used for authentication.
Password	Type a password for such account which will be used for authentication.
Allow Dial-in Type	Allow the remote dial-in user to make a PPTP/IPSec/L2TP/SSL VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
Specify Remote Node	You can specify the IP address of the remote dial-in user if you check this box. If you want to build a VPN that all the IP address can connect through the router. Do not check the box.
Remote Client IP	Type the IP address of the remote client that is allowed to pass through VPN connection.
LAN Subnet	Type the subnet address for local CPE.
Assign Static IP Address	Assign an IP address for the client connecting to Vigor device for accessing Internet. Later VigorACS 2 can make security configuration for the specified IP address.
IKE Authentication Method	It is available when IPSec is selected as Allow Dial-In Type . IKE Pre-Shared Key - Type in the required characters (1-63) as the pre-shared key if IPSec is selected as Allow Dial-in Type .
Save	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

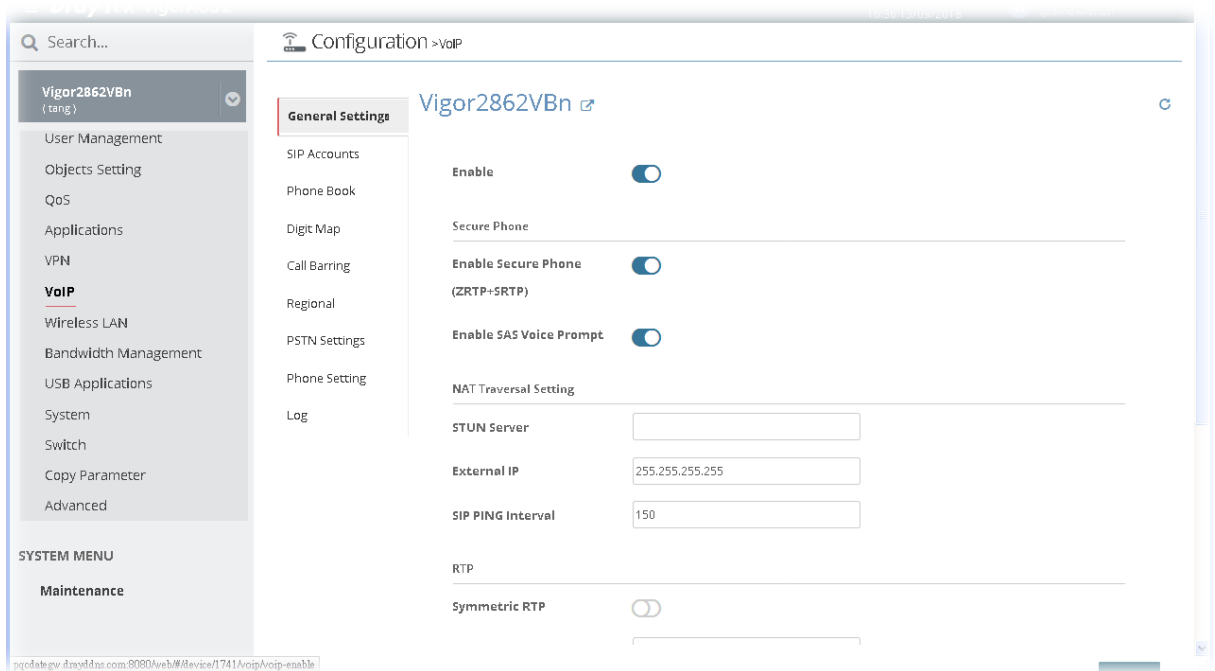
13.13 VoIP Settings for CPE

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

In such section, Vigor2862VBn is selected as an example for displaying VoIP settings.

13.13.1 General Setting

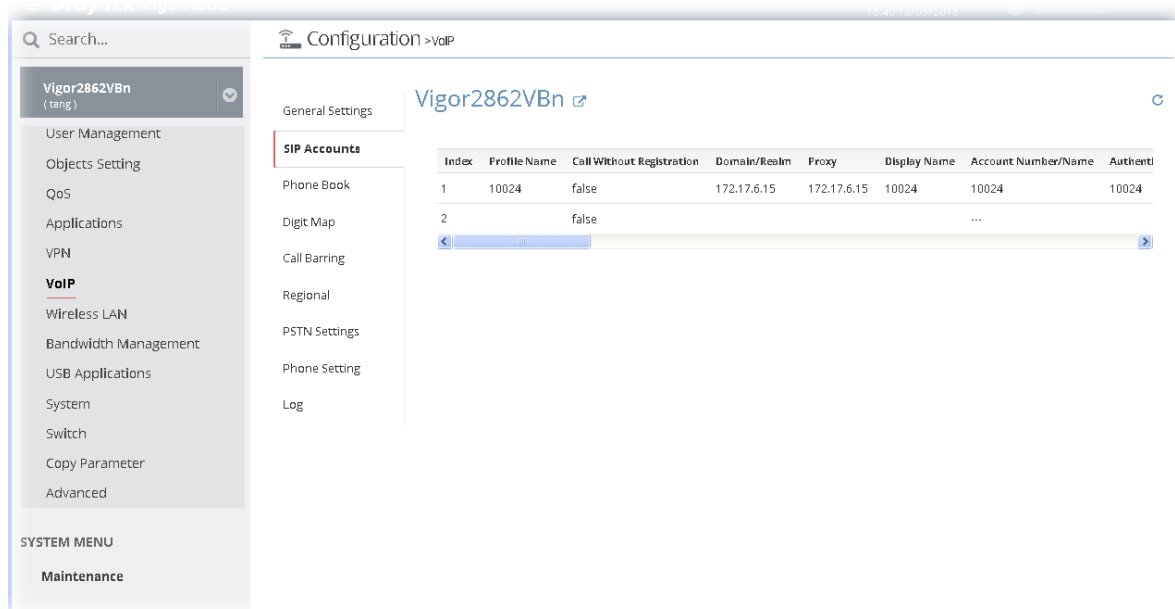
This page allows you to configure secure phone, set NAT Traversal Setting, and RTP for the VoIP function.



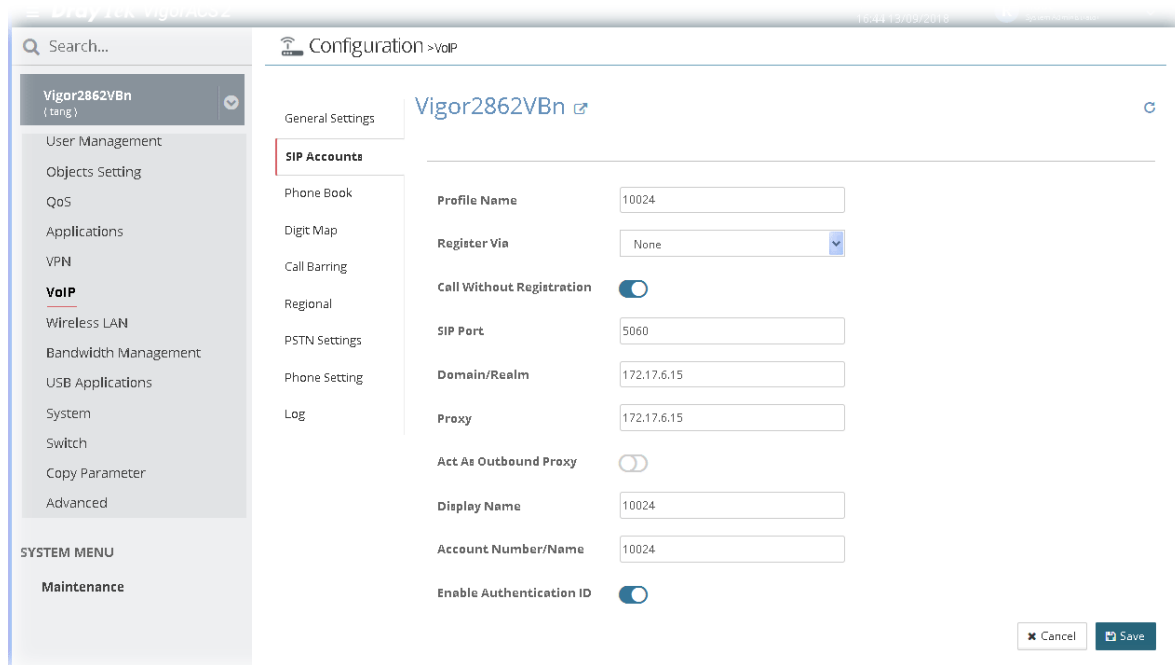
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.13.2 SIP Accounts

When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar**, **Proxy**, and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**.



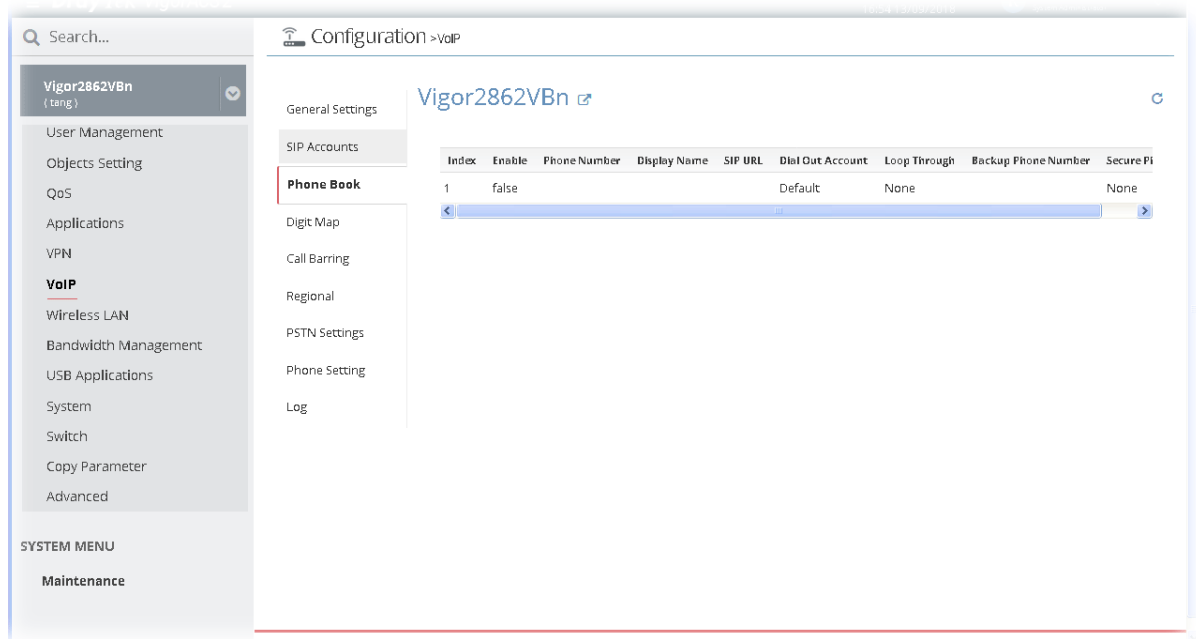
To modify SIP Account profile, move the mouse cursor on the table and click any one of the index number (e.g., #1) to get the following page.



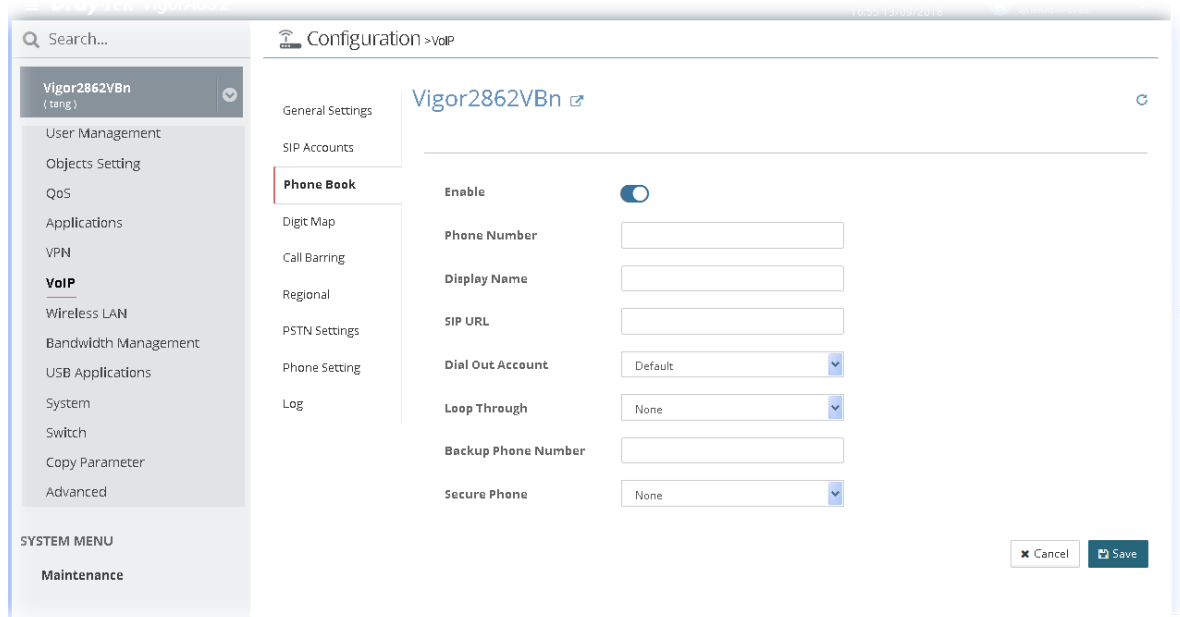
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.13.3 Phone Book

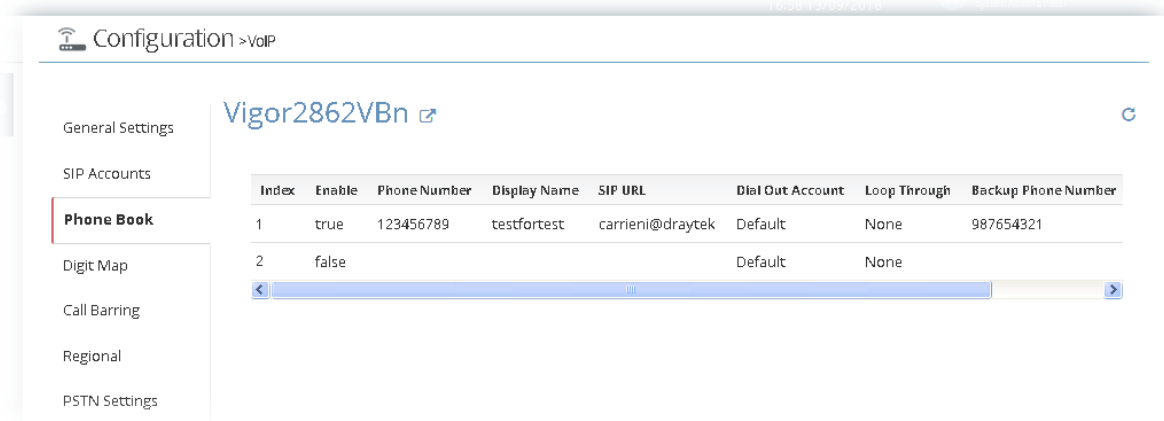
It can help you to make calls quickly and easily by using “speed-dial” Phone Number. There are total 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses.



To create / modify a phone book profile, move the mouse cursor on the table and click any one of the index number (e.g., #1 for a new profile) to get the following page.

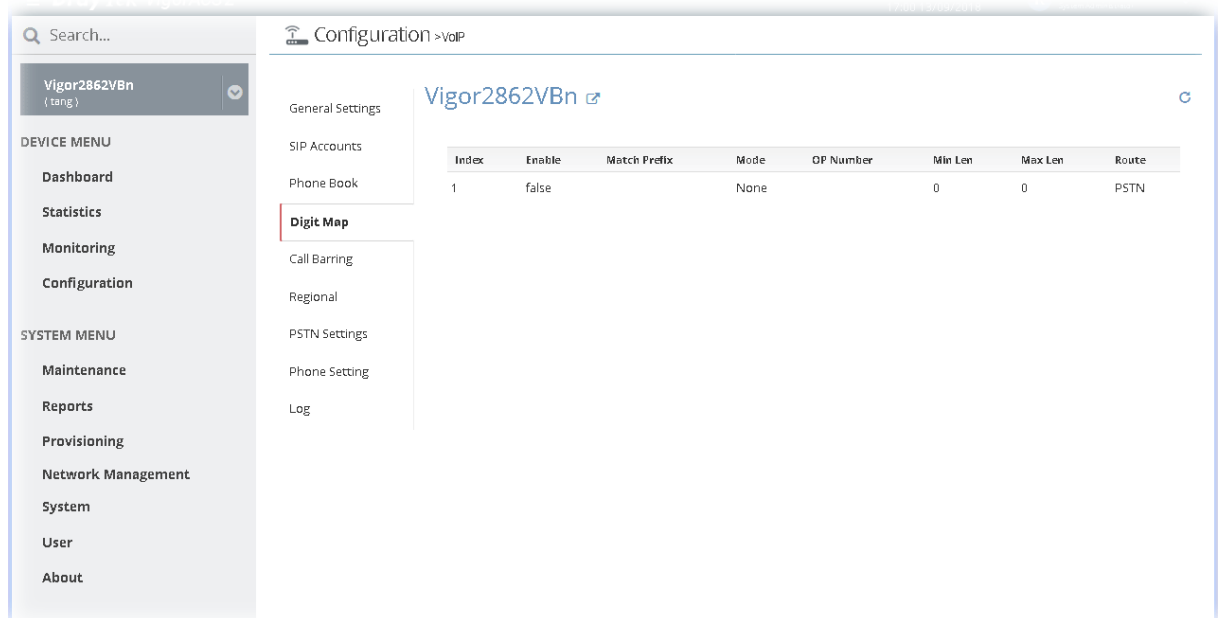


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

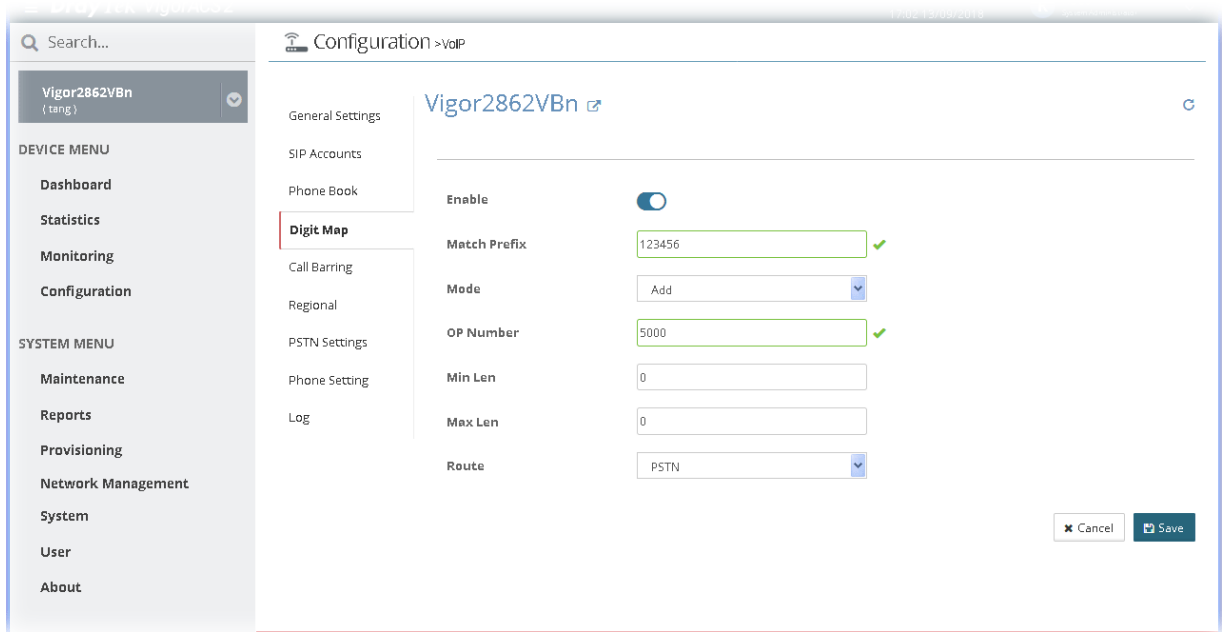


13.13.4 Digit Map

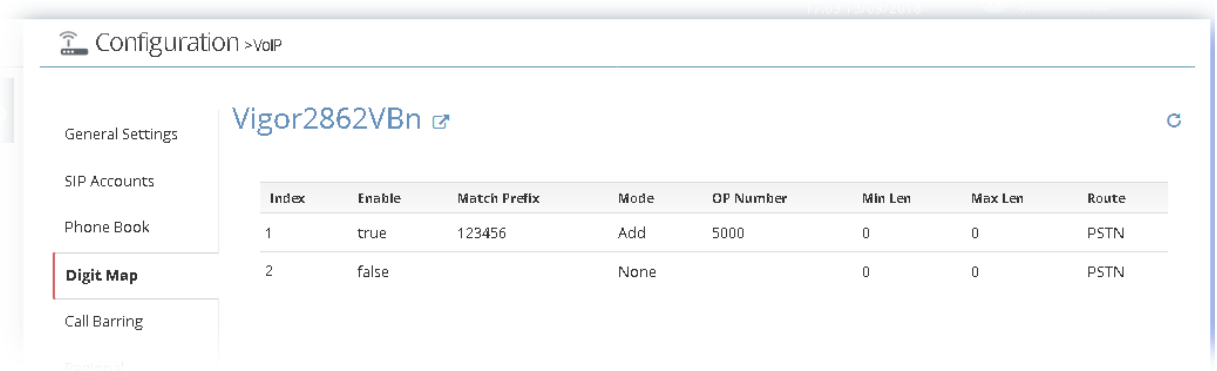
For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user have a quick and easy way to dial out through VoIP interface.



To create / modify a digit map profile, move the mouse cursor on the table and click any one of the index number (e.g., #1 for a new profile) to get the following page.

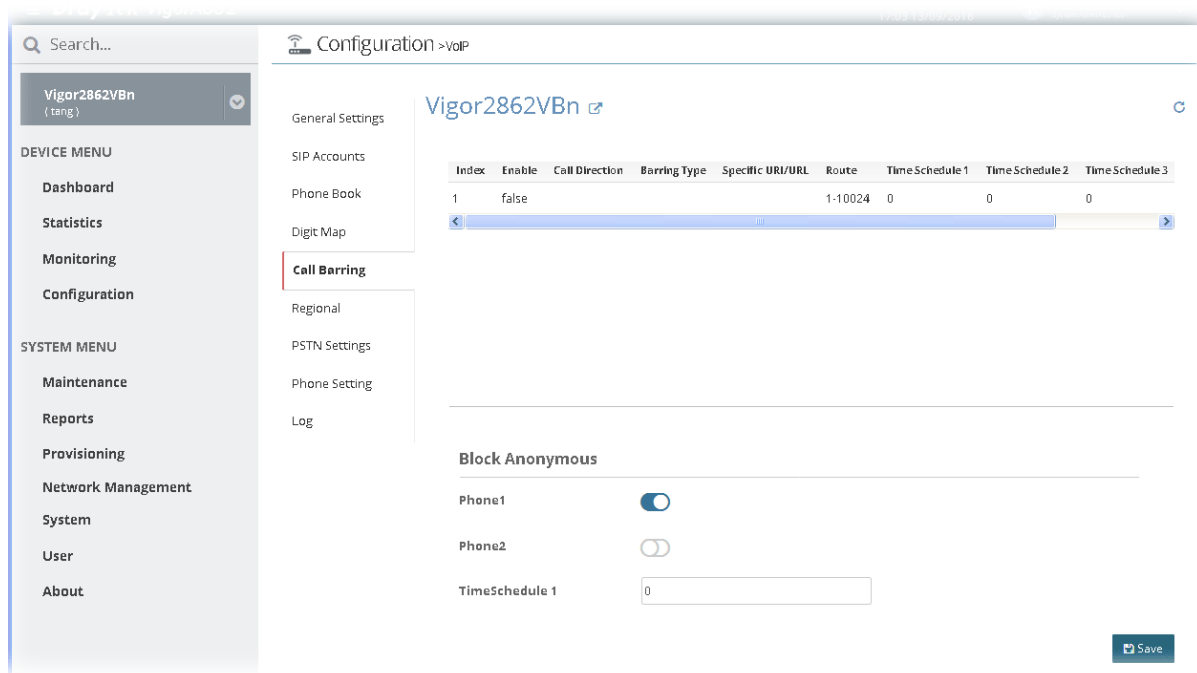


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

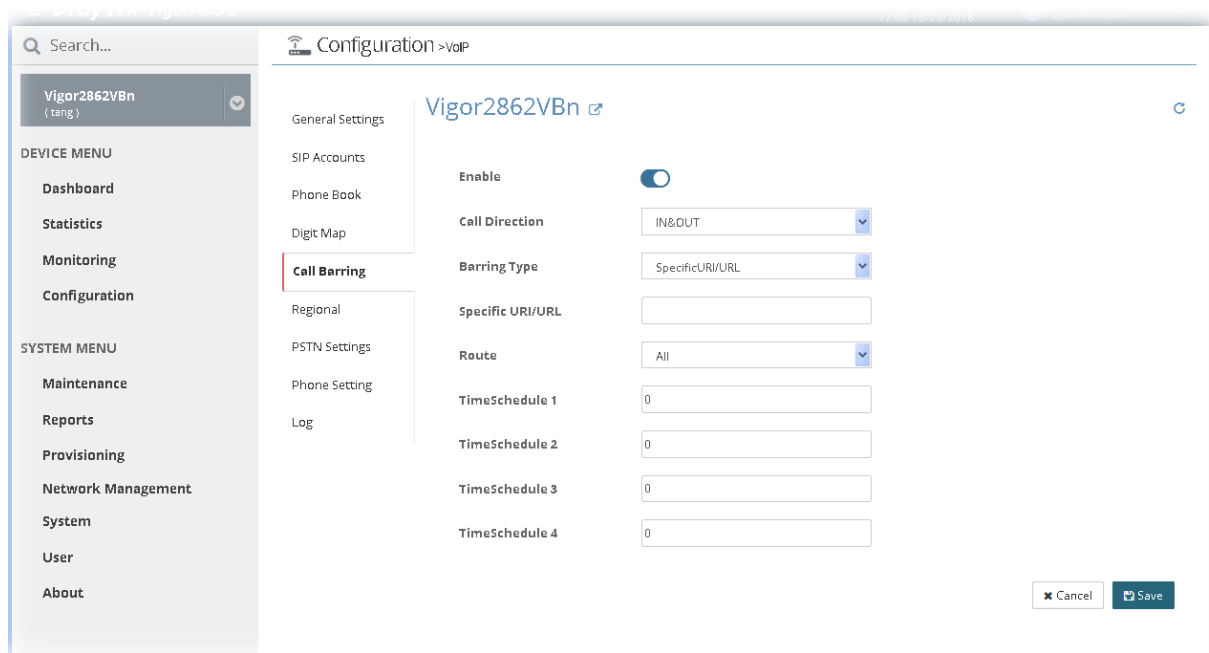


13.13.5 Call Barring

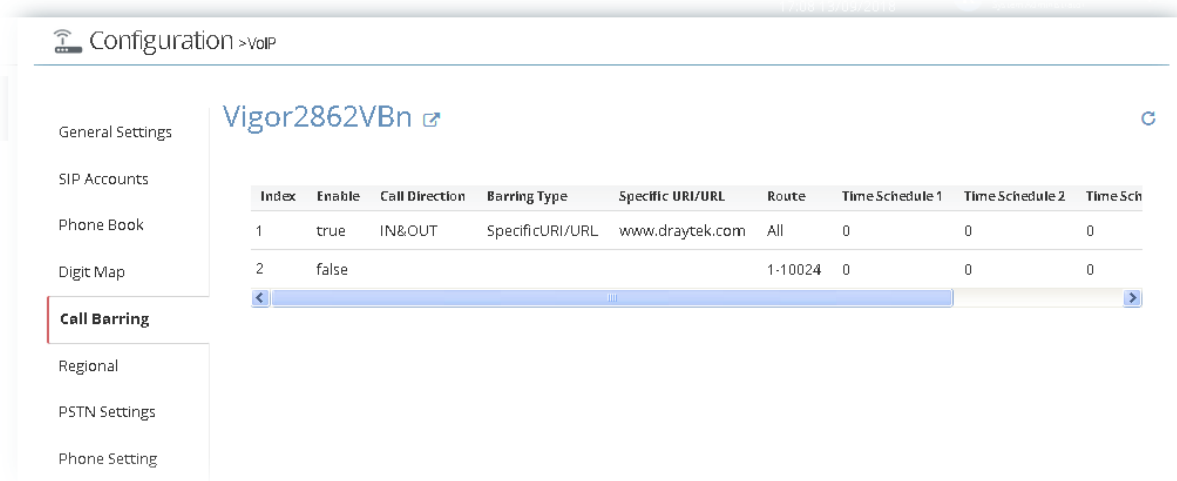
Call barring is used to block phone calls coming from the one that is not welcomed.



