



VigorACS SI

Centralized Management System



Your reliable networking solutions partner

User's Guide

V2.6



VigorACS SI

Centralization Managment System

User's Guide

Version: 2.6

Date: August 10, 2016

Software Version: 1.1.10

© 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, Windows 95, 98, Me, NT, 2000, XP, Vista, 7 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 SI 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 SI (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 SI.

Table of Contents

Part I Introduction	xii
Chapter 1 Features	1
1.1 Main Features and Benefit	1
1.2 System Architecture.....	1
1.3 Web Service	2
Chapter 2 Installation	3
2.1 Platform for Windows 2000, XP, Vista, 7 or 10	3
2.1.1 Installation for Java	3
2.1.2 Installation for MariaDB	7
2.1.3 Installation for VigorACS SI	12
2.2 Platform for Linux / Solaris	20
2.3 Registering VigorACS.....	23
2.3.1 For Windows 2000, XP, Vista, 7 and 10	23
2.3.2 For Linux / Solaris	29
Chapter 3 Getting Start.....	31
3.1 Brief Introduction of Main Screen	31
3.2 Operation Procedure	32
3.3 Creating a New Network and Device.....	34
3.4 Creating a User and User Group.....	35
3.5 Logout VigorACS	36
Part II Web Configuration.....	37
Chapter 4 Admin Operation	39
4.1 Device Management.....	40
4.2 Creating a New Network to Manage Devices (CPEs)	42
4.3 Changing the Network for Devices (CPEs)	43
4.4 Modifying General Information of Selected CPE.....	45
4.5 Topology Management.....	48
Chapter 5 User Operation	49
5.1 User	49
5.1.1 Add a User	50
5.1.2 Edit a User	51
5.1.3 Delete a User	51
5.2 User Group	52
5.2.1 Add a User Group	53

5.2.2 Edit a User Group.....	53
5.2.3 Delete a User Group	53
5.3 User Group Management	54
5.4 Role Management	55
5.5 Function Management.....	56
5.6 Device Group.....	57
5.7 Wholesale Wizard.....	58
Chapter 6 Device Management.....	63
6.1 Networks.....	67
6.1.1 Network Summary.....	70
6.1.2 Network devices	71
6.1.3 Network map	72
6.1.4 Dashboard	73
6.1.5 Refresh.....	73
6.1.6 Sub devices recursively.....	74
6.1.7 VPN	75
<i>How to Build a Simple VPN Connection</i>	<i>76</i>
6.1.8 Wireless.....	79
6.1.9 AP Management.....	80
6.2 Devices	82
6.2.1 Device Summary	83
6.2.2 Device Map	84
6.2.3 System Management for Selected CPE.....	85
<i>Checking Device SysLog for the Selected CPE</i>	<i>86</i>
<i>Checking the Firmware Status for the Selected CPE</i>	<i>87</i>
<i>Specifying the Time Setting for the Selected CPE.....</i>	<i>88</i>
<i>Checking the TR-069 Settings for the Selected CPE</i>	<i>89</i>
<i>Checking the Statistics for the Selected CPE</i>	<i>91</i>
<i>Pinging or Tracing the Route for the Selected CPE.....</i>	<i>92</i>
<i>Upgrading the Firmware for the Selected CPE.....</i>	<i>93</i>
<i>Performing the Firmware Update</i>	<i>95</i>
<i>Checking the Firmware Update Log.....</i>	<i>96</i>
<i>Rebooting the Selected CPE</i>	<i>98</i>
<i>Returning to Factory Default Settings for Selected CPE</i>	<i>99</i>
<i>Copying Parameters for Selected CPE.....</i>	<i>100</i>
<i>Checking the Copying Parameters Log</i>	<i>103</i>
6.2.4 LAN Settings for the Selected CPE.....	105
<i>Checking and Editing VLAN Settings for the Selected CPE.....</i>	<i>106</i>
<i>Checking and Editing IP Routing Settings for the Selected CPE</i>	<i>108</i>

6.2.5 WAN Settings for the Selected CPE	110
<i>Checking WAN Status for the Selected CPE</i>	112
6.2.6 VoIP Settings for the Selected CPE.....	113
6.2.7 VPN Settings for the Selected CPE	116
<i>VPN Wizard - Creating VPN Connection between Two CPEs</i>	116
<i>VPN Creator Wizard - Creating LAN to LAN VPN Connection</i>	125
<i>Creating Remote Dial-in User Profile for VPN Connection</i>	129
<i>Checking VPN Connection Status</i>	131
<i>Monitoring VPN Tunnel</i>	132
6.2.8 DSL Settings for the Selected CPE.....	133
6.2.9 Wireless Settings for the Selected CPE.....	136
<i>General Setting for Wireless Connection</i>	136
<i>General SSID Setting for Wireless Connection</i>	137
<i>Security Setting for Wireless Connection</i>	140
<i>Access Control Setting for Wireless Connection</i>	143
<i>WPS Setting for Wireless Connection</i>	145
<i>AP Discovery Setting for Wireless Connection</i>	147
<i>Station List for Wireless Connection</i>	147
6.2.10 Wireless 5G Settings for the Selected CPE.....	148
<i>General SSID Setting for 5G Wireless Connection</i>	150
<i>Security Setting for 5G Wireless Connection</i>	152
<i>Access Control Setting for 5G Wireless Connection</i>	157
<i>AP Discovery Setting for 5G Wireless Connection</i>	159
<i>Station List for 5G Wireless Connection</i>	160
6.2.11 Multi-PVCs for the Selected CPE.....	160
<i>General Settings for Multi-PVCs</i>	160
<i>ATM QoS for Multi-PVCs</i>	163
<i>Port-Based Bridge for Multi-PVCs</i>	165
6.2.12 Configuring NAT Setting for the Selected CPE.....	167
<i>Port Redirection</i>	167
<i>DMZ Host</i>	170
<i>Open Ports</i>	172
6.2.13 Bandwidth Settings for the Selected CPE.....	174
<i>Configuring QoS WAN Setting for the Selected CPE</i>	174
<i>Configuring QoS Class Setting for the Selected CPE</i>	176
<i>Configuring QoS Service Type Setting for the Selected CPE</i>	179
6.2.14 Firewall Settings for the Selected CPE	181
<i>Configuring General Setup of Firewall for the Selected CPE</i>	181
<i>Configuring Filter Setup of Firewall for the Selected CPE</i>	184
<i>Configuring DoS Defense of Firewall for the Selected CPE</i>	187

<i>Configuring IP Object Setting of Firewall for the Selected CPE</i>	<i>189</i>
<i>Configuring IP Group Setting of Firewall for the Selected CPE.....</i>	<i>192</i>
<i>Configuring Service Type Object Setting of Firewall for the Selected CPE.....</i>	<i>195</i>
<i>Configuring Service Type Group Setting of Firewall for the Selected CPE</i>	<i>199</i>
<i>Configuring Keyword Object Setting of Firewall for the Selected CPE.....</i>	<i>201</i>
<i>Configuring Keyword Group Setting of Firewall for the Selected CPE</i>	<i>203</i>
<i>Configuring File Extension Setting of Firewall for the Selected CPE.....</i>	<i>205</i>
<i>Configuring APP Enforcement Setting of Firewall for the Selected CPE.....</i>	<i>207</i>
<i>Configuring URL Content Filter Setting of Firewall for the Selected CPE</i>	<i>210</i>
<i>Configuring Web Content Filter Setting of Firewall for the Selected CPE</i>	<i>214</i>
6.3 Wizards.....	218
6.3.1 Backup Configuration	218
6.3.2 Restore configuration	220
6.3.3 Firmware Upgrade for Selected CPE.....	221
6.3.4 Reboot for Selected CPE(s)	223
6.3.5 Factory Reset for Selected CPE(s)	225
6.3.6 Batch Activation of MyVigor License for Selected CPE(s).....	226
6.3.7 Bind with MyVigor Account for Selected CPE(s)	227
6.4 Reports	229
6.4.1 LAN/WAN Statistic	229
6.4.2 NAT Sessions.....	230
6.4.3 LAN/WAN/NAT Graph.....	232
6.4.4 Firmware Overview	233
6.4.5 Firmware Groupview	234
6.4.6 Firmware Upgrade Wizard	235
6.4.7 Network IP Overview (WAN/LAN).....	236
6.4.8 Status Overview / USB Modem Overview / Port Status Overview.....	237
6.4.9 Information Note Overview.....	238
6.4.10 Information Device Information Overview / Detail Device Information Overview.....	239
6.4.11 Batch Activation Overview.....	240
6.4.12 Bind with MyVigor Account Overivew	241
6.5 Inventory Monitor	242
Chapter 7 System Operation.....	243
7.1 System Parameter Setting.....	244
7.2 Language Setting.....	245
7.3 Global Mail Server Setting.....	246
7.4 Global SNMP Server Setting.....	248
7.5 Health Server Setting.....	249
7.6 Block Host Setting	250

7.7 Clear Logs Setting	250
7.8 Upload Serial Number Setting	251
Chapter 8 Alarm Information	253
8.1 Alarm	253
8.2 Alarm History	258
8.3 Mail Server.....	260
8.4 SMS Server	262
8.5 SNMP Server.....	263
8.6 Latest Alarms.....	265
Chapter 9 Log View	267
9.1 Device Action.....	268
9.1.1 Action Log.....	268
9.1.2 Reboot Log	270
9.1.3 RebootByCPELog / ResetSystemPasswordLog	272
9.1.4 SetParameterLog	274
9.1.5 FileTransferLog	276
9.1.6 FirmwareUpgradeWizard	279
9.1.7 SettingProfileLog	281
9.1.8 DeviceSysLog	285
9.1.9 CPENotifyLog	287
9.2 System	289
9.2.1 System Log	289
9.2.2 LoginLog.....	291
9.2.3 DeviceInformationLog	293
9.2.4 DeviceOperateLog	295
Chapter 10 Provision Configuration.....	297
10.1 General Setting	298
10.1.1 Upload File	298
10.1.2 Trigger	300
10.2 FirmwareUpgrade	302
10.2.1 UpgradeSetting	302
10.2.2 AuthkeyCheck	305
10.2.3 IncludeList	306
10.2.4 ExcludeList	308
10.2.5 RemoteFileList	310
10.3 Backup	311
10.3.1 BackupSetting	311
10.3.2 Backup.....	313

10.4 Restore	314
10.4.1 RestoreSetting.....	314
10.4.2 Restore	316
10.5 Provision Setting.....	317
10.5.1 KeepProfile Setting.....	317
WAN Settings.....	318
10.5.2 SettingProfile	321
Information Tab	322
Settings Tab	323
10.6 Global Parameters.....	325
10.6.1 Parameters.....	325
Primary Setting.....	327
Complete Parameter	327
APM Wizard	328
10.6.2 IncludeNetwork.....	329
Chapter 11 Help for License	331
11.1 About VigorACS.....	331
11.2 License Key Information	333
11.3 License Agreements.....	333
Part III Application	335
Chapter 12 Tutorials	337
12.1 How to Manage CPE through VigorACS.....	337
12.1.1 Set ACS URL on CPE	337
12.1.2 Invoke Remote Management for CPE	338
12.1.3 Enable WAN Connection on CPE	339
12.1.4 Connect to ACS Server through PVC Channel.....	339
12.2 How to upgrade CPE firmware by using VigorACS SI Provision	341
12.3 How to upgrade CPE firmware by using VigorACS SI Firmware Upgrade Wizard.....	347
12.4 How to use Copy Parameter	349
12.5 How to create a VPN by using VPN Wizard.....	356
12.6 Creating an Account for MyVigor.....	363
12.6.1 Creating an Account via VigorACS SI.....	363
12.6.2 Creating an Account via MyVigor Web Site	367
12.7 Upgrade VigorACS with New License Key.....	370
12.7.1 License Is Invalid or Expired	370
12.7.2 License Is Valid Still	375
12.8 How to Backup CPE's Configuration via Wizards	380
12.9 How to Restore CPE's Configuration via Wizards.....	382

12.10 How to apply KeepProfile Setting in Provision for a New CPE	384
12.11 How to Backup the Database of VigorACS SI.....	387
12.11.1 For Linux Platform – Backup Instantly	387
12.11.2 For Linux Platform – Backup by Schedule.....	389
12.11.3 For Windows Platform – Backup Instantly	391
12.11.4 For Windows Platform – Backup by Schedule.....	393
12.12 How to Restore the Database of VigorACS SI	395
For Linux Platform.....	395
For Windows Platform	395
12.13 How to use VigorACS SI to do batch firmware upgrade	397
12.14 How to create user account and network group by Wholesale Wizard.....	401
Chapter 13 Trouble Shooting.....	405
13.1 Contacting DrayTek.....	405
Chapter 14 Reference Information	407
14.1 For Linux System.....	407
14.2 For Windows XP System	407

Part I Introduction

Chapter 1 Features

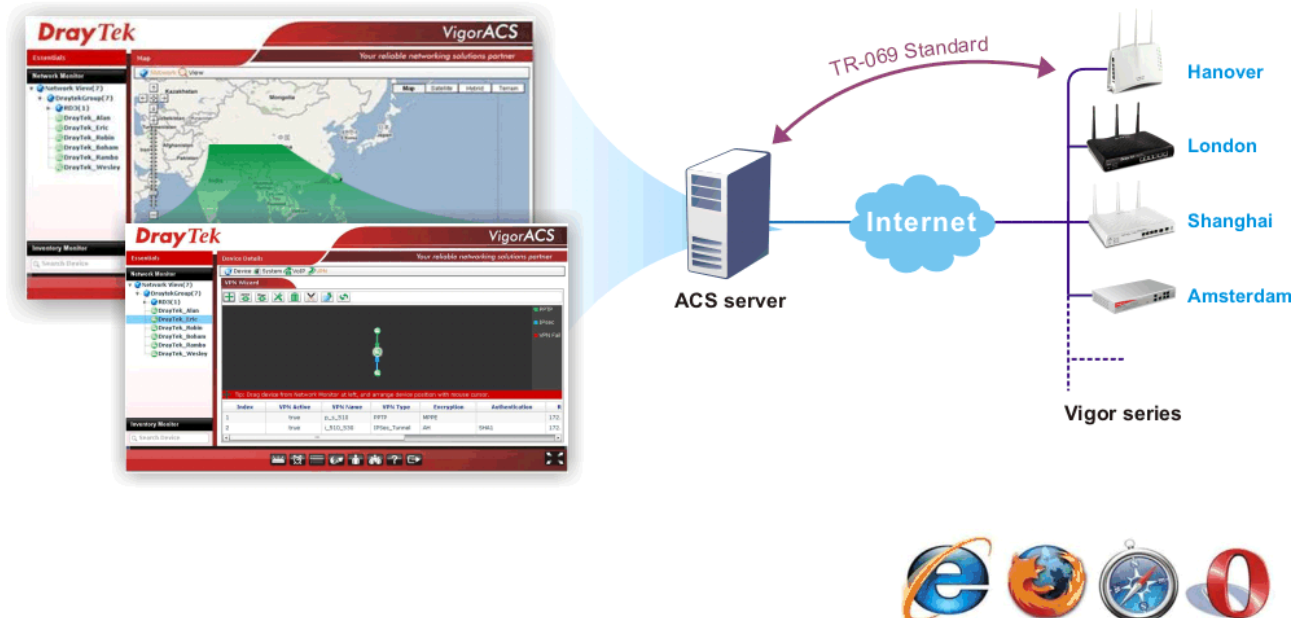
VigorACS is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway and wireless AP. VigorACS has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore and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

Chapter 2 Installation

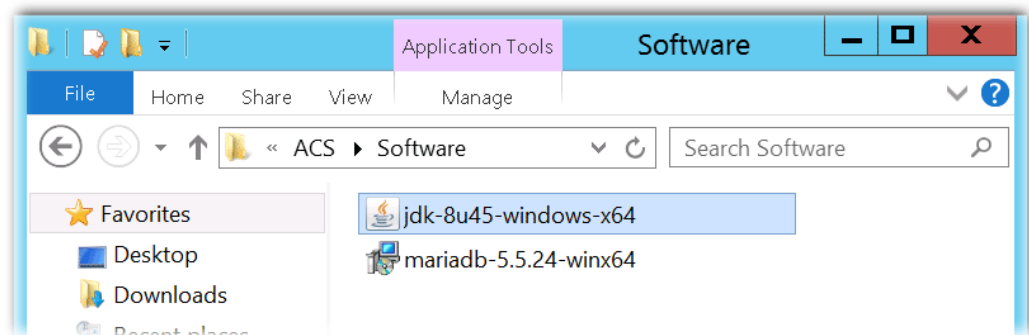
Please follow the procedure listed below to install VigorACS completely. The installation for different platforms might be different.

2.1 Platform for Windows 2000, XP, Vista, 7 or 10

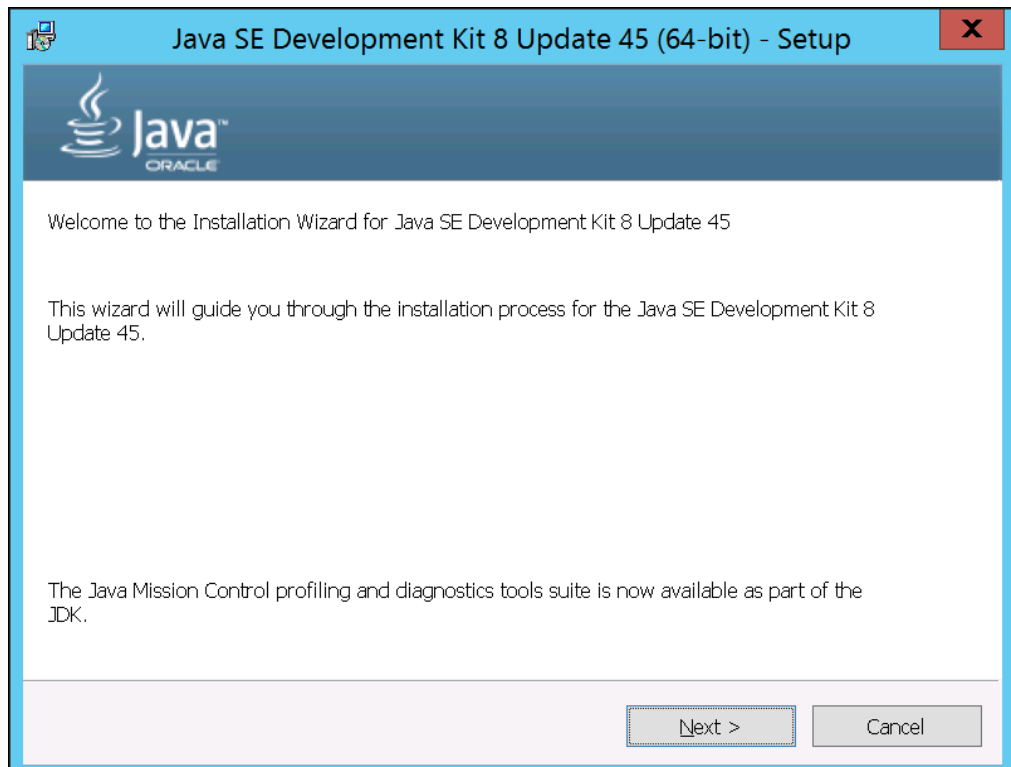
There are three programs needed to be installed for operating VigorACS.

2.1.1 Installation for Java

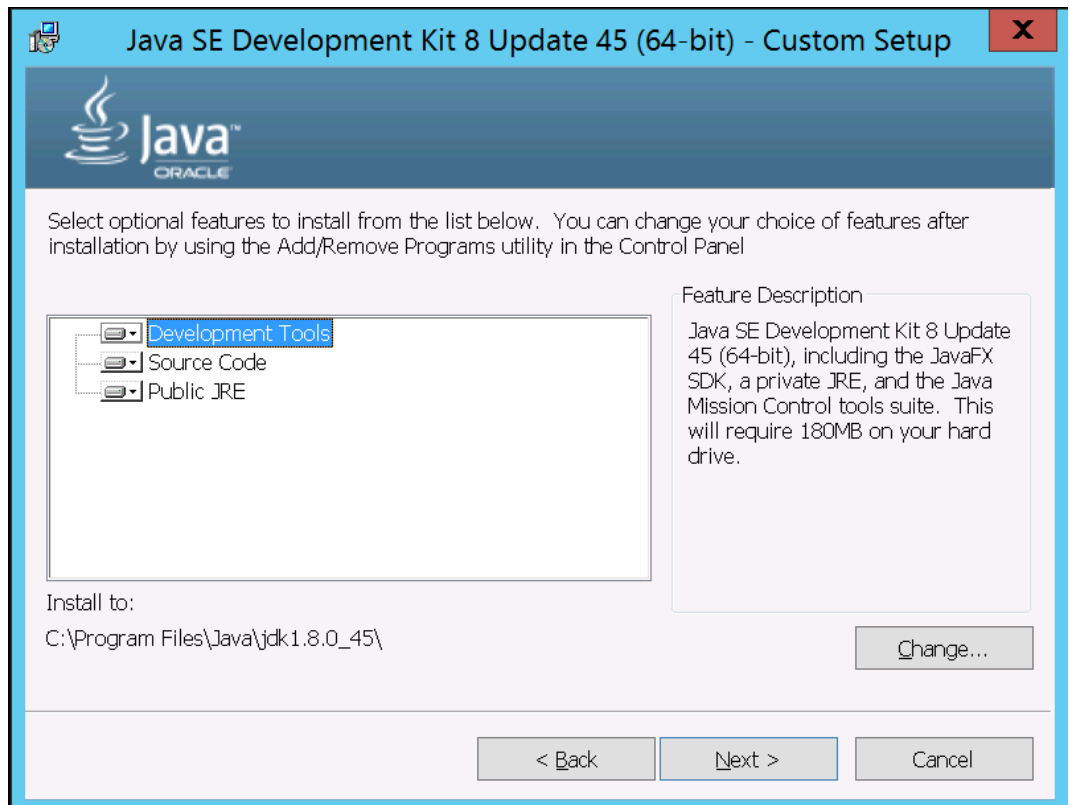
1. Install Java by clicking “jdk-8u45-windows-x64” it to execute the installation.



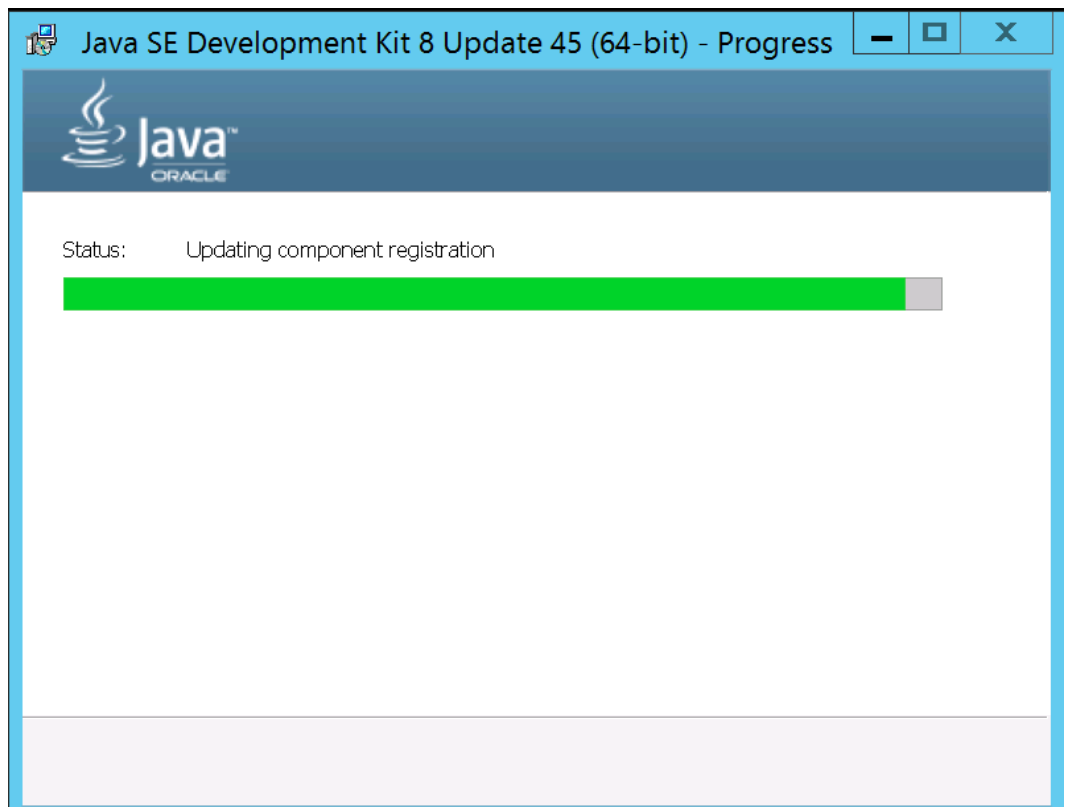
2. The first page will be shown as follows. Click **Next** to get into next page.



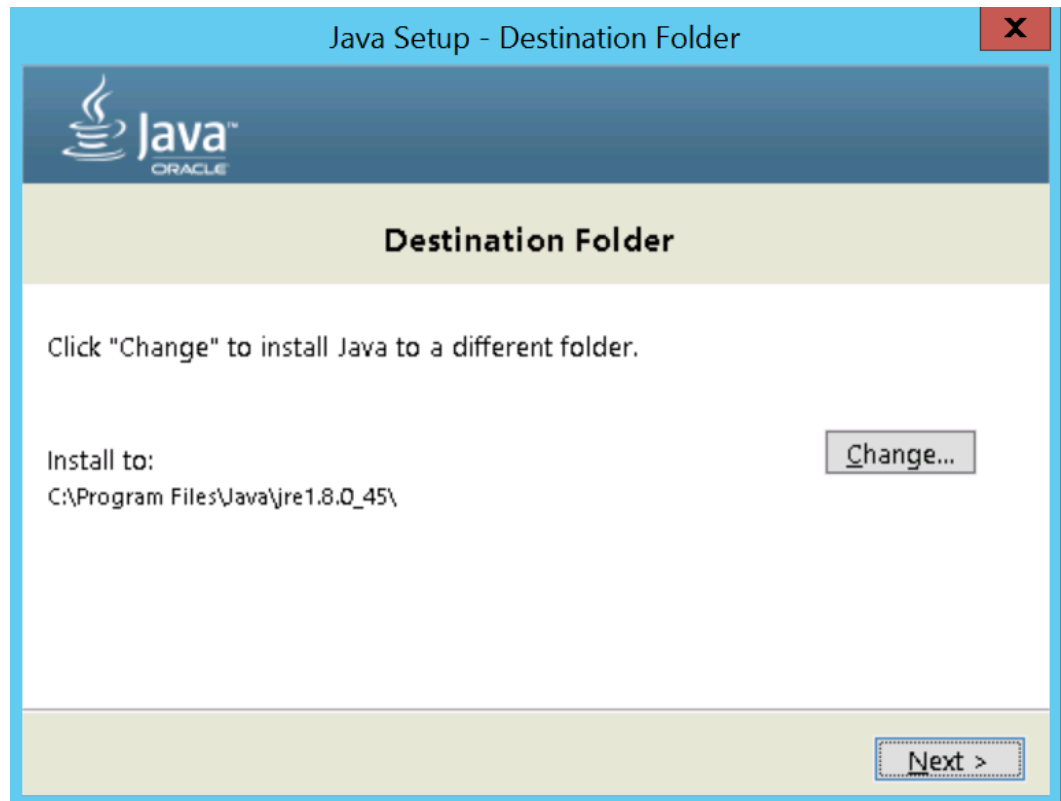
3. In this page, optional features will be listed for you to choose for installation. Choose the one you need and click **Next**.