To create / modify a call barring profile, move the mouse cursor on the table and click any one of the index number (e.g., #1 for a new profile) to get the following page.

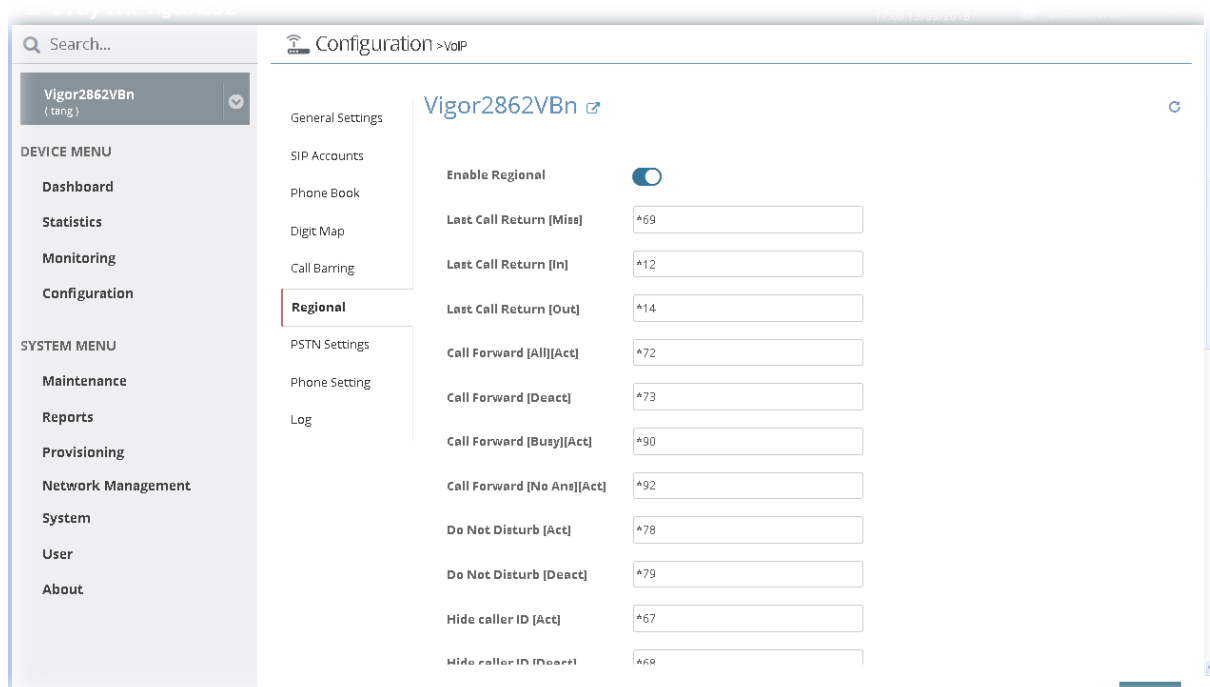


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.



13.13.6 Regional

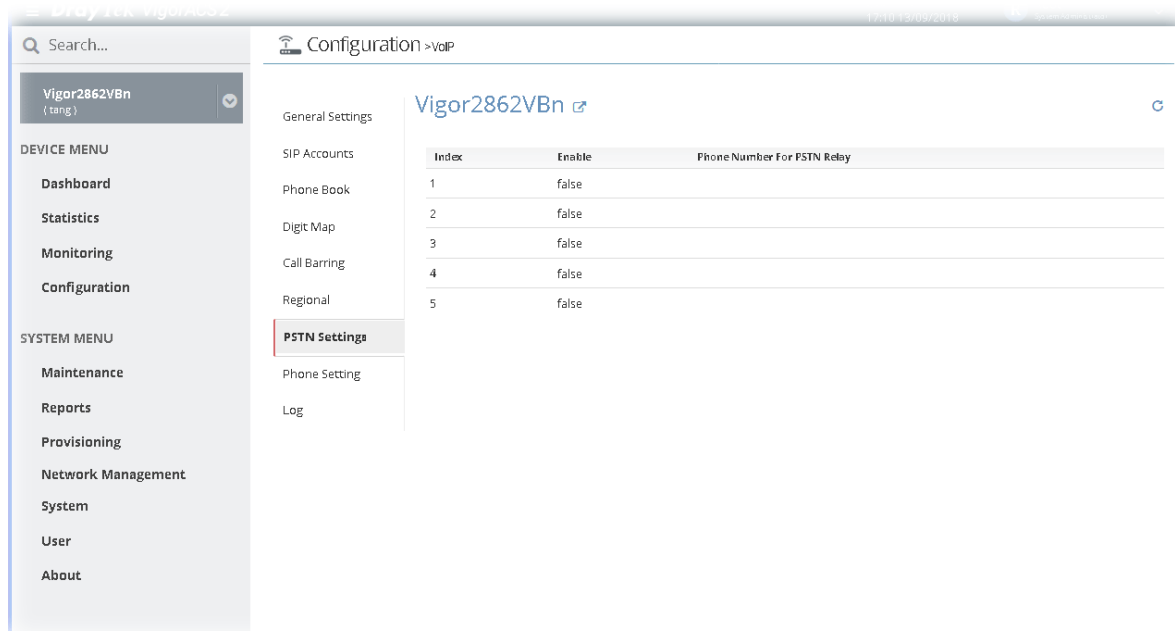
This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.



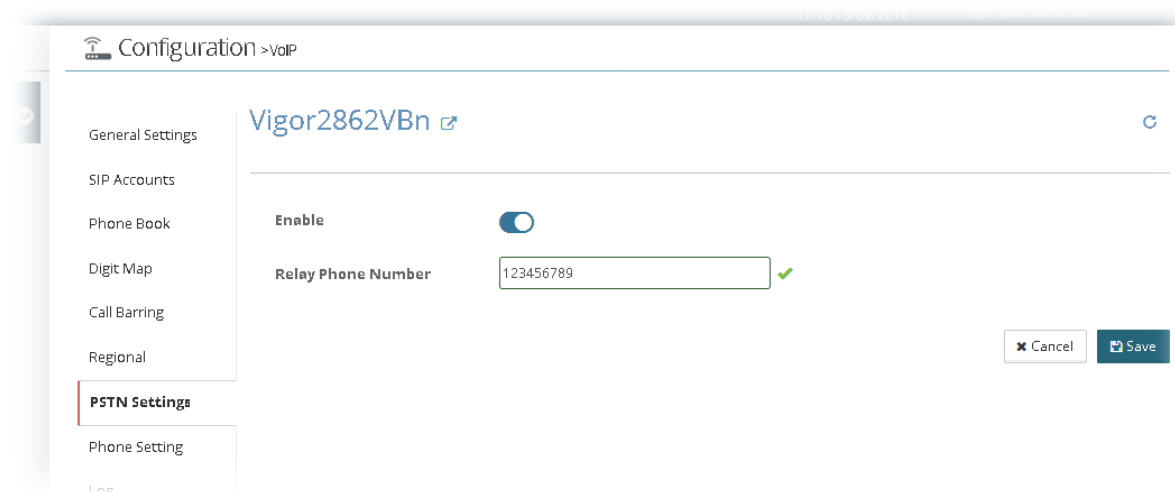
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.13.7 PSTN Settings

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Check the **Enable** box to make the PSTN number available for dial whenever you need and type the number in the field of **Phone number for PSTN relay**.



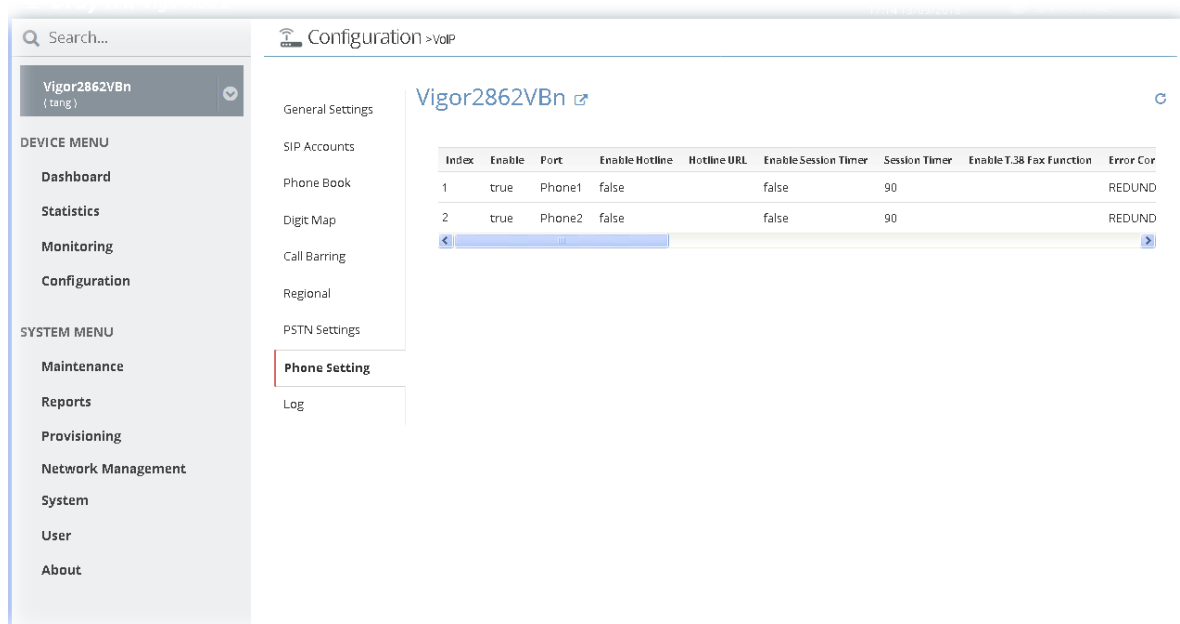
To modify a PSTN profile, move the mouse cursor on the table and click any one of the index number to get the following page.



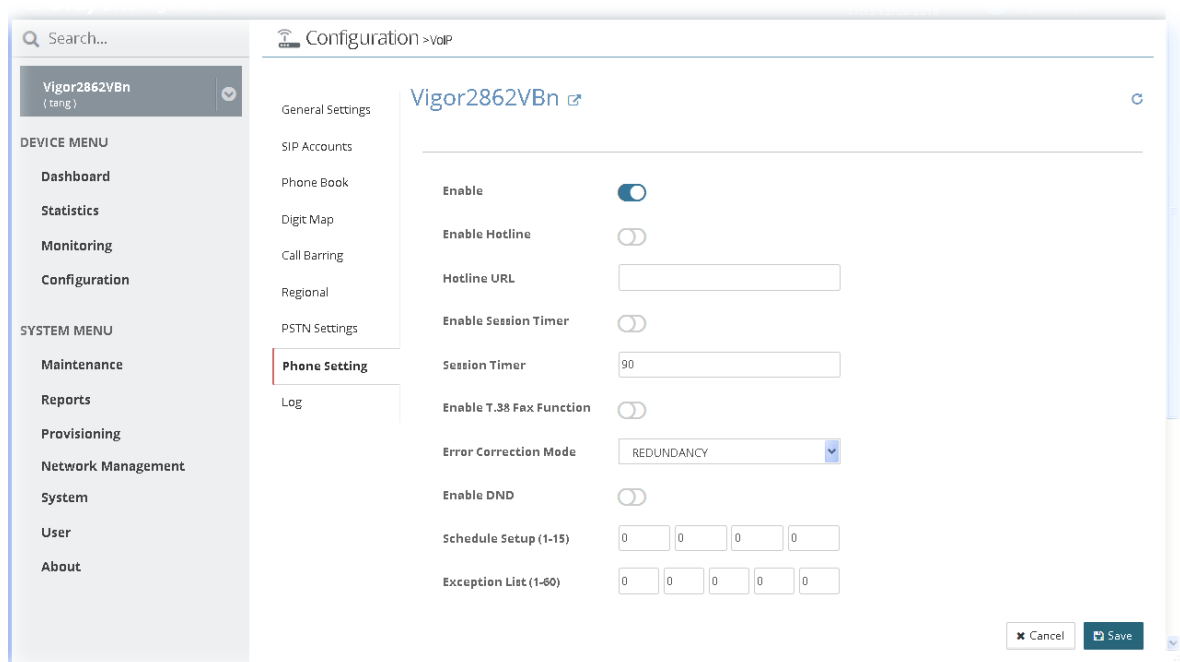
After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.13.8 Phone Setting

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.



To modify a phone setting profile, move the mouse cursor on the table and click any one of the index number to get the following page.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.13.9 Log

From this page, you can connection and other important call status for each port.

The screenshot shows the configuration interface for a Vigor2862VBn device. The main content area displays the 'Log' page, which contains a table of call records. The table has the following columns: Index, Date, Time, Duration, In/Out/Miss, Account ID, and Peer Number. The data in the table is as follows:

Index	Date	Time	Duration	In/Out/Miss	Account ID	Peer Number
1	00-00-0	00:00:00	00:00:00		0	
2	00-00-0	00:00:00	00:00:00		0	
3	00-00-0	00:00:00	00:00:00		0	
4	00-00-0	00:00:00	00:00:00		0	
5	00-00-0	00:00:00	00:00:00		0	
6	00-00-0	00:00:00	00:00:00		0	
7	00-00-0	00:00:00	00:00:00		0	
8	00-00-0	00:00:00	00:00:00		0	
9	00-00-0	00:00:00	00:00:00		0	
10	00-00-0	00:00:00	00:00:00		0	

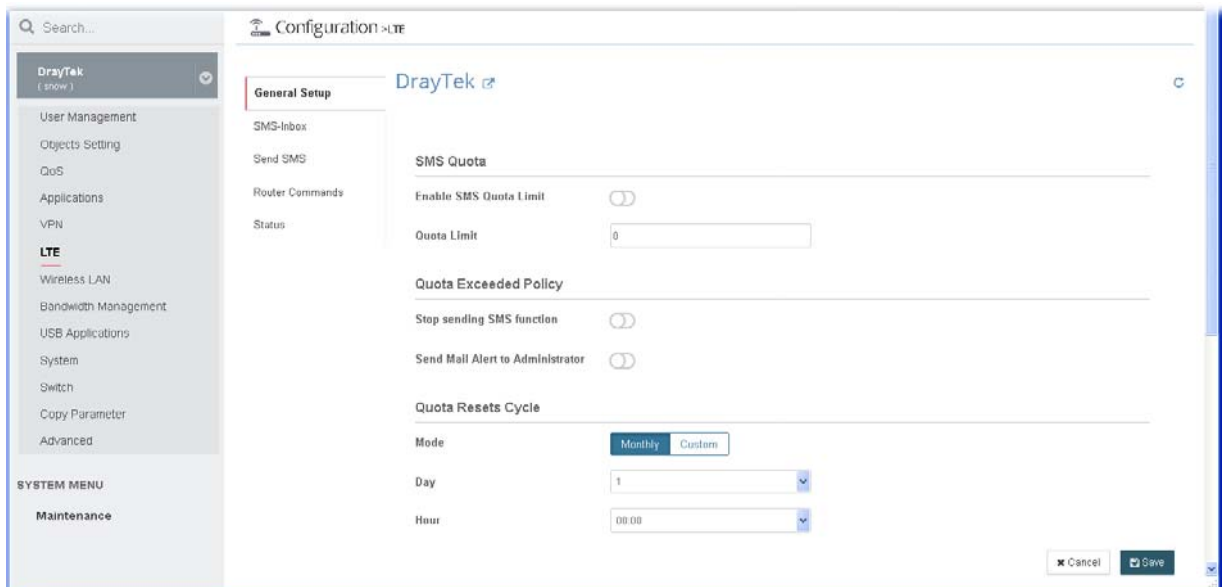
13.14 LTE Settings for CPE

LTE WAN with SIM card can provide convenient Internet access for Vigor router. VigorACS system administrator can configure LTE WAN settings for the selected CPE to perform SMS related operations.

13.14.1 General Setup

VigorACS user (with the privilege above the operator) can configure general settings of LTE router. When SMS Quota Limit is enabled, you can specify the number of SMS quota, actions to perform when quota exceeded, and the period of resetting SMS quota used.

This web page allows you to determine which policy shall be used for SMS inbox/outbox.

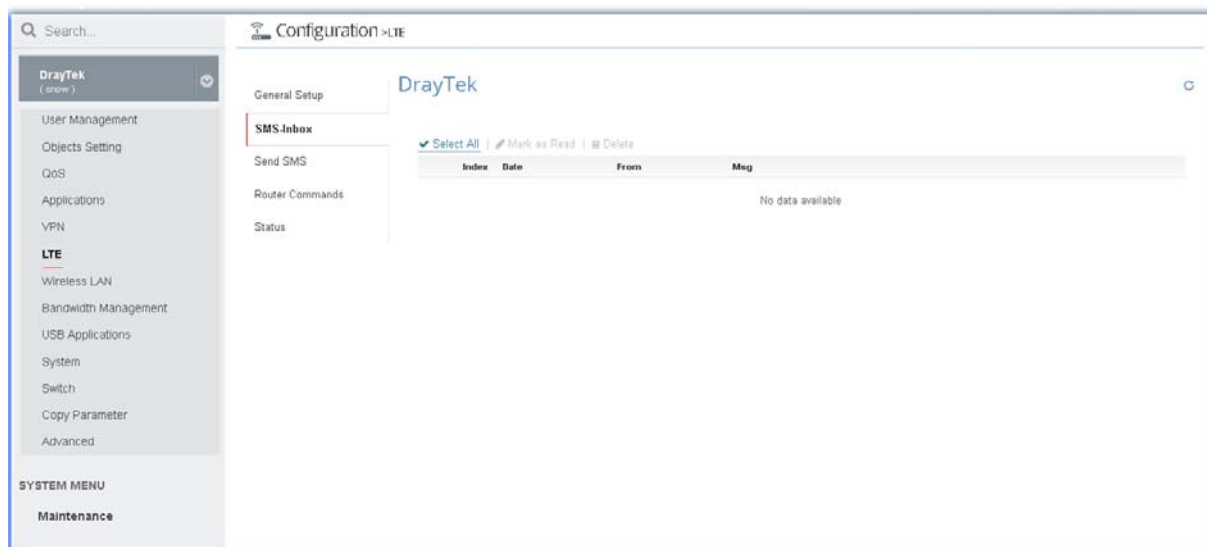


The screenshot shows the DrayTek Configuration interface for LTE settings. The left sidebar contains a navigation menu with categories like User Management, Objects Setting, QoS, Applications, VPN, LTE, Wireless LAN, Bandwidth Management, USB Applications, System, Switch, Copy Parameter, and Advanced. The main content area is titled 'Configuration > LTE' and 'General Setup'. It includes sections for 'SMS-Inbox', 'Send SMS', 'Router Commands', and 'Status'. The 'SMS Quota' section has a toggle for 'Enable SMS Quota Limit' (disabled) and a text input for 'Quota Limit' (0). The 'Quota Exceeded Policy' section has toggles for 'Stop sending SMS function' (disabled) and 'Send Mail Alert to Administrator' (disabled). The 'Quota Resets Cycle' section has a 'Mode' selector (Monthly/Custom), a 'Day' dropdown (1), and a 'Hour' dropdown (00:00). 'Cancel' and 'Save' buttons are at the bottom right.

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

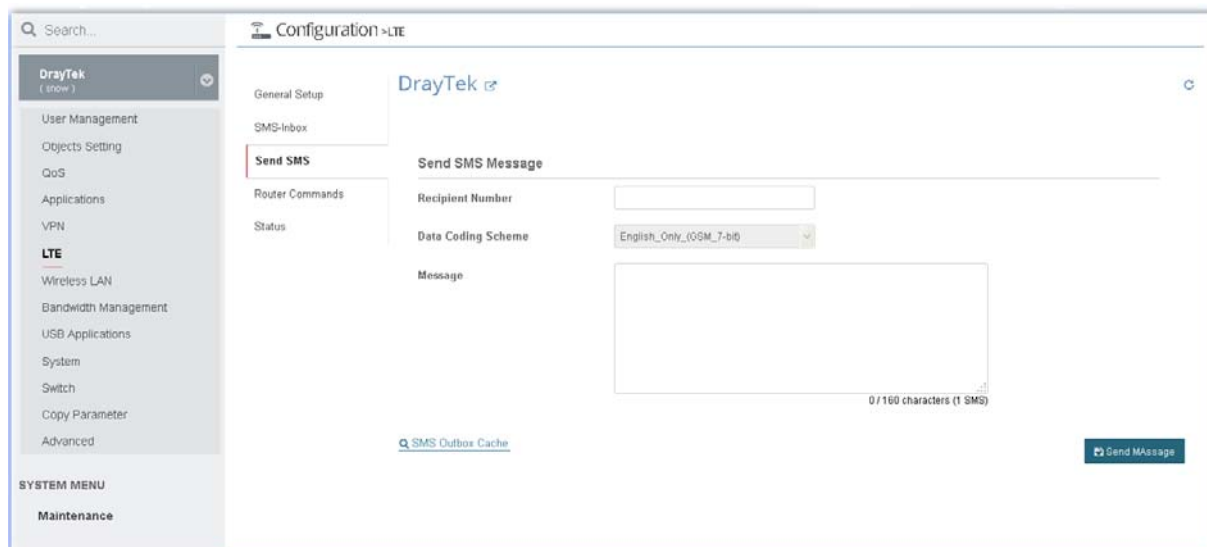
13.14.2 SMS-Inbox

This page will list the received SMS messages in the LTE SIM card. The SMS Inbox table shows the received date, the phone number or sender ID where this message was from, and the beginning of the message content.



13.14.3 Send SMS

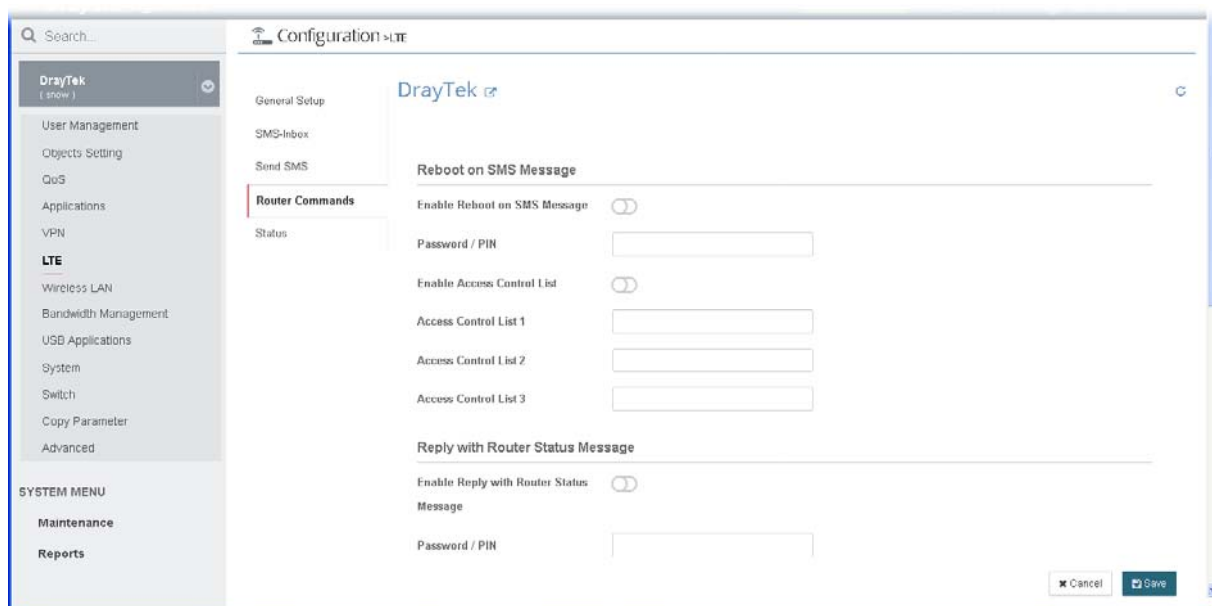
This page is used to send SMS messages by the LTE SIM card. It also displays the number of SMS required to send the message.



After finished the settings configuration, click **Send Message** to send this SMS message to the recipient immediately.

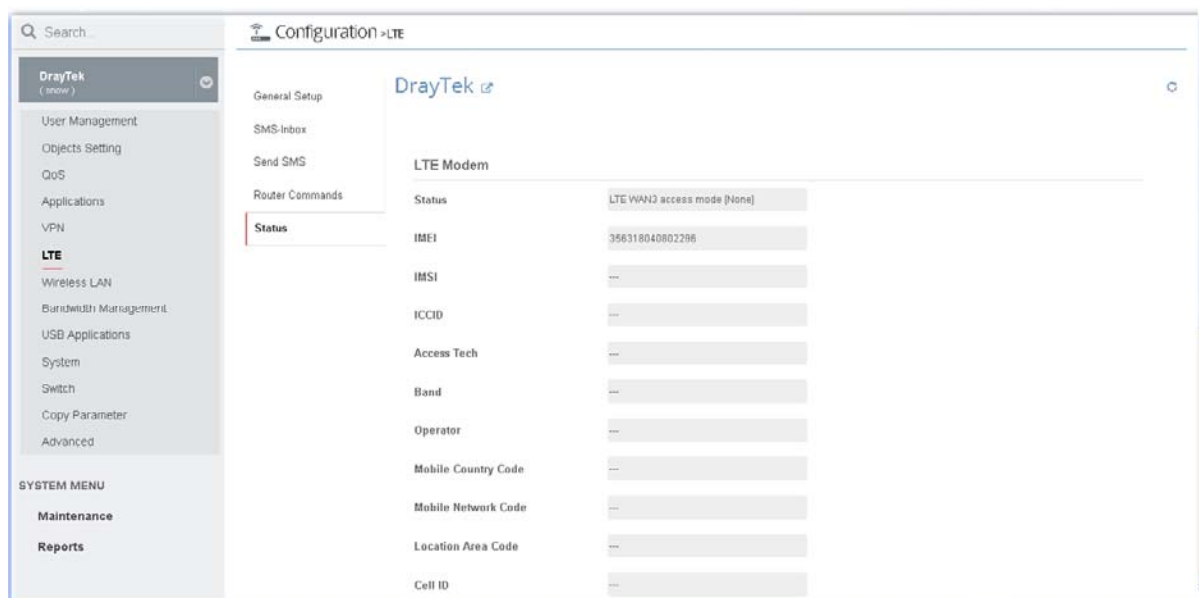
13.14.4 Router Commands

VigorACS system administrator can set functions to reboot Vigor router remotely and get the router status via SMS.



13.14.5 Status

This page can display basic information about the embedded LTE module and the current LTE connection of the selected CPE.

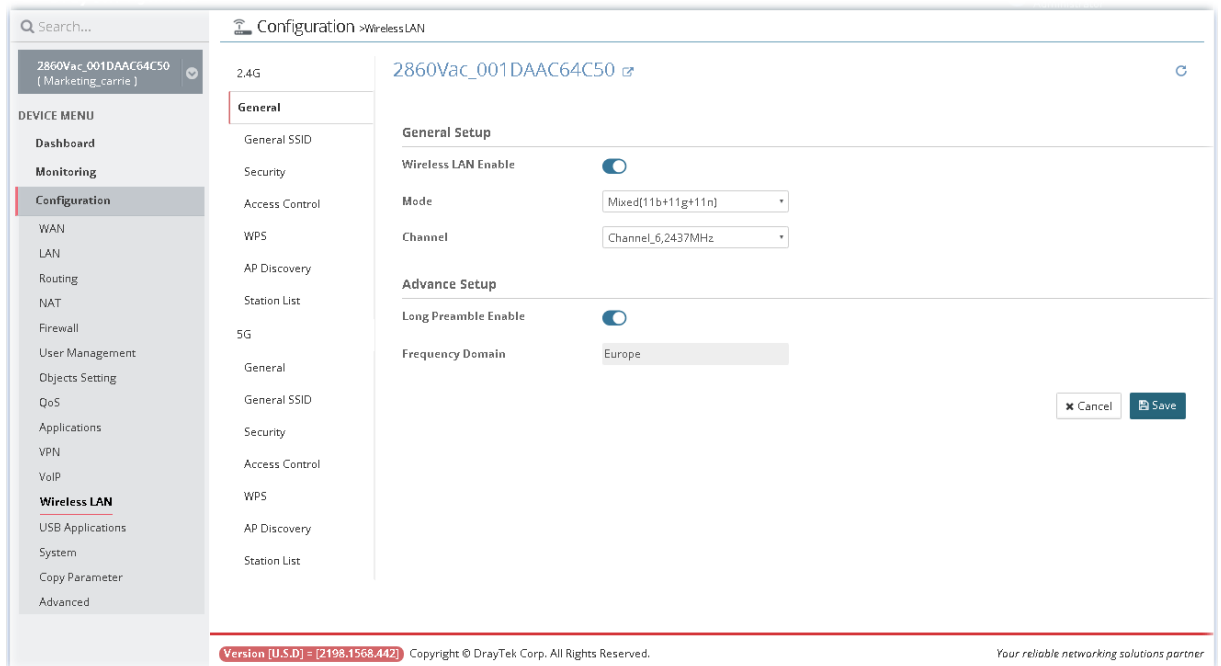


13.15 Wireless LAN Settings for CPE

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

13.15.1 General Setting for 2.4G/5G

Such page allows system administrator / user to configure the wireless mode, the wireless channel, and enable long preamble (2.4GHz / 5GHz wireless network).



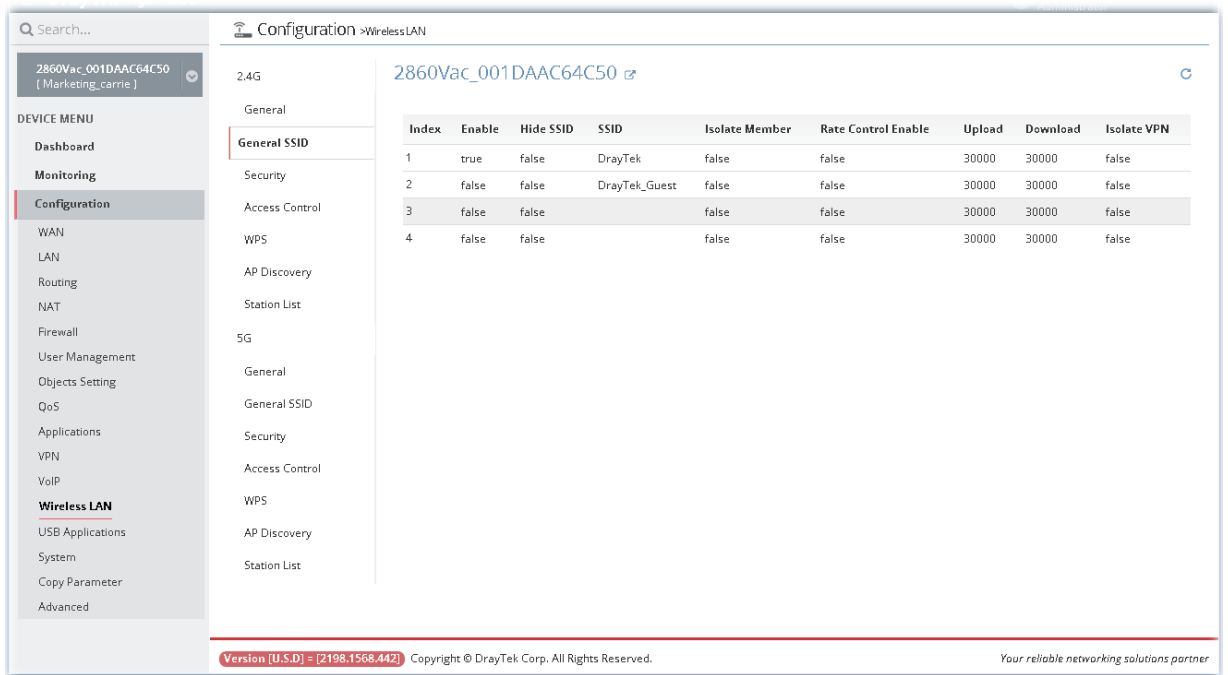
The screenshot shows the configuration page for a wireless LAN interface. The interface is divided into several sections:

- Left Sidebar (DEVICE MENU):** Contains navigation options such as Dashboard, Monitoring, Configuration (highlighted), WAN, LAN, Routing, NAT, Firewall, User Management, Objects Setting, QoS, Applications, VPN, VoIP, Wireless LAN (highlighted), USB Applications, System, Copy Parameter, and Advanced.
- Top Bar:** Shows the current configuration path: Configuration > Wireless LAN.
- Main Content Area:**
 - 2.4G Section:** Includes a sub-menu for General (selected), Security, Access Control, WPS, AP Discovery, and Station List.
 - 2860Vac_001DAAC64C50 Section:** Includes a sub-menu for General (selected), Security, Access Control, WPS, AP Discovery, and Station List.
 - General Setup:**
 - Wireless LAN Enable:
 - Mode: Mixed(11b+11g+11n)
 - Channel: Channel_6,2437MHz
 - Advance Setup:**
 - Long Preamble Enable:
 - Frequency Domain: Europe
- Bottom Bar:** Contains the text "Version [U.S.D] = [2198.1568.442] Copyright © DrayTek Corp. All Rights Reserved." and "Your reliable networking solutions partner".

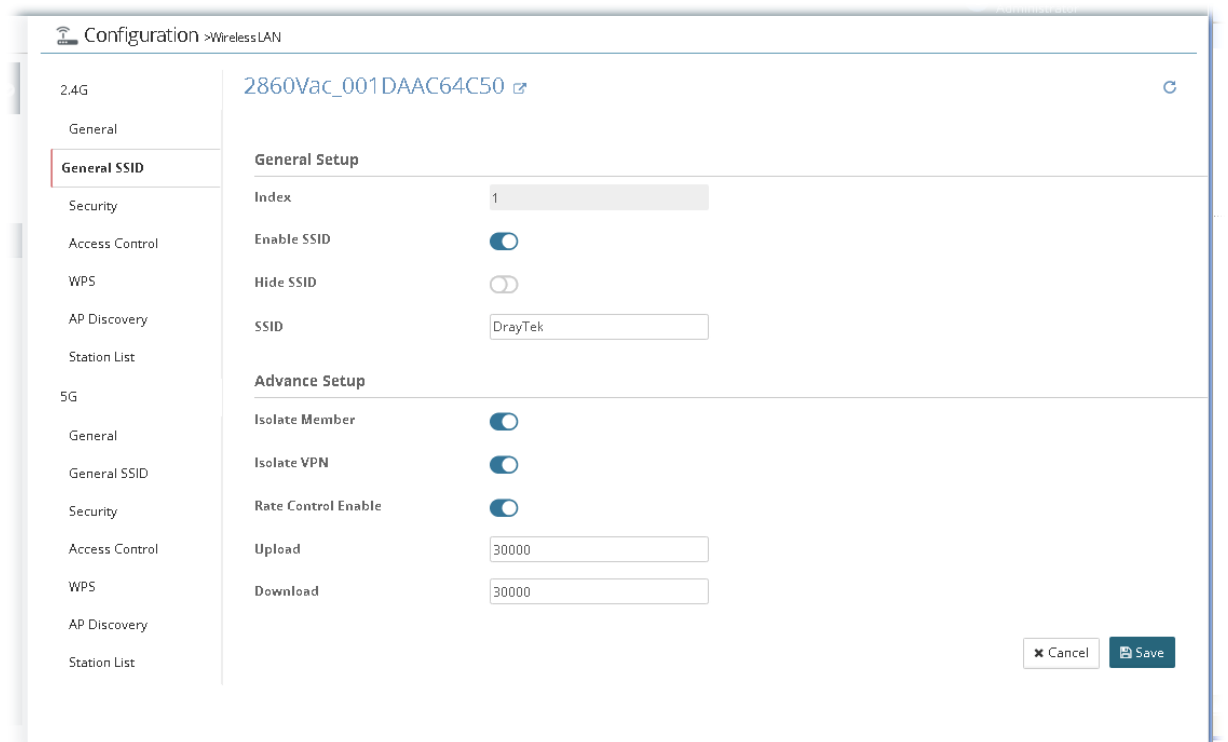
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.2 General SSID for 2.4G/5G

Such page allows system administrator / user to configure the SSID, isolate LAN user, isolate VPN, and enable rate control (for 2.4GHz / 5GHz wireless network).



To modify SSID, move the mouse cursor on the table and click any one of the index number (e.g., #1) to get the following page.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.3 Security for 2.4G/5G

Such page is used for configuring security with different modes for SSID 1, 2, 3 and 4 respectively.

Index	Mode	WPA Encryption Mode	WEP Encryption Mode	WEP Key Index
1	Mixed(WPA+WPA2)/PSK	TKIP_for_WPA/AES_for_WPA2		1
2	Disable	TKIP_for_WPA/AES_for_WPA2		1
3	Disable	TKIP_for_WPA/AES_for_WPA2		1
4	Disable	TKIP_for_WPA/AES_for_WPA2		1

To modify the security profile, move the mouse cursor on the table and click any one of the index number (e.g., #1) to get the following page.

General Setup

Index: 1

Mode: Mixed(WPA+WPA2)/PSK

WPA

WPA Encryption Mode: TKIP_for_WPA/AES_for_WPA2

WPA Pre-shared Key:

Type 8-63 ASCII character or 64 Hexadecimal digits leading by "0x"

Cancel Save

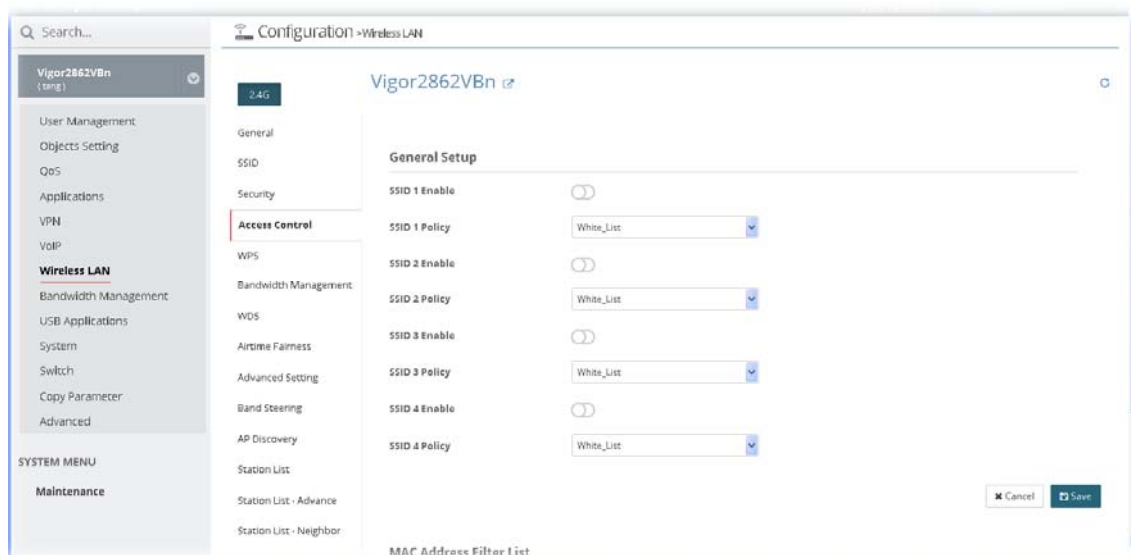
After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.4 Access Control for 2.4G/5G

Vigor router can restrict wireless connection to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

This page allows the administrator / user to configure access control settings for the router via VigorACS 2.

In such section, Vigor2862VBn is selected as an example for displaying access control settings.

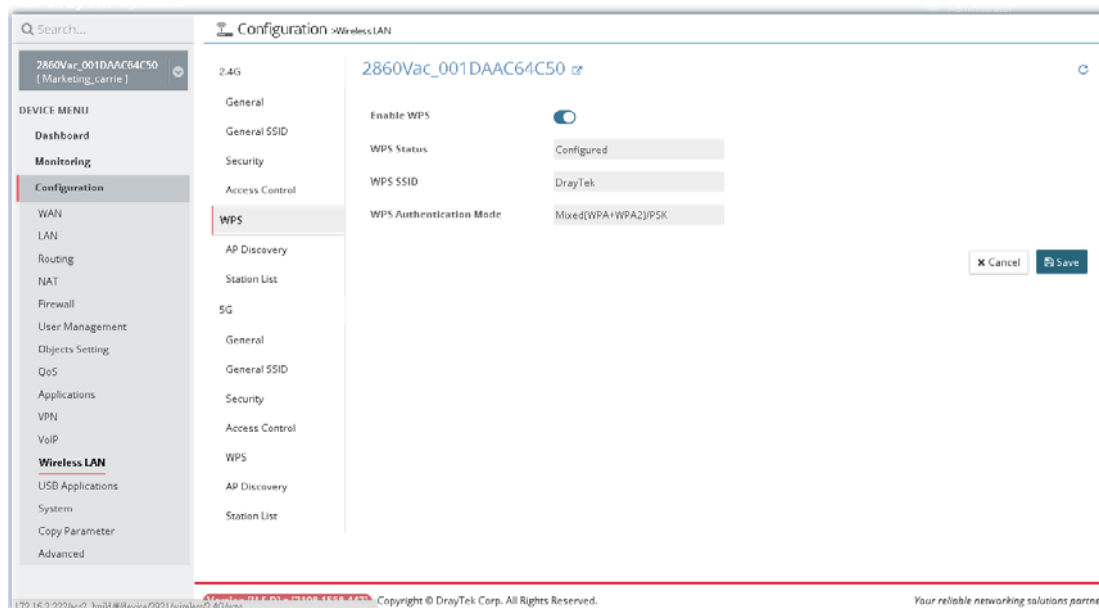


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.5 WPS for 2.4G/5G

WPS provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

This page allows the administrator / user to configure WPS settings for the router via VigorACS 2.

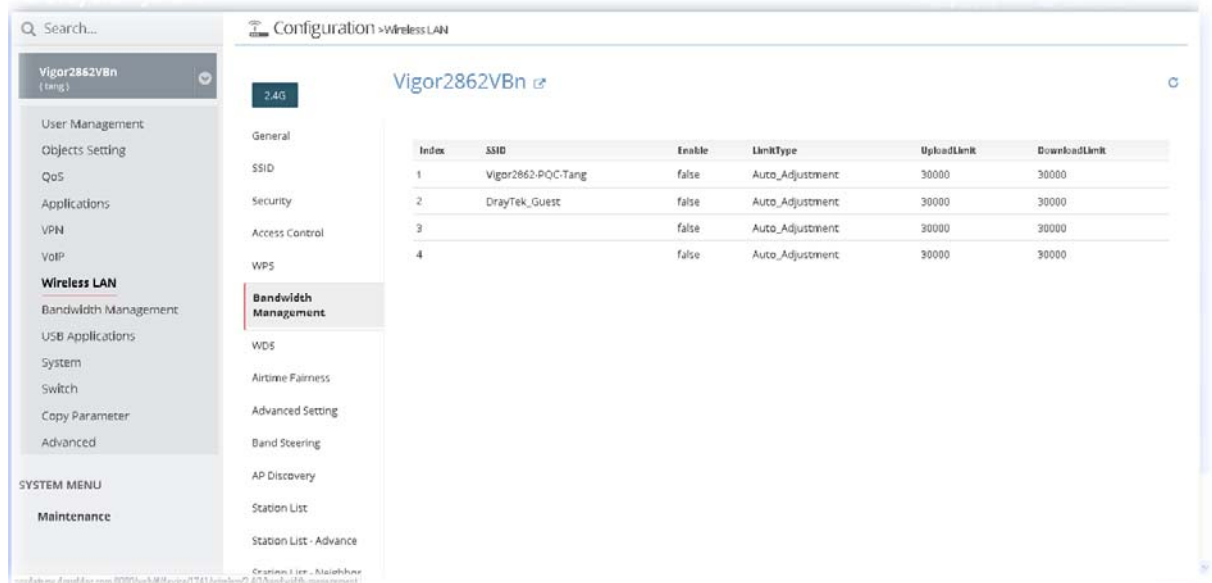


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

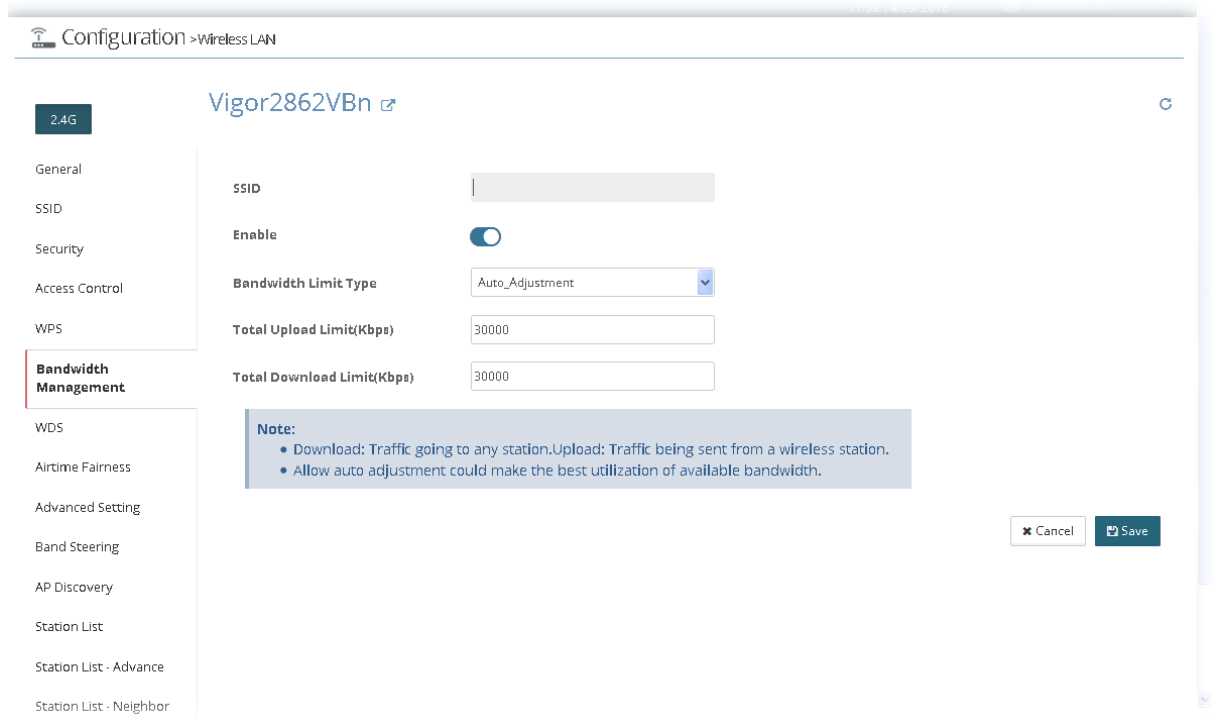
13.15.6 Bandwidth Management for 2.4G/5G

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.

In such section, Vigor2862VBn is selected as an example for displaying bandwidth management settings.



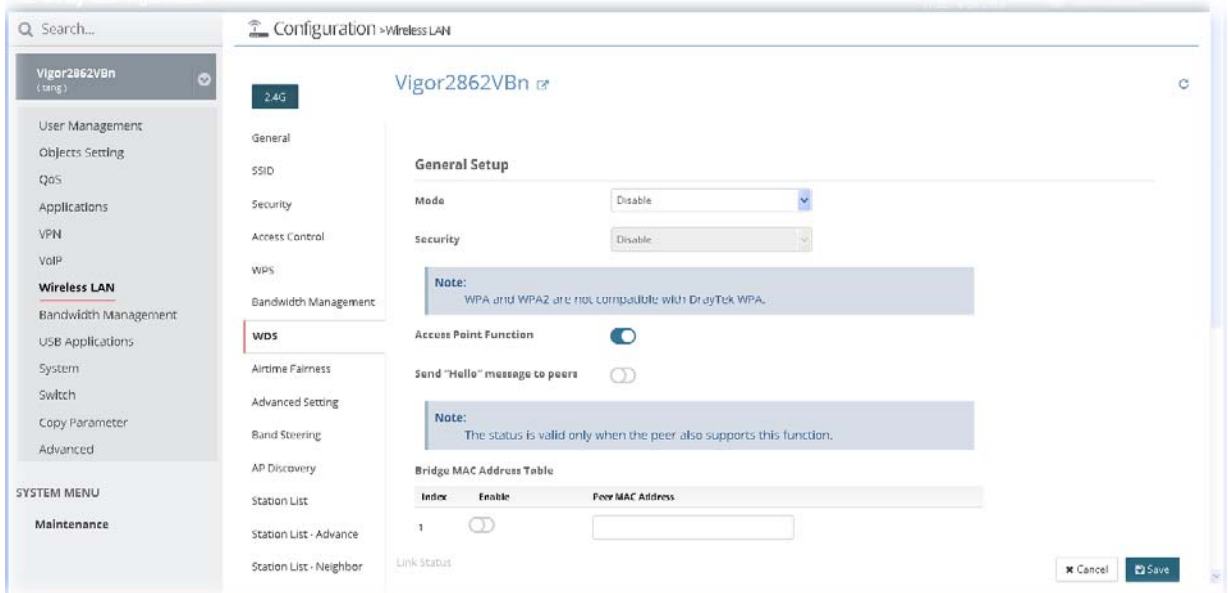
To modify the bandwidth management profile, move the mouse cursor on the table and click any one of the index number (e.g., #1) to get the following page.