4. Wait for a while to install the selected feature.



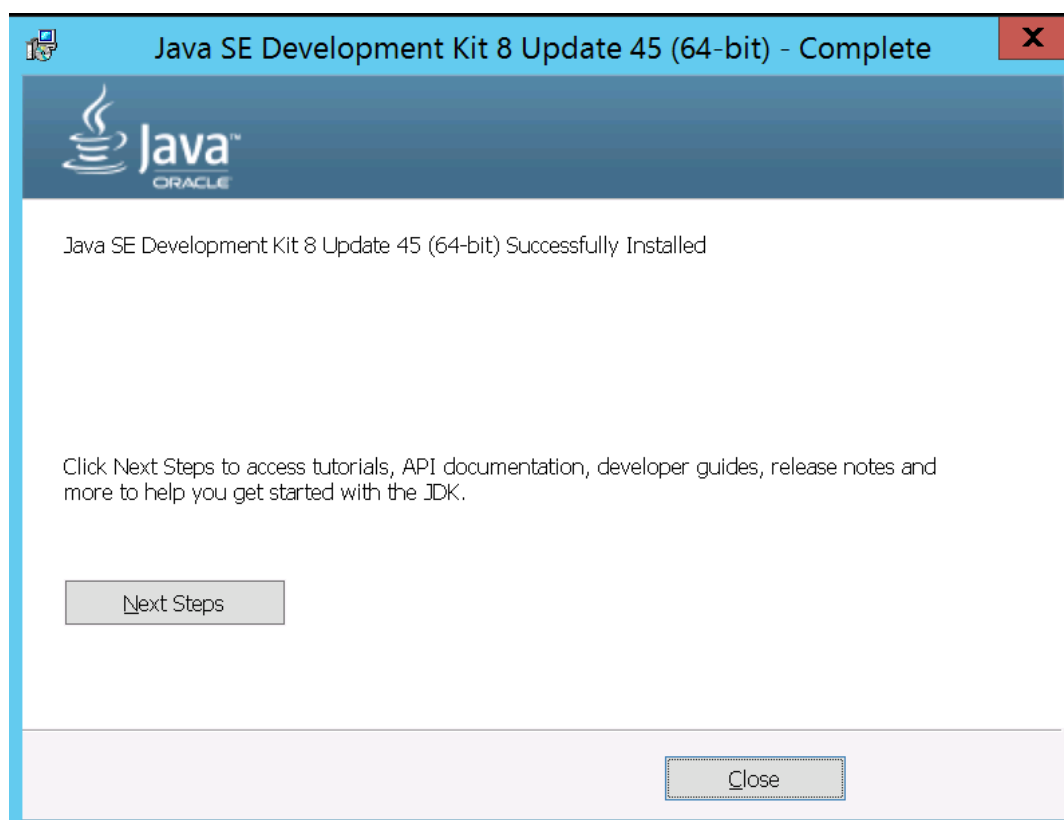
5. A page to specify the destination folder for JAVA driver will appear. Use the default location or click **Change** to specify another location. Then, click **Next**.



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

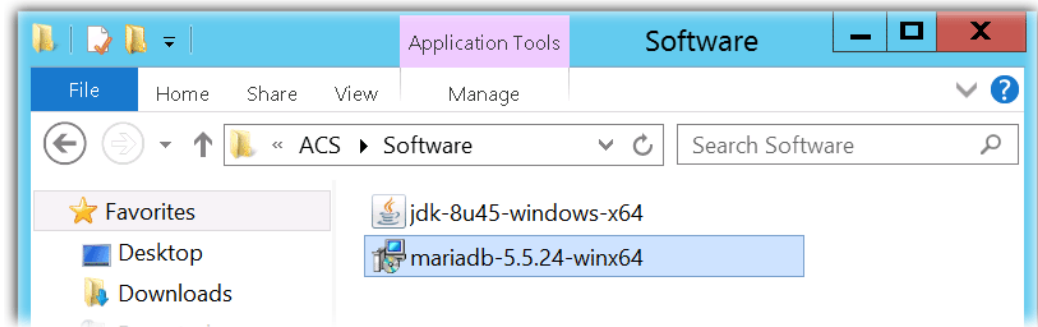


7. When the following page appears, the installation is completed. Click **Close** to exit the installing program.

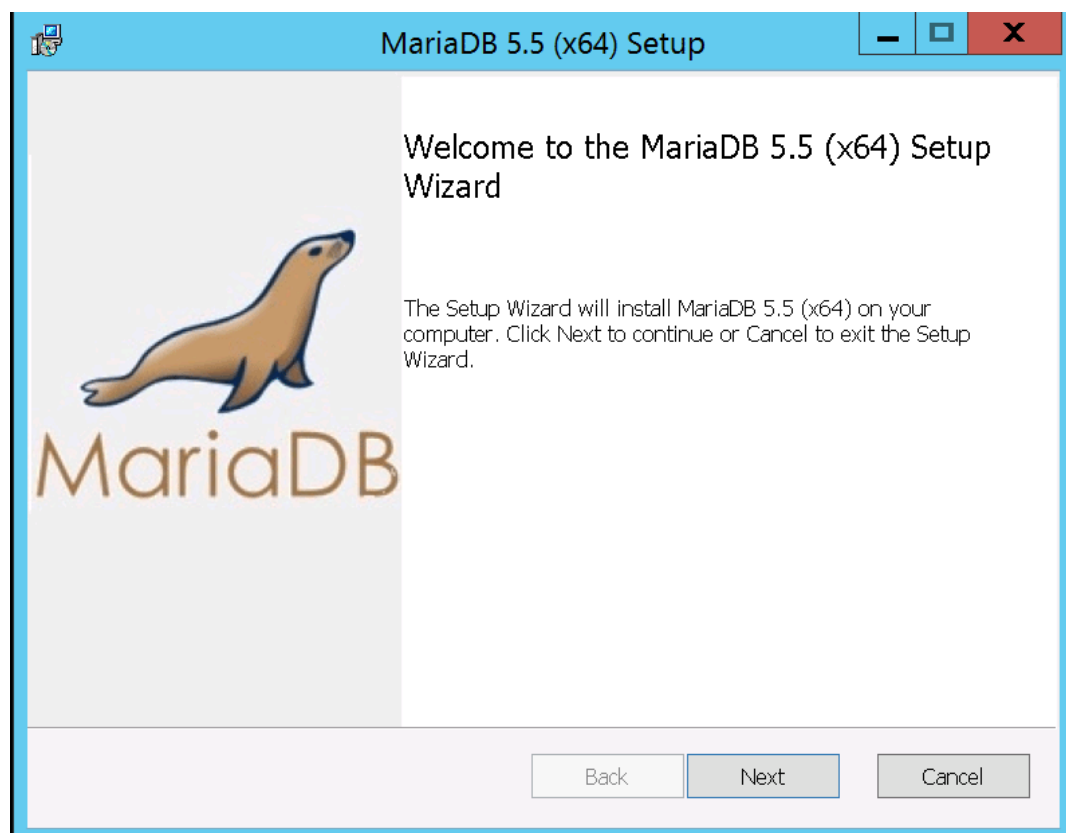


2.1.2 Installation for MariaDB

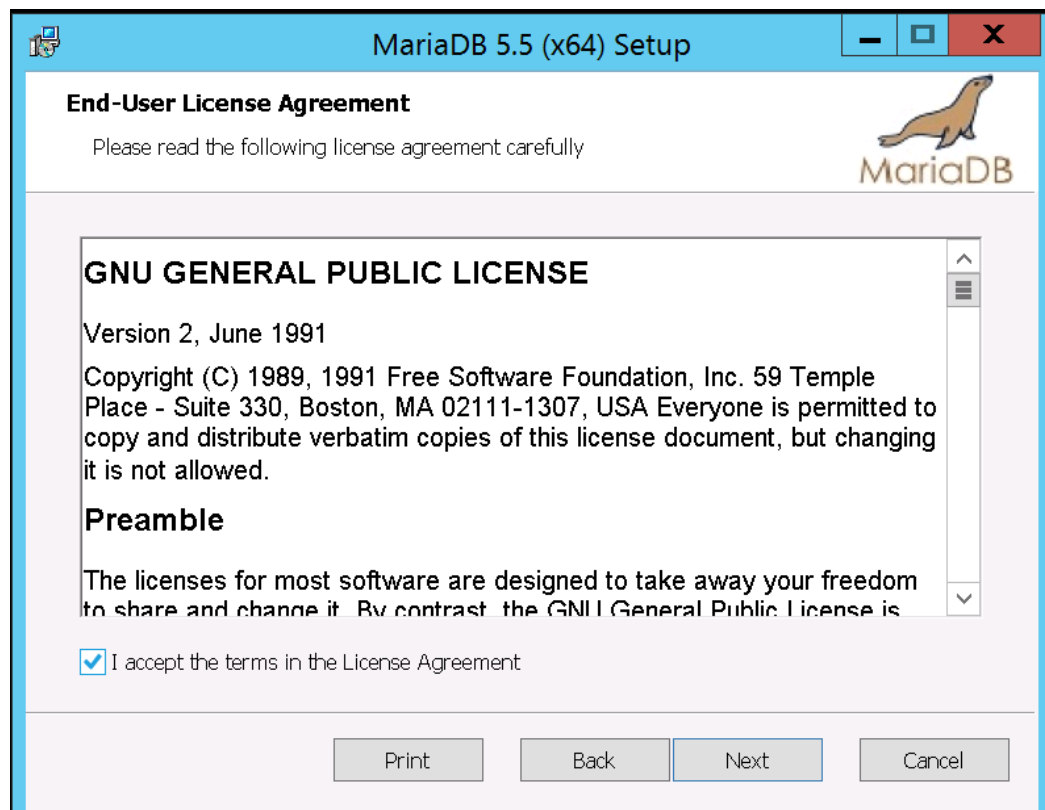
1. Install MariaDB by clicking “mariadb-5.5.24-winx64” it to execute the installation.



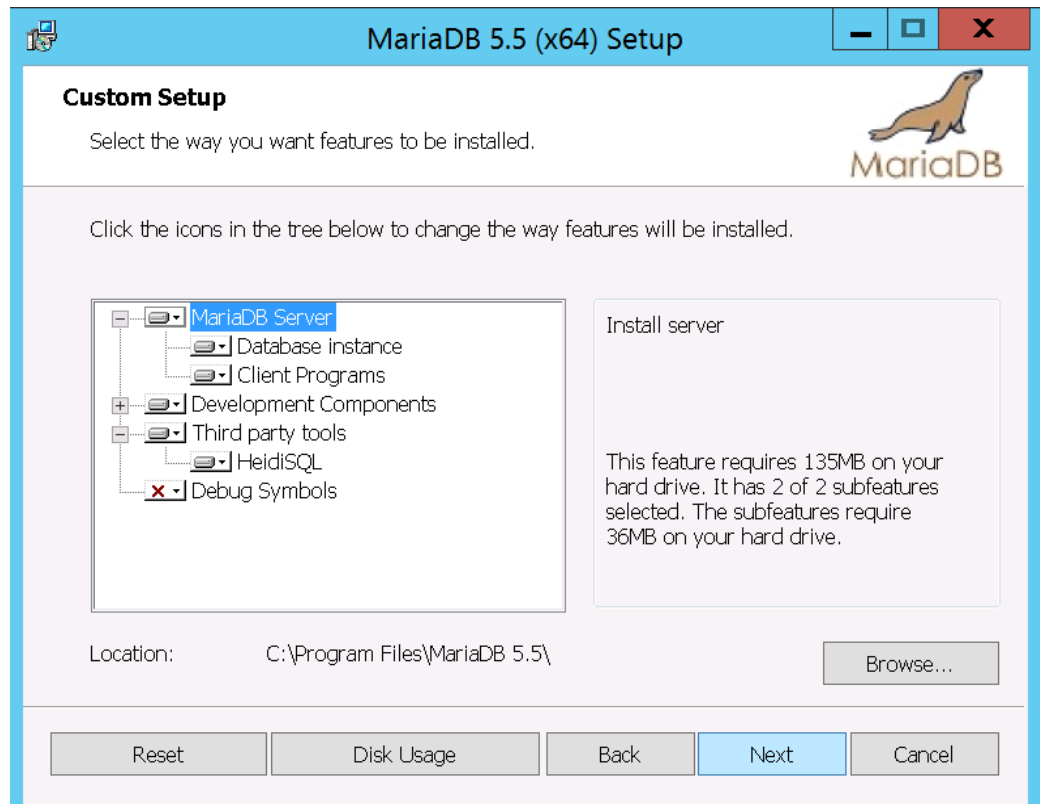
2. When the welcome screen appears, please click **Next** for next step.



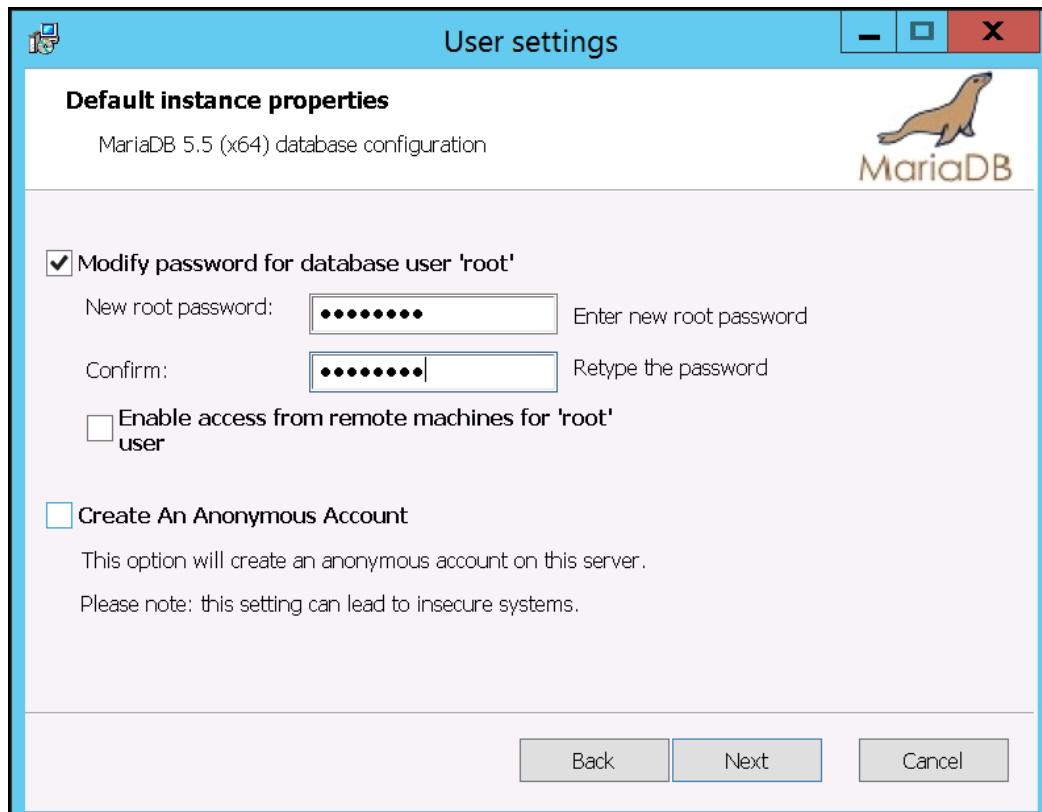
3. On this dialog box, check the box of “I accept the terms....” and click **Next**.



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**.

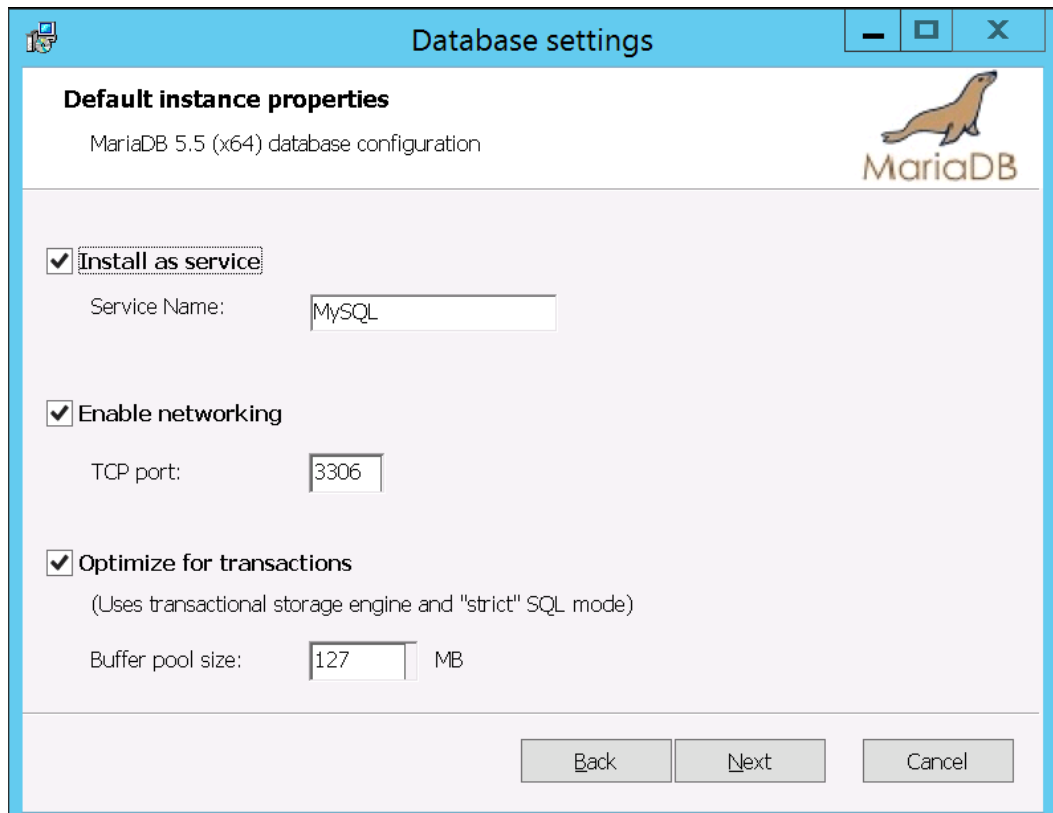


The 'User settings' window for MariaDB 5.5 (x64) database configuration. It features a title bar with standard window controls. The main content area is titled 'Default instance properties' and includes the MariaDB logo. The configuration options are as follows:

- ☒ **Modify password for database user 'root'**
 - New root password: [password field] Enter new root password
 - Confirm: [password field] Retype the password
 - ☐ **Enable access from remote machines for 'root' user**
- ☐ **Create An Anonymous Account**
 - This option will create an anonymous account on this server.
 - Please note: this setting can lead to insecure systems.

At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

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

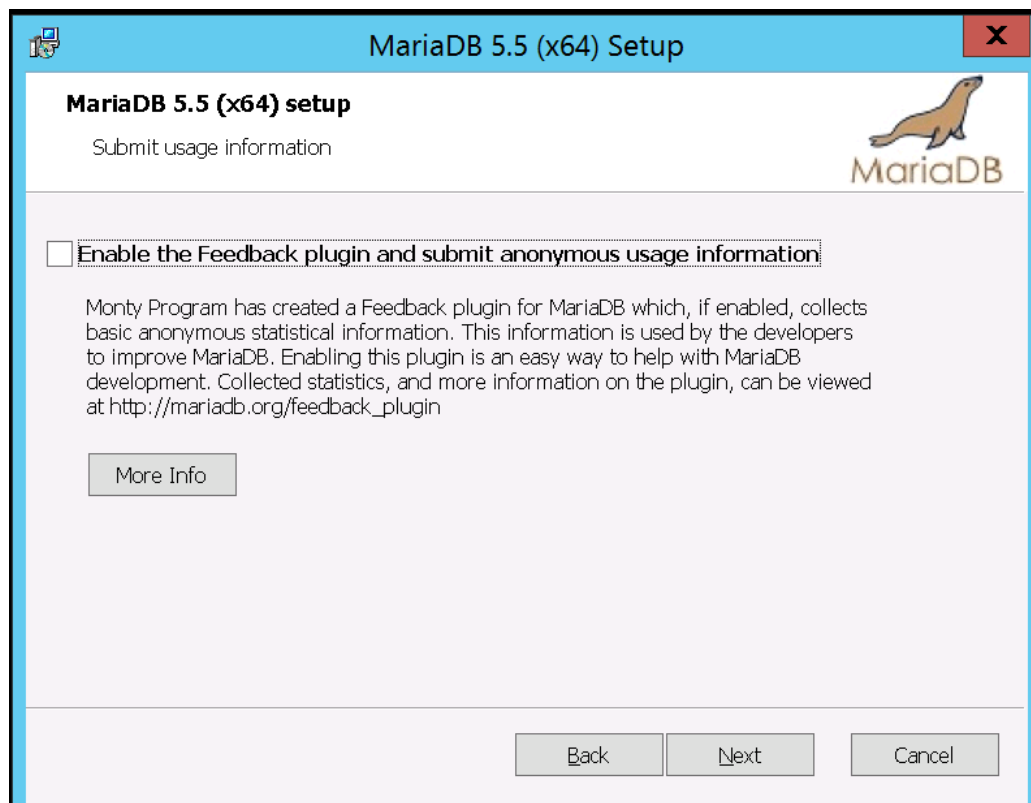


The 'Database settings' window for MariaDB 5.5 (x64) database configuration. It features a title bar with standard window controls. The main content area is titled 'Default instance properties' and includes the MariaDB logo. The configuration options are as follows:

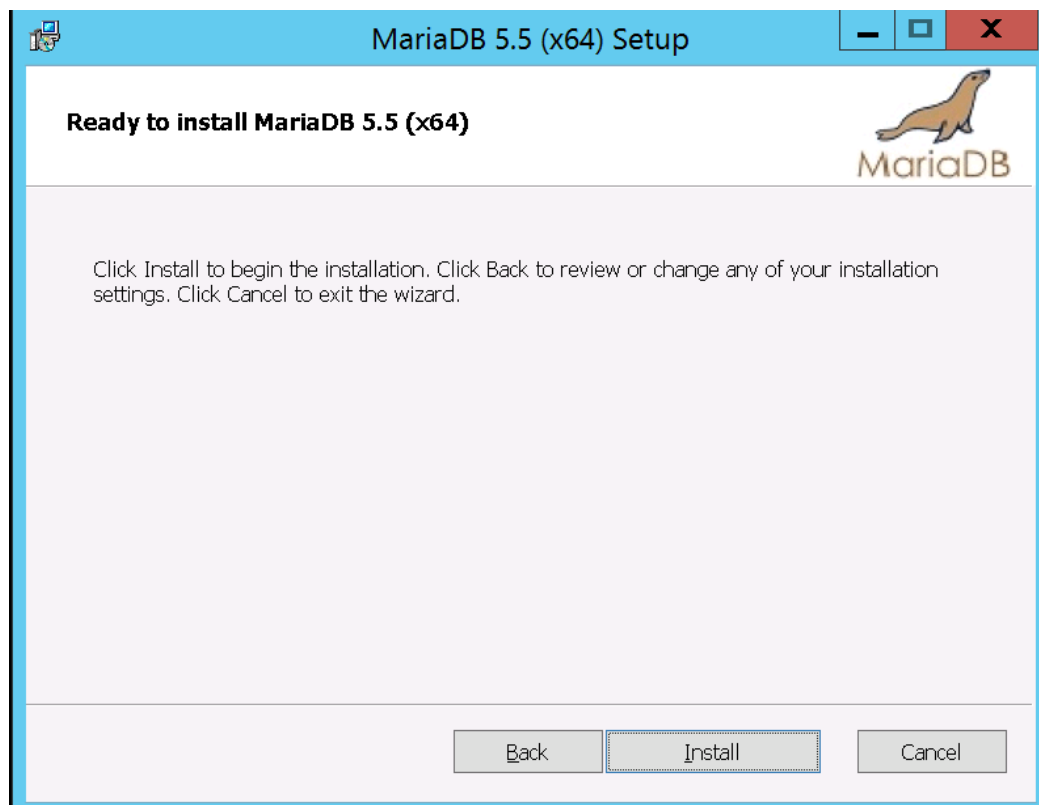
- ☒ **Install as service**
 - Service Name: [MySQL]
- ☒ **Enable networking**
 - TCP port: [3306]
- ☒ **Optimize for transactions**
 - (Uses transactional storage engine and "strict" SQL mode)
 - Buffer pool size: [127] MB

At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

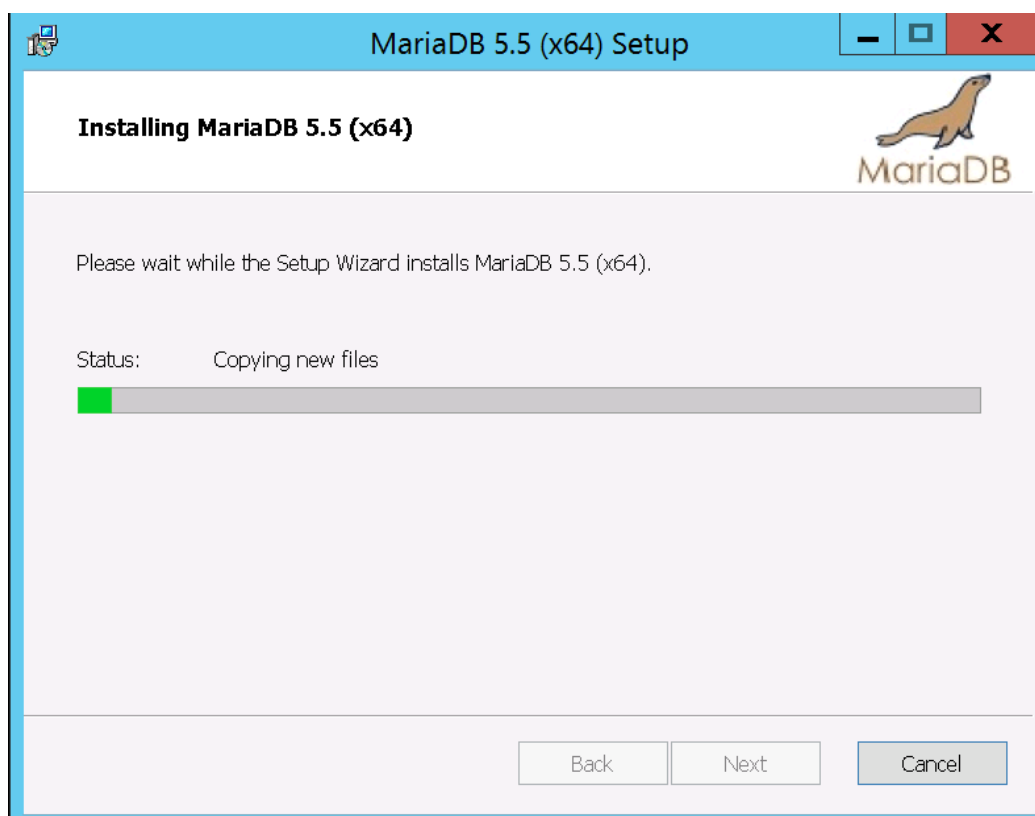
7. On this dialog box, click **Next**.



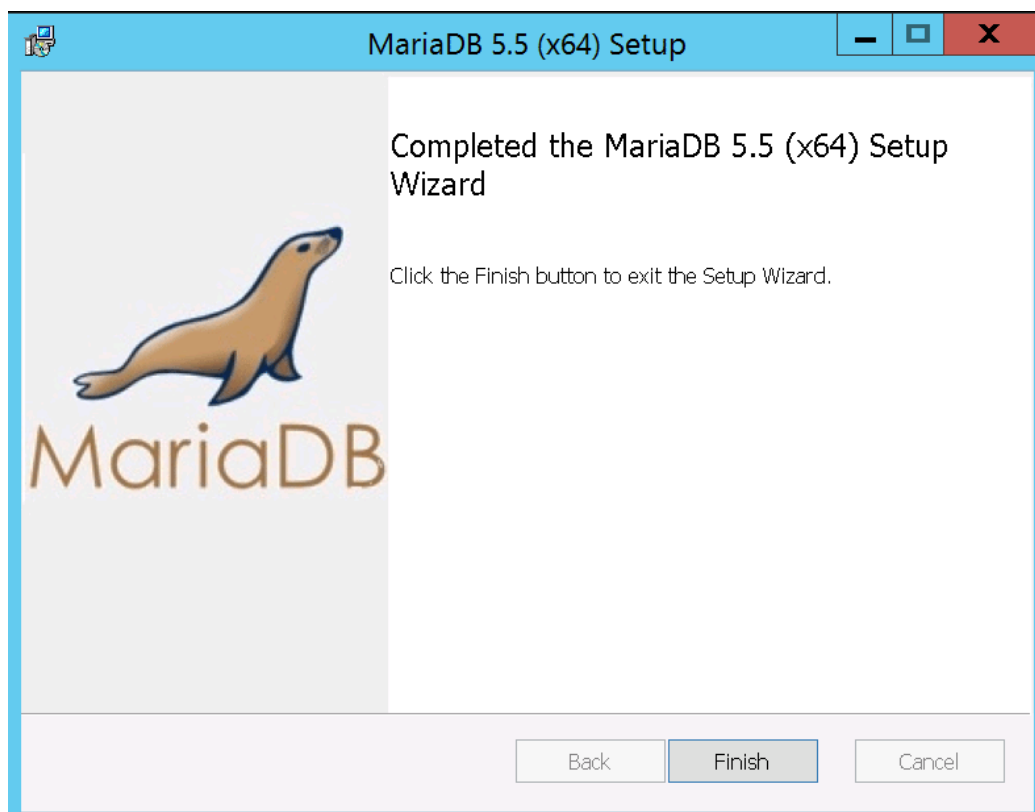
8. On this dialog box, click **Install**.