After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.15.7 WDS for 2.4G/5G

In such section, Vigor2862VBn is selected as an example for displaying WDS settings.



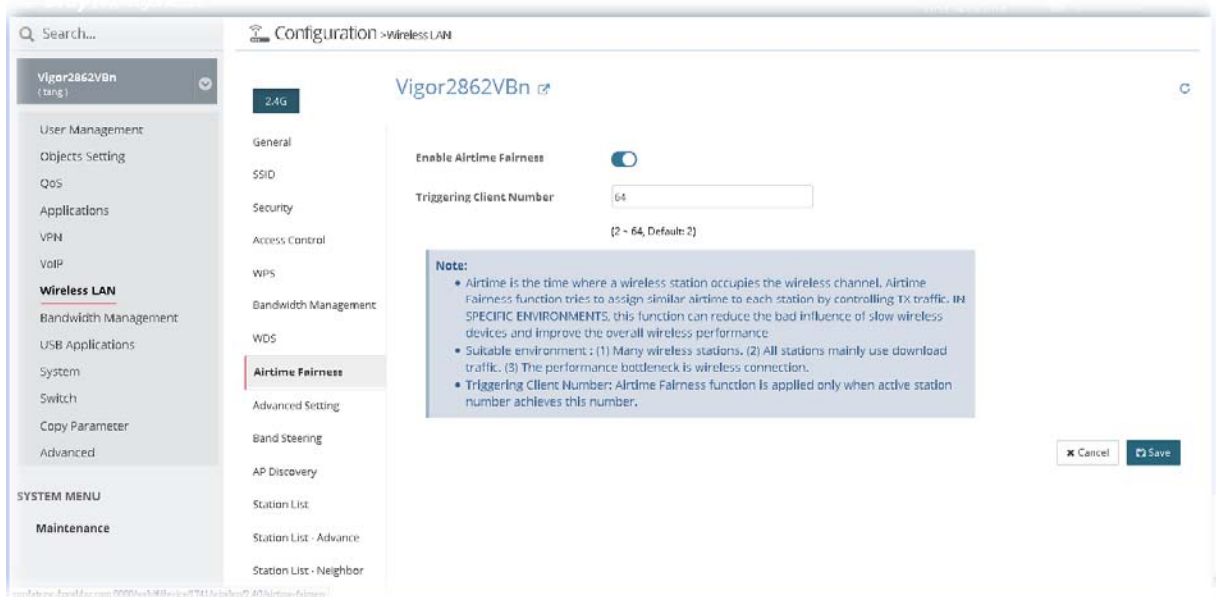
After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.15.8 Airtime Fairness for 2.4G/5G

IN SPECIFIC ENVIRONMENTS, airtime fairness can reduce the bad influence of slow wireless devices and improve the overall wireless performance. Suitable environment:

- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

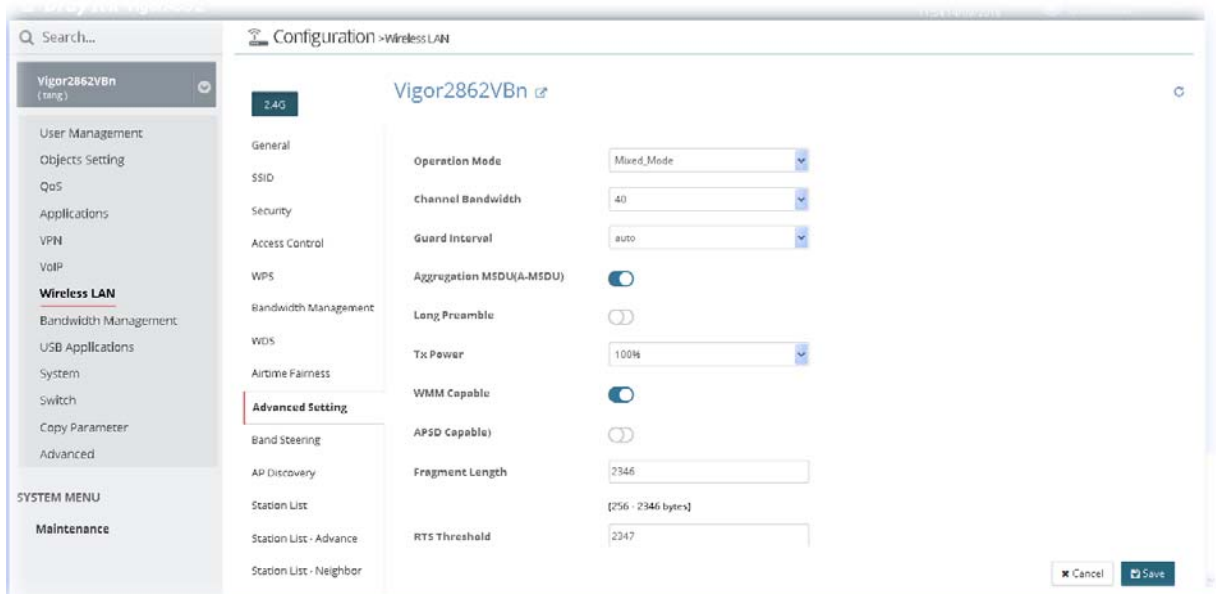
In such section, Vigor2862VBn is selected as an example for displaying airtime fairness settings.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.9 Advanced Setting for 2.4G/5G

In such section, Vigor2862VBn is selected as an example for displaying advanced settings.

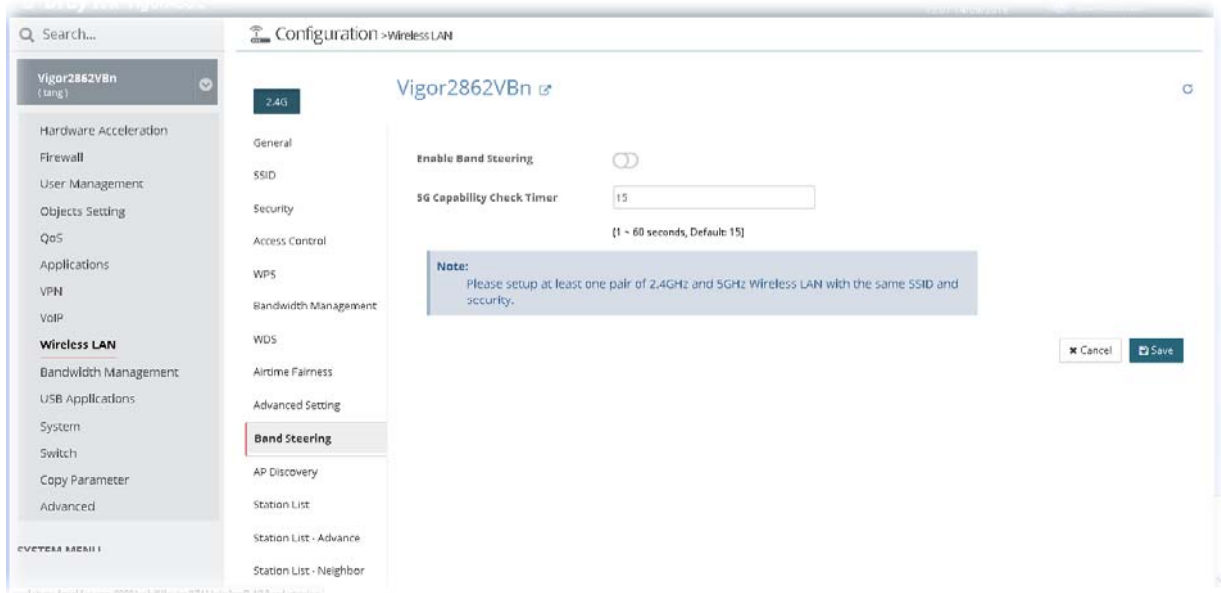


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.10 Band Steering for 2.4G/5G

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

In such section, Vigor2862VBn is selected as an example for displaying band steering settings.

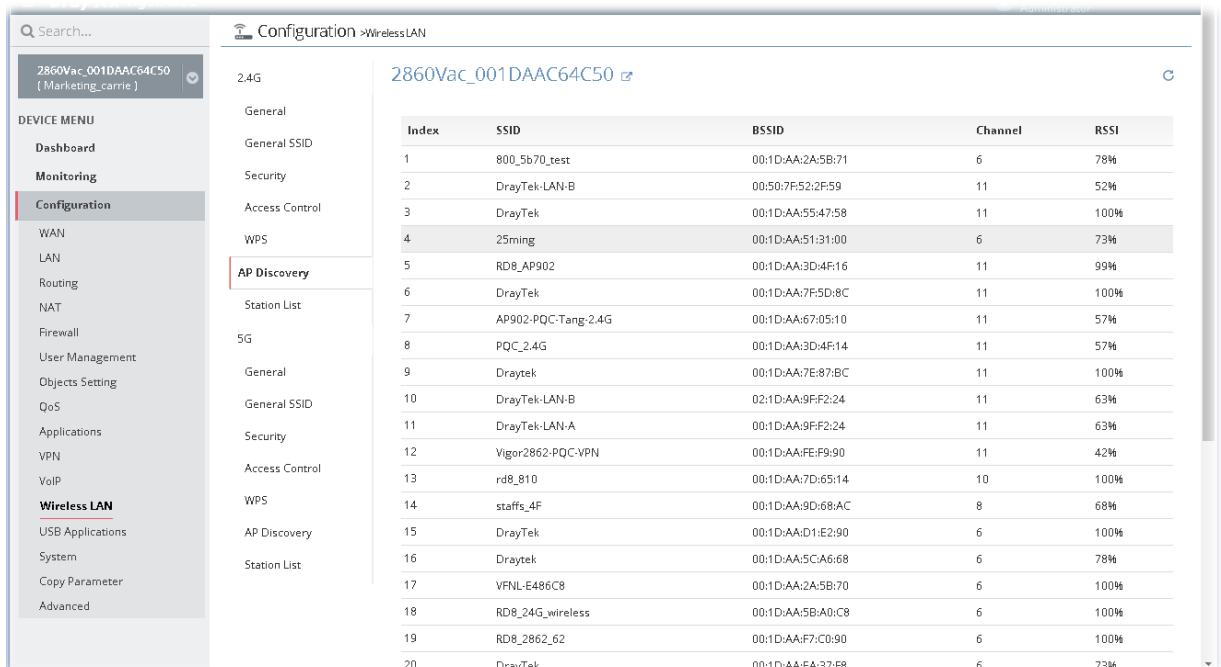


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.11 AP Discovery for 2.4G/5G

VigorACS 2 can scan all regulatory channels and find working APs in the neighborhood for Vigor router. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor router.

This page is used to scan the existence of the APs on the wireless LAN.



13.15.12 Station List for 2.4G/5G

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, neighbor) will display different status information (including IP address, MAC address, Associated with, AID, RSSI, Rate, BW, PSM, WMM, PhMd, MCS, Venfor, Approx. Distance, SSID, Visit Time and so on).

Version [U.S.D.] = [2198.1568.442] Copyright © DrayTek Corp. All Rights Reserved. Your reliable networking solutions partner

13.15.13 Roaming for 2.4G/5G

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

In such section, Vigor2862VBn is selected as an example for displaying roaming settings.

Cancel Save

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.15.14 Station Control for 2.4G/5G

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

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

In such section, VigorAP 903 is selected as an example for displaying roaming settings.

The screenshot displays the configuration page for AP 903_00507FF17ECA. The left sidebar contains two main menu sections: 'DEVICE MENU' and 'SYSTEM MENU'. Under 'DEVICE MENU', 'Configuration' is selected, and 'Wireless LAN' is highlighted. Under 'SYSTEM MENU', 'Maintenance' is selected, and 'Station Control' is highlighted. The main content area shows the 'Station Control' settings for the selected AP. A table lists four SSIDs with their respective 'Enable' status, 'Connect Time', and 'Reconnect Time'.

Index	SSID	Enable	Connect Time	Reconnect Time
1	rd8_ap903_SSID1	false	0_days_1_hours_0_mins	1_days_0_hours_0_mins
2	rd8_ap903_SSID2	false	0_days_1_hours_0_mins	1_days_0_hours_0_mins
3	rd8_ap903_SSID3	false	0_days_1_hours_0_mins	1_days_0_hours_0_mins
4	rd8_ap903_SSID4	false	0_days_1_hours_0_mins	1_days_0_hours_0_mins

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.16 Bandwidth Management Settings for CPE

In such section, Vigor2862VBn is selected as an example for displaying Bandwidth Management settings.

13.16.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

The screenshot shows the 'Sessions Limit' configuration page for Vigor2862VBn. The interface includes a sidebar with navigation options and a main content area with the following details:

- IPv4 Section:**
 - Enable:
 - Default Max Sessions: 65534
 - Limitation List table:

Index	Start IP	End IP	Max Sessions
1	0.0.0.0	0.0.0.0	0
 - Clear All link
- IPv6 Section:**
 - Enable:
 - Default Max Sessions: 100
 - Limitation List table:

Index	Start IP	End IP	Max Sessions
1			0

Buttons: Cancel, Save

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

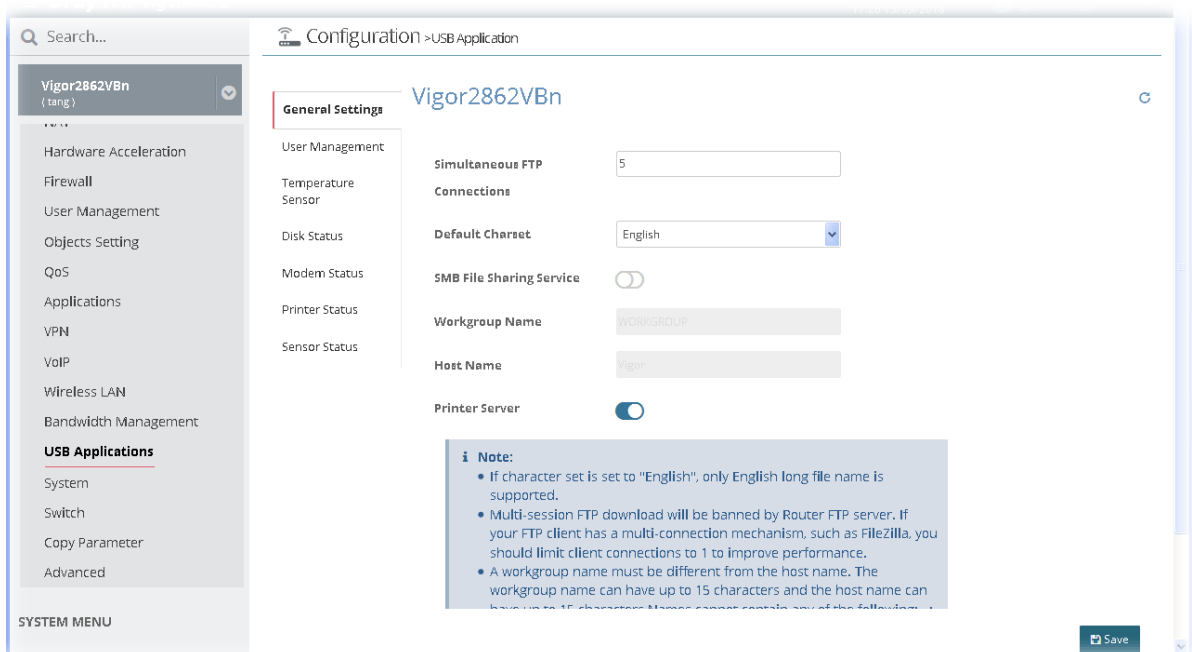
13.17 USB Applications Settings for CPE

In such section, Vigor2862VBn is selected as an example for displaying USB Applications settings.

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the SMB service through Vigor router.

13.17.1 General Settings

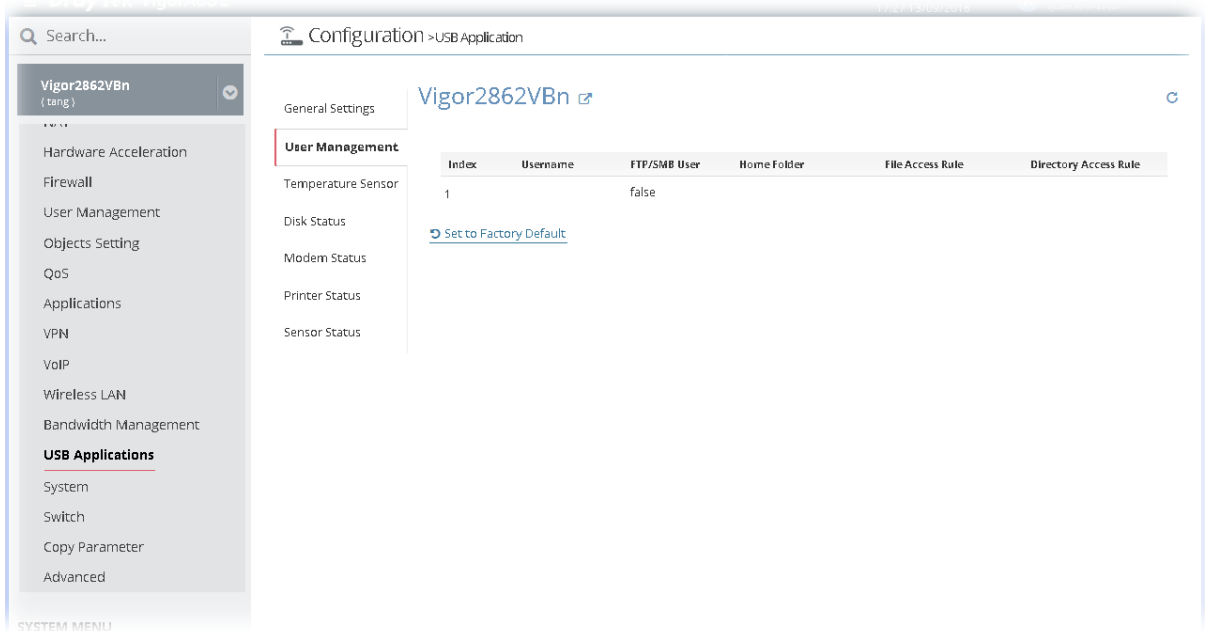
It determines the number of concurrent FTP connection, default charset for FTP server and enable SMB service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).



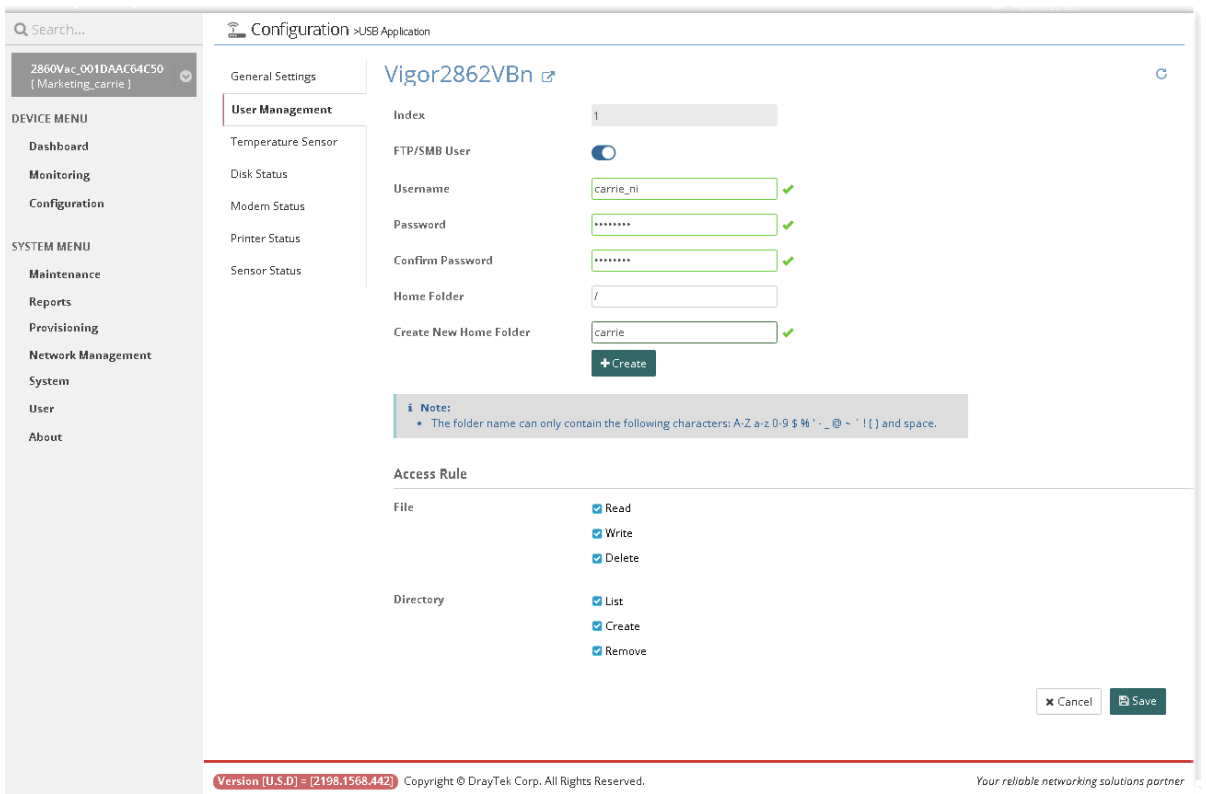
After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.17.2 User Management

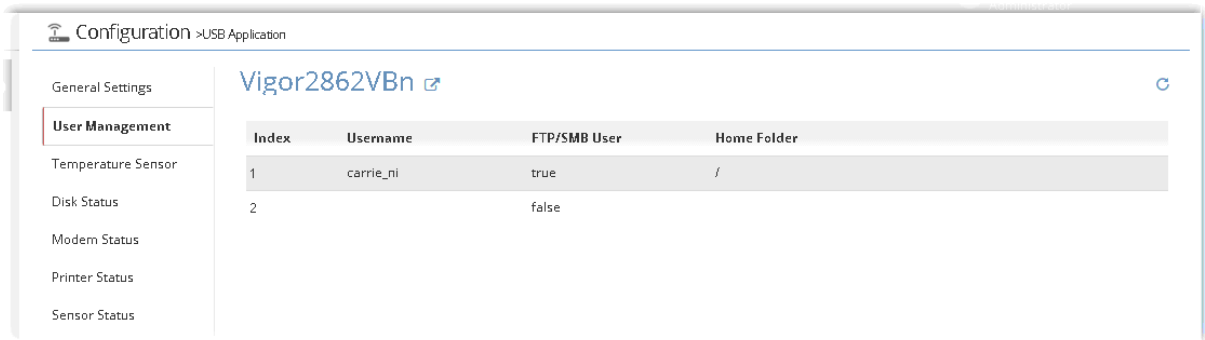
This page allows you to set profiles for FTP/SMB users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.



Click the number under index field to access into configuration page.

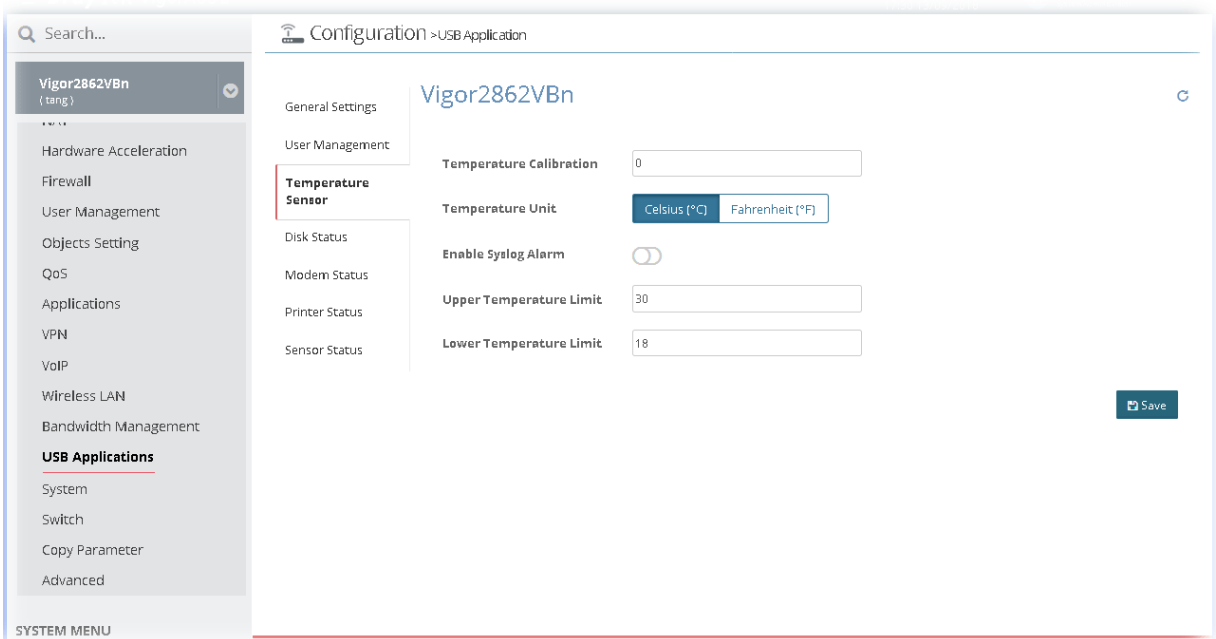


After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.