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



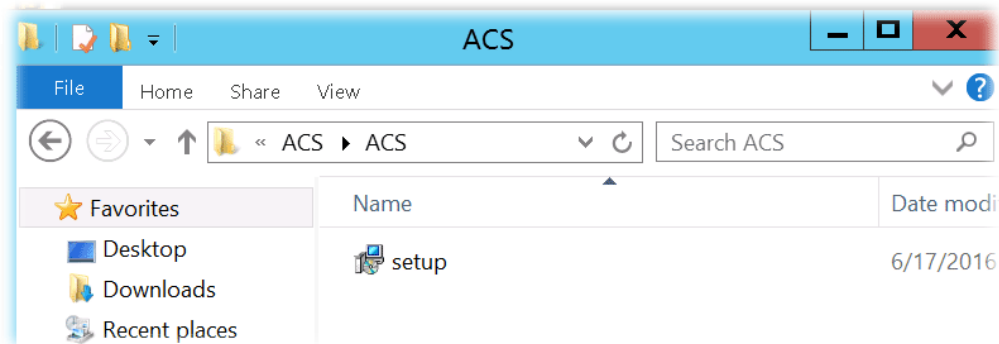
10. After finishing the configuration, please click **Finish** to exit the wizard.



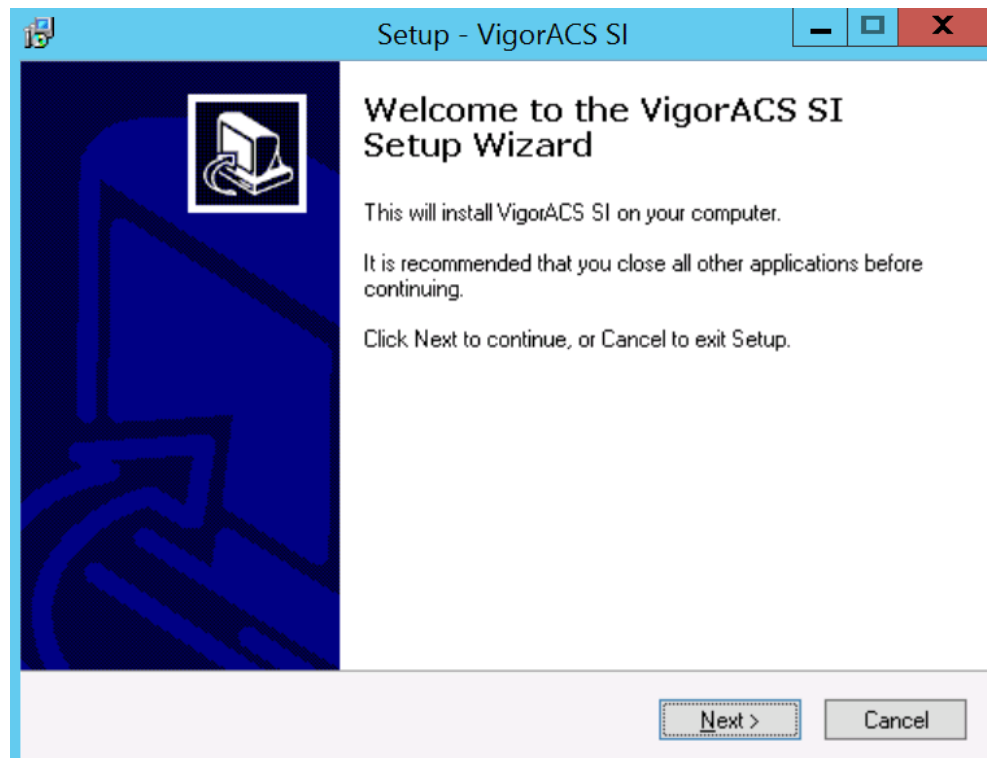
2.1.3 Installation for VigorACS SI

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

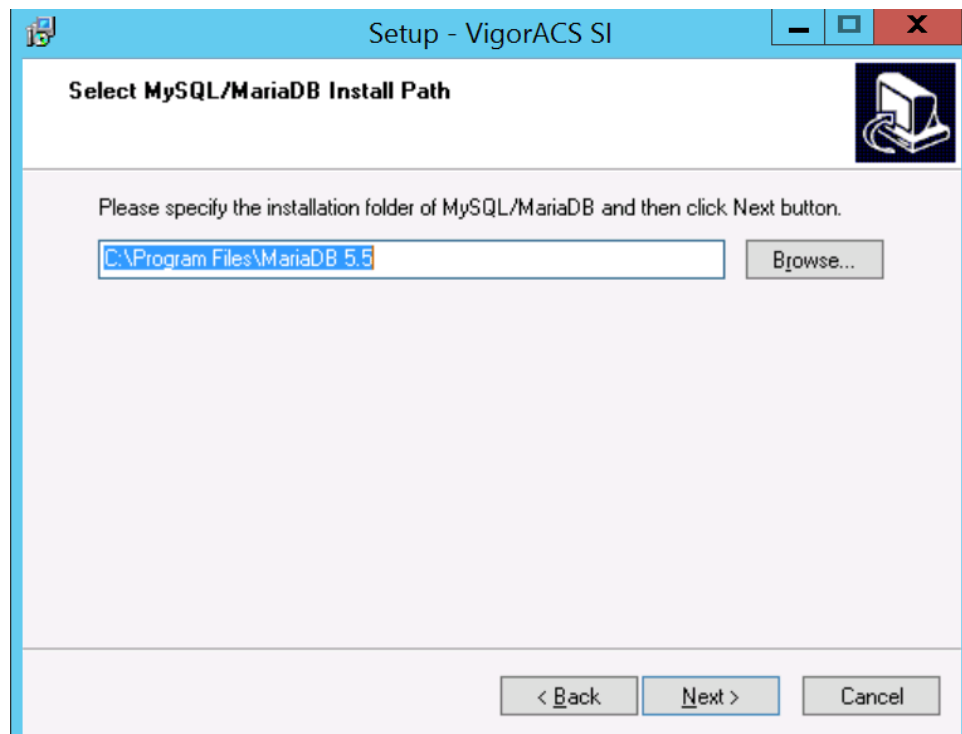
1. Click **Setup** to run VigorACS SI setup wizard.



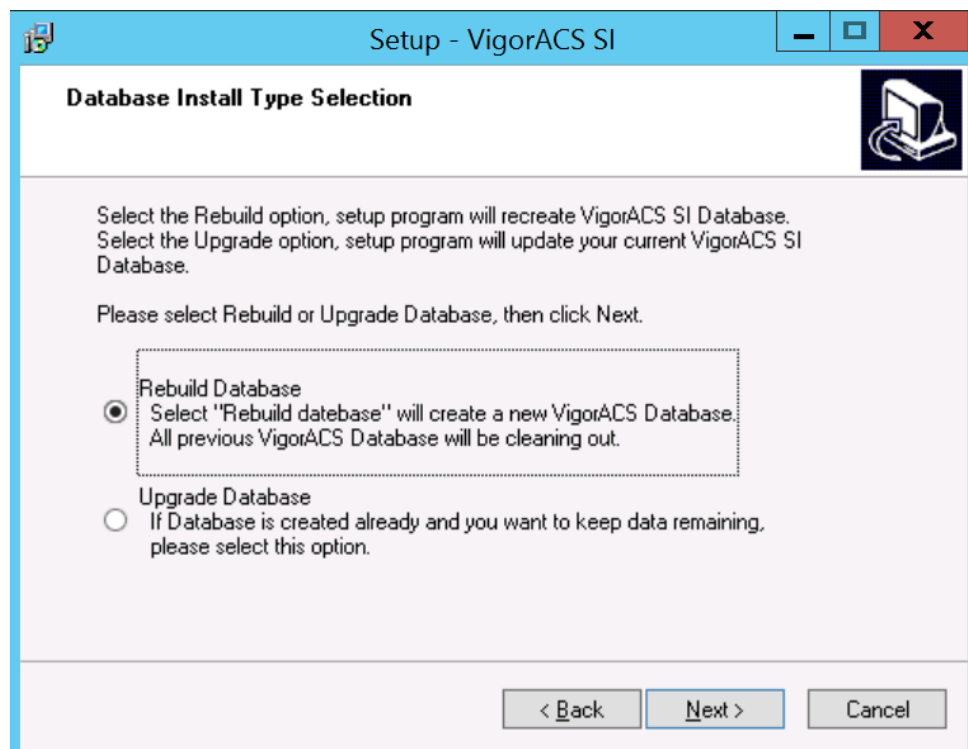
2. When the following dialog appears, click **Next**.



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**.



- 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**.

Setup - VigorACS SI

MySQL/MariaDB Account Setting

Please specify password of root of MySQL/MariaDB, this step can be ignored if MySQL/MariaDB database has not been configured.

root password

confirm root password

< Back Next > Cancel

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

Setup - VigorACS SI

Maximum And Minimum Memory

What is your maximum and minimum memory?

Please specify your maximum and minimum memory, then click Next.

Maximum Memory:

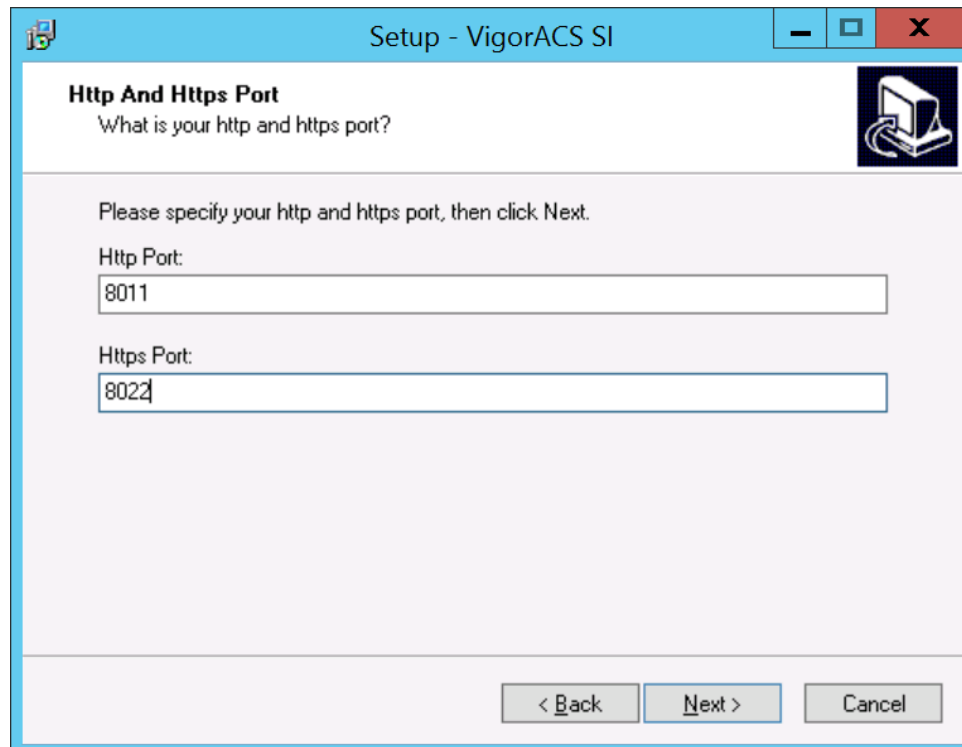
Minimum Memory:

512

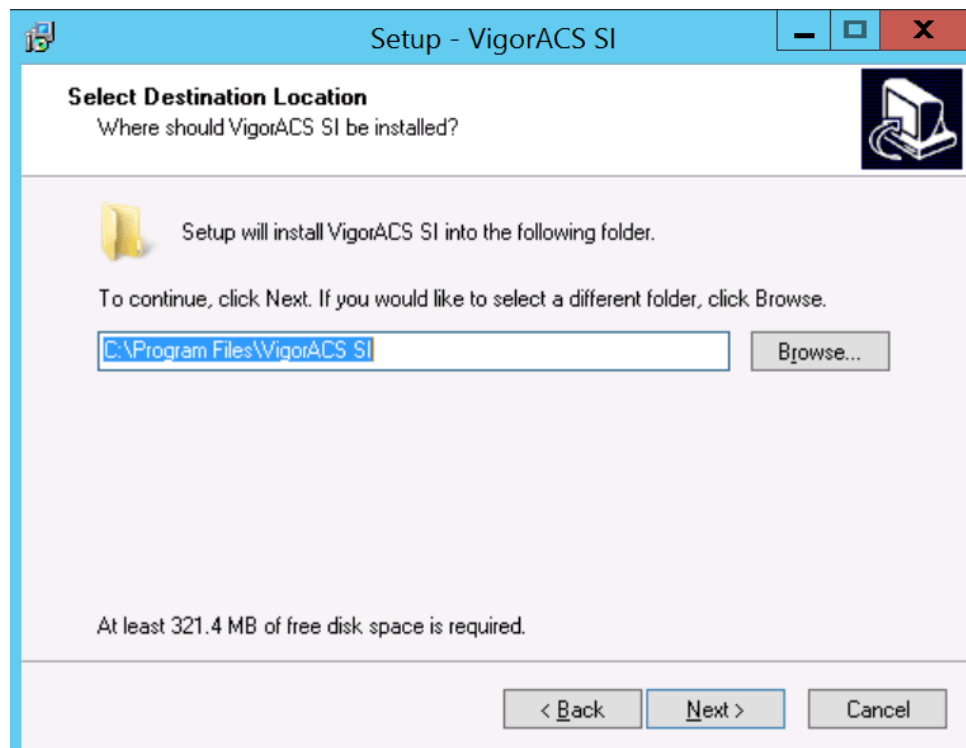
128

< Back Next > Cancel

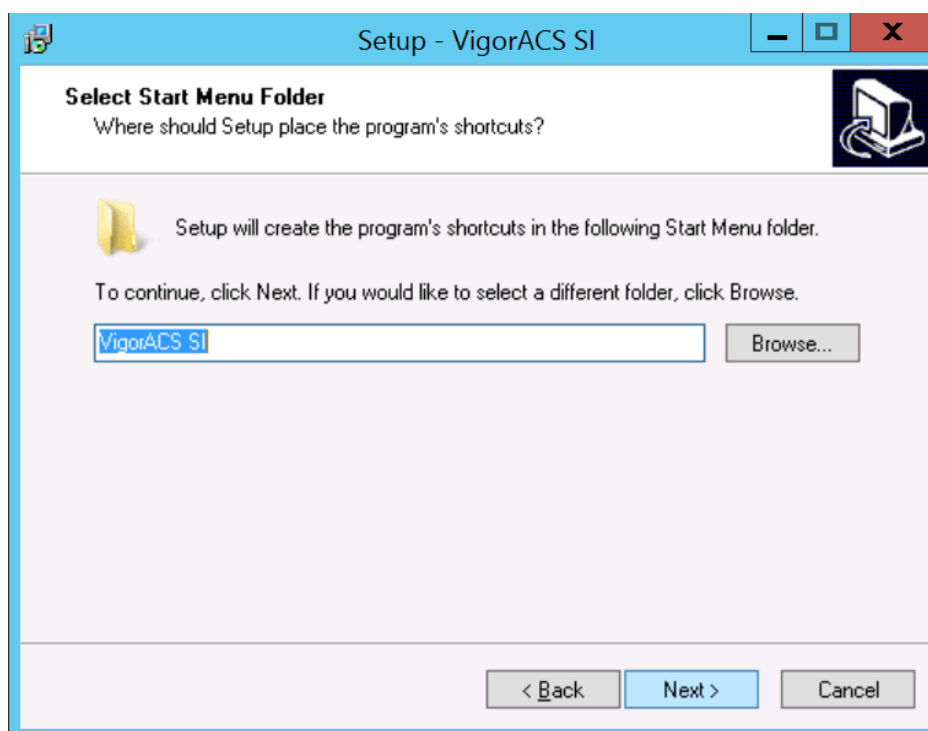
7. Setup ACS HTTP and HTTPS port, we'll suggest using others port instead of default 80 and 443 port to prevent conflict.



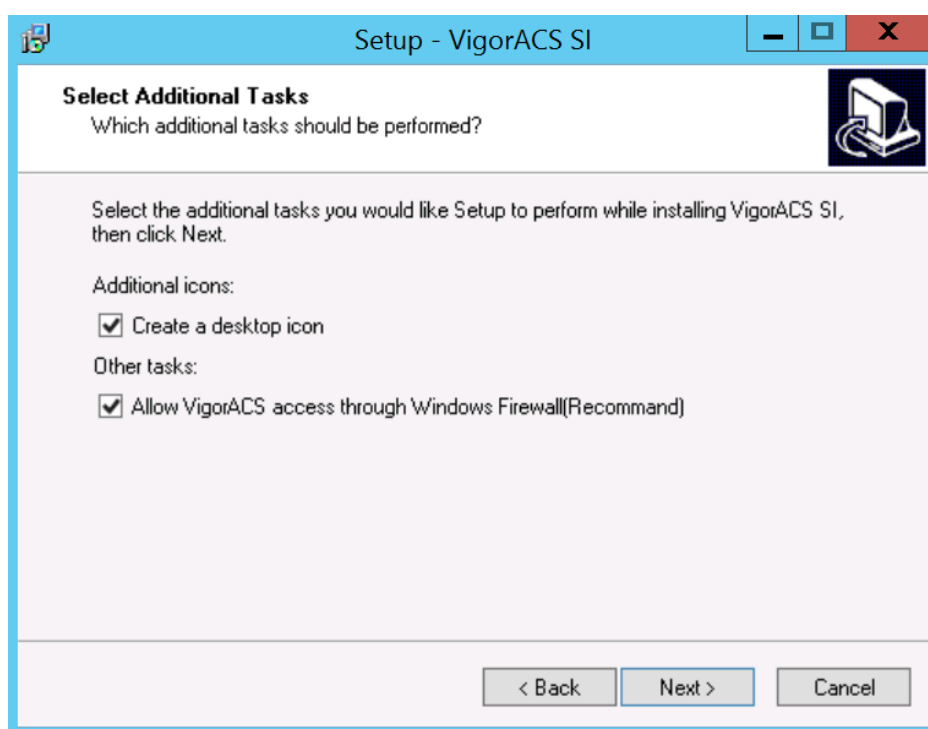
8. Determine the destination folder and click **Next**. The default directory used by this program is *c:\Program Files\VigorACS SI*. You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS SI in installation.



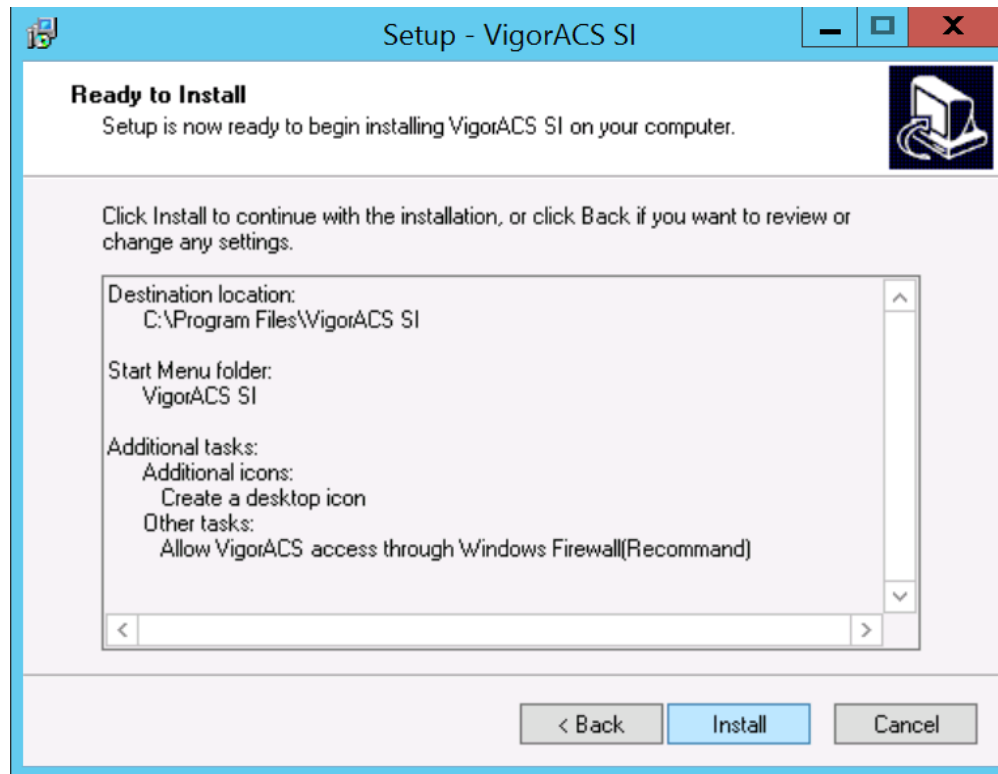
9. Determine the program name of VigorACS SI for you to start up. Then click **Next**.



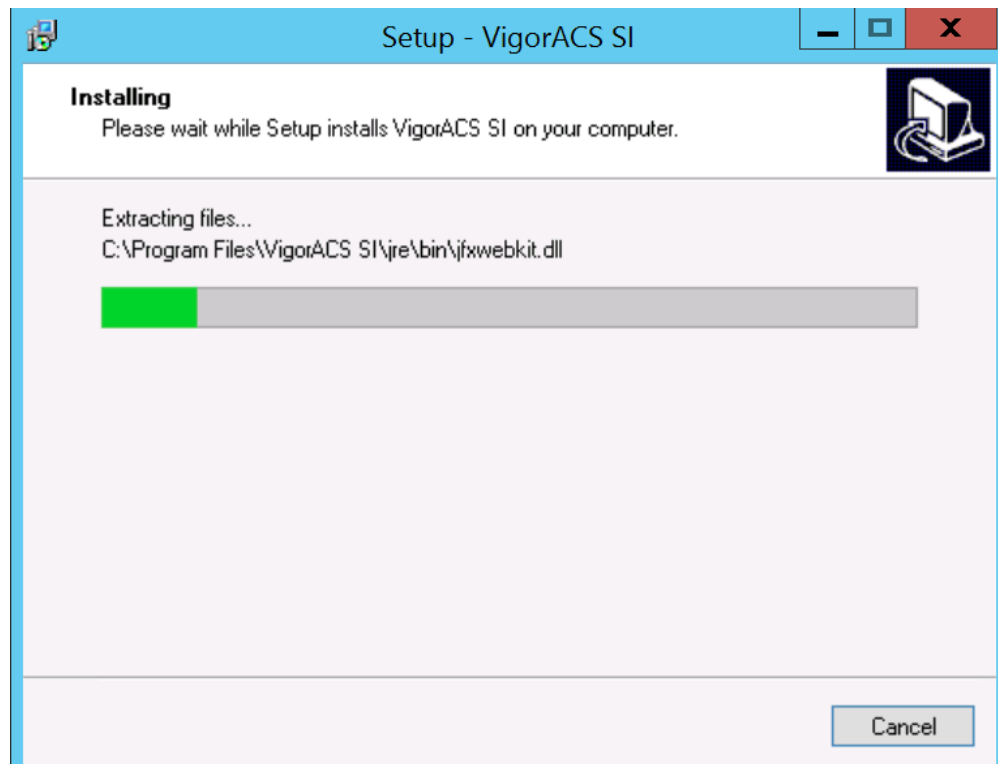
10. In this dialog, check the box of "**Create a desktop icon**" for your necessity. Click **Next**.



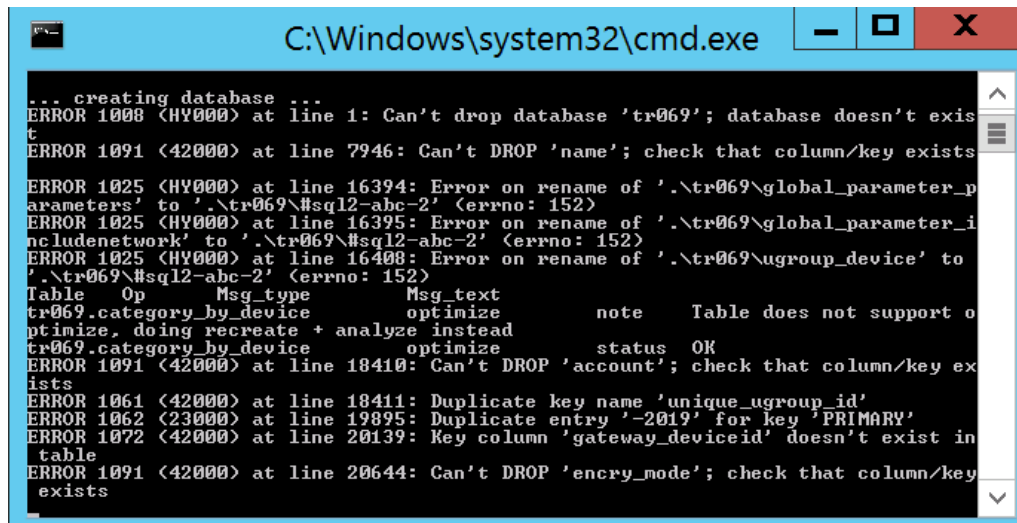
11. Now, the program is ready to install necessary features and files to your computer. Please click **Install** to start.



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

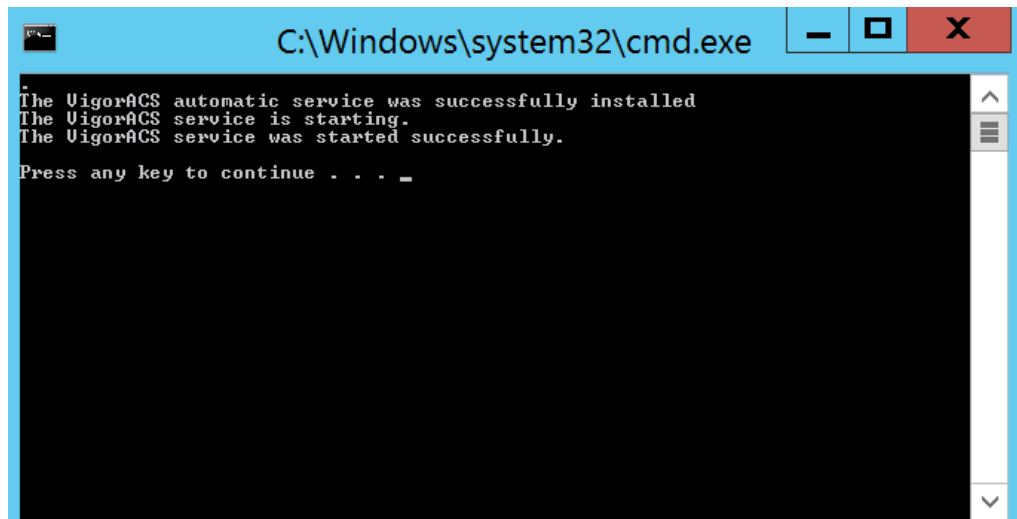


13. While installing, the following screen will appear to show that MariaDB has been activated. Please wait for next dialog appearing.