13.17.3 Temperature Sensor

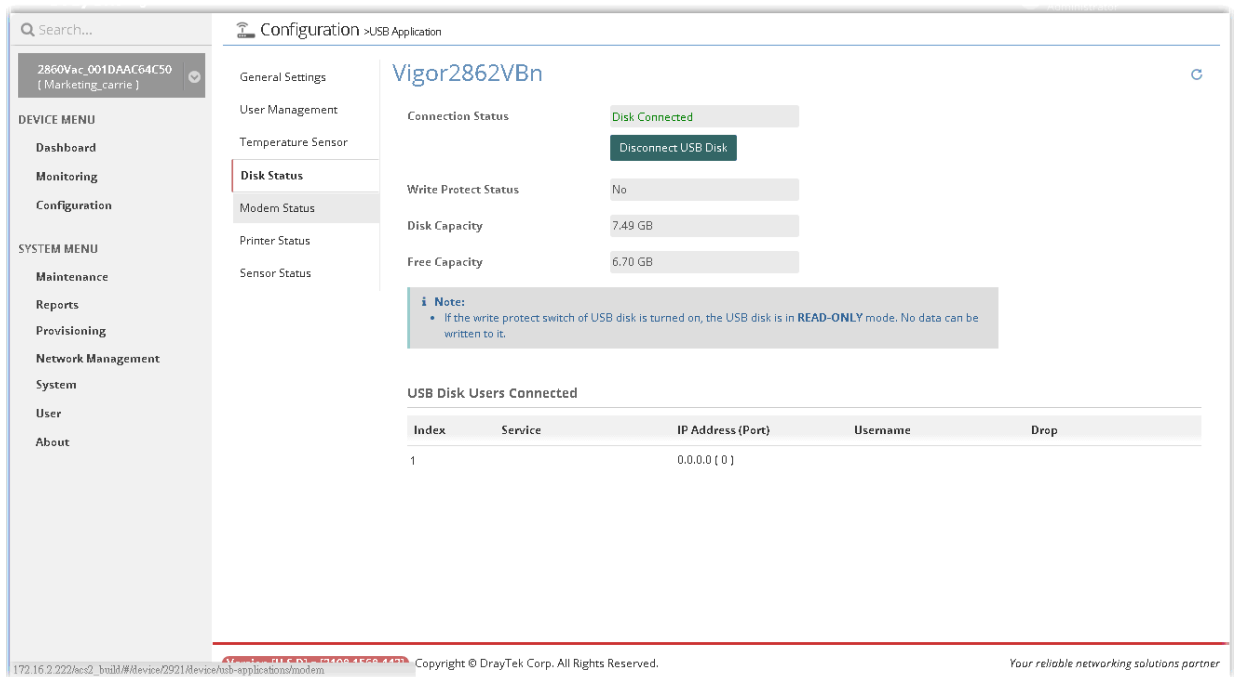
A USB thermometer attached to Vigor router can help monitor the server or data communications for room environment, and notify if the server room or data communications room is overheating.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

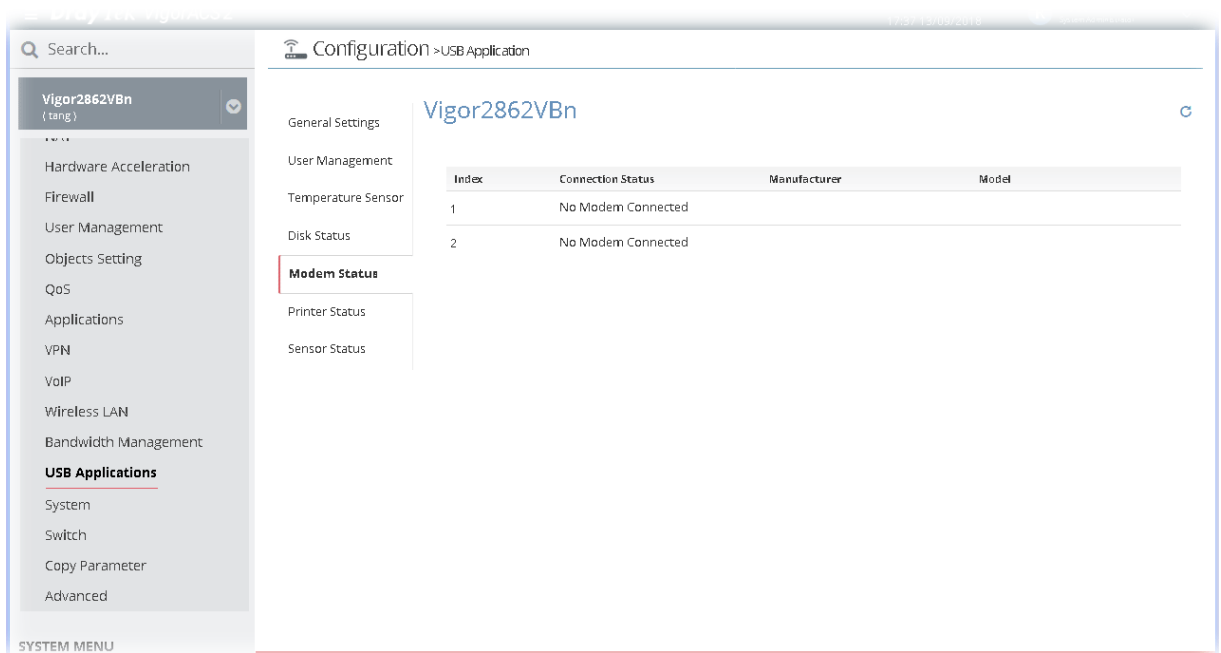
13.17.4 Disk Status

This page allows you to set profiles for FTP/SMB users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

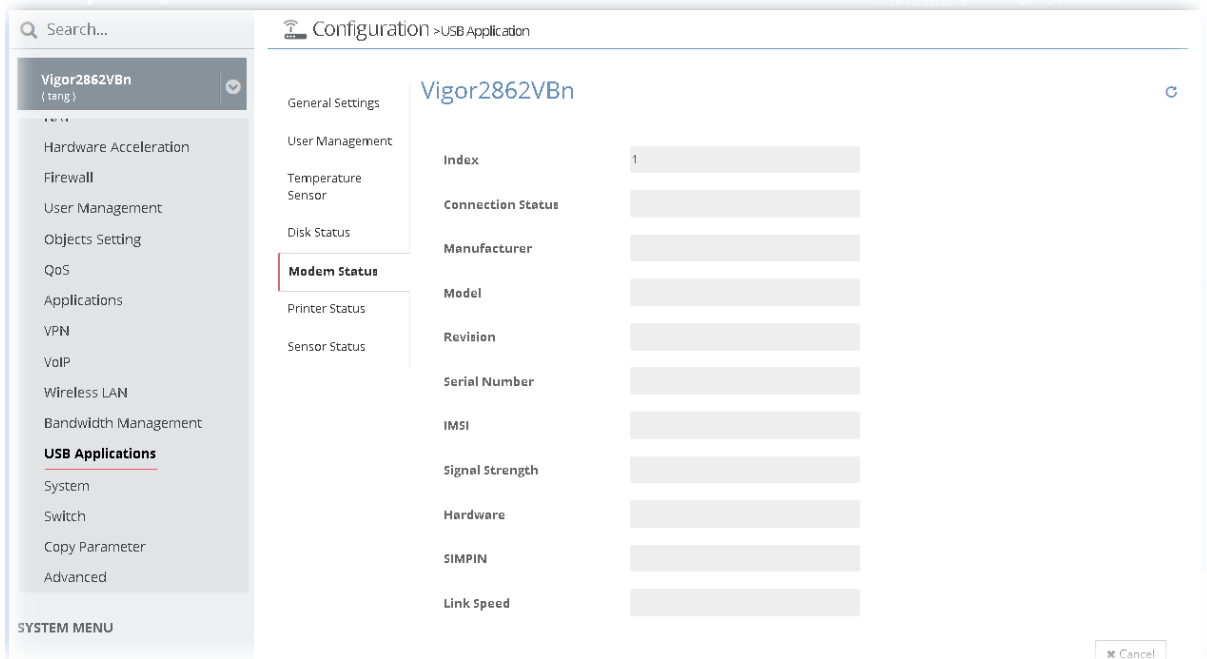


13.17.5 Modem Status

This page displays current status for the USB modem connecting to Vigor router managed by VigorACS 2.

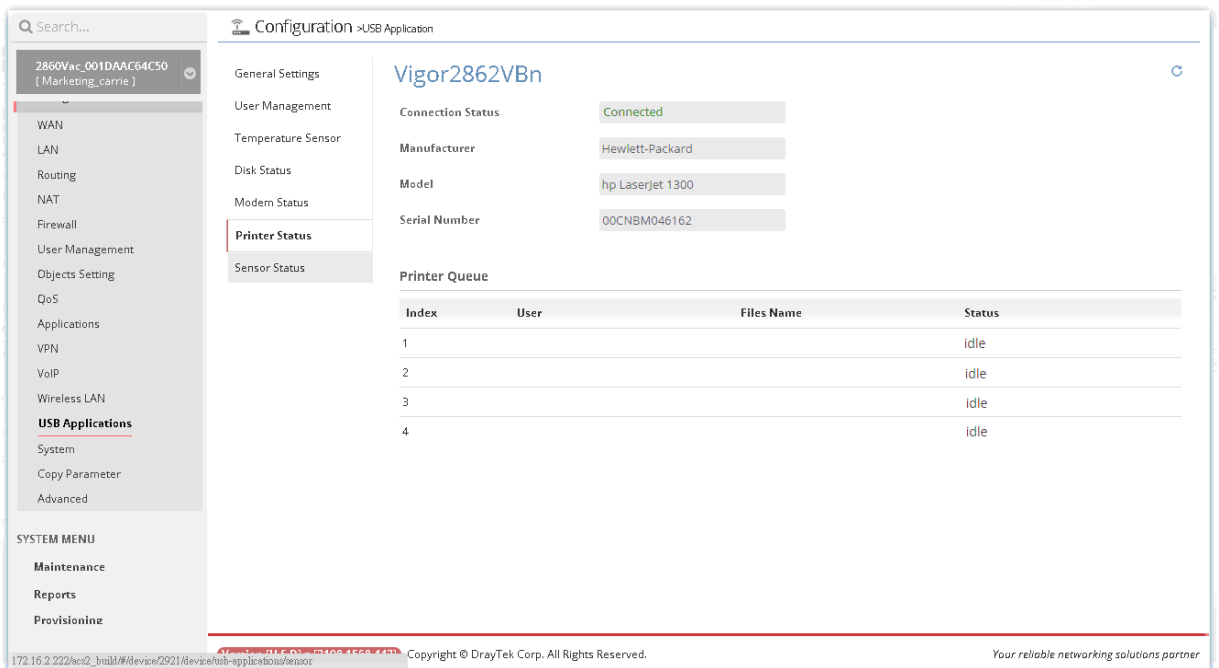


Click the index number to open the following for viewing detailed information for parameter settings.



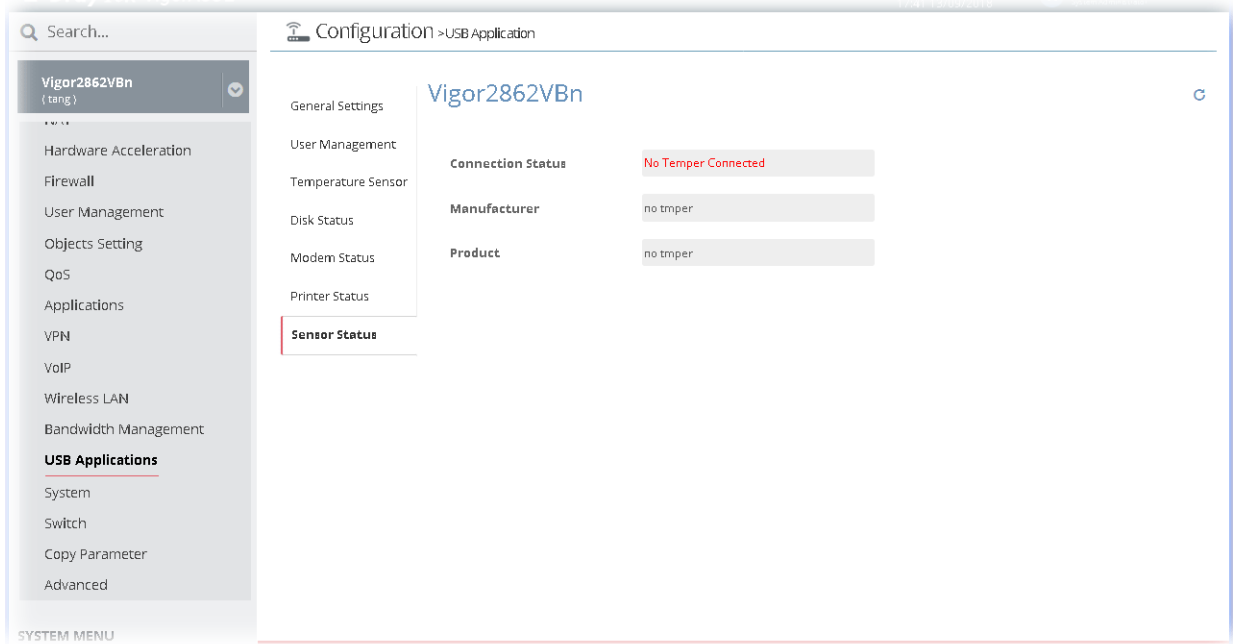
13.17.6 Printer Status

This page displays current status for the USB printer connecting to Vigor router managed by VigorACS 2.



13.17.7 Sensor Status

This page displays current status for the USB thermometer connecting to Vigor router managed by VigorACS 2.

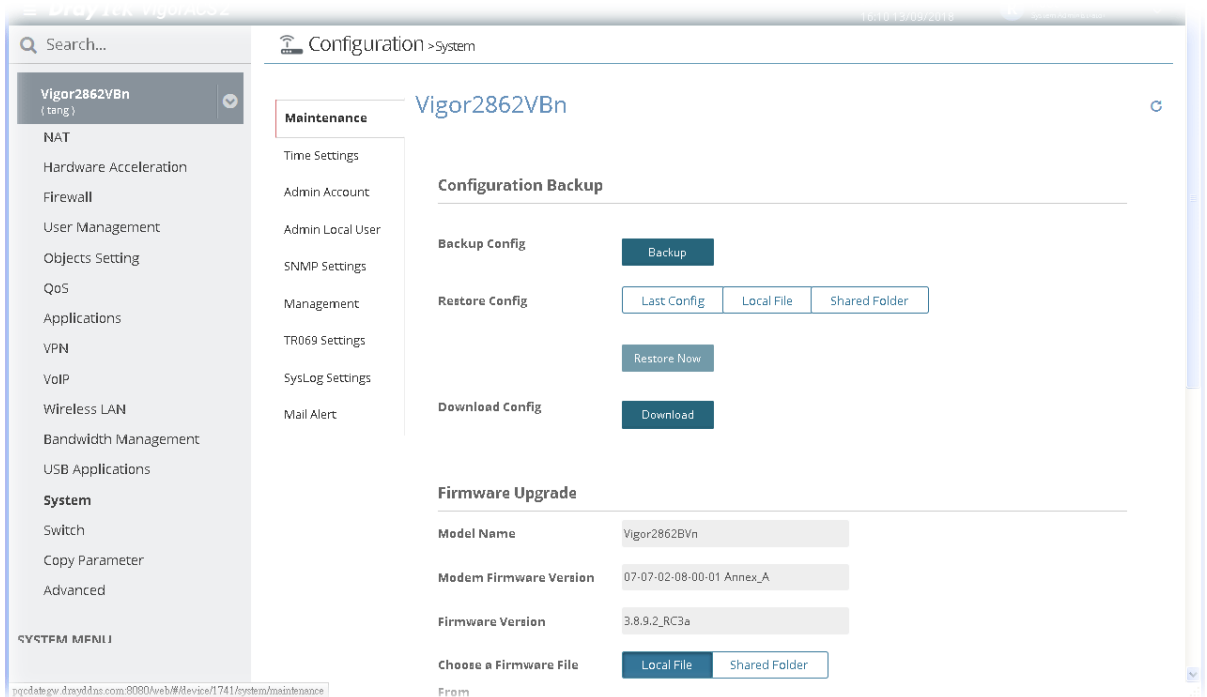


13.18 System Settings for CPE

In such section, Vigor2862VBn is selected as an example for displaying Applications settings.

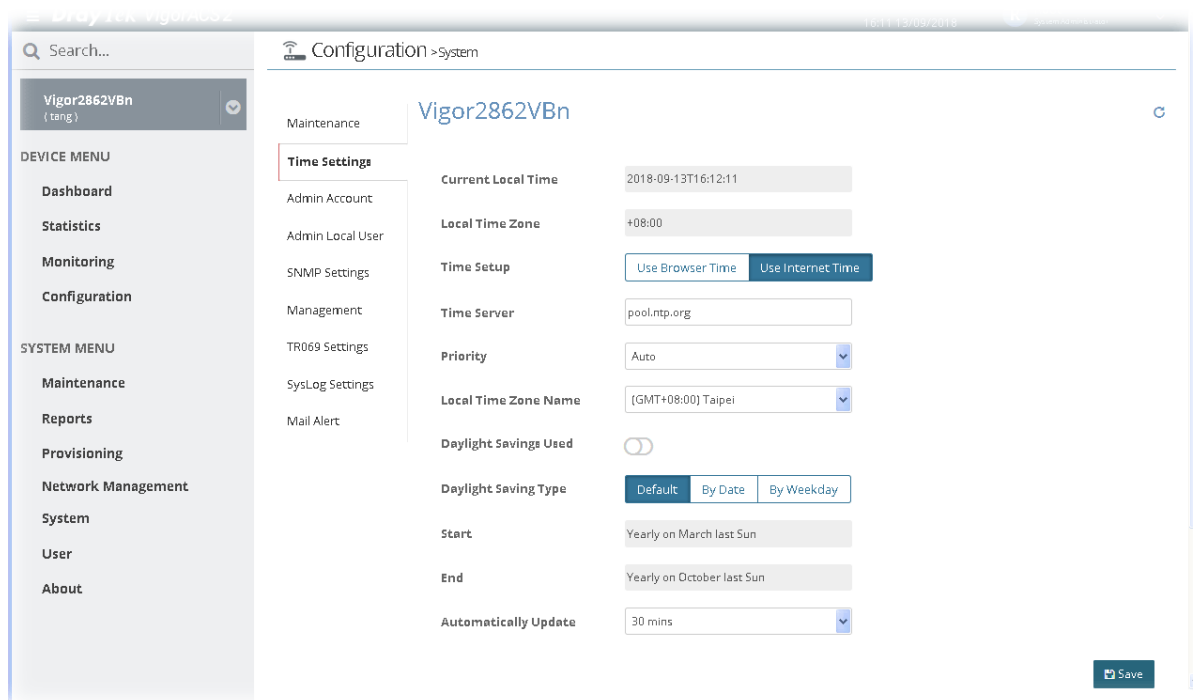
13.18.1 Maintenance

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 2.



13.18.2 Time Settings

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

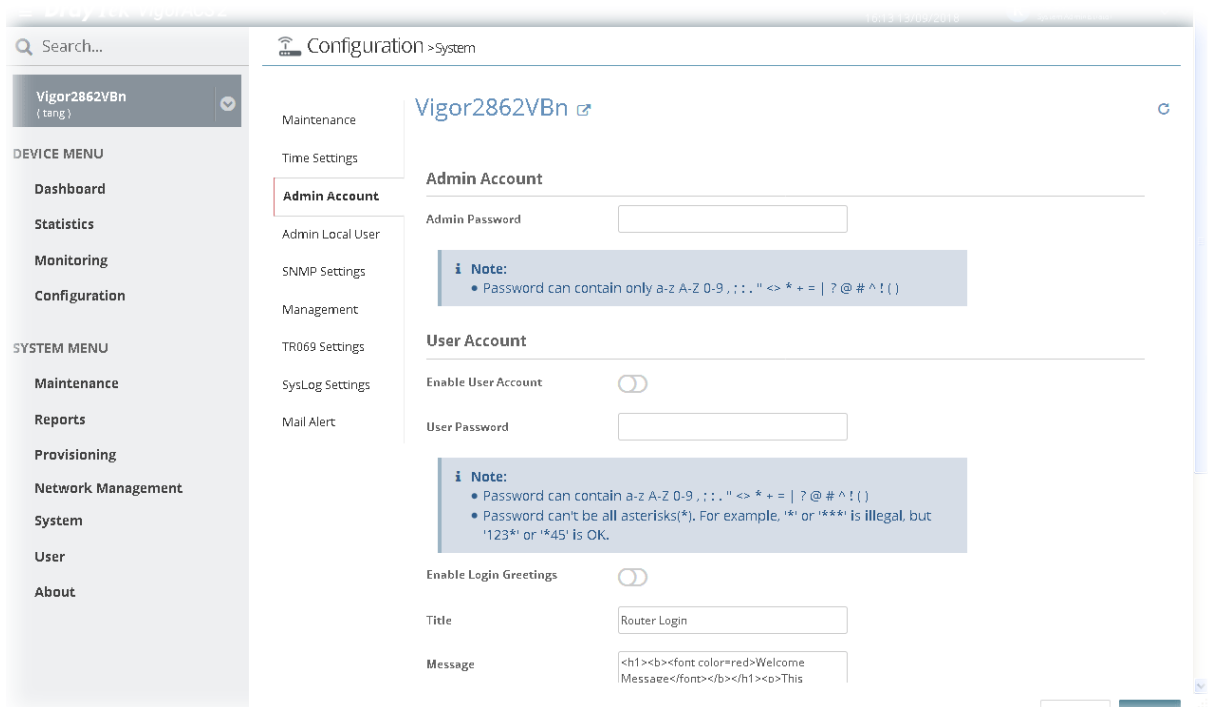


After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately

13.18.3 Admin Account

To configure the password for system administrator to access into the web user interface of device, open this web page for editing.

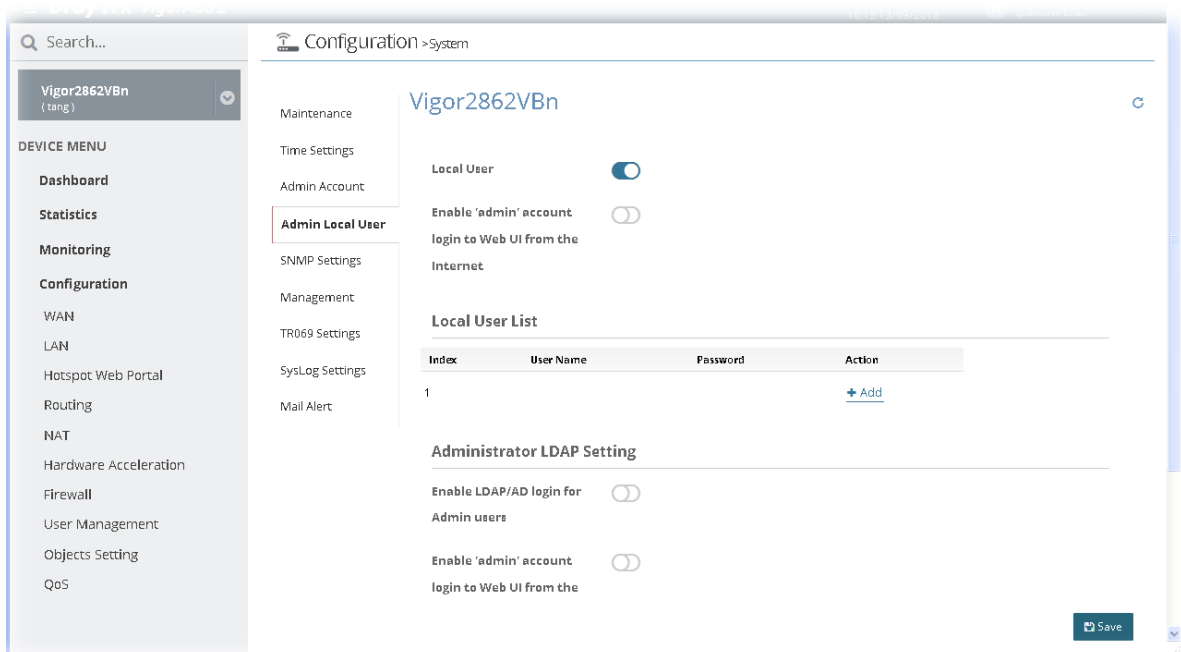
In addition, when you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. Login Greetings field allows you to specify login title on the Login window if you have such requirement.



After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.18.4 Admin Local User

The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. This feature allows other user in LAN (local user) who can access into the web user interface with the same privilege of the administrator.



After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.18.5 SNMP Settings

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

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

The screenshot shows the configuration page for a Vigor2862VBn device, specifically the SNMP Settings section. The page is titled "Configuration > System" and "Vigor2862VBn". The left sidebar contains a "DEVICE MENU" with options like Dashboard, Statistics, Monitoring, Configuration, and a "SYSTEM MENU" with options like Maintenance, Reports, Provisioning, Network Management, System, User, and About. The "SNMP Settings" option is highlighted in the left sidebar. The main content area shows the following settings:

- Enable SNMP Agent:**
- Get Community:**
- Set Community:**
- Trap Community:**
- Trap Timeout:**
- Manager Host IP (IPv4):**
 - Index 1: IP:**
 - Index 1: Subnet Mask:**
 - Index 2: IP:**
 - Index 2: Subnet Mask:**

A "Save" button is located at the bottom right of the configuration area.

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.18.6 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, and Management Port Setup

The screenshot shows the configuration page for a Vigor2862VBn device, specifically the Management section. The page is titled "Configuration > System" and "Vigor2862VBn". The left sidebar contains a "DEVICE MENU" with options like Dashboard, Statistics, Monitoring, Configuration, and a "SYSTEM MENU" with options like Maintenance, Reports, Provisioning, Network Management, System, User, and About. The "Management" option is highlighted in the left sidebar. The main content area shows the following settings:

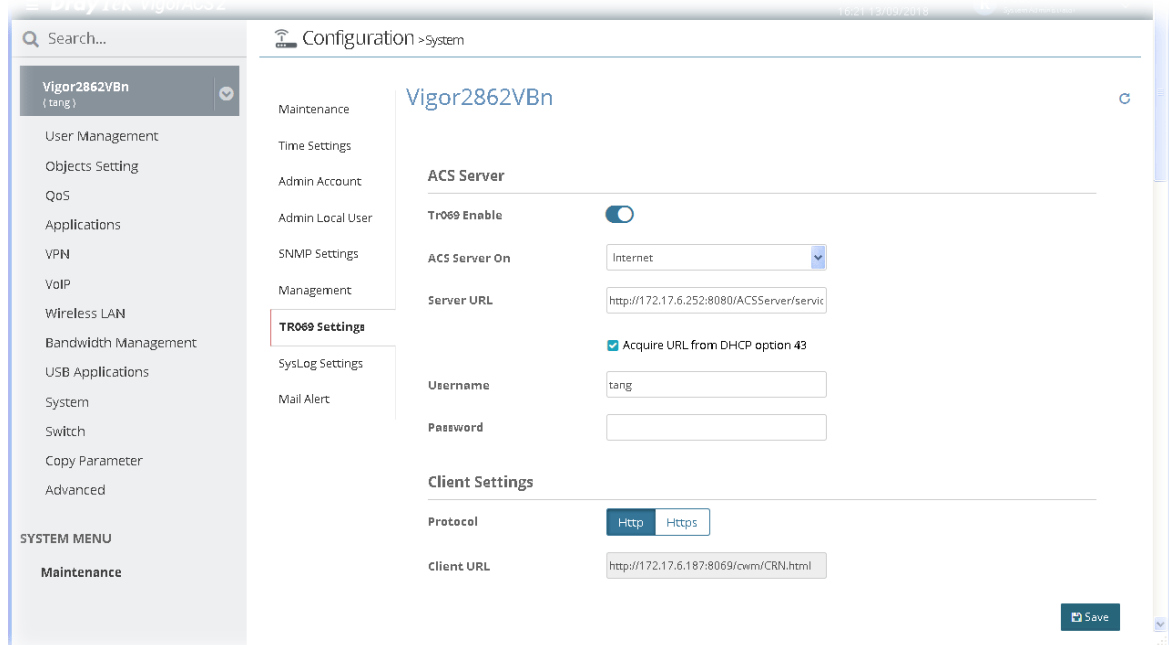
- Router Name:**
- Default:Disable:**
- Auto-Logout:**
- Enable Validation Code in Internet/LAN Access:**
- Internet Access Control:**
 - Allow management from the Internet:**
 - Domain name allowed:**
 - FTP Server:**
 - HTTP Server:**
 - Enforce HTTPS Access:**

A "Save" button is located at the bottom right of the configuration area.

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.18.7 TR069 Settings

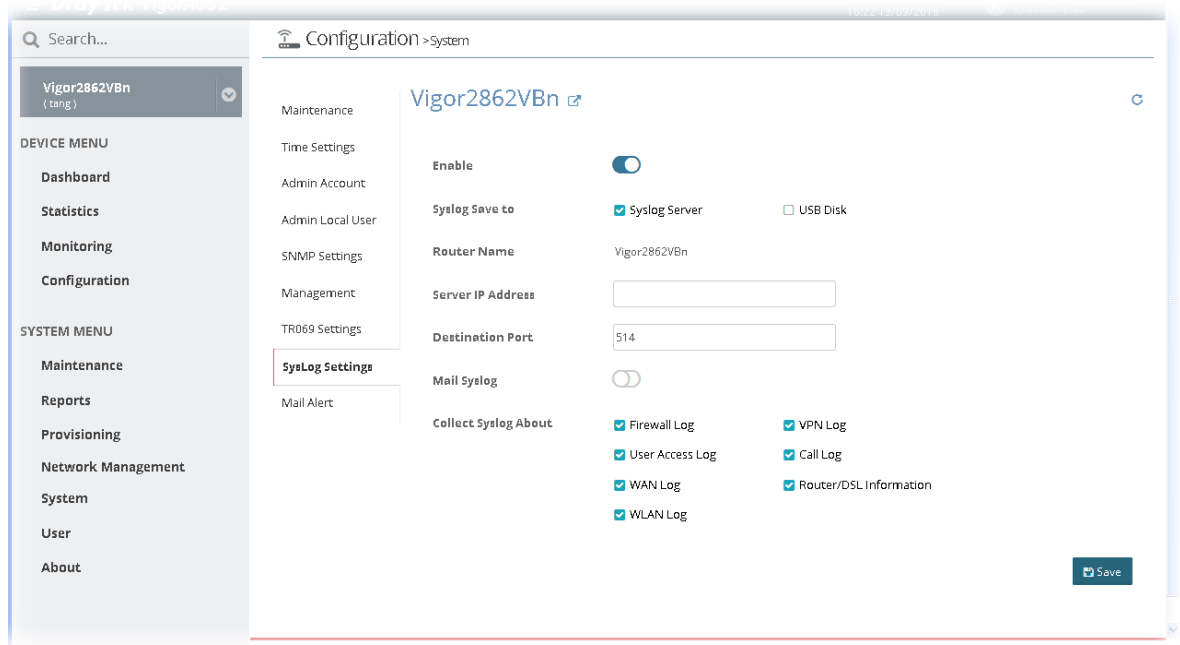
Vigor device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through VigorACS 2.



After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.18.8 SysLog Settings

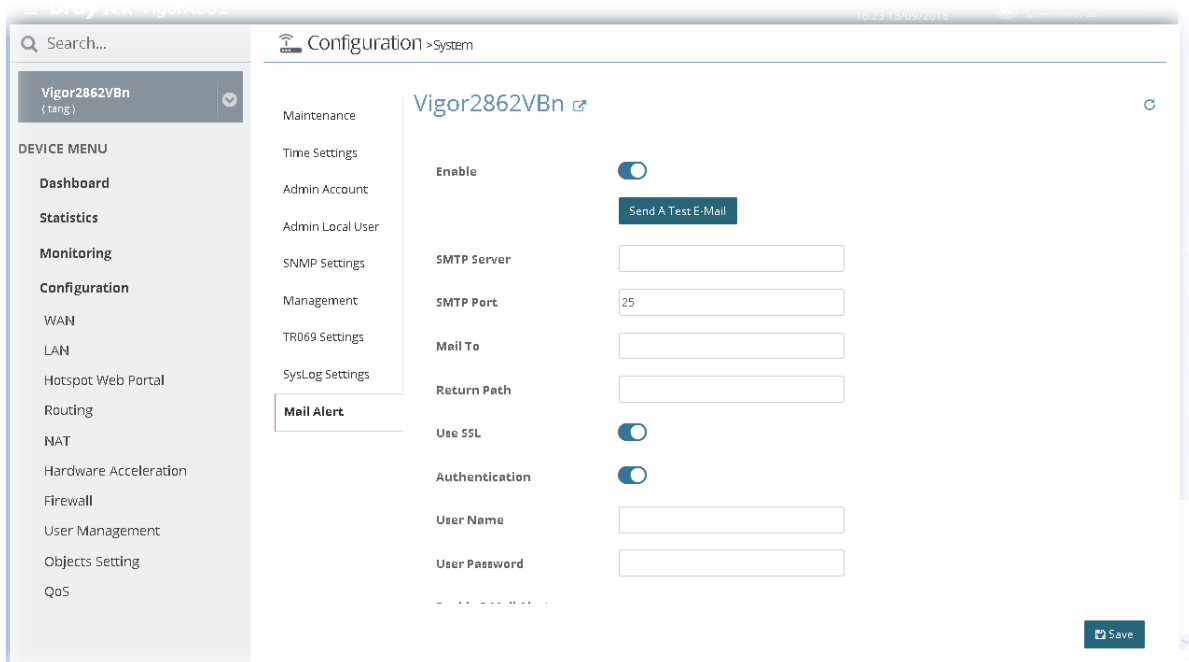
SysLog function is provided for monitoring Vigor router.



After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.18.9 Mail Alert

System administrator can make a simple test for the e-mail address specified in this page; send alert message to the e-mail box when Vigor router detects DoS Attack, VPN and/ or APPE event.

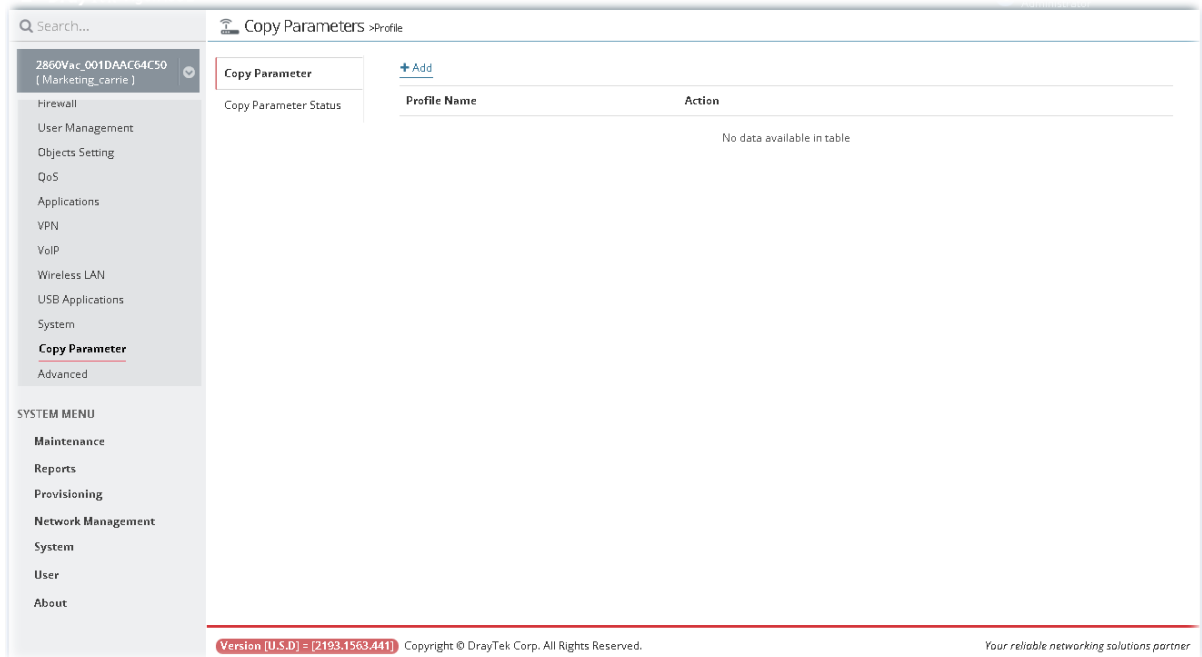


After finished the settings configuration, click **Save**. The modification for the CPE will take effect immediately.

13.19 Copy Parameter for CPE

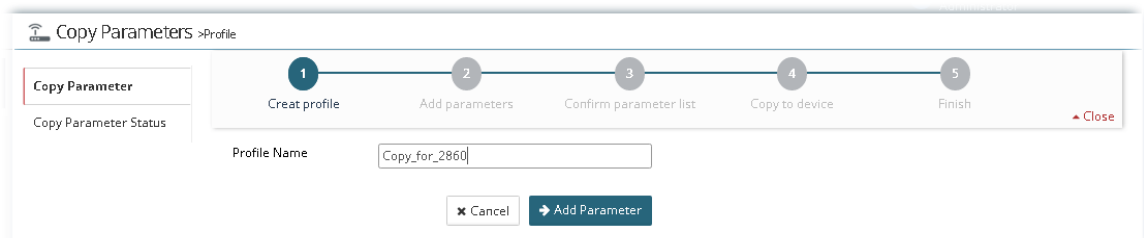
13.19.1 Copy Parameter

VigorACS 2 supports to copy parameters from one of the registered CPE(s) to other CPE(s) with the same model. It is convenience for duplication and configuration with large setting profiles.

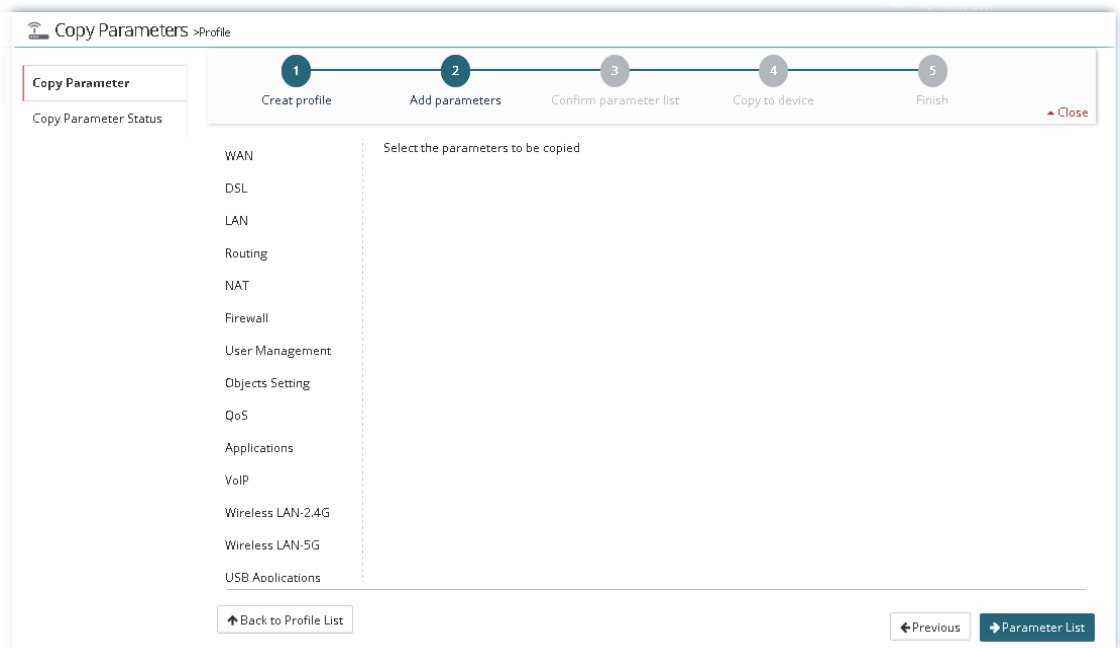


Follow the steps below to perform the operation of Copy Parameter.

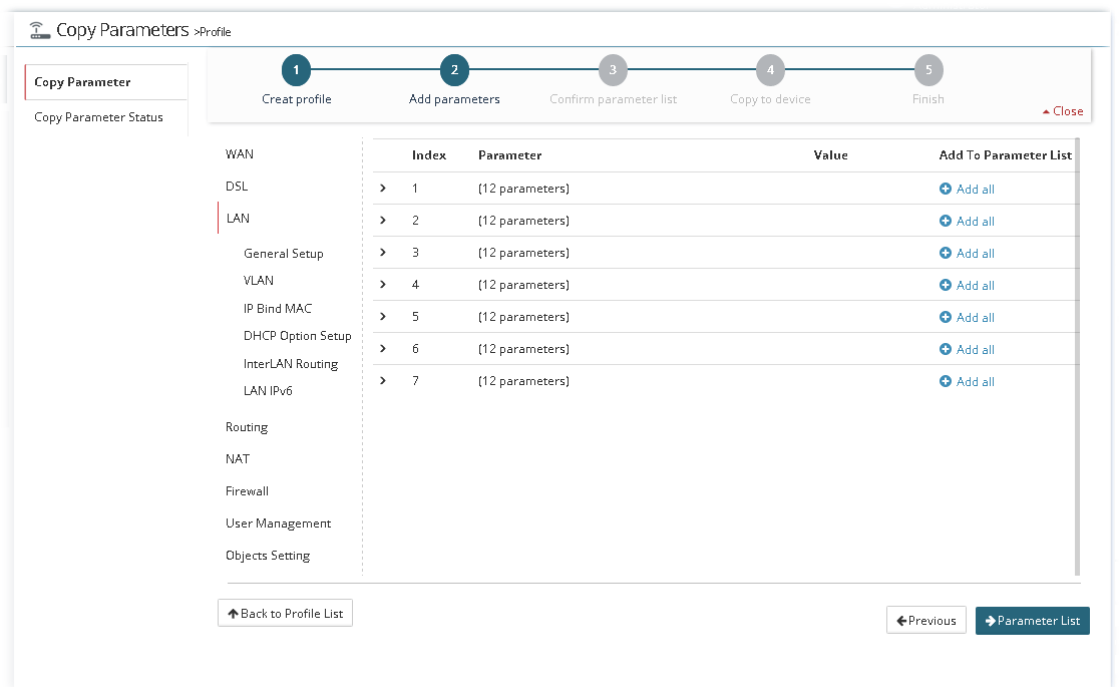
1. Open Configuration>>Copy Parameter and click Add.
2. On the following page (1 Create Profile), type a name for the copy parameter profile.



3. Click Add Parameter to get the following page (2 Add Parameter).



- Here, we take LAN settings as an example. Move the mouse to LAN and click it to display the submenu items. Then, click **General Setup**.



There are 12 parameters available for copying for each index. Choose the parameter you want to copy and click **+**. When the icon becomes **✓**, it means that parameter has been selected for copying.

Copy Parameters > Profile

1 Create profile 2 Add parameters 3 Confirm parameter list 4 Copy to device 5 Finish Close

Copy Parameter
Copy Parameter Status

	Index	Parameter	Value	Add To Parameter List
WAN				
DSL	> 1	[12 parameters]		+ Add all
LAN	∨ 2	[12 parameters]		+ Add all
General Setup		DHCP Max Address	192.168.2.109	✓
VLAN		DNS Servers	0.0.0.0,0.0.0.0	+
IP Bind MAC		Nat Or Routing Usage	For_NAT_Usage	+
DHCP Option Setup		IP Address	192.168.2.1	✓
InterLAN Routing		DHCP Relay	false	+
LAN IPv6		Subnet Mask	255.255.255.0	+
Routing		IP Routers	192.168.2.1	✓
NAT		Enable	false	✓
Firewall		DHCP Server Enable	true	✓
User Management		DHCP Min Address	192.168.2.10	+
Objects Setting				

Back to Profile List Previous Parameter List

5. Next, click **Parameter List** to display the following page (3 Confirm parameter list).

Copy Parameters > Profile

1 Create profile 2 Add parameters 3 Confirm parameter list 4 Copy to device 5 Finish Close

Copy Parameter
Copy Parameter Status

[Edit](#) / [Delete](#)

<input type="checkbox"/>	Parameter	Value	Is Copy
<input checked="" type="checkbox"/>	InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.MaxAddress	192.168.2.109	<input type="checkbox"/>
<input type="checkbox"/>	InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress	192.168.2.1	<input type="checkbox"/>
<input type="checkbox"/>	InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.IPRouters	192.168.2.1	<input type="checkbox"/>
<input type="checkbox"/>	InternetGatewayDevice.LANDevice.2.LANEthernetInterfaceConfig.1.Enable	false	<input type="checkbox"/>
<input checked="" type="checkbox"/>	InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.DHCPServerEnable	true	<input type="checkbox"/>

Back to Profile List Previous Copy to Device

If required, click **Edit** to change the value(s) for parameter(s).

The screenshot shows the 'Copy Parameters > Profile' interface. At the top, there is a progress bar with five steps: 1. Create profile, 2. Add parameters, 3. Confirm parameter list, 4. Copy to device, and 5. Finish. The current step is 4. Below the progress bar, there are 'Edit' and 'Delete' icons. The main area contains a table of parameters:

Parameter	Value	Is Copy
InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.MaxAddress	192.168.2.109	<input checked="" type="checkbox"/>
InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress	192.168.2.1	<input checked="" type="checkbox"/>
InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.IPRouters	192.168.2.1	<input checked="" type="checkbox"/>
InternetGatewayDevice.LANDevice.2.LANEthernetInterfaceConfig.1.Enable	false	<input checked="" type="checkbox"/>
InternetGatewayDevice.LANDevice.2.LANHostConfigManagement.DHCPSEnable	true	<input checked="" type="checkbox"/>

At the bottom right, there are 'Cancel' and 'Save' buttons.

After modifying the parameter, click **Save** to return to previous page.

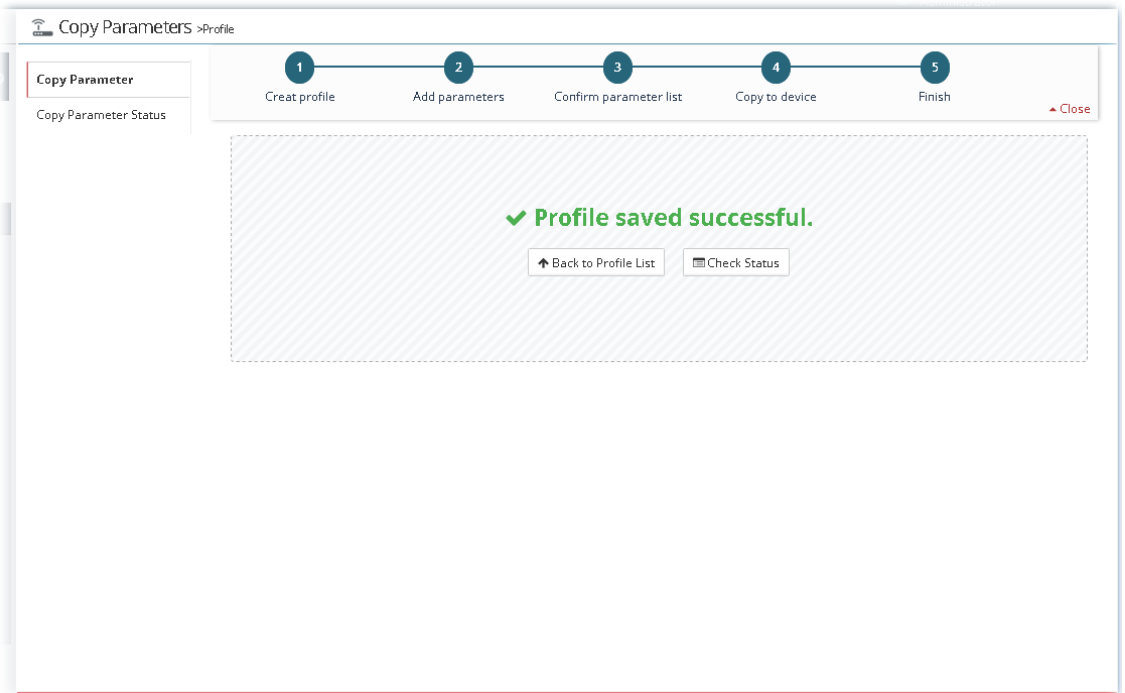
- Next, click **Copy to Device** to display the following page (4 Copy to device). Select the target device by clicking it.

The screenshot shows the 'Copy Parameters > Profile' interface at step 4, 'Copy to device'. The progress bar is the same as in the previous screenshot. Below the progress bar, there is a 'Select target devices' section with a list of devices:

Device ID	Device Name	IP Address
<input checked="" type="checkbox"/> 2860ac_00507F000033	Vigor2860ac	3.8.2.1_RC4b_STD
<input type="checkbox"/> 2860ac_00507F000036	Vigor2860ac	3.8.2.1_RC4b_STD
<input type="checkbox"/> 2860ac_00507F00003a	Vigor2860ac	3.8.2.1_RC4b_STD
<input type="checkbox"/> 2860ac_00507F000048	Vigor2860ac	3.8.2.1_RC4b_STD
<input type="checkbox"/> 2860ac_00507F000049	Vigor2860ac	3.8.2.1_RC4b_STD
<input type="checkbox"/> 2860ac_00507F00004a	Vigor2860ac	3.8.2.1_RC4b_STD

Below the device list, there is a 'Copy Time' section with 'Now' and 'Schedule' buttons. Under 'Schedule', there are fields for 'Start day' (05/04/2017), 'Start time' (11:00 AM), and 'End time' (11:00 AM). At the bottom right, there are 'Previous' and 'Finish' buttons.

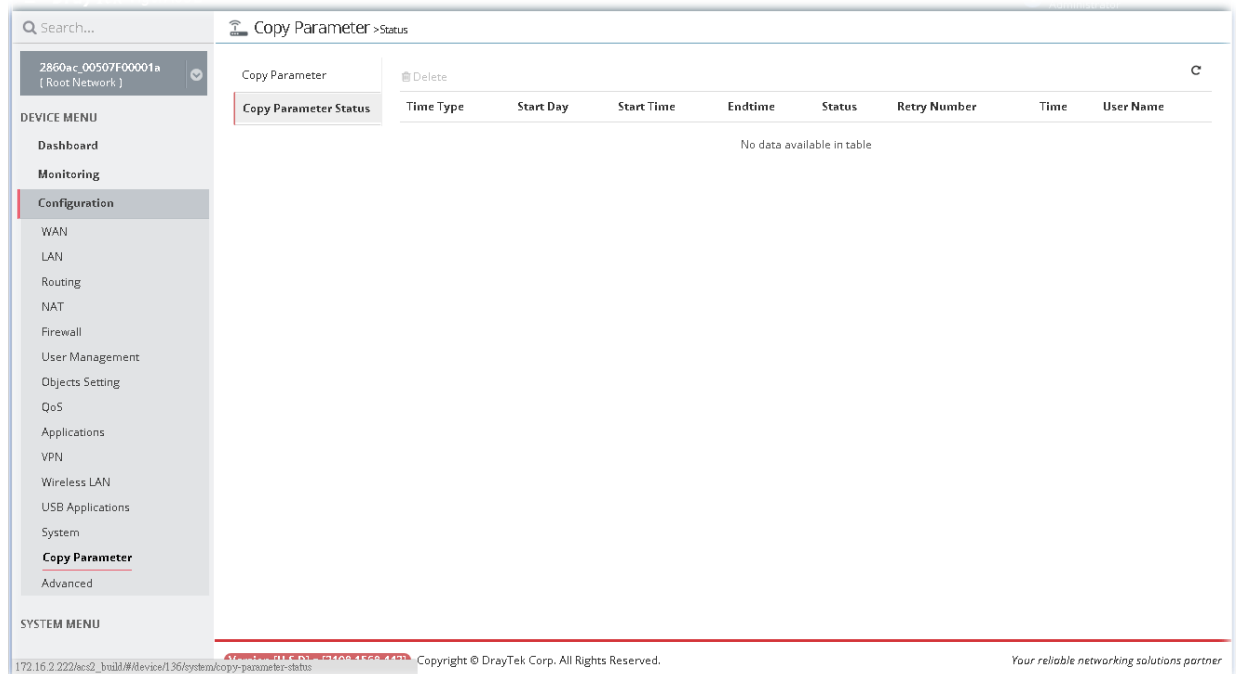
- Click **Finish**.