C:\Windows\system32\cmd.exe

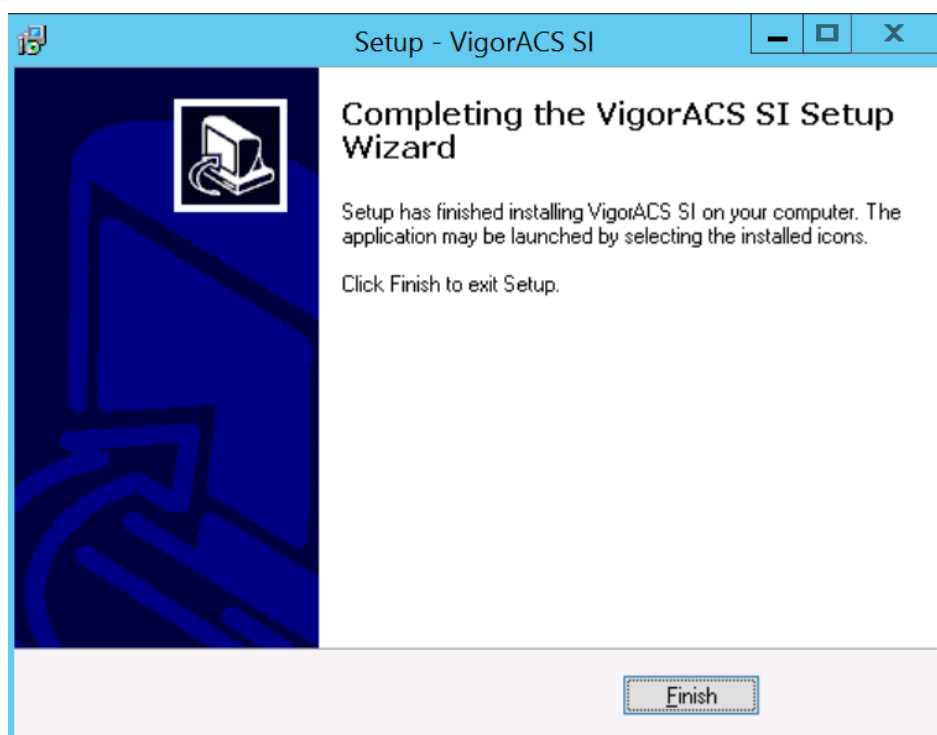
```
... creating database ...  
ERROR 1008 (HY000) at line 1: Can't drop database 'tr069'; database doesn't exist  
ERROR 1091 (42000) at line 7946: Can't DROP 'name'; check that column/key exists  
ERROR 1025 (HY000) at line 16394: Error on rename of '.\tr069\global_parameter_p  
arameters' to '.\tr069\#sql2-abc-2' (errno: 152)  
ERROR 1025 (HY000) at line 16395: Error on rename of '.\tr069\global_parameter_i  
ncludenetwork' to '.\tr069\#sql2-abc-2' (errno: 152)  
ERROR 1025 (HY000) at line 16408: Error on rename of '.\tr069\ugroup_device' to  
'.\tr069\#sql2-abc-2' (errno: 152)  
Table Op Msg_type Msg_text  
tr069.category_by_device optimize note Table does not support o  
ptimize, doing recreate + analyze instead  
tr069.category_by_device optimize status OK  
ERROR 1091 (42000) at line 18410: Can't DROP 'account'; check that column/key ex  
ists  
ERROR 1061 (42000) at line 18411: Duplicate key name 'unique_ugroup_id'  
ERROR 1062 (23000) at line 19895: Duplicate entry '-2019' for key 'PRIMARY'  
ERROR 1072 (42000) at line 20139: Key column 'gateway_deviceid' doesn't exist in  
table  
ERROR 1091 (42000) at line 20644: Can't DROP 'encry_mode'; check that column/key  
exists
```



C:\Windows\system32\cmd.exe

```
..  
The VigorACS automatic service was successfully installed  
The VigorACS service is starting.  
The VigorACS service was started successfully.  
Press any key to continue . . . _
```

14. Now the program has completed the installation of VigorACS SI. Click **Finish** to exit it.



2.2 Platform for Linux / Solaris

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 -
```

```
drwxr-x--- 17 root root 4096
drwxr-xr-x 2 root root 8192
drwxr-xr-x 3 root root 4096
drwxrwxrwt 18 root root 4096
drwxr-xr-x 16 root root 4096
drwxr-xr-x 28 root root 4096
-rw-r--r-- 1 root root 185348096
[root@localhost /]# rm vigoracs
rm: remove regular file 'vigoracs' ? y
[root@localhost /]# ls
bin boot dev etc home initrd lib lost+found misc mnt opt proc root shin tftpboot tmp usr var
[root@localhost /]# cd home/
[root@localhost home]# cd robin/
[root@localhost robin]# ls
vigoracs
[root@localhost robin]# cd vigoracs/
[root@localhost vigoracs]# ls
0.0.1.3 0.0.1.3.1
[root@localhost vigoracs]# cd 0.0.1.3.1/
[root@localhost 0.0.1.3.1]# ls
VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar.gz
[root@localhost 0.0.1.3.1]# ls
VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar.gz
[root@localhost 0.0.1.3.1]# ls
VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar.gz
[root@localhost 0.0.1.3.1]# gzip -cd VigorACS_Unix_Like_Draytek_Pro_0.0.1.3.tar.gz |tar xvf -
```

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

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

```
linux/my.cnf
linux/mysql-standard-4.0.24-pc-linux-gnu-i686.tar.gz
solaris_8/coreutils-4.5.4-sol8-sparc-local.gz
solaris_8/jdk-1_5_0_07-solaris-sparc.tar.Z
solaris_8/jdk-1_5_0_07-solaris-sparcv9.tar.Z
solaris_8/libgcc-3.3-sol8-sparc-local.gz
solaris_8/libiconv-1.8-sol8-sparc-local.gz
solaris_8/my.cnf
solaris_8/mysql-4.0.21-sol8-sparc-local.gz
solaris_8/ncurses-5.4-sol8-sparc-local.gz
solaris_8/unzip-5.50-sol8-sparc-local.gz
solaris_9/coreutils-4.5.4-sol9-sparc-local.gz
solaris_9/jdk-1_5_0_07-solaris-sparc.tar.Z
solaris_9/jdk-1_5_0_07-solaris-sparcv9.tar.Z
solaris_9/libgcc-3.3-sol9-sparc-local.gz
solaris_9/libiconv-1.8-sol9-sparc-local.gz
solaris_9/my.cnf
solaris_9/mysql-4.0.21-sol9-sparc-local.gz
solaris_9/ncurses-5.4-sol9-sparc-local.gz
solaris_9/unzip-5.50-sol9-sparc-local.gz
uninstall.sh
vigoracs
vigoracsmysqld
[root@localhost 0.0.1.3.1]# chmod 755 ./install.sh
[root@localhost 0.0.1.3.1]# chmod 755 ./uninstall.sh
[root@localhost 0.0.1.3.1]#
```

5. Execute ./install.sh installation file. Please make sure you have /usr/bin/sh first. If you don't have /usr/bin/sh, please type the command:

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

```
[root@ip-172-31-17-131 VigorACS_Unix_Like_Draytek_Pro64_1.1.9]# ls
acs          install_sqlite.sh      Install VigorACS Guide.txt      linux          solaris_8
install_acs.sh install_Synology_NAS.sh  Install VigorACS on Synology Guide.txt Quick Start Guide.txt solaris_9
install.sh   install_user_vigoracs.sh jcelib                          scripts        uninstall.sh
[root@ip-172-31-17-131 VigorACS_Unix_Like_Draytek_Pro64_1.1.9]# ./install.sh
entering /home/ec2-user/VigorACS_Unix_Like_Draytek_Pro64_1.1.9/linux.....
Please create /usr/local/vigoracs
Create it now? (y/n)
y
```

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

1. Install MariaDB
2. Install java
3. Install VigorACS (It will build one MariaDB database: tr069)
4. Upgrade VigorACS (It will upgrade tr069 database)
5. Exit

input select num :

Note: 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 4 is used to upgrade VigorACS, so it is not necessary for you to execute for the first time of installation.

7. 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'
```

```
1. Install mysql/mariadb
2. Install java
3. Install VigorACS ( It will build one mysql/mariadb database : tr069 )
4. Upgrade VigorACS ( It will upgrade tr069 database )
5. Exit
input select num :
1
Do you want to install mariadb(mariadb-5.5.24-linux-x86_64.tar.gz) ... (y/n)?
y
```



```
Starting VigorACS MYSQL: [OK]
```

8. Input 2 to install Java.

9. Install 3 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.

```
1. Install mysql/mariadb
2. Install java
3. Install VigorACS ( It will build one mysql/mariadb database : tr069 )
4. Upgrade VigorACS ( It will upgrade tr069 database )
5. Exit
input select num :
3
After installing VigorACS , tr069 will be created automatically.
Which Mysql do you want to use ? (1: ACS , 2: OS default)( 1,2 or Enter for ACS mysql)
1
Please keyin password of root of MySQL/MariaDB.
```



```
Start to create tr069 db ....
MySQL is running!!
Create tr069 db successfully....
Create tr069 db table....
Create tr069 table successfully....
VigorACS and tr069 install Successfully
```

10. Go to /usr/local/vigoracs/VigorACS/bin/ and execute ./vigoracs.sh, input 3 to start VigorACS. You could type 0.0.0.0 for binding IP which means VigorACS will auto obtain your network adapter IP for VigorACS.

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

Follow the steps listed below to install VigorACS under Solaris:

VigorACS supports Solaris 8 or 9, please confirm the OS version first. For Solaris System, please follow the order to install all the necessary programs.

1. Install library: *libgcc coreutils libiconv ncurses install* (installing mysql/mariadb need).
2. Install mysql/mariadb.
3. Install java.
4. Install VigorACS (it will build one mysql/mariadb database: tr-069).
5. Upgrade VigorACS (It will upgrade tr-069 database).
6. Exit.

2.3 Registering VigorACS

The normal procedure of starting up the VigorACS:

- Start MariaDB Database
- Initiate VigorACS
- Register VigorACS

Different platform has different way of initiation. Please follow the steps listed below for each platform.

2.3.1 For Windows 2000, XP, Vista, 7 and 10

1. Start MariaDB Database

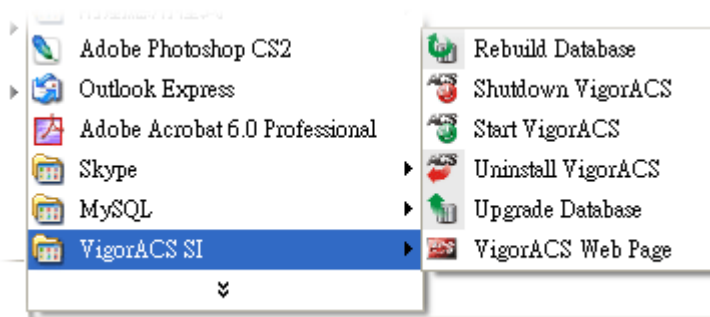
After installing VigorACS, installing program will register MariaDB to Windows Service. MariaDB will startup automatically after installing VigorACS or rebooting system. Normally, you don't need to worry about this step on Windows. But, if you find any problem on VigorACS, you should check MariaDB first.

Please open **Start >Setup >Control Panel >Administrative Tools >Service** to check if the MariaDB Service has been initiated or not. If not, please double click it to enable.

2. Initiate VigorACS

After installing VigorACS, it 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.

Please open **Start >Setup >Control Panel >Administrative Tools >Service** to check if the VigorACS Service has been initiated or not. If not, please double click it to enable.



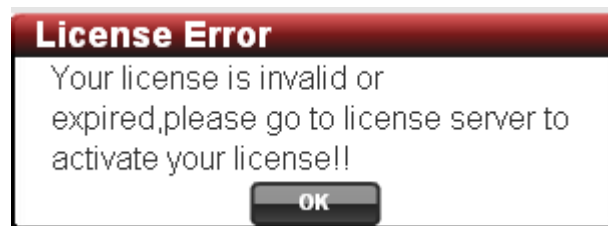
3. Register VigorACS

1. Click **Programs> VigorACS SI> VigorACS Web Page** to access into VigorACS. The login page of VigorACS will be shown as the following:

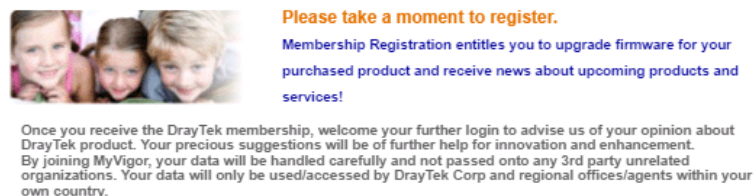


The image shows the VigorACS login interface. At the top, there is a red banner with the 'DrayTek' logo on the left and 'VigorACS' on the right. Below the banner, the word 'Login' is displayed in a black box. The login form contains three input fields: 'User Name' with the text 'root', 'Password' with masked characters '*****', and 'Validated Code' with a blue box containing '7xxS' and a red box containing '7 x x S'. Below these fields are two buttons: 'EN' with a dropdown arrow and a 'Login' button.

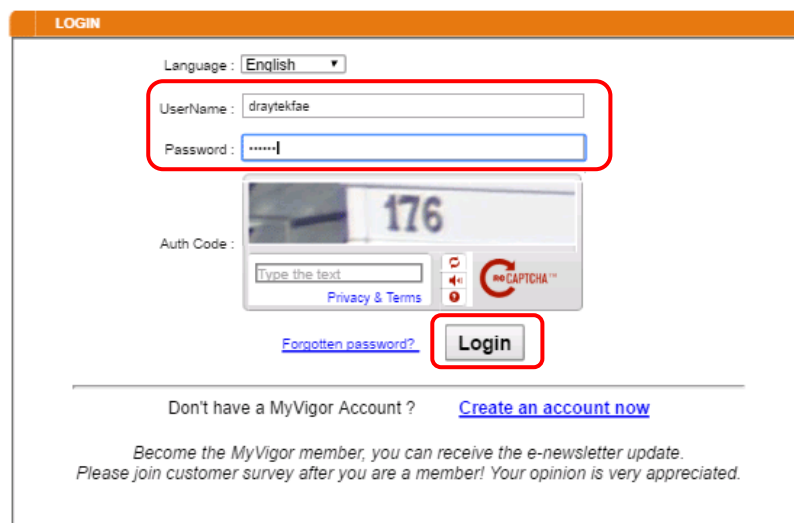
2. Please type “root” as user name and “admin123” as password. Then click **Login**. A License Error dialog appears as follows:



3. Click **OK**. A login page for MyVigor web site will pop up automatically.



The image shows a banner for MyVigor registration. On the left is a photo of three children. To the right, the text reads: 'Please take a moment to register. Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!'. Below this, a paragraph states: 'Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.'



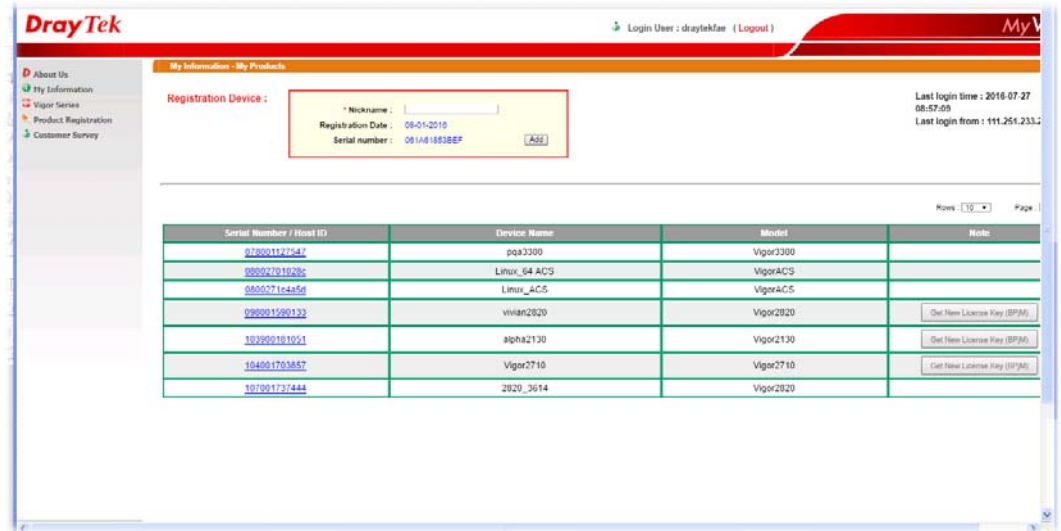
The image shows the MyVigor login page. At the top is an orange bar with the word 'LOGIN'. Below it, there is a 'Language' dropdown menu set to 'English'. The 'UserName' field contains 'draytekfae' and the 'Password' field contains masked characters '*****'. Below these fields is a 'Auth Code' section with a CAPTCHA image showing the number '176' and a text input field. To the right of the CAPTCHA is a 'reCAPTCHA' logo. Below the CAPTCHA is a 'Privacy & Terms' link. At the bottom of the login section is a 'Forgotten password?' link and a 'Login' button. Below the login section is a link 'Create an account now' and a paragraph: 'Become the MyVigor member, you can receive the e-newsletter update. Please join customer survey after you are a member! Your opinion is very appreciated.'

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 567 2727 or
email to : webmaster@draytek.com

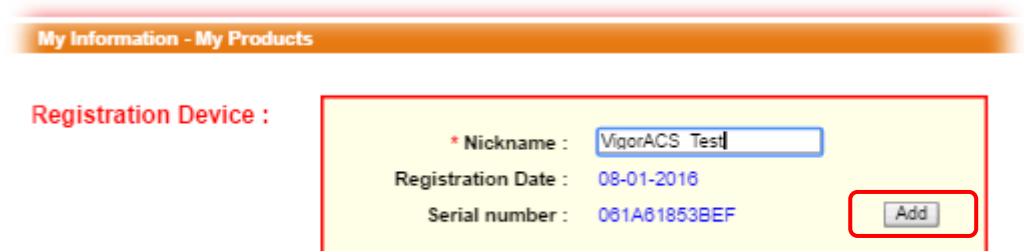
4. Type your account (user name) and password in this page. Enter the authentication code with the characters displayed on the screen. Then, click **Login**.

Note: 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. Refer to Appendix C Creating an Account for MyVigor.

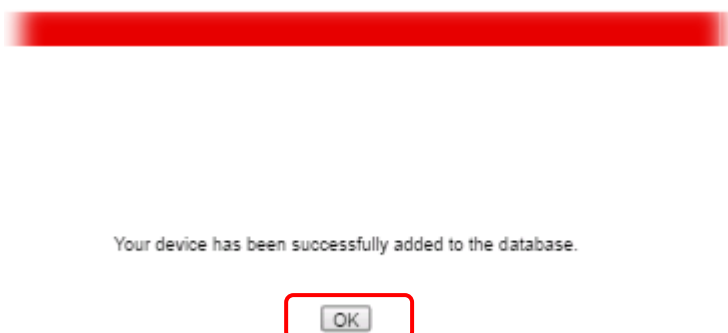
5. MyVigor will verify and authenticate if the user account you typed is allowed to access into the web site. If yes, the following screen will appear.



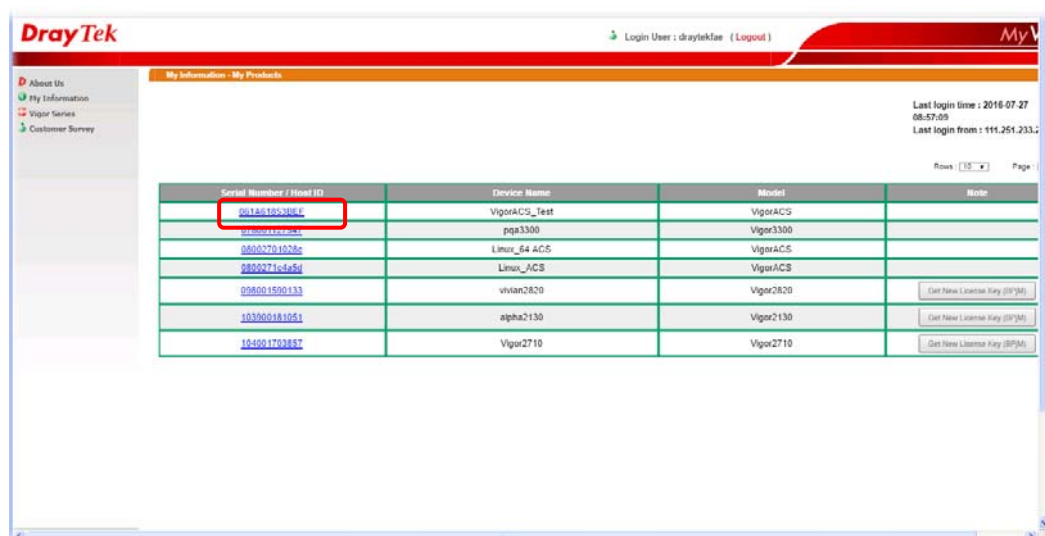
6. Type a nickname for VigorACS SI and click **Add**.



7. Type a name for identification in the field of **Nickname** and click **Submit**. You can see the following screen. Click **OK**.

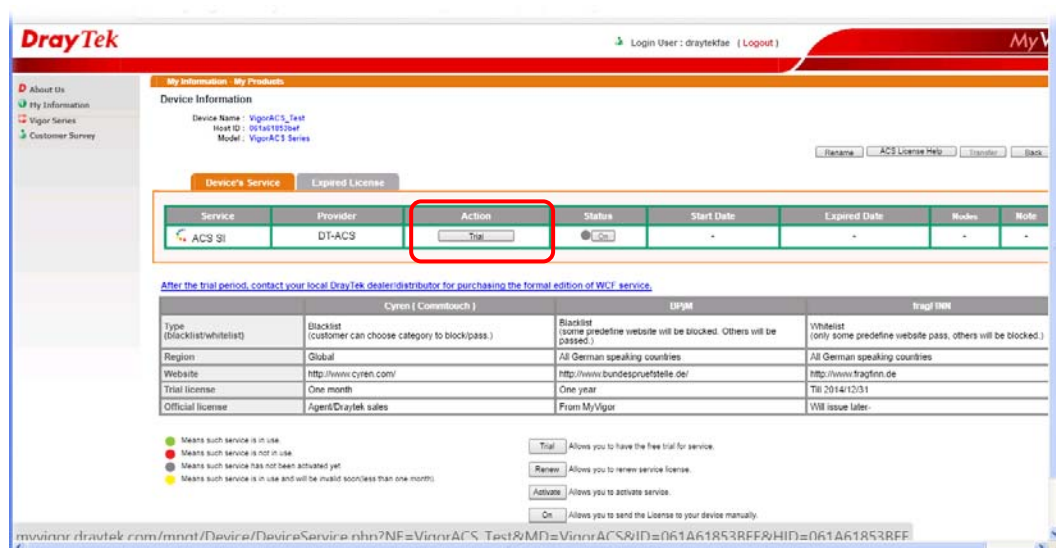


8. In this page, click the serial number link (in this case, it is 061A61853BEF).



Serial Number / Host ID	Device Name	Model	Mode
061A61853BEF	VigorACS_Test	VigorACS	
0180021412945	pqa3300	Vigor3300	
000027016286	Linux_64_ACS	VigorACS	
0000271cd454	Linux_ACS	VigorACS	
090001590133	vivian2820	Vigor2820	Get New License Key (PDF)
103000181051	alpha2130	Vigor2130	Get New License Key (PDF)
104001702657	Vigor2710	Vigor2710	Get New License Key (PDF)

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



Device Information

Device Name : VigorACS_Test
Host ID : 061A61853BEF
Model : VigorACS Series

Device's Service | Expired License

Service	Provider	Action	Status	Start Date	Expired Date	Notes	Note
ACS SI	DT-ACS	Trial	On	-	-	-	-

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

	Cyren Comintouch	USPM	fragl INN
Type (Blacklist/whitelist)	Blacklist (customer can choose category to block/pass.)	Blacklist (some predefined website will be blocked. Others will be passed.)	Whitelist (only some predefined website pass, others will be blocked.)
Region	Global	All German speaking countries	All German speaking countries
Website	http://www.cyren.com/	http://www.bundespruefstelle.de/	http://www.fraglinn.de
Trial license	One month	One year	Till 2014/12/31
Official license	Agent/DrayTek sales	From MyVigor	Will issue later.

● Means such service is in use.
● Means such service is not in use.
● Means such service has not been activated yet.
● Means such service is in use and will be invalid soon/less than one month.

[Trial](#) Allows you to have the free trial for service.
[Renew](#) Allows you to renew service license.
[Activate](#) Allows you to activate service.
[On](#) Allows you to send the License to your device manually.

myvigor.draytek.com/mvnt/Device/DeviceService.nhn?NF=VigorACS_Test&MD=VigorACS&ID=061A61853BEF&HID=061A61853BEF

10. Form the following screen, check the box of “**I have read and accept the above....**” and click **Next**.

Confirm Message

User Name : draytekfae
Host ID : 061a61853bef
Model : VigorACS

DrayTek VigorACS SI Series End-User License Agreement

IMPORTANT:

DrayTek IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN DrayTek IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

BY JOINING MYVIGOR, YOUR DATA WILL BE HANDLED CAREFULLY AND NOT PASSED ONTO ANY 3RD PARTY UNRELATED ORGANIZATIONS. YOUR DATA WILL ONLY BE USED/ACCESSED BY DRAYTEK CORP AND REGIONAL OFFICES/AGENTS WITHIN YOUR OWN COUNTRY.

1. Grant of License for Personal Use
DrayTek grants you a non-exclusive, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by DrayTek to you are reserved by DrayTek, and all implied licenses are disclaimed.

2. Ownership
You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and

☒ I have read and accept the above Agreement. (Please check this box).

Next

11. In the page below, click **Register**.

Apply For A License Number

Service Name : ACS SI

STEP 2

Activation Date (MM-DD-YYYY) : 08-01-2016

Register

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

VigorACS License Information

Operation	1000 : License Key OK
License id	00017ed6
Start date	2016-08-01
Expire date	2016-08-31
Max node	00000020
Trial license	Yes

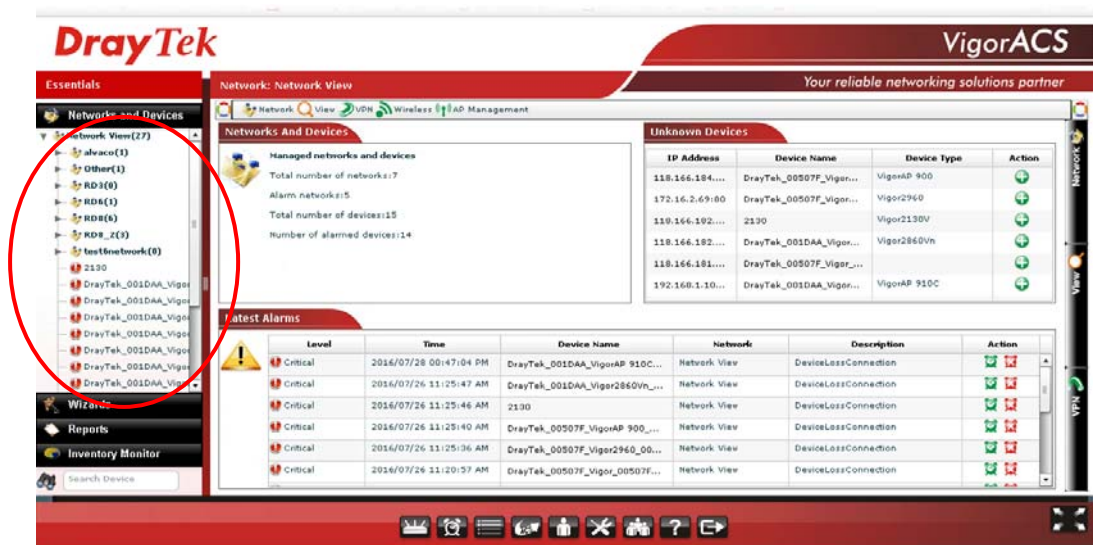
Login to ACS

13. The login page will appear as follows.



The login page features the DrayTek logo and the VigorACS title. It includes a 'Login' section with three input fields: 'User Name' (containing 'root'), 'Password' (containing '*****'), and 'Validated Code' (containing '7xXS'). A dropdown menu is set to 'EN'. A 'Login' button is located at the bottom right. A small box to the right of the 'Validated Code' field displays '7 x x S'.

14. Type the default settings of User Name (root) and Password (admin123) and type the validated code. Then, click **Login**. The main screen of VigorACS will be shown as follows.



The main screen displays the VigorACS interface with a sidebar on the left containing 'Essentials', 'Networks and Devices', 'Wizards', 'Reports', and 'Inventory Monitor'. The 'Networks and Devices' section is highlighted with a red circle. The main area shows 'Network: Network View' with a tree of managed networks and devices. A table titled 'Unknown Devices' lists IP addresses, device names, and types. A 'Latest Alarms' table at the bottom shows critical alerts for device loss of connection.

IP Address	Device Name	Device Type	Action
118.166.184....	DrayTek_00507F_Vigor...	VigorAP 900	[Icon]
172.16.2.69:80	DrayTek_00507F_Vigor...	Vigor2960	[Icon]
119.166.192....	2130	Vigor2130V	[Icon]
118.166.192....	DrayTek_001DAA_Vigor...	Vigor2860Vn	[Icon]
118.166.181....	DrayTek_00507F_Vigor...		[Icon]
192.168.1.10...	DrayTek_001DAA_Vigor...	VigorAP 910C	[Icon]

Level	Time	Device Name	Network	Description	Action
Critical	2016/07/26 00:47:04 PM	DrayTek_001DAA_VigorAP 910C...	Network View	DeviceLossConnection	[Icon]
Critical	2016/07/26 11:25:47 AM	DrayTek_001DAA_Vigor2860Vn...	Network View	DeviceLossConnection	[Icon]
Critical	2016/07/26 11:25:46 AM	2130	Network View	DeviceLossConnection	[Icon]
Critical	2016/07/26 11:25:40 AM	DrayTek_00507F_VigorAP 900...	Network View	DeviceLossConnection	[Icon]
Critical	2016/07/26 11:25:36 AM	DrayTek_00507F_Vigor2960_00...	Network View	DeviceLossConnection	[Icon]
Critical	2016/07/26 11:20:57 AM	DrayTek_00507F_Vigor_00507F...	Network View	DeviceLossConnection	[Icon]

Above shows the view of CPEs added to the database and controlled by VigorACS.

2.3.2 For Linux / Solaris

Start/Shutdown MySQL Database

Execute `"/usr/local/vigoracs/VigorACS/bin/vigoracs.sh"` instruction. The following menu will appear.

1. start mysql
2. shutdown mysql
3. start VigorACS
4. shutdown VigorACS
5. edit bind ip of VigorACS Server(please keying IP or server name)
6. set the MAX and MIN memory value of running java (It will valid after restarting VigorACS)
7. view the MAX and MIN memory value of running java
8. exit

input select num:

```
Start to create snmpdb db ....
VigorACS MySQL:
MySQL:
Create snmpdb db successfully....
Create snmpdb db table....
Create snmpdb table successfully....
VigorACS and snmpdb install Successfully

1. Install mysql
2. Install java
3. Install VigorACS < It will build one mysql database : snmpdb >
4. Upgrade VigorACS < It will upgrade snmpdb database >
5. Exit
input select num :
5
[root@localhost 0.0.1.3.11# /usr/local/vigoracs/VigorACS/bin/vigoracs.sh
1. start mysql
2. shutdown mysql
3. start VigorACS
4. shutdown VigorACS
5. edit bind ip of VigorACS Server(please keyin ip or servername)
6. set the MAX and MIN memory vaule of running java <It will valid after restarting VigorACS >
7. view the MAX and MIN memory vaule of running java
8. exit
input select num :
```

Type item number **1** to start MySQL database if necessary. Usually MySQL daemon will start automatically after installing VigorACS server.

Note: You can type `"ps -ef|grep mysql"` to view the content of MySQL. If you want to shutdown MySQL database, simply type the menu item 2 to close MySQL.

Start/Shutdown VigorACS

For the first time of starting the VigorACS on Linux system, the startup program will need you to input Server IP. Select item number **3** for starting VigorACS. And type the required IP address used for initiating.

```

# http://developer.java.sun.com/developer/bugParade/bugs/4465334.html
done
fi

"vigoracsserver.sh"
[root@localhost bin]# ls
changeip.bat      jboss_init_redhat.sh  probe.sh      set_memory.sh      StartVigorACS.bat  vigoracs.sh
changeip.bat.bak  jboss_init_suse.sh   run.bat       shutdown.bat       twiddle.bat        VigorACS.url
classpath.sh      memory.txt            run.conf      shutdown.jar        twiddle.jar        wstools.bat
hs_err_pid508.log  noip.bat             run.jar       shutdown.sh         twiddle.sh         wstools.sh
jboss_init_hpux.sh  probe.bat            run.sh        ShutdownVigorACS.bat  vigoracsserver.sh
[root@localhost bin]# chmod 755 vigoracs.sh
[root@localhost bin]# chmod 755 vigoracsserver.sh
[root@localhost bin]# ./vigoracs.sh
1. start mysql
2. shutdown mysql
3. start VigorACS
4. shutdown VigorACS
5. edit bind ip of VigorACS Server(please keyin ip or servername)
6. set the MAX and MIN memory vaule of running java (It will valid after restarting VigorACS )
7. view the MAX and MIN memory vaule of running java
8. exit
input select num :
3
Which ip address do you want to bind for VigorACS service ( x.x.x.x or Enter for bind localhost.localdomain server)?
172.17.3.132

```

The system will start VigorACS with the specified IP address.

Edit VigorACS IP

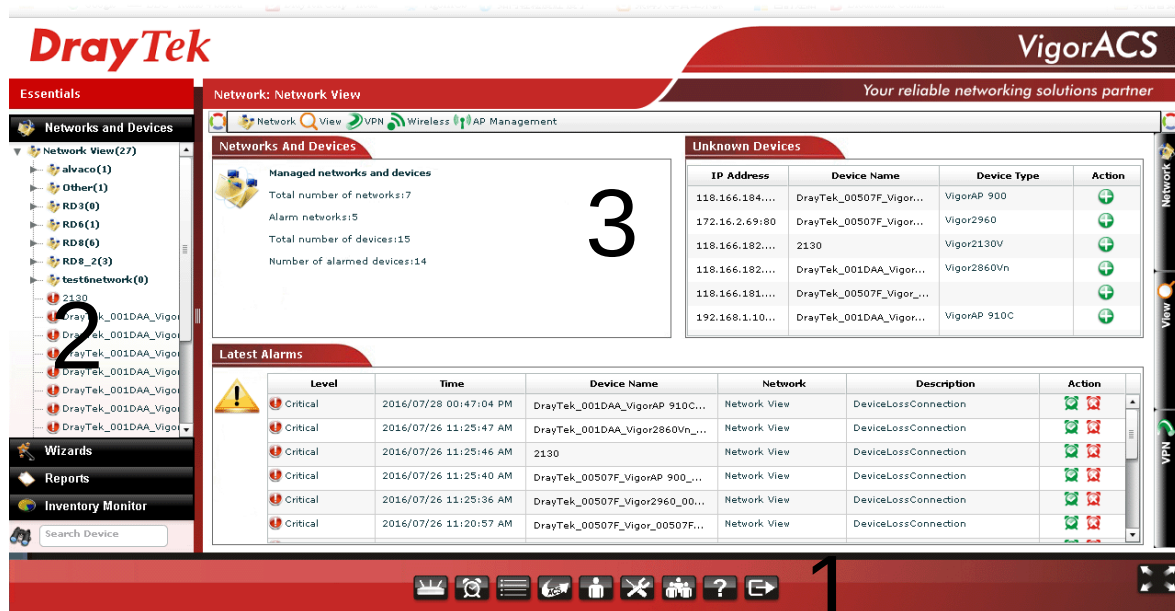
Once you input the IP address, VigorACS will keep it on *startway.txt*. However, if you want to change the server bind IP for some reason, please follow the steps below:

1. Execute `"/usr/local/vigoracs/VigorACS/bin/vigoracs.sh"` instruction.
2. Stop VigorACS by selecting item number 2 to shutdown VigorACS. Such action can make sure the new changed IP setting being effective.
3. Then select item number 5 to edit *startway.txt* by using *vi* editor.
4. When you finished the change of bind IP, please select item number 3 to start VigorACS again.

Chapter 3 Getting Start

3.1 Brief Introduction of Main Screen

The main screen of VigorACS SI is shown as below and it can be divided into several parts:



Part 1

Such area displays different **operation modes**. Each mode will bring out different parameters for configuration or different information for reviewing. Simply move your mouse on each one of them to open the corresponding web page.



Device Management



Alarm



Log



Provision



Admin



System



User



Help



Logout

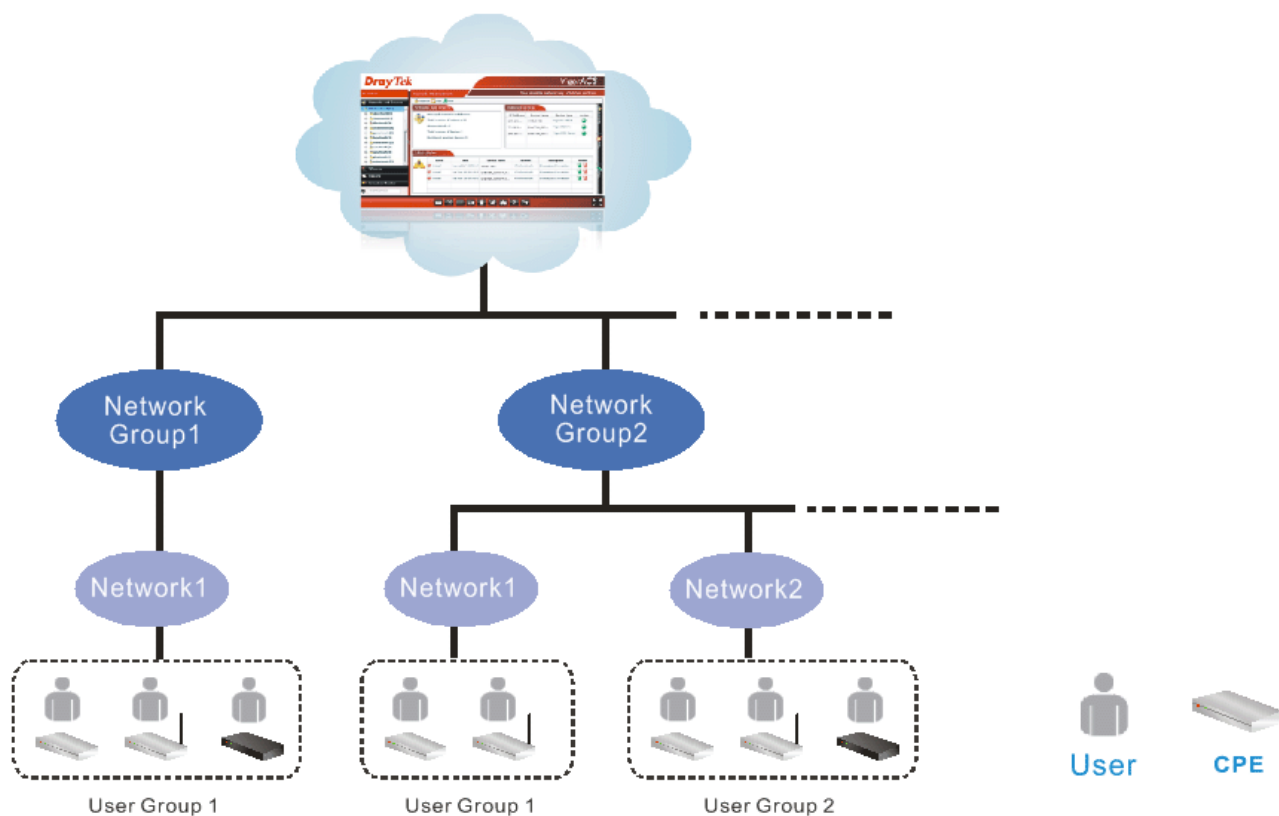
Part 2	Such area displays device(s) managed by VigorACS SI. All of the devices will be queued automatically. More Devices – If the number of CPE managed by VigorACS SI is over 100, such icon will appear. By clicking it, the next 100 CPEs will be shown in queue.
Part 3	Such area displays information about the number of networks and devices, unknown devices and latest alarms.  In addition, the menu bar provides menu items which are classified into Network, View, VPN, Wireless and AP Management. Network – Display the devices managed by VigorACS in icons, with pie chart, with map and text. View – Click Refresh to renew current page. However, if you click Sub Devices Recursively, VigorACS will display the devices with the ones grouped under the devices. VPN - VigorACS can manage Vigor router easily. In the home page of VigorACS, VPN wizard is offered in default which allows the system administrator to build VPN among different Vigor devices. Wireless – In the home page of VigorACS, wireless WDS wizard is offered in default to assist the system administrator to make WDS connection if required. AP Management – VigorACS can manage VigorAP devices via Internet. Therefore, the function of AP Status can open a web page with brief status information for all of VigorAP devices.

3.2 Operation Procedure

Follow the instruction listed below to operate VigorACS:

- Create networks and add devices (CPE).
For more details, go to **Chapter 4 Admin Operation**.
- Create users,
For more details, go to **Chapter 5 User Operation**.
Each CPE device can be assigned to one user group only.
- Create user groups,
For more details, go to **Chapter 5 User Operation**.
Assign users under different user groups.
RootGroup is the group defined in factory.
- Edit and modify the settings for the TR-069 devices, refer to **Chapter 6 Device Management**.

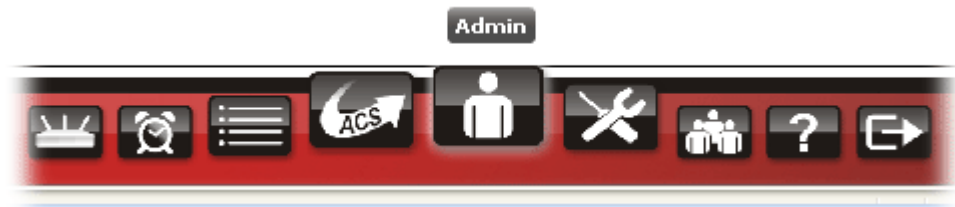
Below shows a brief illustration to describe the relationships among CPE, user group, network and network group.



3.3 Creating a New Network and Device

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

1. Click the **Admin** tab to access into administration operation mode.



2. Click the **Device Management** button.



3. Click **Network View** under **Networks And Devices** field to make the **Add** button being available on the right side.



4. Click  to open the following screen to add a new network.

A dialog box titled "Add Network" with a red header bar. It contains the following fields:

- Parent Network: Main network
- Name: Marketing
- Location: HsinChu
- User Name: market
- Password: market

At the bottom, there are "OK" and "Cancel" buttons. The "Password" field is highlighted with a blue border.

5. Fill in the name, location, user name and password. Click **OK** to save the settings and exit the dialog. The new network has been created and displayed under **Networks And Devices**.



3.4 Creating a User and User Group

Follow the steps below to create a user.

1. Click the **User** tab to access into administration operation mode.

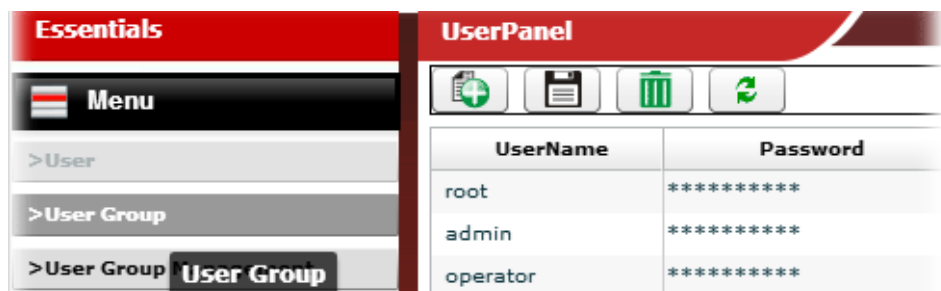


2. To insert a user, simply click .
3. A new line with input boxes will appear for the user to type personal information for being identified by VigorACS.

CustomCut	ADt6VJJcmF4970KEtEMuP	thomas@custom-cut.co.za	+27766321930
itbi	btUtIdXMFedumHlnX0vQ3		
BrotherTW	4c7XBYY7QkVhf3dtM4Csc	emma@brother.com.tw	(02)27582171

Follow the steps below to create a user group.

1. Click **User Group** item under **Menu**.



2. To insert a user group, simply click .
3. A new line with an input box will appear for the user to type personal information for identified by VigorACS.

#	Group_V	☐	☐	-
5	Group_V	☒	☒	-1
6	Group_Test	☒	☒	-1
7	carrie	☒	☐	-1
8	Tim_Group	☒	☒	-1
0		☒	☒	-1

3.5 Logout VigorACS

Simply click **Logout** icon to logout.



Part II Web Configuration

This page is left blank.

Chapter 4 Admin Operation

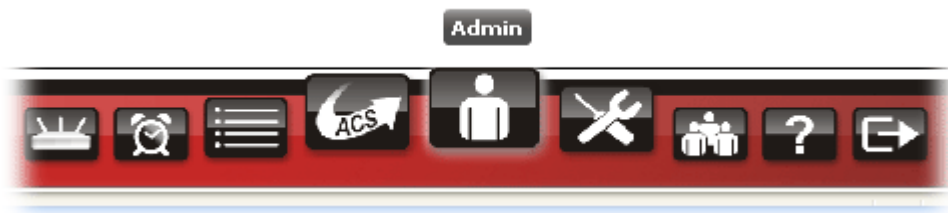
Admin page allows you to modify the information for Networks and Devices.

For network, 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.

For device, it can

- 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.

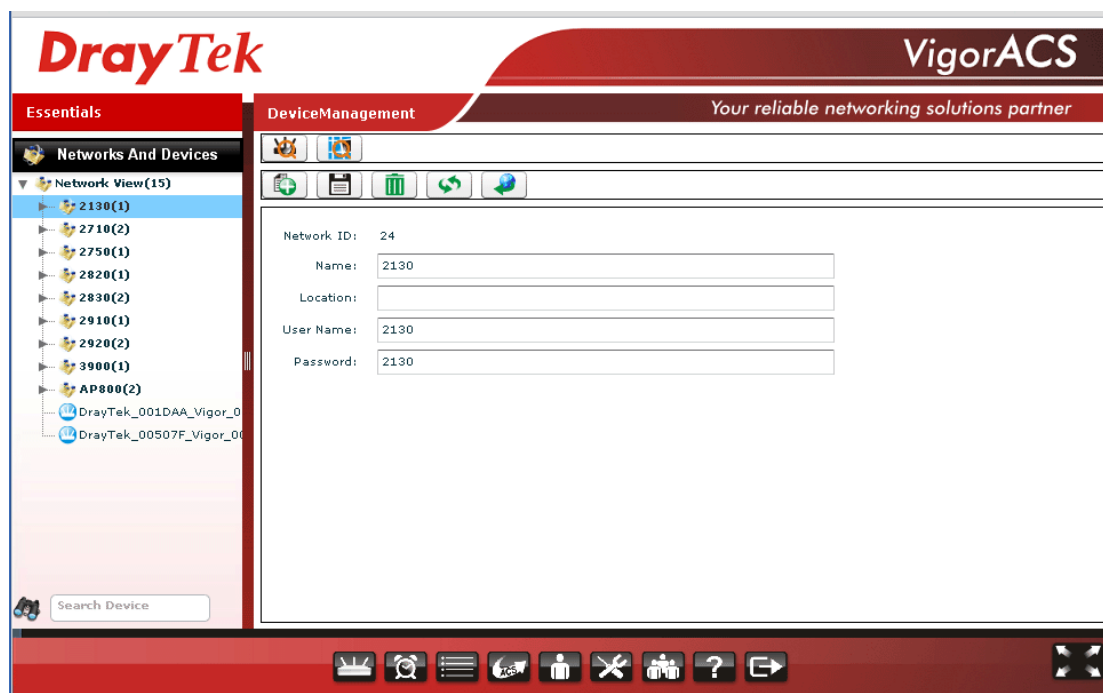


It can be divided into two parts, Device Management and Topology Management.

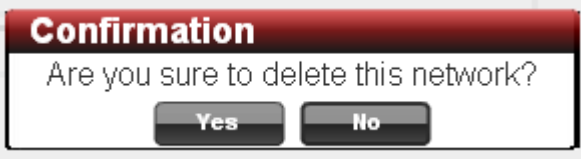


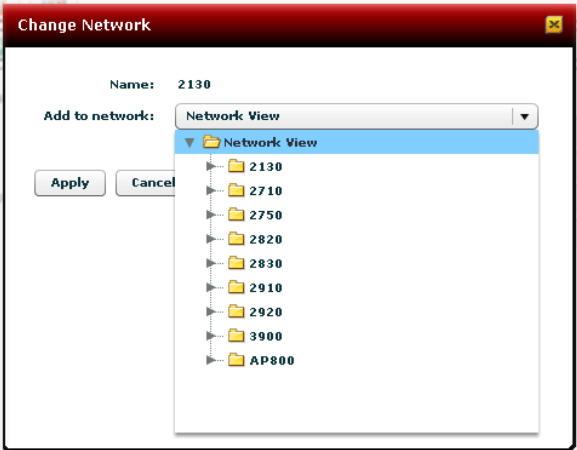
4.1 Device Management

To edit, change or delete devices under different network or add, change or delete a network, please click  **Device Management** for advanced operation. Then, choose any one of the CPE displayed on **Networks And Devices** tree view to make the options for **Device Management** being available.



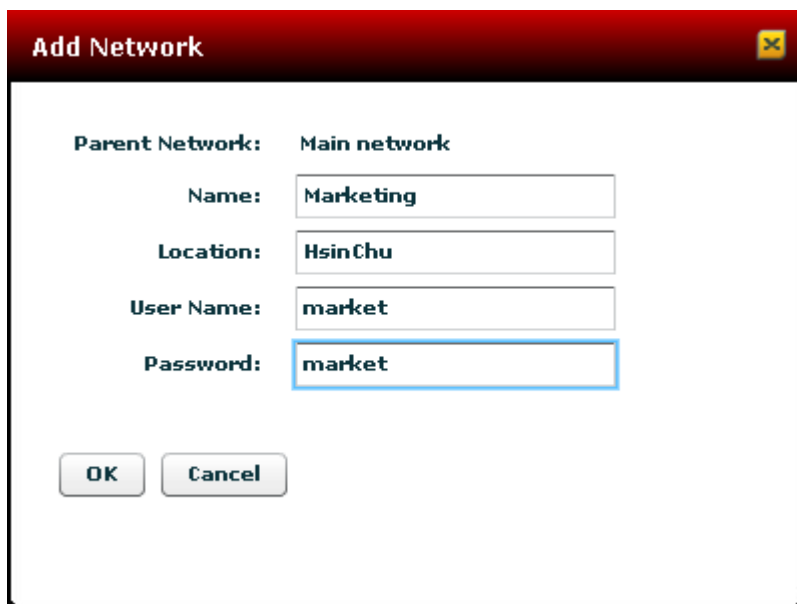
Available settings for such feature will be shown as follows:

Items	Description
 Add New Network	Click this button to add a new network.
 Save Network	Click this button to save the change.
 Remove Network	Click this button to delete selected network. 
 Refresh Record	Click this button to refresh current page.
 Change Network	After clicking this button, a dialog box will appear for you to specify the selected CPE to be placed in another network.

Items	Description
	
Name	You can modify the name of the parent network.
Location	Type the address 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.

4.2 Creating a New Network to Manage Devices (CPEs)

VigorACS allows the administrator to build several networks (and sub-network) for different CPE devices under the *root level*, Main network. Click  to open the following screen to add a new network.

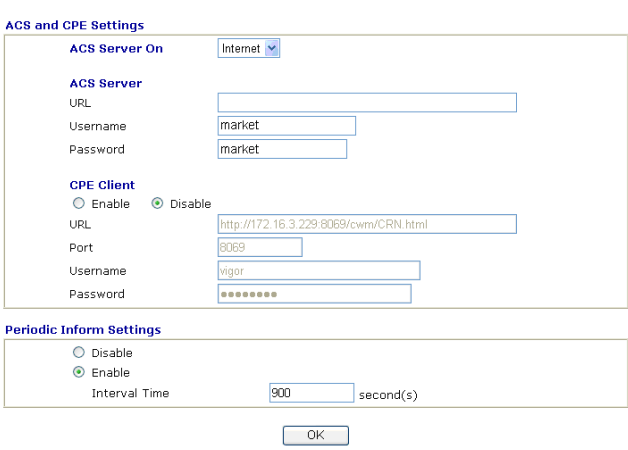


The 'Add Network' dialog box has a red title bar with a close button. It contains the following fields:

- Parent Network:** Main network
- Name:** Marketing
- Location:** HsinChu
- User Name:** market
- Password:** market

At the bottom are 'OK' and 'Cancel' buttons.

Available settings for such feature will be shown as follows:

Items	Description
Name	Type name for the new network.
Location	Type a brief description 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. If you are going to group several CPE devices under such network, please open System Maintenance>>TR-069 in the web configuration page of CPE. Next, type the same user name and password (in this case, both are <i>market</i>) in the corresponding fields. System Maintenance >> TR-069 Setting  The screenshot shows the 'ACS and CPE Settings' page. It includes sections for 'ACS Server On' (set to Internet), 'ACS Server' (with fields for URL, Username: market, Password: market), 'CPE Client' (with 'Enable' selected and fields for URL, Port: 8069, Username: vigor, Password: masked), and 'Periodic Inform Settings' (with 'Enable' selected and Interval Time: 900 seconds). An 'OK' button is at the bottom.



Deleting a Network

To delete a network, click to select the network link displayed under **Network View** and click



Remove Network

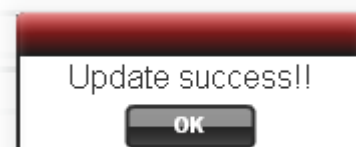
VigorACS will ask you to confirm such action. You can click **OK** to execute the action, otherwise, click **No** to cancel this action.

If there is still one device grouped under a sub-network, such network cannot be deleted by this function unless that device is removed.

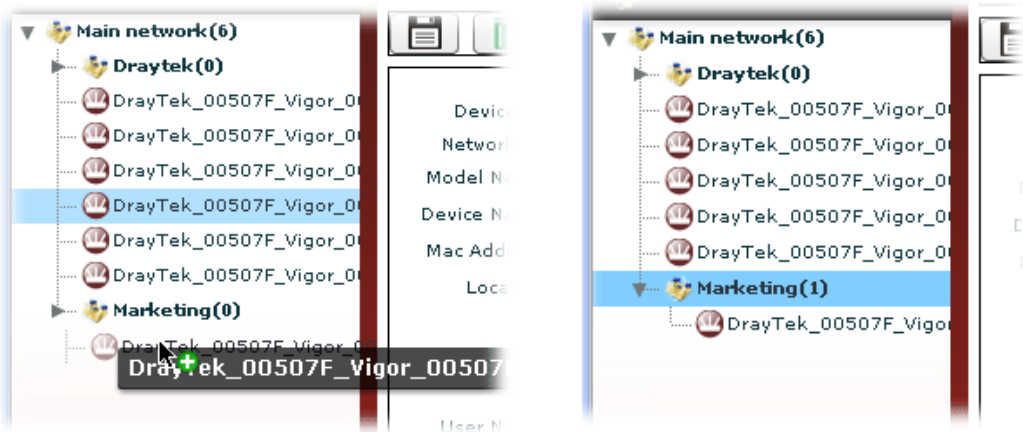
4.3 Changing the Network for Devices (CPEs)

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

To change the network, simply click that network and drag it to the directory you want. VigorACS will ask you to confirm such action. You can click **Yes** to execute the action (Update success), otherwise, click **No** to cancel this action.



For example, you want to move **DrayTek_00507_Vigor_XXXXX** onto **Marketing**. You can drag and hold it to that group directly. When the mouse cursor changes into “+”, please release your mouse cursor. VigorACS will ask you to confirm such action. If you click **Yes**, it will be moved to the new location.

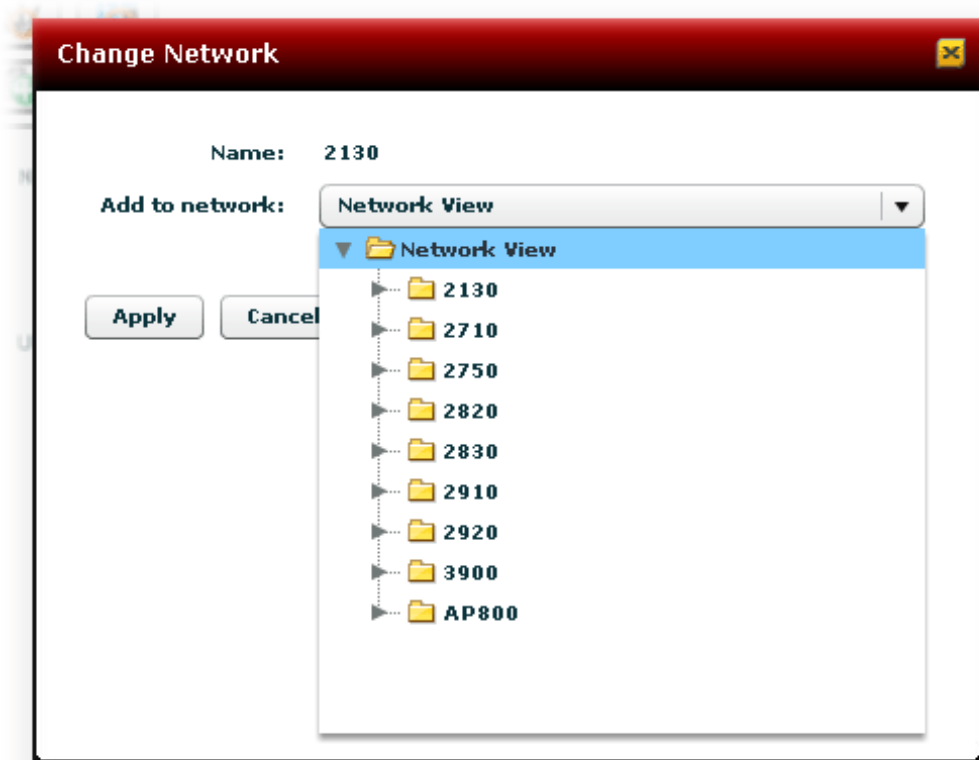


Or,

Open the tree view of **Networks And Devices** and select the CPE you want. Click the button of



Change Network to specify which network will have such selected CPE.