8. A Copy Parameter profile has been created. Later, the selected parameters will be copied to the target device immediately or on scheduled time.

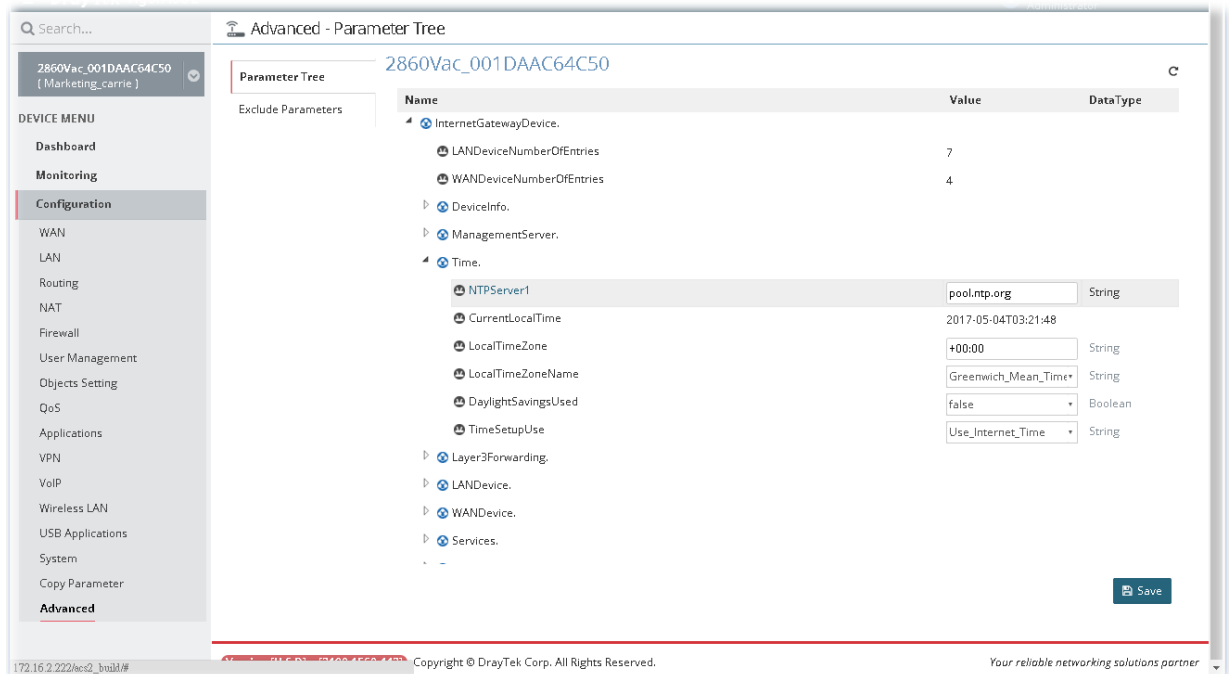
13.19.2 Checking the Copying Parameters Status

Only the operation that failed to copy parameters will be displayed in this page.



13.20 Advanced Settings for CPE

13.20.1 Parameter Tree



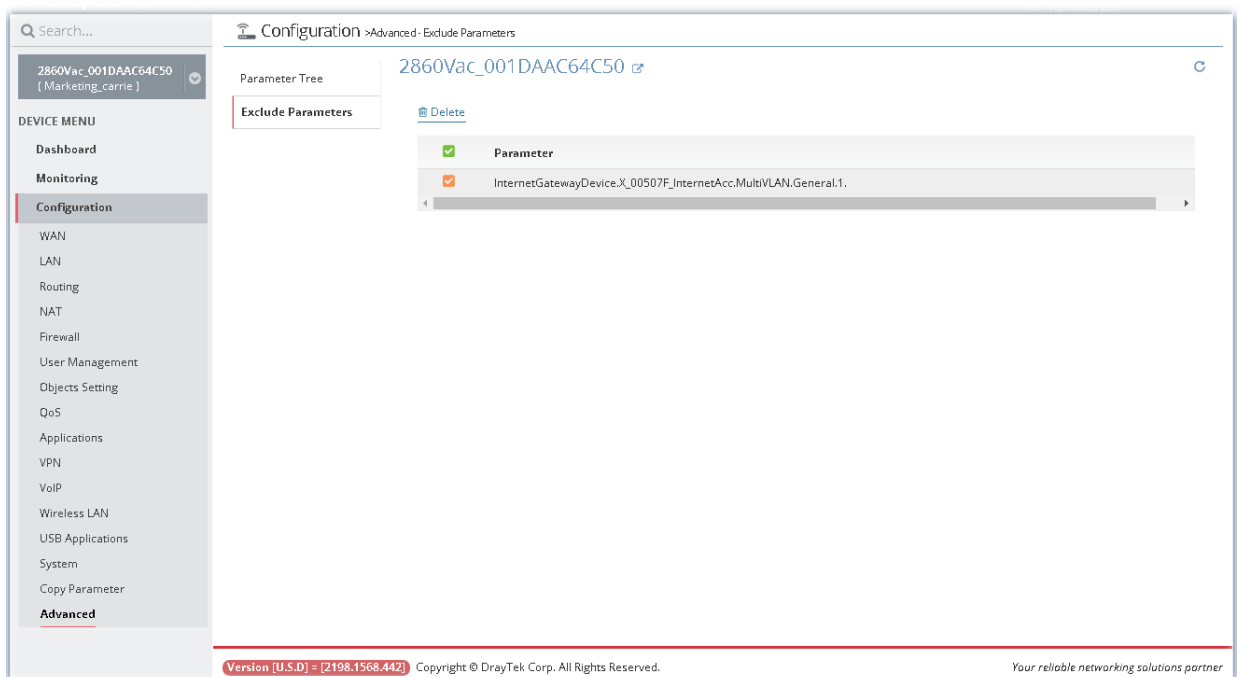
The screenshot shows the 'Advanced - Parameter Tree' configuration page. The left sidebar contains a 'DEVICE MENU' with options like Dashboard, Monitoring, Configuration, WAN, LAN, Routing, NAT, Firewall, User Management, Objects Setting, QoS, Applications, VPN, VoIP, Wireless LAN, USB Applications, System, Copy Parameter, and Advanced. The main content area shows a tree structure of parameters for device 2860Vac_001DAAC64C50. The 'Time' section is expanded, showing a table of parameters:

Name	Value	Data Type
InternetGatewayDevice.		
LANDeviceNumberOfEntries	7	
WANDeviceNumberOfEntries	4	
DeviceInfo.		
ManagementServer.		
Time.		
NTPServer1	pool.ntp.org	String
CurrentLocalTime	2017-05-04T03:21:48	
LocalTimeZone	+00:00	String
LocalTimeZoneName	Greenwich_Mean_Time*	String
DaylightSavingsUsed	false	Boolean
TimeSetupUse	Use_Internet_Time	String
Layer3Forwarding.		
LANDevice.		
WANDevice.		
Services.		

A 'Save' button is located at the bottom right of the parameter tree.

After finished the settings configuration, click Save. The modification for the CPE will take effect immediately.

13.20.2 Exclude Parameters



The screenshot shows the 'Configuration > Advanced - Exclude Parameters' page. The left sidebar is the same as in the previous screenshot. The main content area shows a list of excluded parameters for device 2860Vac_001DAAC64C50. The 'Exclude Parameters' section is active, and a 'Delete' button is visible. The list of excluded parameters is as follows:

Parameter
InternetGatewayDevice.X_00507F_InternetAcc.MultiVLAN.General.1.

Applications

A.1 How to create a VPN by using VPN Wizard?

Vigor ACS 2 supports VPN Wizard which provides an easy way to create a LAN to LAN VPN tunnel between two Vigor routers. The following shows an example for PPTP tunnel created between Vigor2860 and Vigor2925.

VPN server => Vigor2860, LAN network: 192.168.82.0/24

VPN client => Vigor2925, LAN network: 192.168.92.0/24



Info

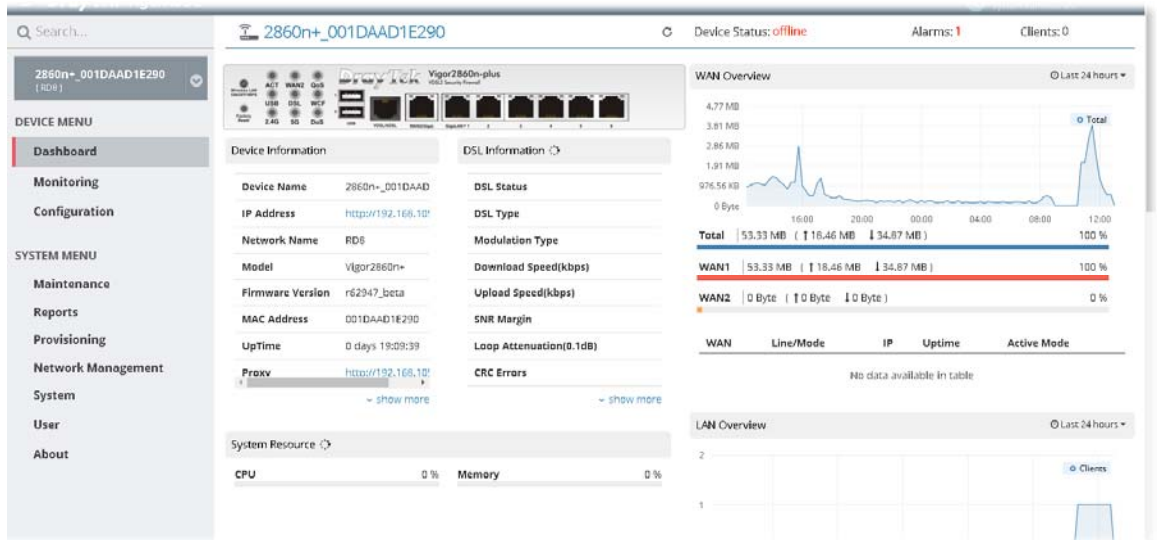
LAN IP address for both routers shall not be the same.

1. Click **Root Network** and display the tree view. Choose Vigor2860 as the VPN server.

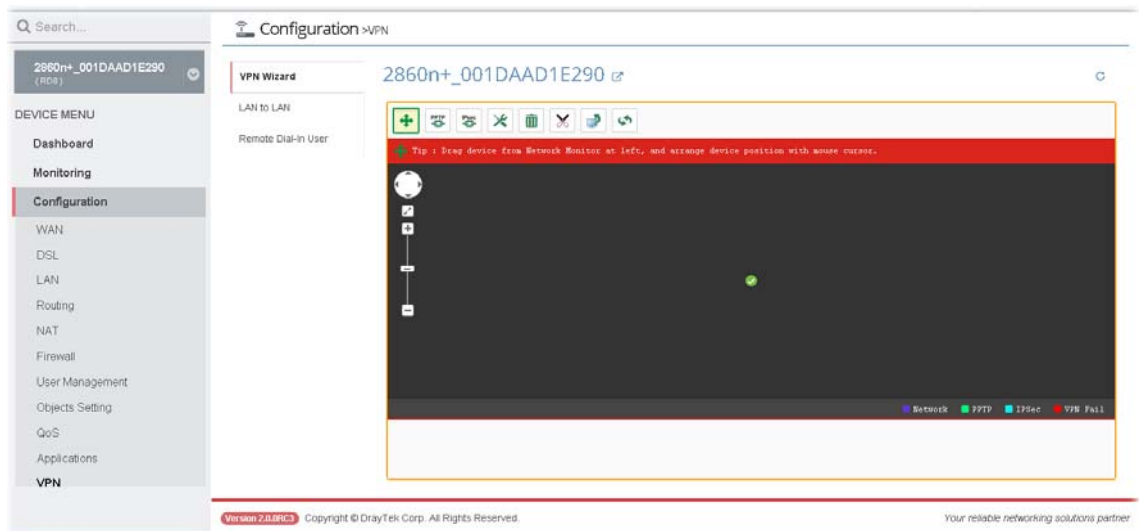
The screenshot displays the Vigor ACS 2 interface. On the left, the 'Root Network' tree view is expanded to show a list of devices under the 'RD8(8)' category. The device '2860n+_001DAAD1E290' is selected and highlighted. On the right, the 'Network Overview' dashboard for this device is shown. It features a grid of network categories with their respective status (Online/Offline) and alarm counts. A tooltip is visible over the selected device ID in the tree view.

Category	Online	Offline	Alarm
Root Networ...	337	25	26
Netherlands	0	4	4
Other	0	3	3
mamie	1	2	2
ap	4	2	2
VPN	0	1	1

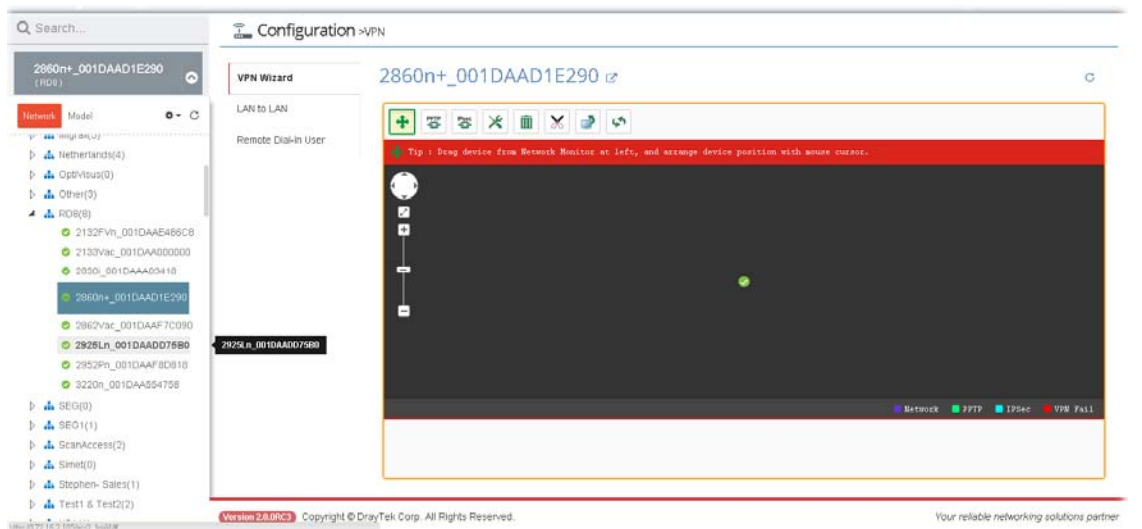
2. The Dashboard for the selected device will be shown as follows.



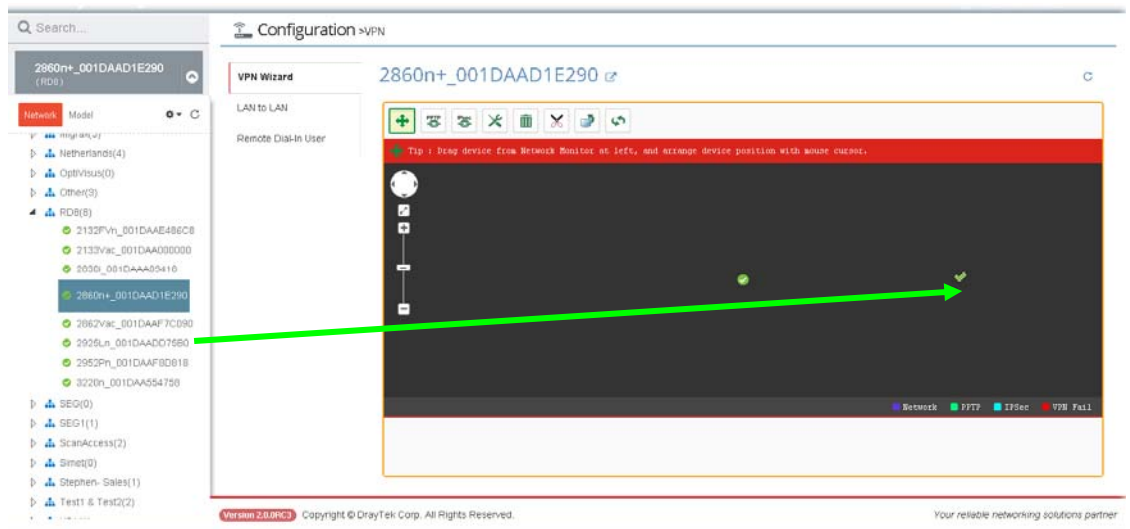
3. Open **DEVICE MENU**>>**Configuration**>> **VPN** function on the top menu of VigorACS 2. Then the VPN Wizard web page will appear as the follows:



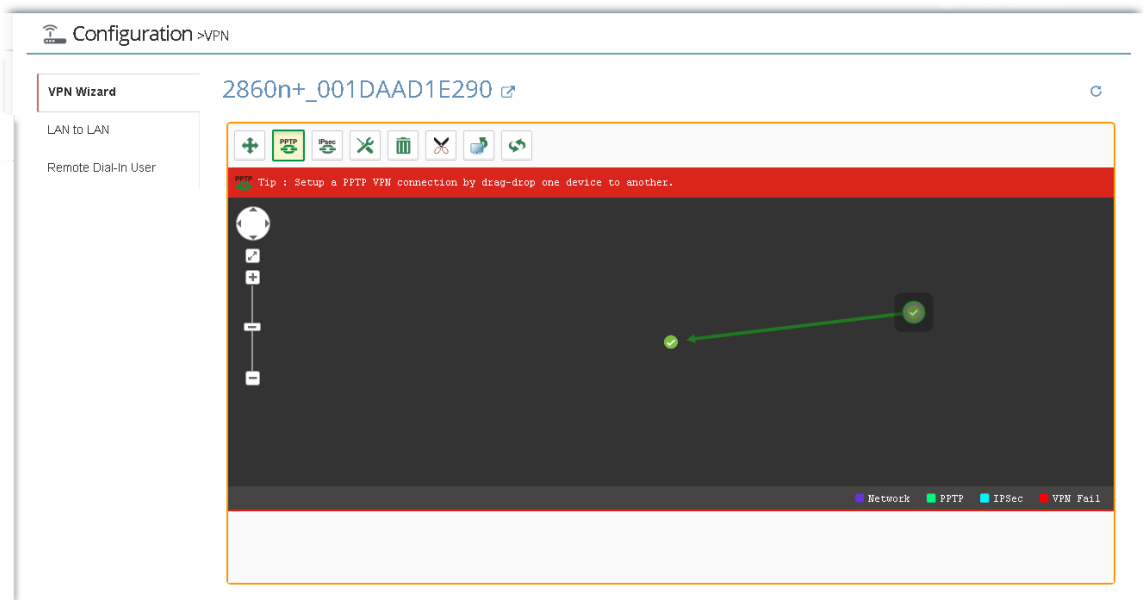
4. Press the **Add device** button, then choose the VPN client (e.g., Vigor2925) at the Network View.



- Click the VPN client (Vigor2925) and drag it to the black area on the right side. Then release it.



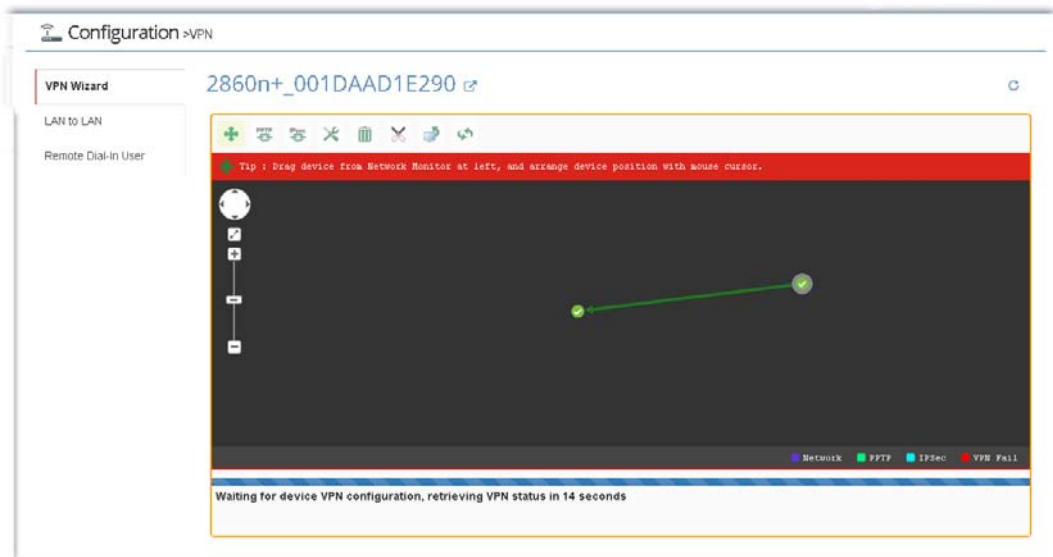
- Press PPTP button, then Press the VPN client icon (Vigor2925) and drag it to the VPN server icon (Vigor2860), release it when you see a yellow ring surrounding the VPN server icon.



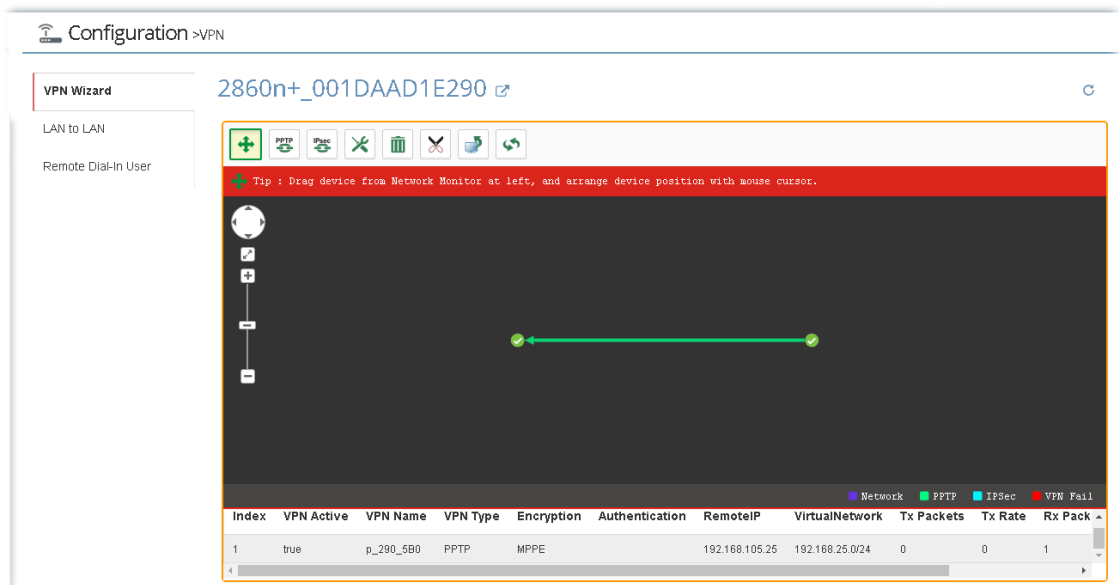
- VigorACS 2 will pop-up a confirmation window, please click the OK button.



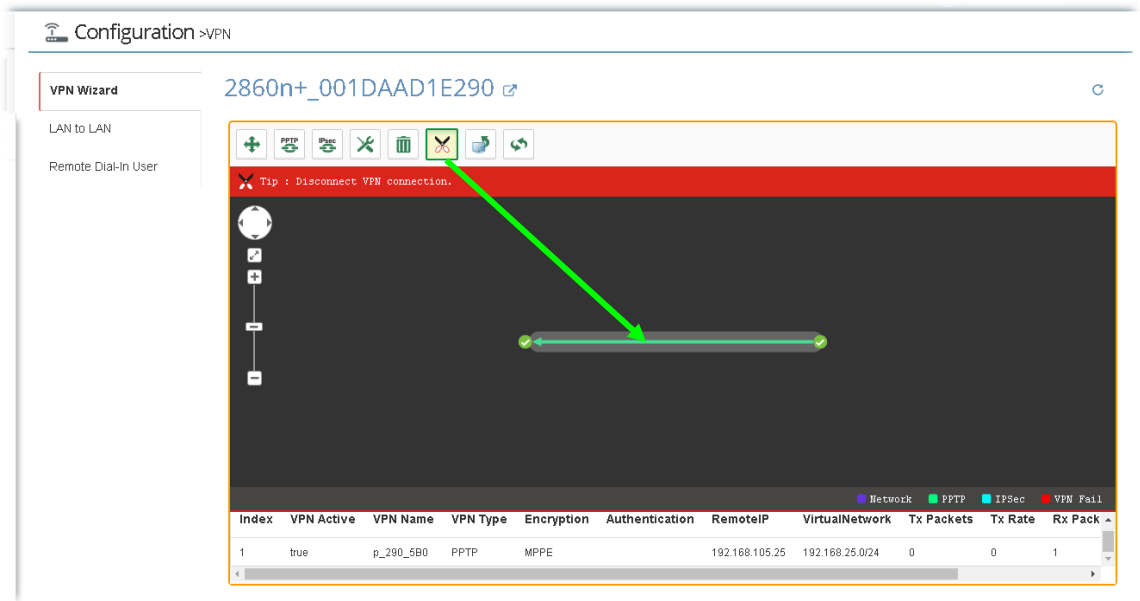
- Wait for device VPN configuration.



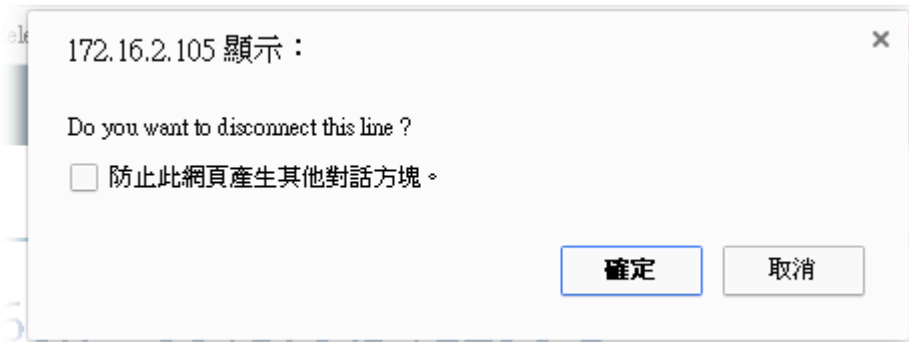
9. After PPTP connection working, there will be a green arrow from VPN client to VPN server, you could check the VPN tunnel status on the bottom of the VigorACS web as well.