Click **Apply** after you make your choice. Later, a dialog will appear to inform you the CPE changing has been done.



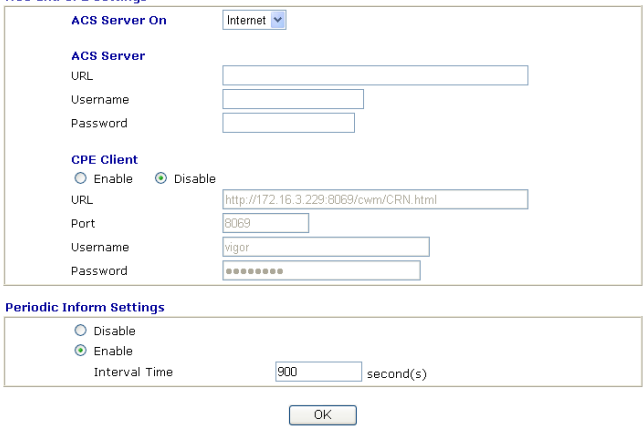
4.4 Modifying General Information of Selected CPE

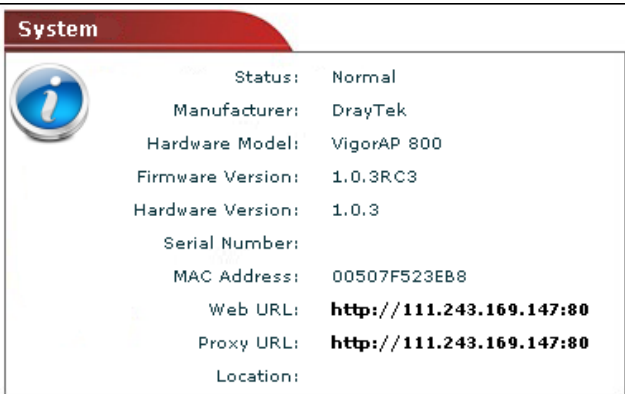
Administrator can modify certain settings (e.g., device name, address for the selected device, and etc.) for the **selected CPE** (device) respectively. Note that different CPE will bring about different configuration pages.



Available settings for such feature will be shown as follows:

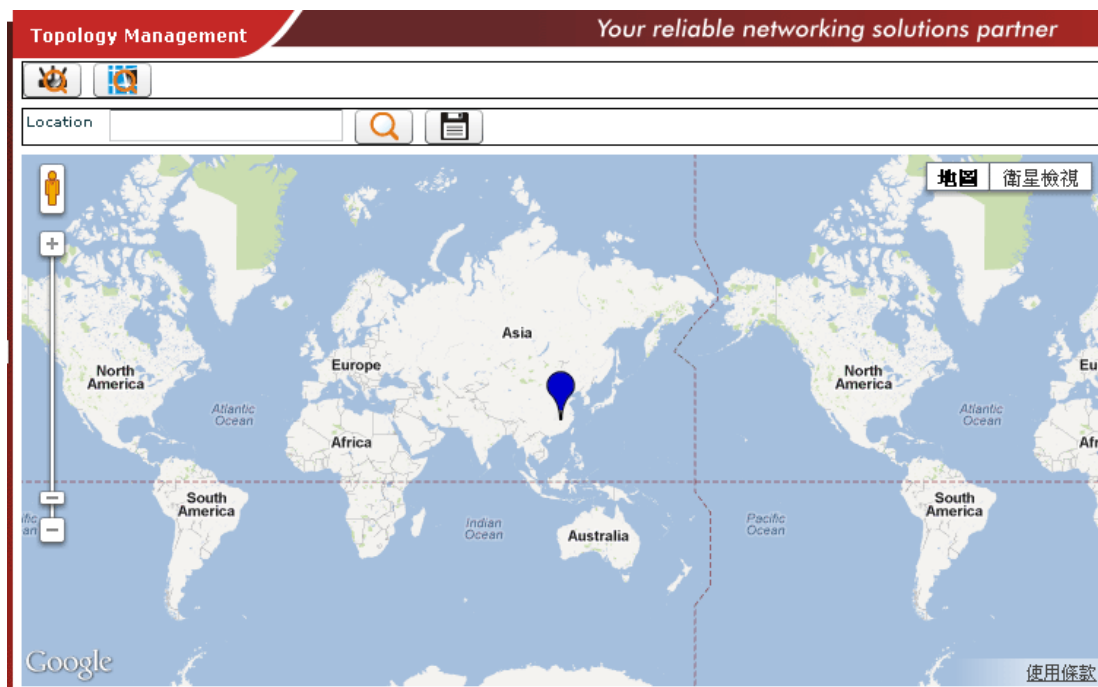
Items	Description
 Save Device	Click this button to save the change.
 Remove Device	Click this button to delete selected device. Confirmation Are you sure to delete this device? Yes No
 Refresh Record	Click this button to refresh current page.
 Change Network	Click this button to change the device into other network. Change Network Device name: DrayTek_00507F_Vigor_00507FA77E80 Add to network: Wholenetwork Apply Cancel - Wholenetwork - uknetwork - itnetwork - tknetwork - usnetwork - gmnetwork - bmnetwork - mxnetwork - arnetwork - gmnetwork - plnetwork - mbnetwork

	Choose the network that you want from the drop down list of Add to network . Then, click Apply . The device will be grouped under the network you specified.
Device ID	Display the identification number for the device.
Network ID	Display the sequence number for the device under such network.
Model Name	Display the model name of the device.
Device Name	Display the name that you specify for such device. If required, you can change the name.
Serial number	Define a serial number of the selected device for identification.
MAC Address	Display the MAC address for the device.
Location	Type the address for the selected device. It will be helpful to be searched while using Topology Management.
Emergency phone number	Type an emergency phone number for contact if required.
IP	Display the WAN IP address of the selected device.
Port	Display the port number of the selected device.
URI	Display the URI for the selected device.
User Name	Such name is set in default for the CPE. Do not change it. You also can find such information from System Maintenance>>TR-069 in the web configuration page of CPE.
Password	Such password is set in default for the CPE. Do not change it. You also can find such information from System Maintenance>>TR-069 in the web configuration page of CPE. System Maintenance >> TR-069 Setting 
Management Protocol	The administrator can specify which protocol (http or https) will be used for accessing into the web page of the CPE controlled by VigorACS. Refer to the following figure.

	 “http” displayed on Web URL and Proxy URL is the management protocol typed in this field.
Management Port	Type the port number according to the port number set by the selected CPE. Refer to the following figure.  “80” displayed on Web URL and Proxy URL is the management port chosen in this field.
Status	Choose Enable to show the status of the selected device; choose Disable to hide the status of the selected device.
Device Type	In general, VigorACS can manage and control the CPEs which follow TR-069 standard. Do not change it.
Known Device	This setting can let the selected CPE not displayed on the Unknown Devices from the Home page of VigorACS SI.

4.5 Topology Management

To display the **location** of the selected CPE with a bird's eye view, choose the CPE first from the tree view of **Networks And Devices** and click  **Topology Management** for advanced operation.



Available settings for such feature will be shown as follows:

Items	Description
	You can type the address (description) manually and click Zoom icon to search the device in the map.
 Search	Click this button to search CPE.
 Save	Click this button to save the change.

Chapter 5 User Operation

Users who want to control CPE through VigorACS server can access VigorACS with private name and password. The user management function allows a user to set name, password, and e-mail address as identification in VigorACS system.

Each time, when the user wants to access into VigorACS, he/she can type the name and password that configured in this page. Other people also can set different name and password for accessing VigorACS. However, the password will be displayed with codes for prevent peeping by other users. Therefore, you have to remember your password.

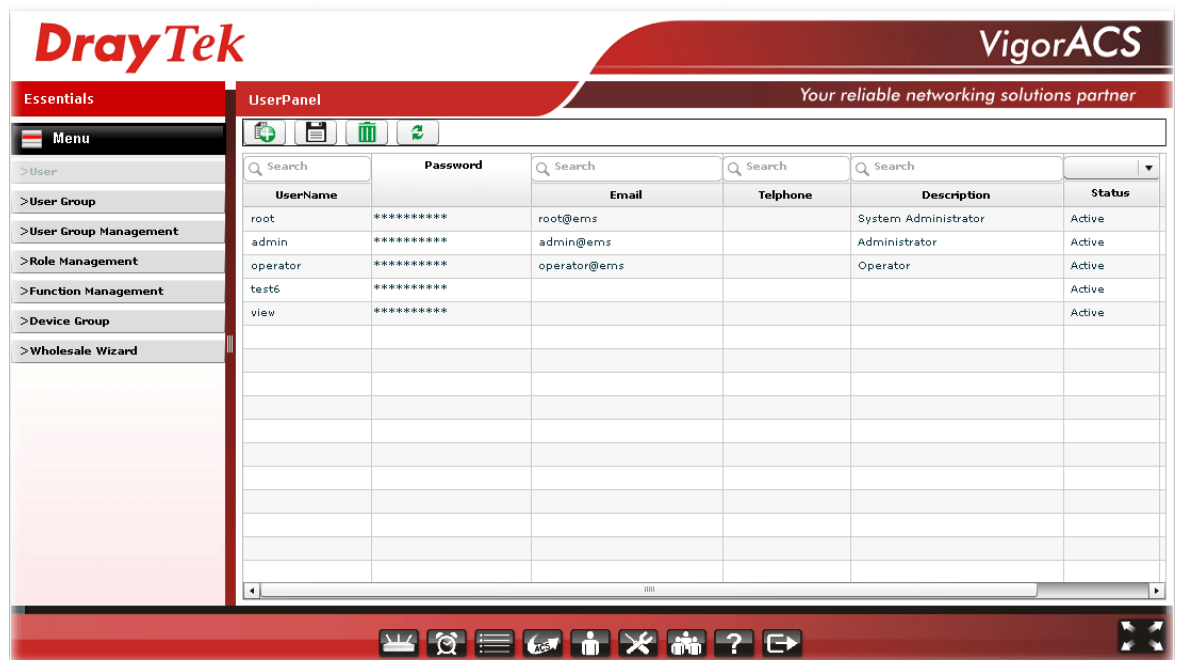


You have to:

- Define User (refer to 5.1)
- Define User Group (refer to 5.2)
- Assign User (s) to certain User Group (refer to 5.3)
- Use Role Management to specify certain authority to User Group(s) for displaying different functions (refer to 5.4)

5.1 User

To add/edit/delete a user, choose **User** item from **Menu**. The following web page will be shown on the screen.

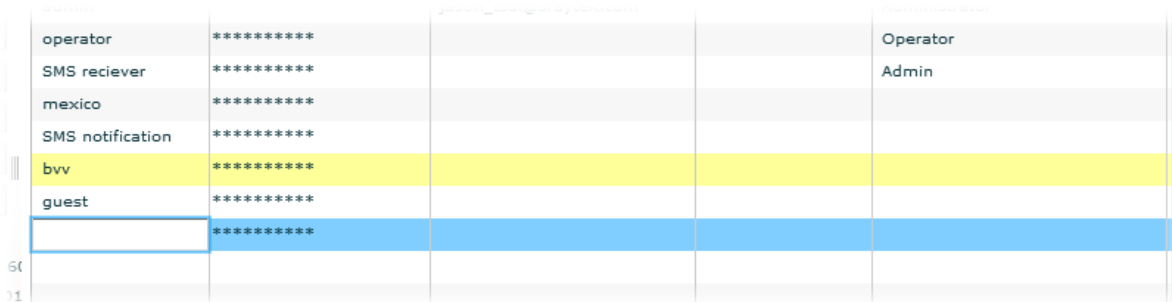


Available settings for such feature will be shown as follows:

Items	Description
 Add user	Click this button to add a new record.
 Save user setting	Click this button to save the record.
 Delete user	Click this button to delete the selected record.
 Refresh	Click this button to refresh current page.
UserName	Display the name that users created.
Password	Display the password that users typed. It will be displayed with random codes. If you forget the password, simply click the item and click Update for changing the password manually.
Email	Display email address for certain user for receiving the mail notification.
Telephone	Display the telephone number for certain user for receiving the SMS notification.
Description	Display the authority of the user. There are three levels – administrator, operator, and system administrator.
Status	Display current status of the user. “Active” means the user is on the network.
MailNotify	When this function is enabled, an e-mail will be sent to the one listed here as a notification when the device gets alarms.
SMS Notify	When this function is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms.

5.1.1 Add a User

To insert a user, simply click  (under Menu>>User). A new line with input boxes will appear for the user to type personal information for being identified by VigorACS.



operator	*****		Operator
SMS reciever	*****		Admin
mexico	*****		
SMS notification	*****		
bvv	*****		
guest	*****		

Available settings for such feature will be shown as follows:

Items	Description
User Name	Type a name for the new added user.
Password	Type the password for the user.
Email	Type the e-mail for communication between the user and VigorACS server.

Items	Description
Telephone	Type the telephone number for receiving the SMS notification.
Description	Type a brief description for the user.
Status	Choose Active to let the user can access into VigorACS at any time. Choose Inactive to prevent the user accessing into VigorACS.
MailNotify	Check the box to enable the function. When it is enabled, an e-mail will be sent to the user as a notification when the connected device gets alarms.
SMS Notify	Check the box to enable the function. When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms.

5.1.2 Edit a User

To edit a user (if it is useless or unsatisfied) setting, please select the one that you want to edit and modify each box directly.

5.1.3 Delete a User

To delete a user (if it is useless or unsatisfied) setting, please select the one that you want to delete and click .

5.2 User Group

This page allows you to add a new user group with common authority which will be shared by the users under the same group. **RootGroup** is defined in factory and owns the highest authority. You can define new user group(s) to fit your requirement.

The screenshot displays the VigorACS User Group Management interface. On the left is a navigation menu with options like User, User Group, User Group Management, Role Management, Function Management, Device Group, and Wholesale Wizard. The main area shows a table of user groups. A tooltip is visible over the 'Delete user group with wholesale' button in the table.

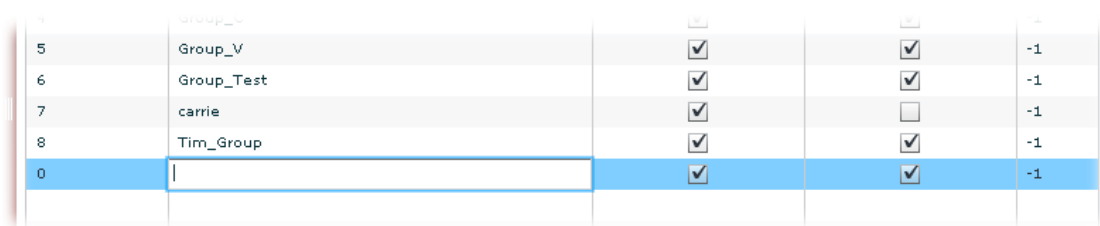
GroupID	GroupName	GlobalSNMPServer	Nodes	EnableExpireDate	ExpireDate	UsedNodes
1	RootGroup	☒	-1	☐		108
2	北信Group	☒	-1	☐		0
3	MexicoGroup	☐	-1	☐		0
4	test4Group	☒	-1	☐		0
5	jasonGroup	☒	-1	☐		17
6	123	☒	-1	☐		0
7	Simet	☒	-1	☐		0
8	DrayTekFAE	☒	-1	☐		6
9	AGNSolutions	☒	-1	☐		5

Available settings for such feature will be shown as follows:

Items	Description
Add user group	Click this button to add a new group.
Save user group setting	Click this button to save the record. When you add, edit or delete a user group, click this button to save the changes.
Delete user group	Click this button to delete the selected group.
Delete user group with wholesale	Click this button to remove the selected user group with wholesale.
Refresh	Click this button to refresh current page.
GroupID	Display the index number for the user group.
GroupName	Display the name of user group.
EnableGlobalMailServer	Display the status of Global Mail Server. It is enabled if the box is checked.
EnableGlobalSNMPServer	Display the status of Global SNMP Server. It is enabled if the box is checked.
Nodes	Display the number of device (CPE) for such group can have. Value “-1” means there is no limit of the number.
EnableExpireDate	Display if Expire Date is enabled or not.
ExpireDate	Display the date of the Expire Date.
UsedNodes	Display the number of used Nodes.

5.2.1 Add a User Group

To insert a user group, simply click . A new line with an input box will appear for the user to type personal information for identified by VigorACS.



5	Group_V	☒	☒	-1
6	Group_Test	☒	☒	-1
7	carrie	☒	☐	-1
8	Tim_Group	☒	☒	-1
0		☒	☒	-1

Available settings for such feature will be shown as follows:

Items	Description
GroupID	Display the index number for the user group.
GroupName	Type the name (e.g., Marketing) that can represent the user group. When you finish the typing, click  to save it.
EnableGlobalMailServer	Check it to display the status of Global Mail Server. It is enabled if the box is checked.
EnableGlobalSNMPServer	Check it to display the status of Global SNMP Server. It is enabled if the box is checked.
Nodes	Double click it to type a new number of device (CPE) for such group can have. Value “-1” means there is no limit of the number.
EnableExpireDate	Check it to display the Expire Date.
ExpireDate	Use the drop down calendar to specify the date you want.
UsedNodes	Display the number of used Nodes.

5.2.2 Edit a User Group

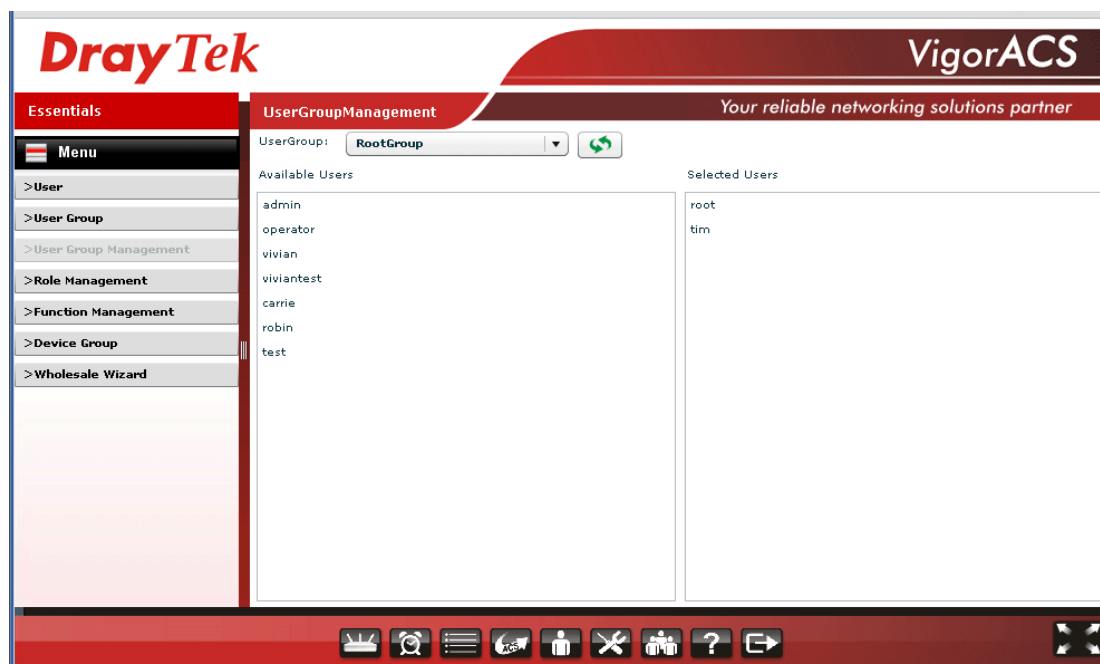
To edit a user group (if it is useless or unsatisfied) setting, please select the one that you want to edit and modify each box directly.

5.2.3 Delete a User Group

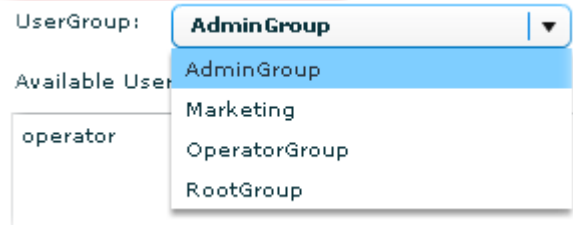
To delete a user group (if it is useless or unsatisfied) setting, please select the one that you want to delete and click .

5.3 User Group Management

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



Available settings for such feature will be shown as follows:

Items	Description
UserGroup	Choose one of the user groups from the drop down list. RootGroup is the default one.  Except RootGroup and AdminGroup, all the other user groups can be defined in the section 10.2 User Group. If you want to add a new group, please refer to section 10.2 User Group for detailed information.
 Refresh	Click this button to refresh current page.
Available Users	This box displays all the selectable users in VigorACS. root – It has the highest authority. The one with such authority has such level can do all of the jobs in VigorACS without limitation. admin – It has the higher authority.
Selected Users	This box displays the users selected by this group. Click one of the users in Available Users and drag to Selected Users, that one will be categorized under such user

Items	Description
	group. As to adding new users in VigorACS, please refer to section 10.1.1 Add a User for detailed information.

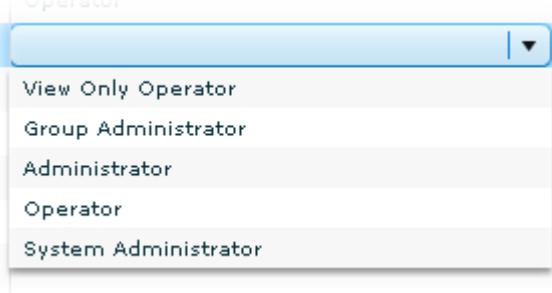
5.4 Role Management

This page can specify the authority for a user / user group.

Basically, each group will be assigned with a Role in default by VigorACS. You can modify the role whenever you want.



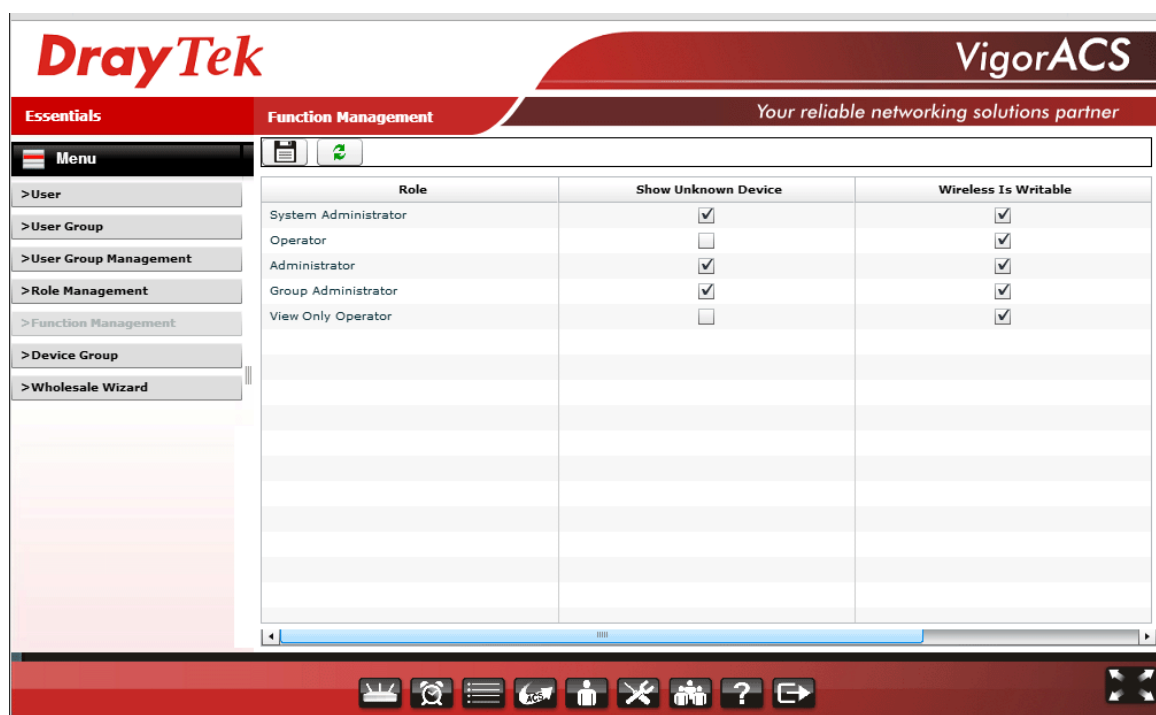
Available settings for such feature will be shown as follows:

Items	Description
 Save user setting	Click this button to save the settings.
 Refresh	Click this button to refresh current page.
Users	This field displays all the users in VigorACS.
Role	Choose the role for the selected user. Different role represents different authority that the user group will have. The great the authority is, the more functions the user /user group can have. 

Items	Description
	View Only Operator – Have the lowest authority. Group Administrator –Have the middle authority high than “Administrator”. Administrator – Have the middle authority. Operator – Have the low authority higher than View Only Operator. System Administrator – Have the highest authority.

5.5 Function Management

In addition to specifying the authority for the user, the administrator also can determine what functions the user can have.



Available settings for such feature will be shown as follows:

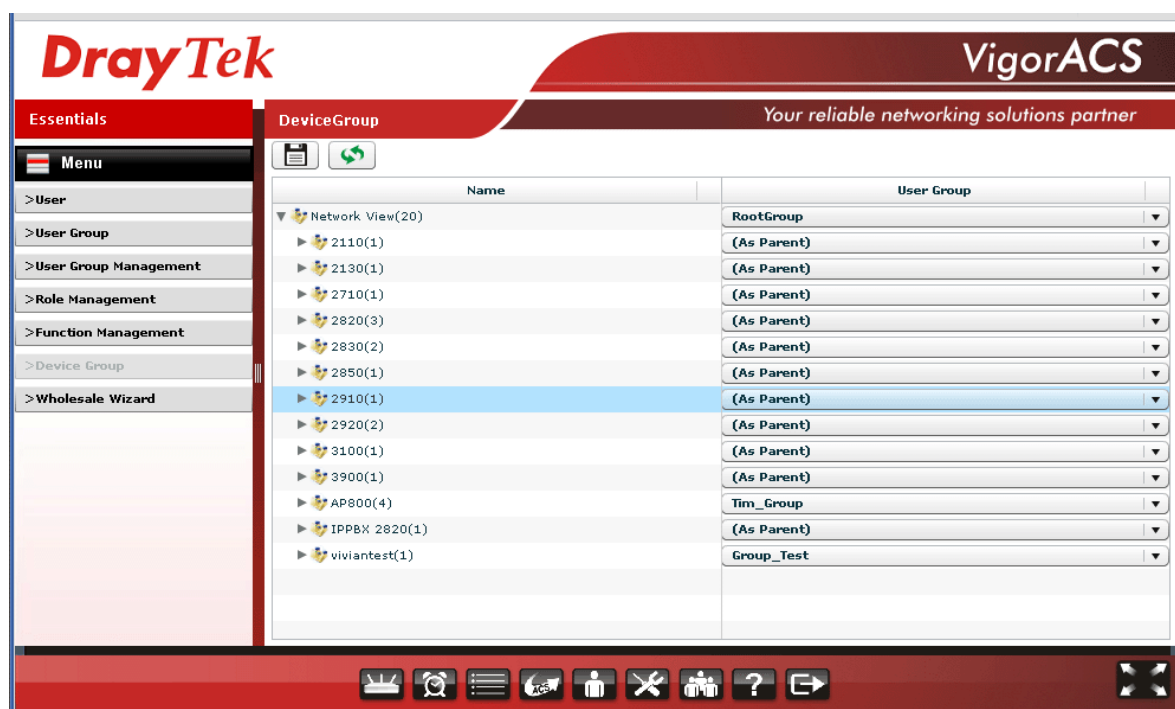
Items	Description
 Save user setting	Click this button to save the settings.
 Refresh	Click this button to refresh current page.
Role	View Only Operator – Have the lowest authority. You can view the information but not edit it. However, there is no time out for viewing the information with such role. Group Administrator –Have the middle authority high than “Administrator”. Administrator – Have the middle authority. Operator – Have the low authority higher than View Only Operator. System Administrator – Have the highest authority.

Items	Description
Show Unknown Device	Unknown device can be seen / hidden if it is checked / unchecked for different role.