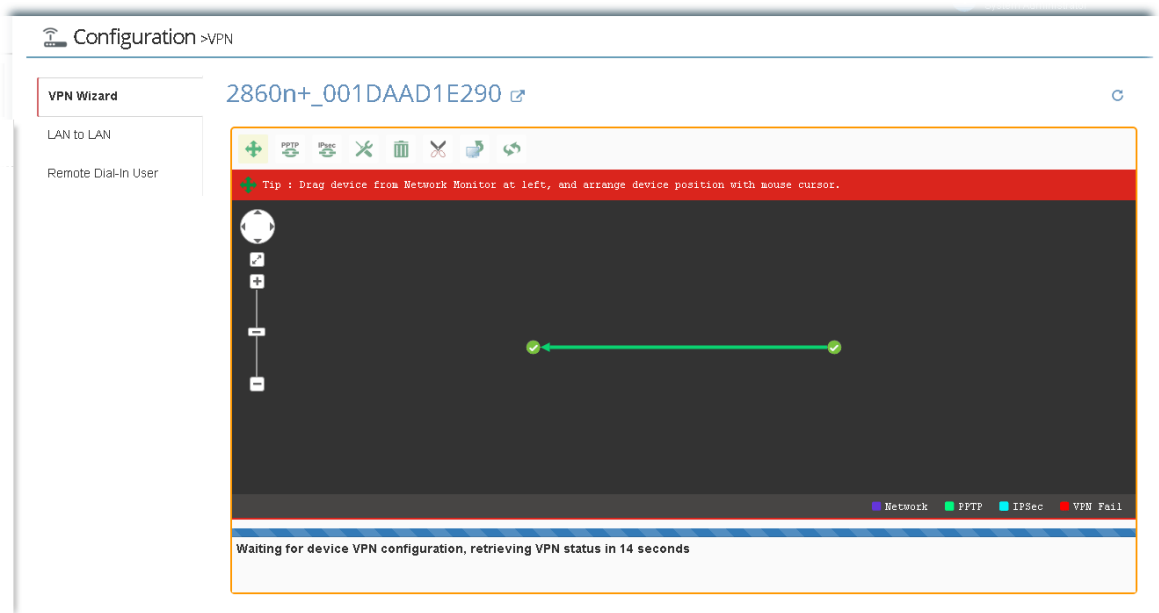
10. If you want to disconnect the VPN tunnel, to press the Disconnect button, then there will be a pair of scissors icon on the VPN line, click it.



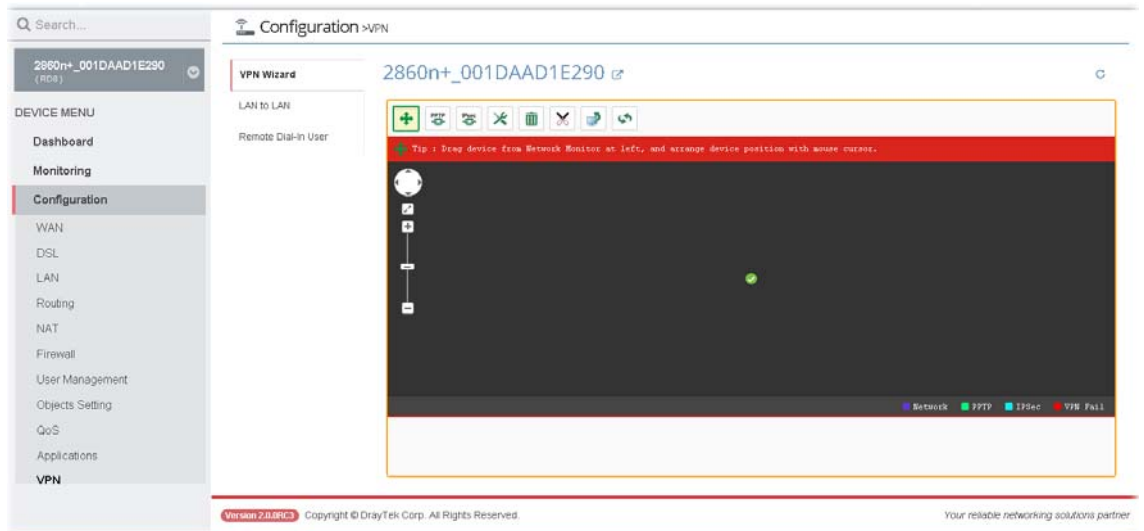
11. VigorACS will pop-up a confirmation window, please click the Yes button.



12. Wait for VPN disconnection.



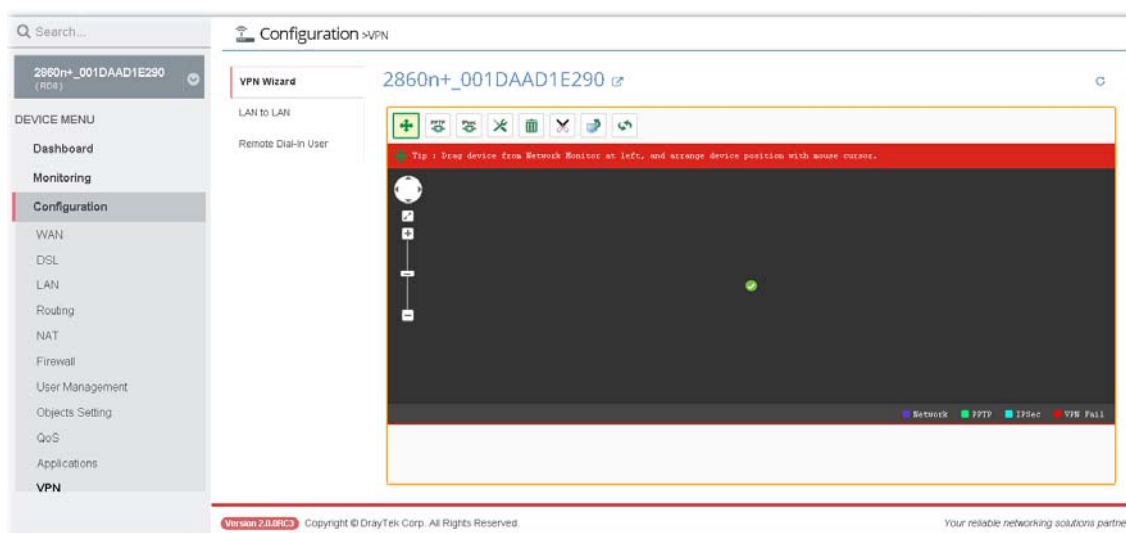
13. After VPN tunnel disconnected, the web page will be shown as follows.



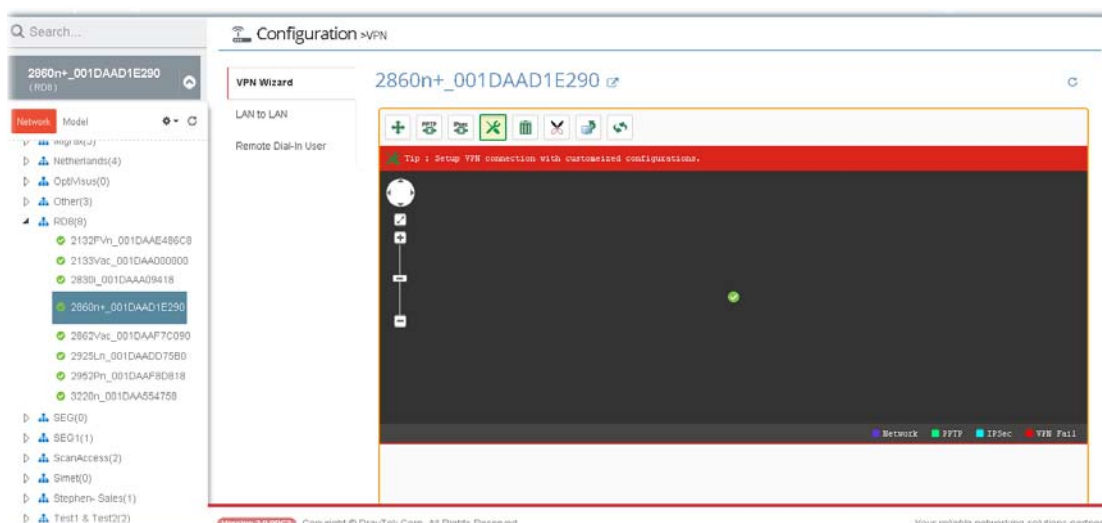
A.2 How to create a VPN Connection with Advanced Settings by using VPN Wizard ?

VPN wizard supports PPTP and IPsec tunnel, the default encryption for PPTP Tunnel is MPPE, for IPsec Tunnel is AH-SHA1. If you want to set more details for VPN connection, you can use **Advance** connection button.

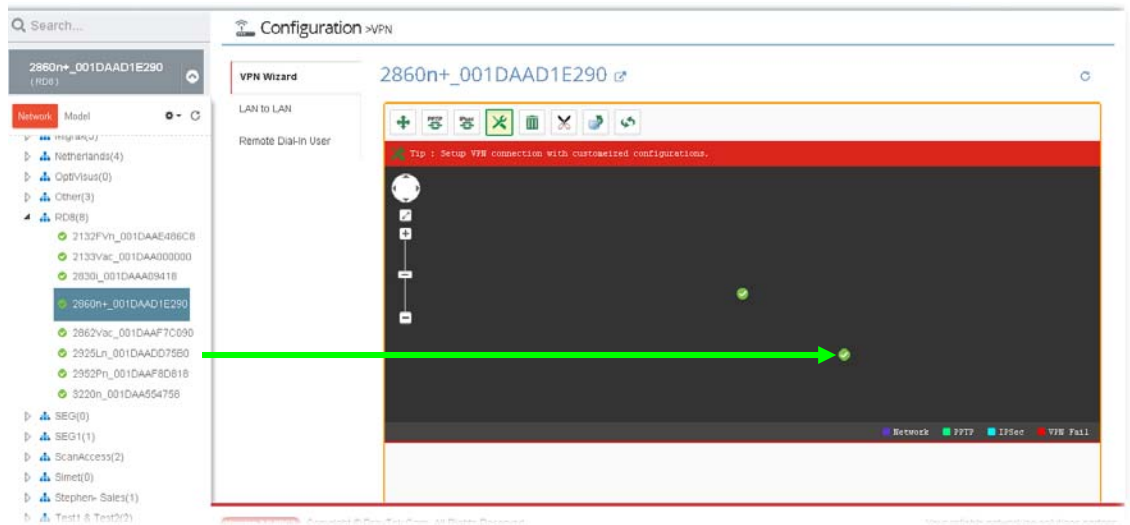
1. Open **DEVICE MENU>>Configuration>> VPN** function on the top menu of VigorACS 2. Then the VPN Wizard web page will appear as the follows:



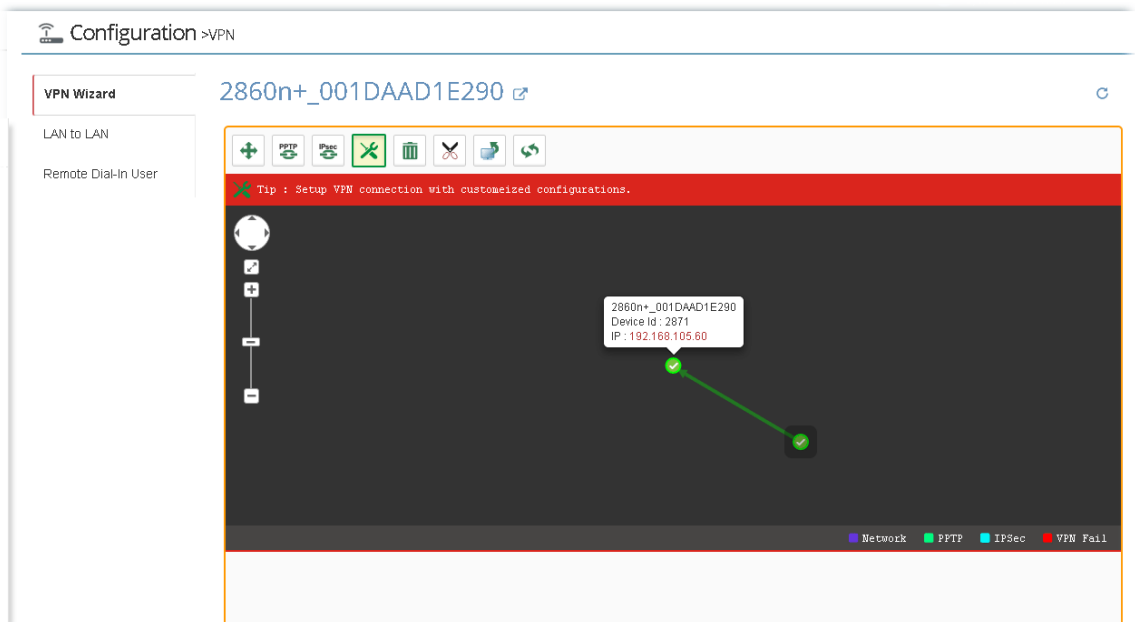
2. Press the **Advance** button, then choose the VPN client (e.g., Vigor2925) at the Network View.



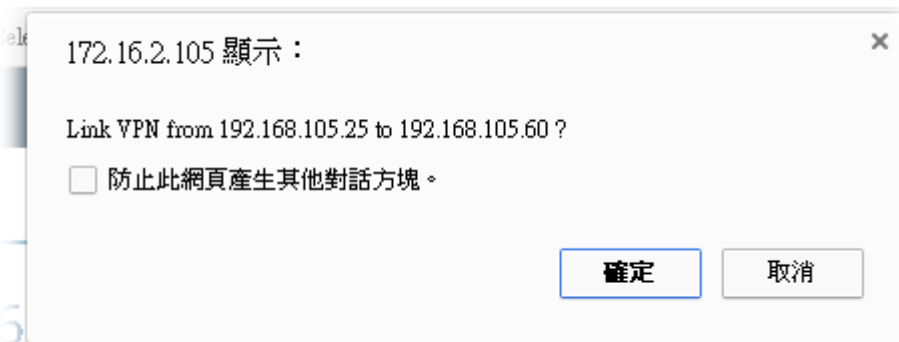
3. Click the VPN client (Vigor2925) and drag it to the black area on the right side. Then release it.



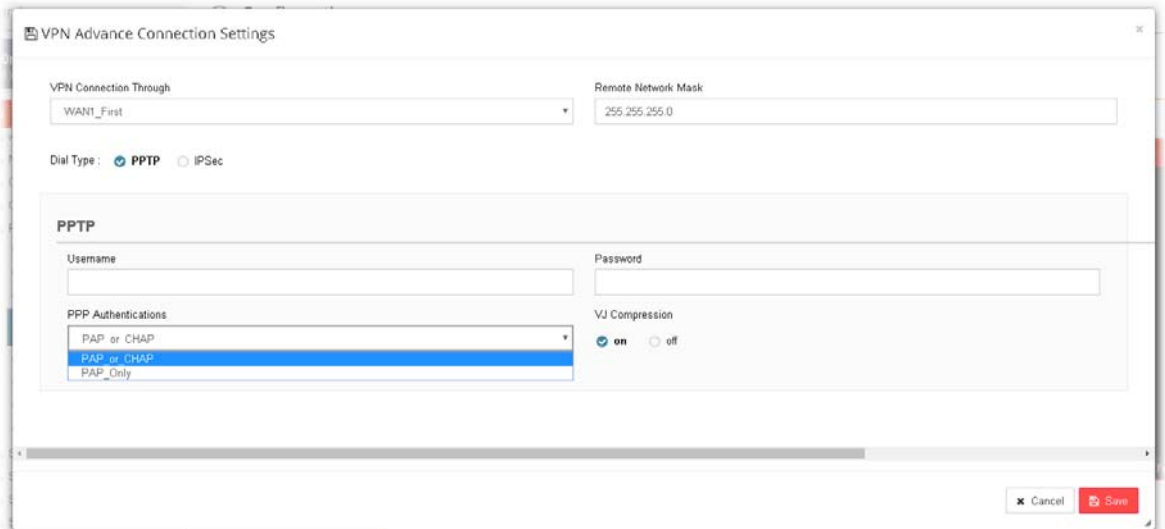
4. Press the VPN client icon (Vigor2925) and drag it to the VPN server icon (Vigor2860), release it when you see a yellow ring surrounding the VPN server icon.



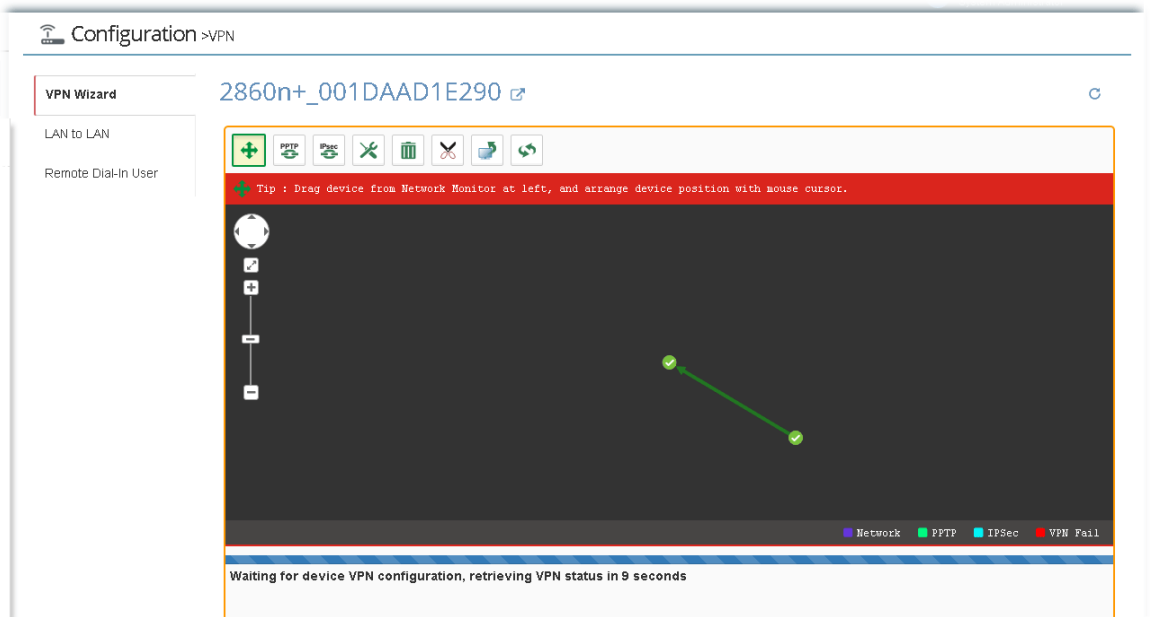
5. VigorACS 2 will pop-up a confirmation window, please click the OK button.



6. A dialog appears as follows. Please set the corresponding parameters and settings manually and click Save.



7. Wait for device VPN configuration.



- There will be a green arrow from VPN client to VPN server, you could check the VPN tunnel status on the bottom of the VigorACS web as well.

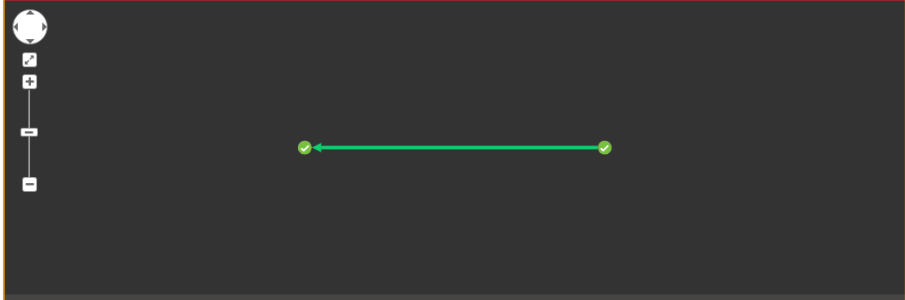
Configuration > VPN

2860n+_001DAAD1E290

VPN Wizard

- LAN to LAN
- Remote Dial-In User

Tip : Drag device from Network Monitor at left, and arrange device position with mouse cursor.



Legend: Network (purple), PPTP (green), IPsec (cyan), VPN Fail (red)

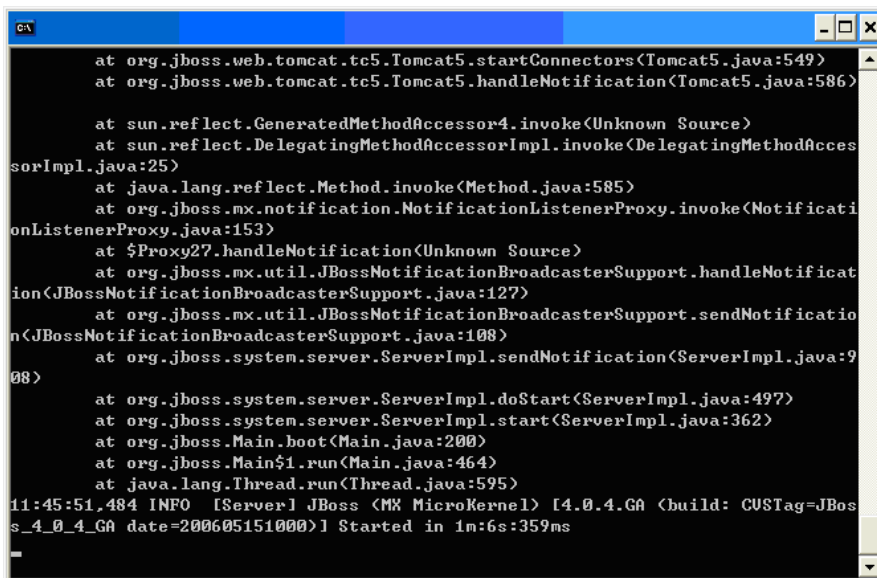
Index	VPN Active	VPN Name	VPN Type	Encryption	Authentication	RemoteIP	VirtualNetwork	Tx Packets	Tx Rate	Rx Pack
1	true	p_290_5B0	PPTP	MPPE		192.168.105.25	192.168.25.0/24	0	0	1

Chapter 14 Trouble Shooting

≡ DrayTek VigorACS2

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

When you try to invoke VigorACS and get the following error message, please locate the file of "server.log" from C:/Program Files/VigorACS 2/server/default/log and send the file to your dealer for further assistance.



```
at org.jboss.web.tomcat.tc5.Tomcat5.startConnectors(Tomcat5.java:549)
at org.jboss.web.tomcat.tc5.Tomcat5.handleNotification(Tomcat5.java:586)

at sun.reflect.GeneratedMethodAccessor4.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccess
sorImpl.java:25)
at java.lang.reflect.Method.invoke(Method.java:585)
at org.jboss.mx.notification.NotificationListenerProxy.invoke(NotificationLi
onListenerProxy.java:153)
at $Proxy27.handleNotification(Unknown Source)
at org.jboss.mx.util.JBossNotificationBroadcasterSupport.handleNotificat
ion(JBossNotificationBroadcasterSupport.java:127)
at org.jboss.mx.util.JBossNotificationBroadcasterSupport.sendNotificatio
n(JBossNotificationBroadcasterSupport.java:108)
at org.jboss.system.server.ServerImpl.sendNotification(ServerImpl.java:9
08)

at org.jboss.system.server.ServerImpl.doStart(ServerImpl.java:497)
at org.jboss.system.server.ServerImpl.start(ServerImpl.java:362)
at org.jboss.Main.boot(Main.java:200)
at org.jboss.Main$1.run(Main.java:464)
at java.lang.Thread.run(Thread.java:595)
11:45:51.484 INFO [Server] JBoss (MX MicroKernel) [4.0.4.GA (build: CUSTag=JBos
s_4_0_4_GA date=200605151000)] Started in 1m:6s:359ms
```

For Linux system, please locate the file of "server.log" from /usr/local/vigoracs/VigorACS/server/default/log/ and send the file to your dealer for further assistance.

14.1 Contacting DrayTek

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

This page is left blank.

Chapter 15 Reference Information

15.1 For Linux System

Corresponding files on Linux system required for VigorACS will be stored in the following paths:

```
java: /usr/local/jdk1.5.0_07
mysql: /usr/local/mysql
vigoracs: /usr/local/vigoracs/VigorACS/

log: /usr/local/vigoracs/VigorACS/server/default/log/server.log
bind ip: /usr/local/vigoracs/VigorACS/bin/startway.txt
mysql data: /usr/local/mysql/data/tr069
start/stop vigoracs : /usr/local/vigoracs/VigorACS/bin/vigoracs.sh
```

To check the current process of VigorACS, please use the following commands to inquire

```
ps(vigoracs): ps -ef | grep "/usr/javase/bin/java -server" |grep -v grep
ps(mysql): ps -ef | grep safe_mysql |grep -v grep
or
ps -ef | grep mysqld_safe |grep -v grep
```

Some link files are required for VigorACS running under Linux system properly. If any one of them is missed, unexpected problems might be happened.

```
ln(java): /usr/javase >> /usr/local/jdk1.5.0_07/
ln(mysql): /usr/local/mysql >> /usr/local/mysql-5.1.41-linux-i686-glibc23
ln(mysql): /tmp/mysql.sock >> /var/lib/mysql/mysql.sock
```

15.2 For Windows XP System

Corresponding files on Windows XP system required for VigorACS will be stored in the following paths:

```
java: C:\Program Files\Java\jdk1.5.0_07
mysql: C:\mysql
vigoracs: C:\Program Files\VigorACS 2

log: C:\Program Files\VigorACS 2\server\default\log\server.log
license key: C:\Program Files\VigorACS 2 version\license.key
bind ip: C:\Program Files\VigorACS 2\bin\bindip.txt
mysql data: C:\mysql\data\tr069
start vigoracs : C:\Program Files\VigorACS 2\bin\StartVigorACS.bat
stop vigoracs : C:\Program Files\VigorACS 2\bin\ShutdownVigorACS.bat
```