5.6 Device Group

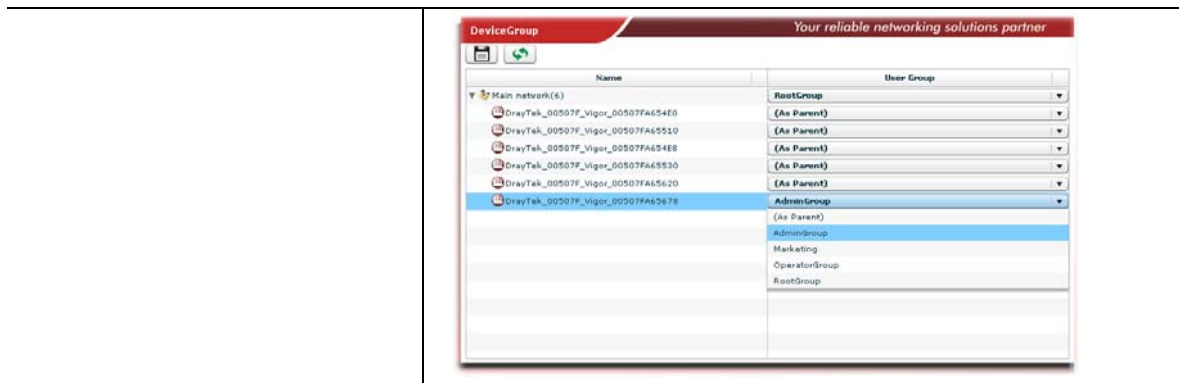
VigorACS allows administrator to manage users who want to access into VigorACS. In addition, it also allows the administrator (user) to manage networks and devices.

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



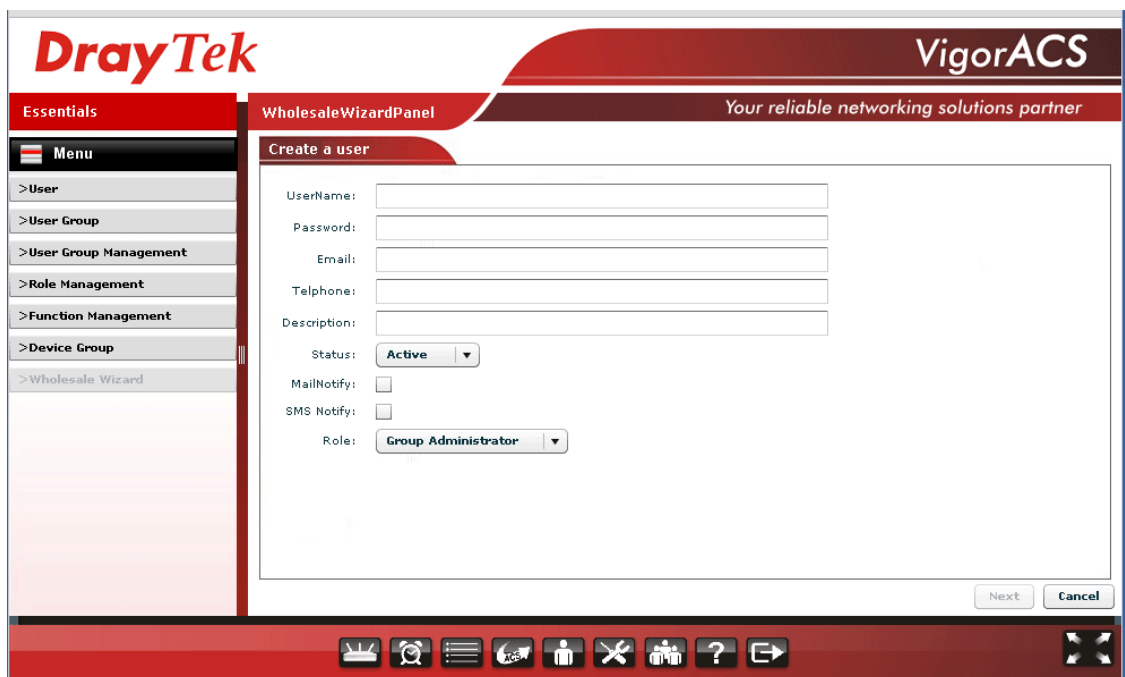
Available settings for such feature will be shown as follows:

Items	Description
 Save	Click this button to save the record.
 Refresh	Click this button to refresh current page.
Name	Display the devices controlled by VigorACS.
User Group	As Parent – Choose the same setting as the previous layer.



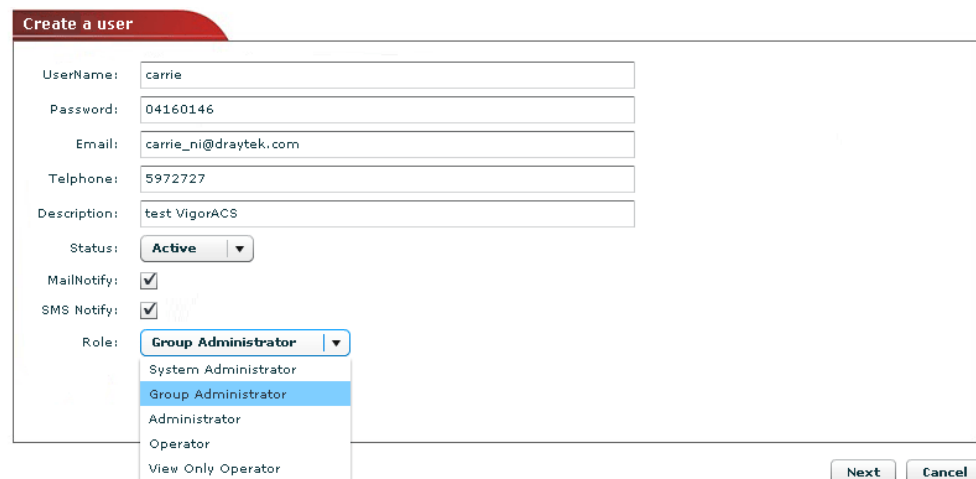
5.7 Wholesale Wizard

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



Please follow the steps listed below to create:

1. Choose **Wholesale Wizard**. The following screen for creating a user will appear.



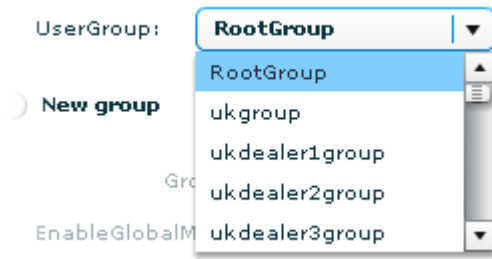
Available settings for such feature will be shown as follows:

Items	Description
UserName	Type a new name.
Password	Type a new password.
Email	Type email address of such user for receiving the mail notification.
Telephone	Type the telephone number of such user for receiving the SMS notification.
Description	Give a brief introduction of such user.
Status	Choose “Active” to make such user being seen on the network.
MailNotify	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.
Role	Assign a Role for such user.
Next	Go to next configuration page.
Cancel	Exit the setting page without saving any configuration.

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

Available settings for such feature will be shown as follows:

Items	Description
Existing group	Click the radio button. The existing user groups will be available for you to choose.

	
New group	Click the radio button to create a new group for such user. GroupName - Type the name (e.g., Marketing) that can represent the user group. EnableGlobalMailServer – Check the box to enable the global mail server. Nodes - Type the number of Nodes for such group. The default number is “-1”. EnableExpireDate - Check the box to enable 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.
Cancel	Exit the setting page without saving any configuration.

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

Create a network

☐ Existing network

Network:

☒ New network

Parent Network:

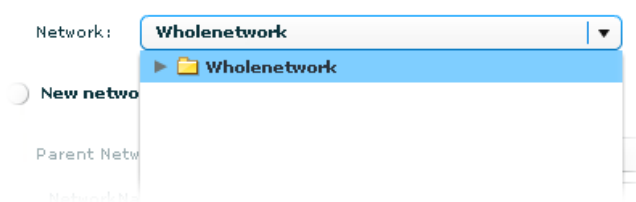
NetworkName:

Location:

User Name:

Password:

Available settings for such feature will be shown as follows:

Items	Description
Existing network	Click the radio button. The existing network will be available for you to choose. 
New Network	Click the radio button to create a new network for such user. Parent Network – Choose one of the existing networks as the Parent Network. NetworkName – Type a name for the new network. Location - Type a brief description 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.
Previous	Back to previous configuration page.
Next	Go to next configuration page.
Cancel	Exit the setting page without saving any configuration.

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

Summary

User:

UserName: carrie

Password: 04160146

Email: carrie_ni@draytek.com

Telephone: 5972727

Description: test VigorACS

Status: Active

MailNotify: true

SMS Notify: true

Role: Group Administrator

UserGroup:

New group

GroupName: carrie

EnableGlobalMailServer: true

Nodes: -1

EnableExpireDate: true

ExpireDate: 2011/07/15

Previous

Finish

Cancel

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



6. Open **User**. The new added user profile will be shown on the **UserPanel**.

Essentials		UserPanel				Your reliable networking solutions partner	
Menu							
> User							
> User Group							
> User Group Management							
> Role Management							
> Device Group							
> Wholesale Wizard							
		UserName	Password	Email	Telephone		
		root	+GW1NiOxIf007lQmx5Ll	tim_yang@draytek.com		System Admin	
		admin	0DPiKuNrrVmD8lUCuw1h	admin@ems		Administrator	
		operator	/pbdOxVqx8t0KDqSkmUt	operator@ems		Operator	
		tim	eq9E9rhgtA3K4E9JSFRML				
		vivian	+GW1NiOxIf007lQmx5Ll				
		viviantest	+GW1NiOxIf007lQmx5Ll				
		carrie	7qnywHJyP9tY5hVl6KIwH	carrie_ni@draytek.com	5972727	test VigorACS	

Chapter 6 Device Management

The home page for VigorACS is Device Management.

Basically, a summary screen with Network and Devices, Unknown Devices and Latest Alarms will be brought out for your reference whenever such mode (Device) is selected.



The welcome screen for VigorACS can be divided into two boxes, one is Essentials (the left side) and the other is main screen (the right side). **Essentials** contains four groups (containing drop down items), **Networks and Devices**, **Wizards**, **Reports**, and **Inventory Monitor**. Main screen will be changed based on the group selected in Essentials.

IP Address	Device Name	Device Type	Action
192.168....	DrayTek_001DAA...		+
90.145.2...	DrayTek_001DAA...		+
118.166...	DrayTek_00507F...	VigorAP 900	+
172.16.2...	DrayTek_00507F...	Vigor2960	+
118.166...	2130	Vigor2130V	+
118.166...	DrayTek_001DAA...	Vigor2860Vn	+

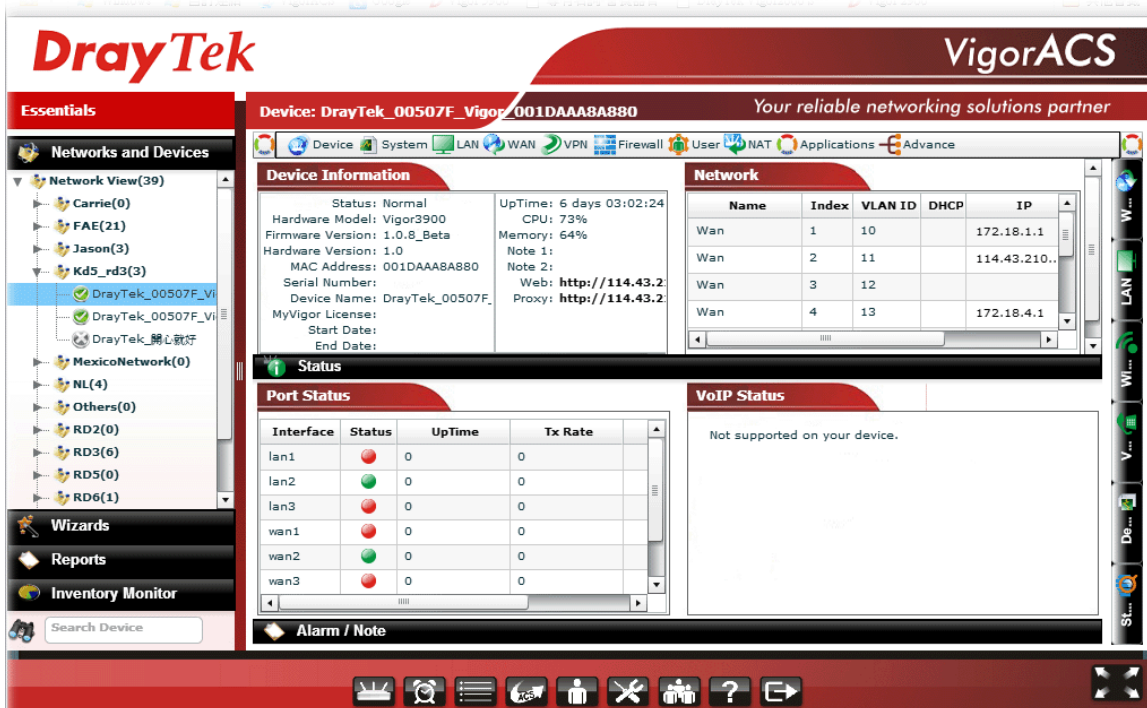
Level	Time	Device Name	Network	Description	Action
Critical	2016/07/28 05:27:30	DrayTek_001DAA_Vigor2...	Network View	DeviceLossConnection	Stop
Critical	2016/07/28 05:27:30	2130	Network View	DeviceLossConnection	Stop
Critical	2016/07/28 05:27:22	DrayTek_00507F_VigorA...	Network View	DeviceLossConnection	Stop
Critical	2016/07/28 05:26:54	DrayTek_00507F_Vigor2...	Network View	DeviceLossConnection	Stop
Critical	2016/07/28 05:12:30	DrayTek_00507F_Vigor...	Network View	DeviceLossConnection	Stop
Critical	2016/07/28 05:12:28	DrayTek_001DAA_Vigor2...	Network View	DeviceLossConnection	Stop

There are four menu items offered for users/administrator to adjust corresponding settings. Move your mouse cursor on any one of them, the drop down menu items will be shown automatically.



Available parameters for NAT DMZ Host settings include:

Items	Description
Networks and Devices	This field displays network and devices controlled by VigorACS. To get the detailed information for each device/network, just click one of device/network. Device Details will be shown on the right side. Refer to the following figure. 



DrayTek VigorACS
Your reliable networking solutions partner

Device: DrayTek_00507F_Vigor_001DAAA8A880

Device Information

Status: Normal	UpTime: 6 days 03:02:24
Hardware Model: Vigor3900	CPU: 73%
Firmware Version: 1.0.8_Beta	Memory: 64%
Hardware Version: 1.0	Note 1:
MAC Address: 001DAAA8A880	Note 2:
Serial Number:	Web: http://114.43.2
Device Name: DrayTek_00507F	Proxy: http://114.43.2
MyVigor License:	
Start Date:	
End Date:	

Network

Name	Index	VLAN ID	DHCP	IP
Wan	1	10		172.18.1.1
Wan	2	11		114.43.210..
Wan	3	12		
Wan	4	13		172.18.4.1

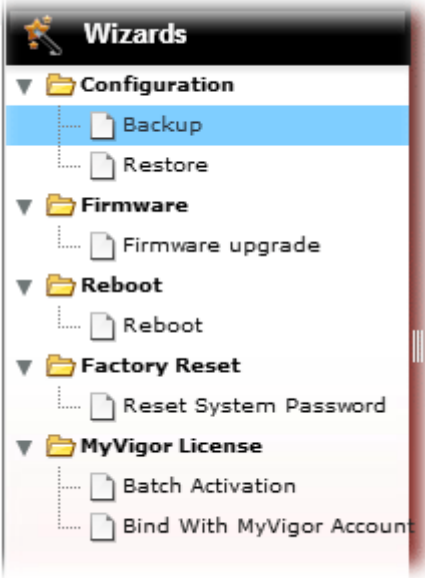
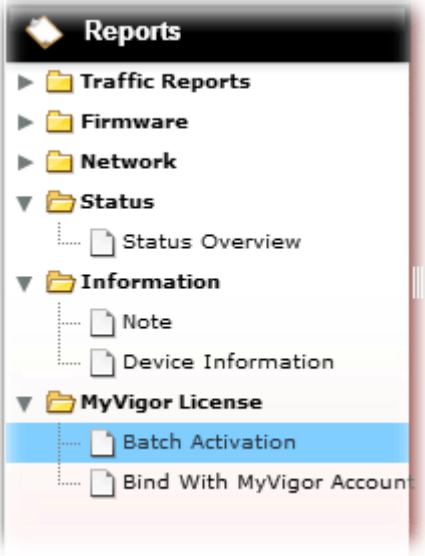
Port Status

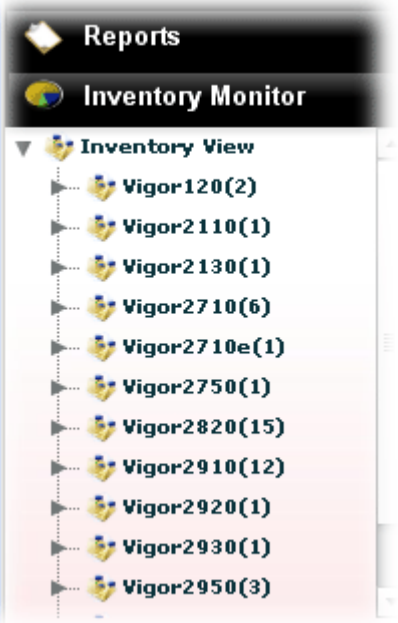
Interface	Status	UpTime	Tx Rate
lan1	●	0	0
lan2	●	0	0
lan3	●	0	0
wan1	●	0	0
wan2	●	0	0
wan3	●	0	0

VoIP Status

Not supported on your device.

Alarm / Note

Items	Description
Wizards	Backup, restore, firmware upgrade, reboot, factory reset and WCF batch operation for CPEs can be done via Wizards.  Note: Refer to Section 6.3 and Chapter 12 for detailed information about wizards operations.
Reports	Such groups allow the user to check traffic statistic, graph, firmware, IP, Status, Device, MyVigor License information for all the CPE controlled by VigorACS.  Note: Refer to Section 6.3 for detailed information for printing reports with PDF files.

Items	Description
Inventory Monitor	Click Inventory Monitor to display the devices (CPEs) under different model series.  The screenshot shows a web interface with a sidebar menu. The 'Reports' section is expanded, and 'Inventory Monitor' is selected. Below it, the 'Inventory View' is displayed, showing a list of device models with their counts in parentheses: - Vigor120(2) - Vigor2110(1) - Vigor2130(1) - Vigor2710(6) - Vigor2710e(1) - Vigor2750(1) - Vigor2820(15) - Vigor2910(12) - Vigor2920(1) - Vigor2930(1) - Vigor2950(3)

6.1 Networks

This page displays the information and current status for network(s) and device(s).

A convenient design offered by VigorACS is that you can select the menu items from menu bar or side bar according to your usage habit.

Menu Bar
Side Bar

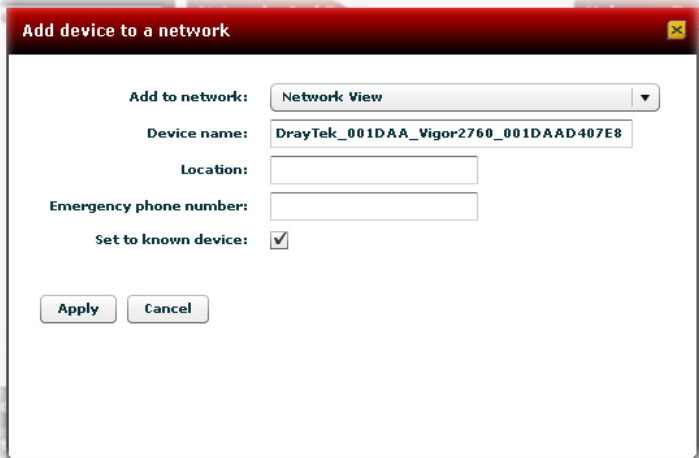
The screenshot shows the VigorACS Network View interface. The top bar is red with the text "Your reliable networking solutions partner". Below it is a menu bar with icons for Network, View, VPN, Wireless, and AP Management. The main content area is divided into three sections: "Managed networks and devices", "Unknown Devices", and "Latest Alarms". The "Managed networks and devices" section shows statistics: Total number of networks: 7, Alarm networks: 5, Total number of devices: 27, and Number of alarmed devices: 25. The "Unknown Devices" section shows a table of devices with IP Address, Device Name, Device Type, and Action. The "Latest Alarms" section shows a table of alarms with Level, Time, Device Name, Network, Description, and Action. A red circle highlights the Menu Bar, and a red rectangle highlights the Side Bar. A blue arrow points from the Side Bar to the Network menu item.

IP Address	Device Name	Device Type	Action
192.168...	DrayTek_001DAA...		+
90.145.2...	DrayTek_001DAA...		+
118.166...	DrayTek_00507F...	VigorAP 900	+
172.16.2...	DrayTek_00507F...	Vigor2960	+
118.166...	2130	Vigor2130V	+
118.166...	DrayTek_001DAA...	Vigor2860Vn	+

Level	Time	Device Name	Network	Description	Action
Critical	2016/07/28 05:27:30	DrayTek_001DAA_Vigor2...	Network View	DeviceLossConnection	+
Critical	2016/07/28 05:27:30	2130	Network View	DeviceLossConnection	+
Critical	2016/07/28 05:27:22	DrayTek_00507F_VigorA...	Network View	DeviceLossConnection	+
Critical	2016/07/28 05:26:54	DrayTek_00507F_Vigor2...	Network View	DeviceLossConnection	+
Critical	2016/07/28 05:12:30	DrayTek_00507F_Vigor_...	Network View	DeviceLossConnection	+
Critical	2016/07/28 05:12:28	DrayTek_001DAA_Vigor2...	Network View	DeviceLossConnection	+

The Side Bar on the right contains a list of menu items: Network, Network Summary, Network Devices, Network Map, and Dashboard. The Network item is highlighted. Below the list are buttons for View and VPN.

Items	Description
Menu Bar	Available menu items for the network contain Network, View, VPN (e.g., VPN wizard), Wireless (e.g., wireless wizard) and AP Management. Available menu items for selected device will be changed based on the model of the selected device.

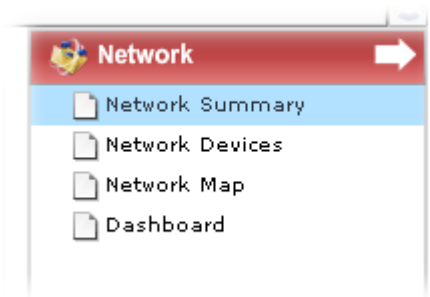
Side Bar	Only the common used menu items for the network will be displayed. That is, not all the available parameters settings can be seen in this area. The Side Bar can be unfolded whenever you click on any one of the menu items.
Network And Devices	This area will display the total number of networks/devices managed by VigorACS.
Unknown Devices	This area will display the devices detected by VigorACS which has not grouped under any network to be managed by VigorACS. If you click the “+” button, a pop-up window (as shown below) will appear for you to specify which network the device can be added to.  After finished the settings, click Apply. The device will be added to the specified network and will be removed from unknown devices area.
Latest Alarms	This area will display the record of the device/network with latest alarm message.

Below shows an example to open a menu item from menu bar or side bar:

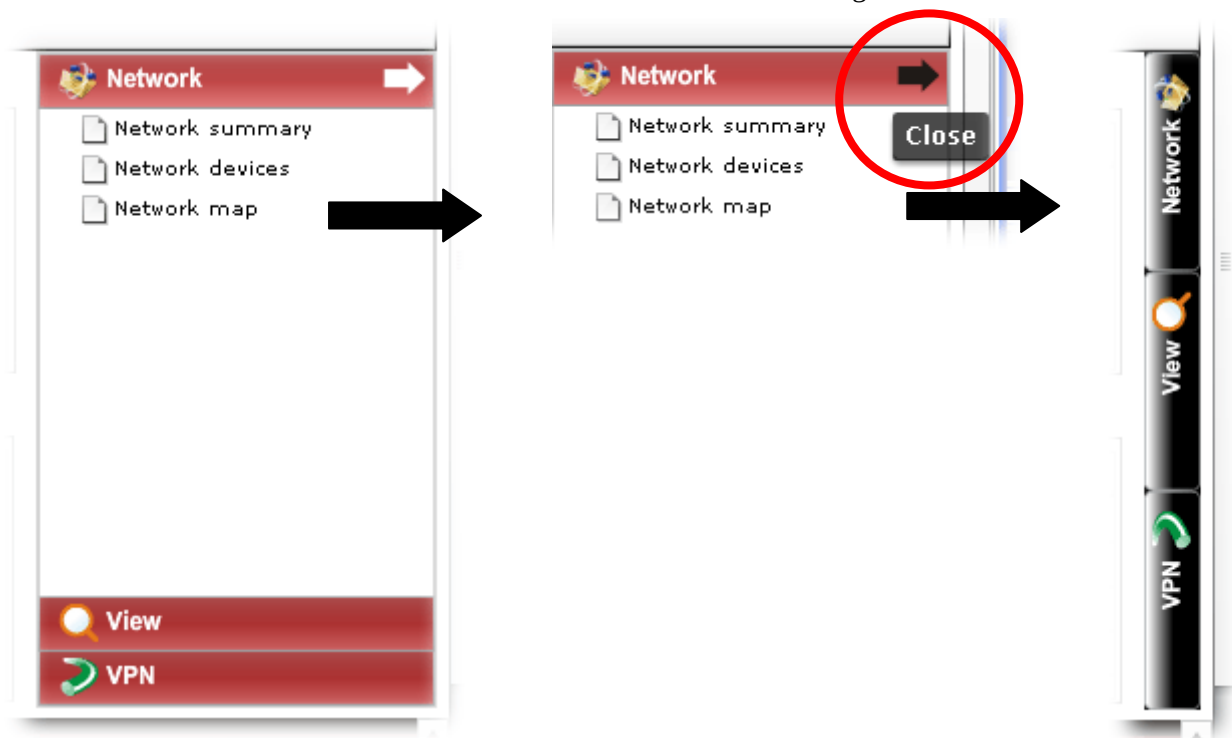
- Click the **Network** menu item from the Menu bar and choose **Network summary**.



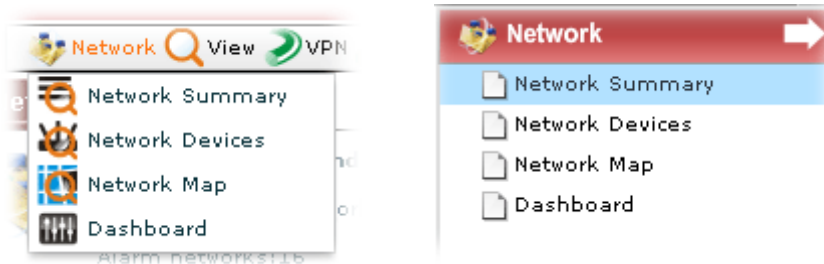
- Click the **Network** icon on the Side Bar, a drop down menu items or expanded menu items will be shown as follows.



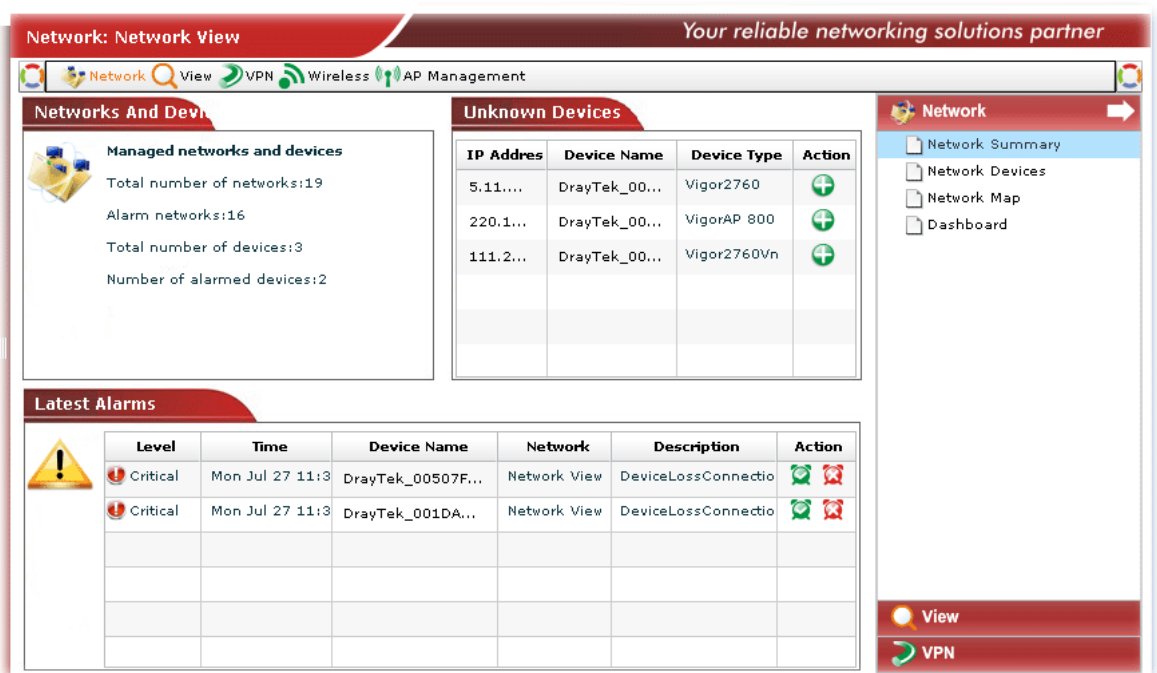
Click the Close arrow on the unfolded side bar to fold the Side Bar again.



6.1.1 Network Summary



Network Summary provides summary for the whole management and shows the Networks information, devices information, latest alarms information and unknown devices information.



Network: Network View *Your reliable networking solutions partner*

Network View VPN Wireless AP Management

Networks And Devices

Managed networks and devices

Total number of networks:19
Alarm networks:16
Total number of devices:3
Number of alarmed devices:2

Unknown Devices

IP Address	Device Name	Device Type	Action
5.11.1...	DrayTek_00...	Vigor2760	
220.1...	DrayTek_00...	VigorAP 800	
111.2...	DrayTek_00...	Vigor2760Vn	

Latest Alarms

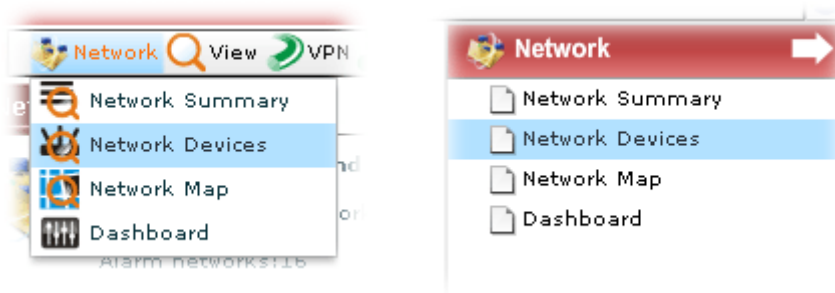
Level	Time	Device Name	Network	Description	Action
Critical	Mon Jul 27 11:3	DrayTek_00507F...	Network View	DeviceLossConnectio	
Critical	Mon Jul 27 11:3	DrayTek_001DA...	Network View	DeviceLossConnectio	

Network

- Network Summary
- Network Devices
- Network Map
- Dashboard

View VPN

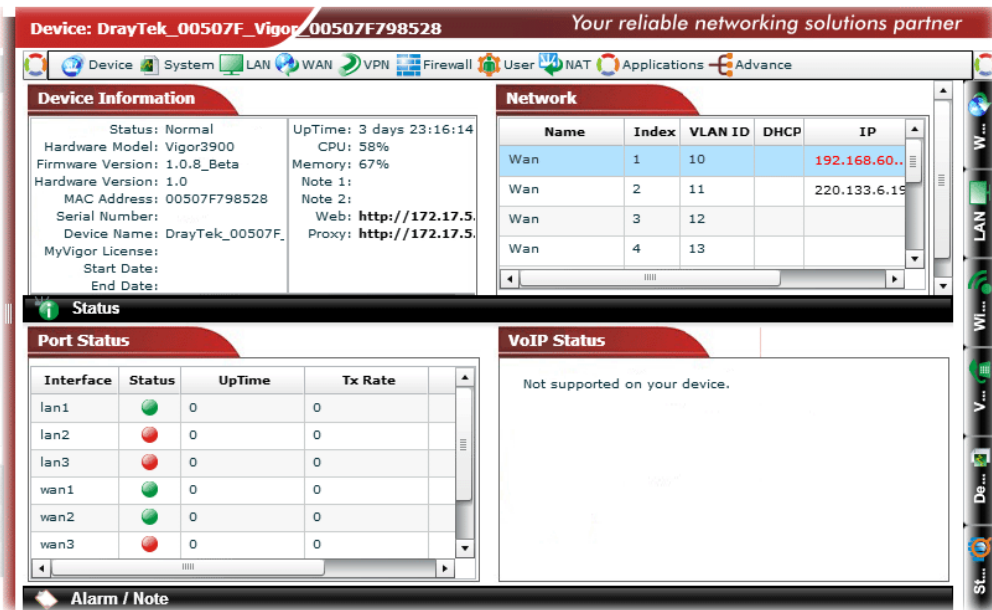
6.1.2 Network devices



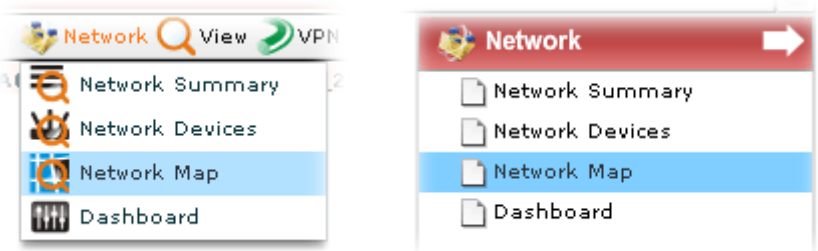
A list of managed and controlled CPEs under the selected network will be displayed with icons in this page. On the left side of the page, the tree view shows all the created groups. On the right side, the CPEs **under selected group** will be displayed.



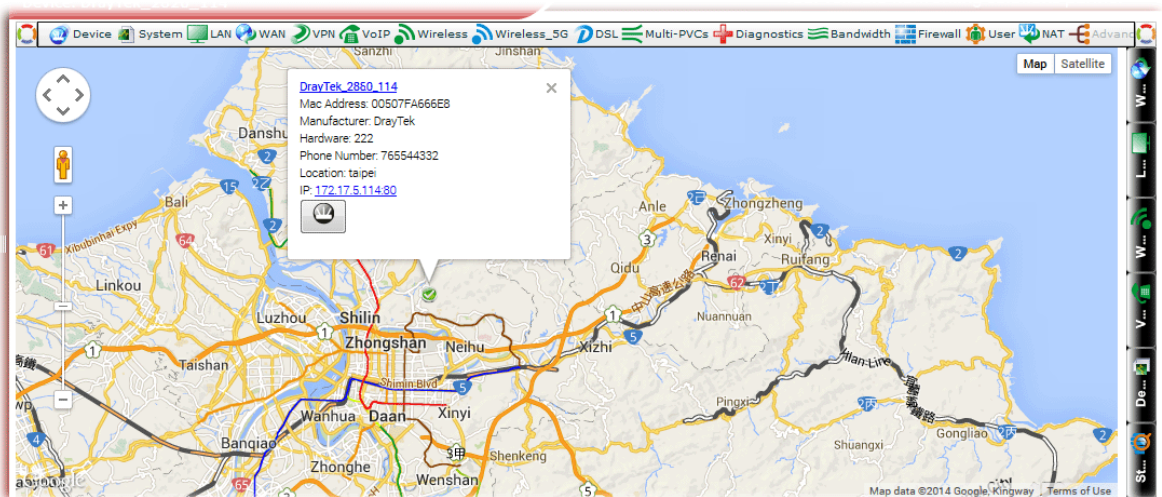
To have the detailed information for each CPE, simply move your mouse to the device (represented as an icon) you want and click on it. A **Device Details** page for the selected CPE will be displayed immediately for your reference.



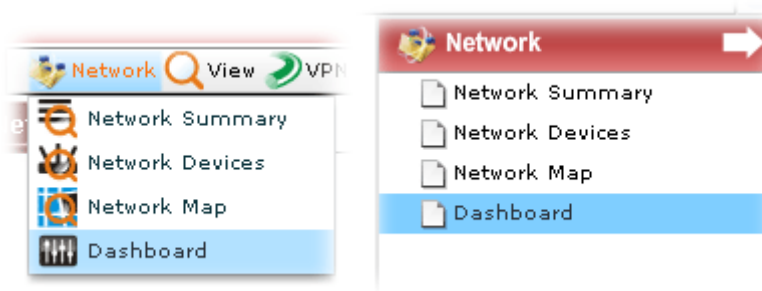
6.1.3 Network map



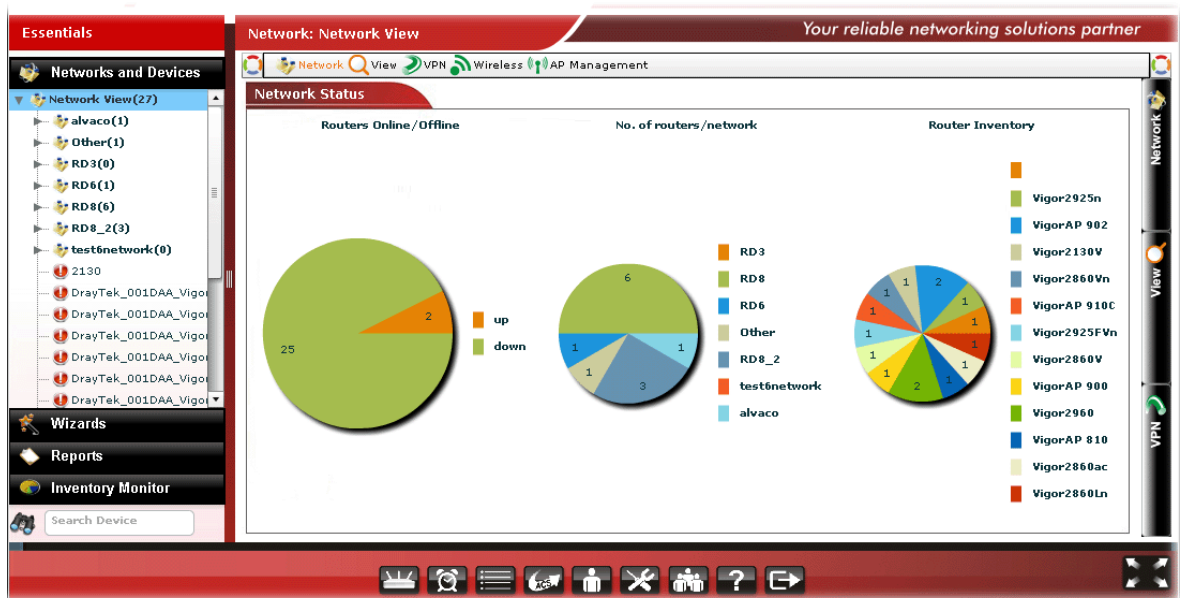
Such mode allows you to view the devices with a bird view. Network map can assist you to find out the location of the devices conveniently and easily.



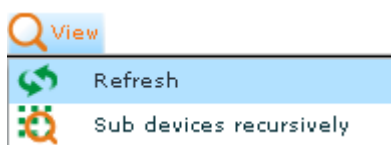
6.1.4 Dashboard



This page can display the network status, online/offline, number of routers/network groups and router inventory for the whole network or for the selected network group by using pie diagrams with different colors.

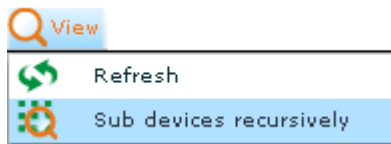


6.1.5 Refresh

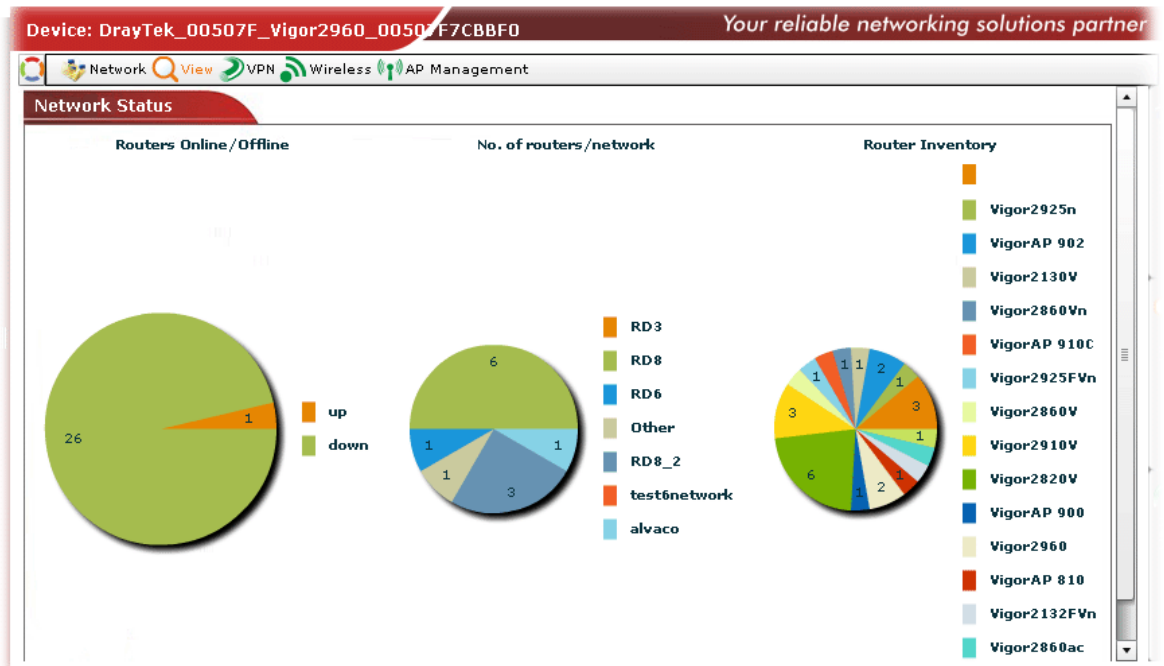


This function can refresh current network information displayed on the screen.

6.1.6 Sub devices recursively



This function can display the statistics for networks and devices through pie chart.

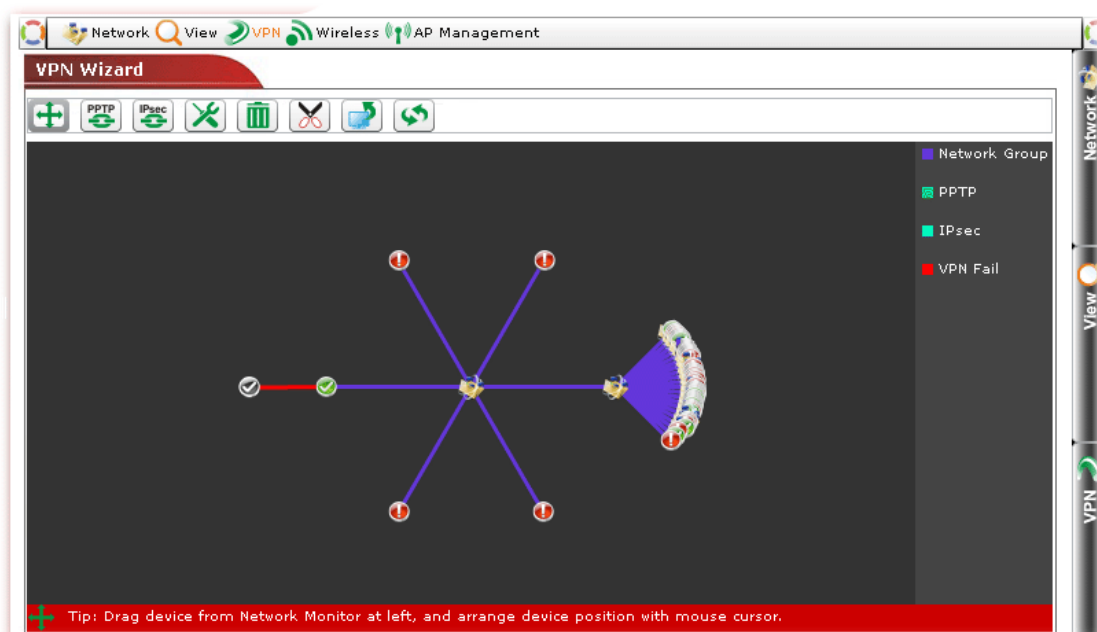


6.1.7 VPN

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

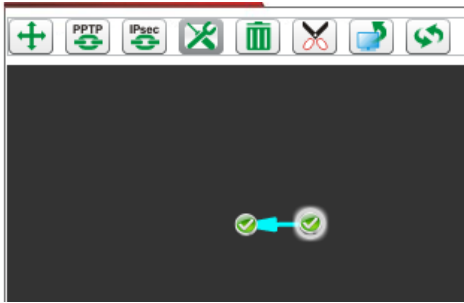
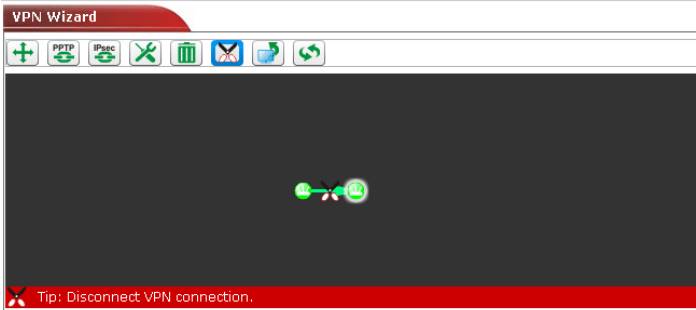


Click **VPN Wizard** from **VPN** menu to open the following page.



Available settings for such feature will be shown as follows:

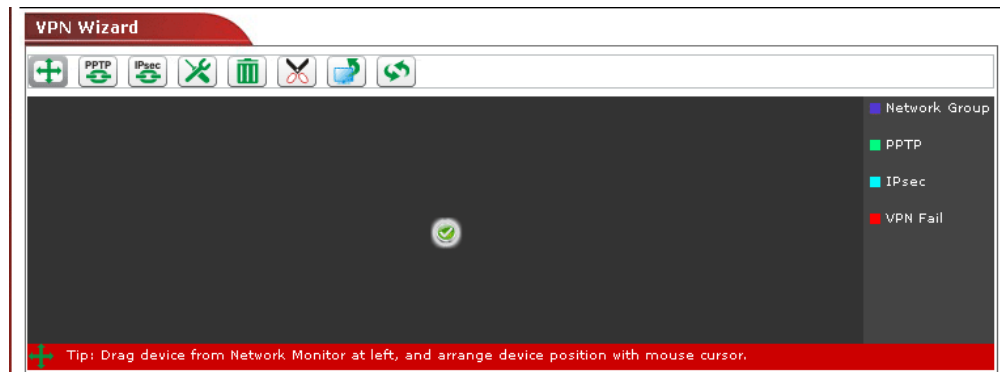
Items	Description
 Add device...	Click this button to add a device for building VPN connection. If you do not click this button first, you can not drag any device from Network View .
 PPTP	To build a quick VPN connection with PPTP , simply click this button first and then drag the device from Network View to the black area.
 IPsec	To build a quick VPN connection with IPSec , simply click this button first and then drag the device from Network View to the black area.
 Advance Connection	To build a VPN connection with detailed configuration, click Advance Connection tool. For detailed information, please refer to the section of Building an Advanced VPN Connection later.

	
 Remove the device....	Click this button to remove the selected device without VPN connection.
 Disconnect	To disconnect a VPN connection, Click this button and move the mouse cursor to the VPN connection that you want to disconnect. Notice that the mouse cursor will be transformed into a scissor.  If you press Enter, a confirmation dialog will appear. You can click Yes and the VPN connection will be cut off immediately. 
 Change LAN IP Setting	If there is LAN IP segment conflict in VPN connection, please select that device and click this button to change LAN IP setting.
 Refresh VPN Wizard	Click this button to reconnect both devices.

How to Build a Simple VPN Connection

Please follow the steps to build a simple VPN connection.

1. Open **VPN>>VPN wizard**. You will get the following page. Selected CPE will be displayed in the middle of the screen. There is no VPN connection existed.



2. Open the **Networks and Devices** and expand the group folder as the following:

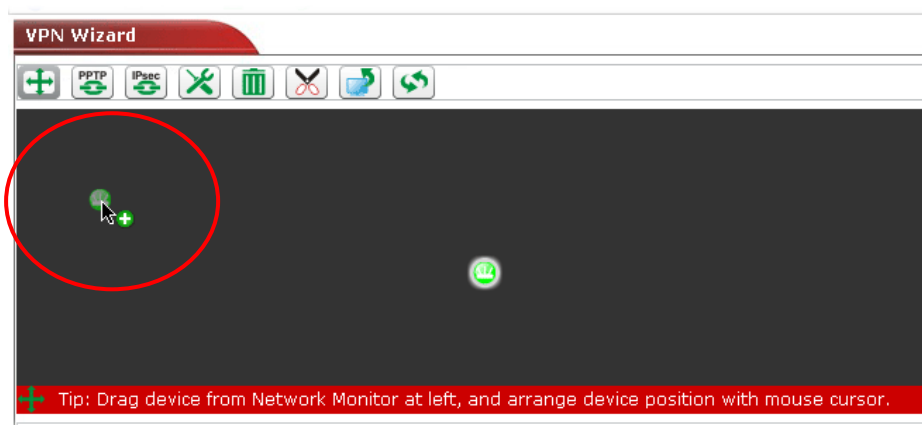


3. Click the **Add device** button.

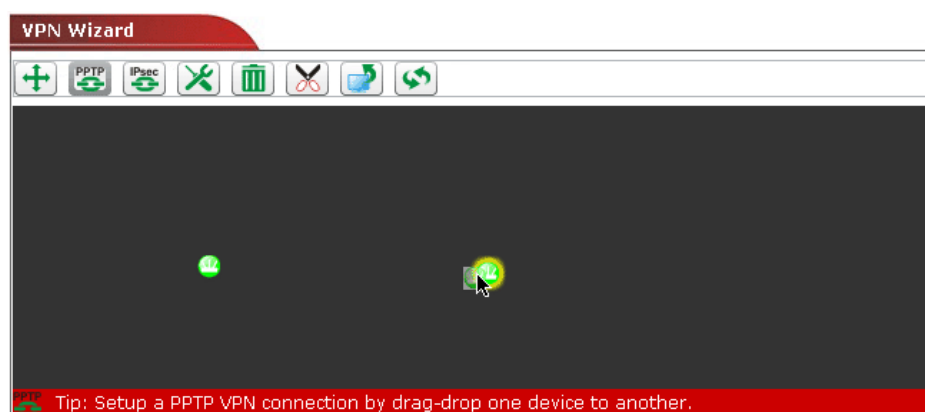


Add device for VPN connection and topology arrangement

4. Choose one device from the **Networks and Devices** that you want to build a VPN connection with the current selected device. **Drag** it from the **Networks and Devices** to the page of **Device Details**.



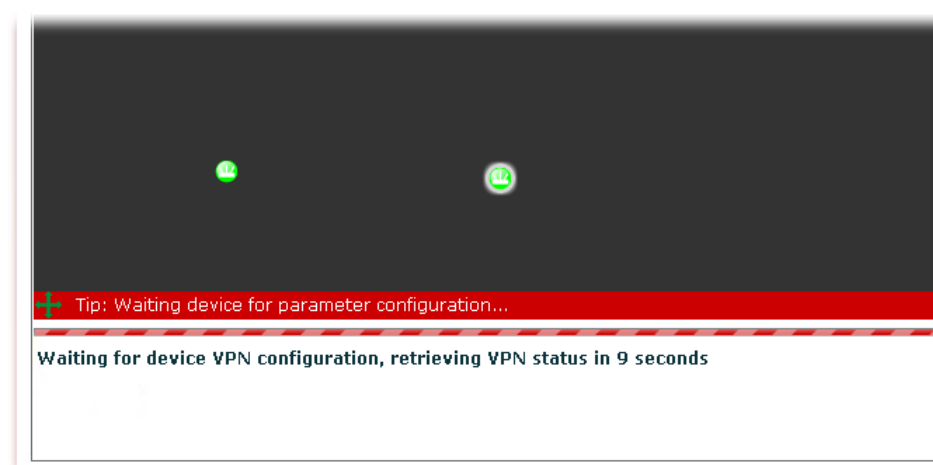
5. If you want to build VPN connection through PPTP or IPsec, click the PPTP or IPsec icon first. Then, drag one of the devices to the other.



6. A confirmation dialog will appear. Click **Yes**.



7. Now, the system will configure parameters automatically between these two devices. Please wait patiently.



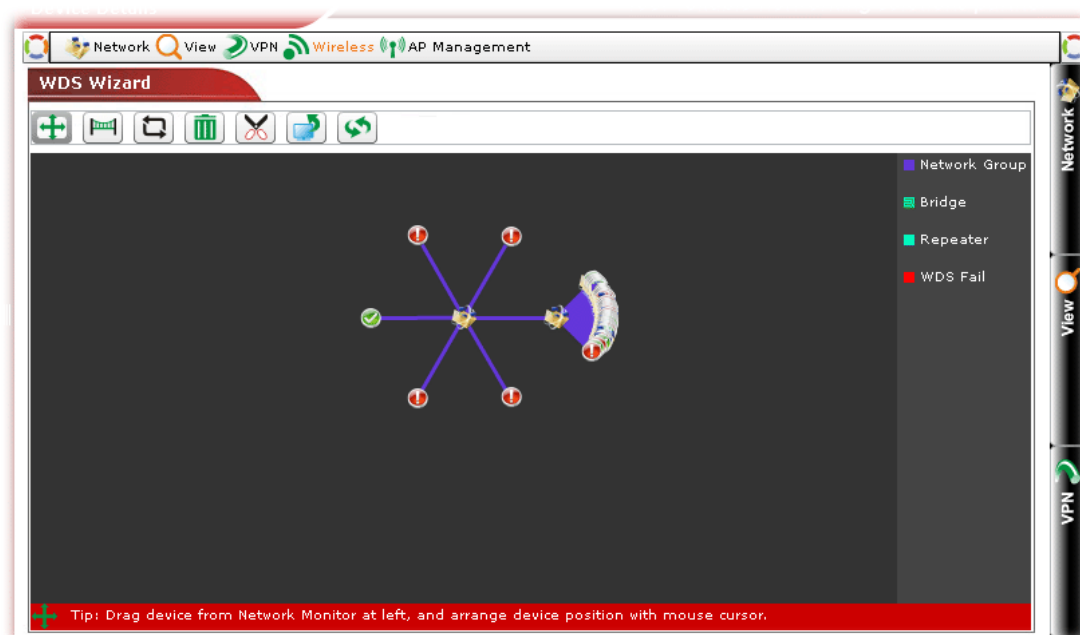
8. When the VPN connection has been done, an arrow will appear and indicate the direction between these two devices. VPN connection information also will be displayed below the black area.
9. Different colors for arrows represent different protocols used in VPN connections. Green means PPTP mode; blue means IPsec mode; and red means the VPN connection is failed.

6.1.8 Wireless

WDS Wizard offers a quick and simple way to build WDS network between Vigor routers and network.

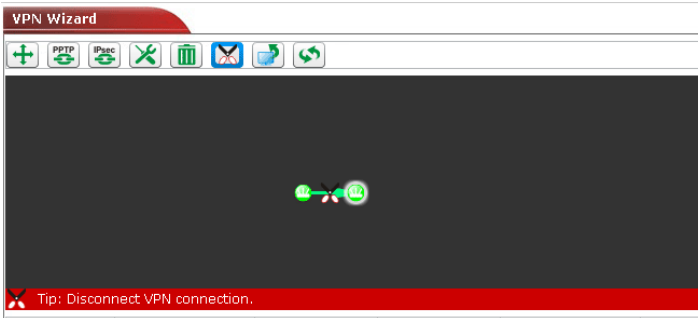


Click **WDS Wizard** from **Wireless** menu to open the following page.



Available parameters for this function include:

Items	Description
 Add device...	Click this button to add a device for building WDS connection. If you do not click this button first, you can not drag any device from Network View .
 Bridge	To build a quick WDS connection in Bridge mode, simply click this button first and then drag the device from Network View to the black area.
 Repeater	To build a quick WDS connection in Repeater mode,, simply click this button first and then drag the device from Network View to the black area.
 Remove the device....	Click this button to remove the selected device without WDS connection.
 Disconnect	To disconnect a WDS connection, click this button and move the mouse cursor to the WDS connection that you want to disconnect. Notice that the mouse cursor will be transformed into a scissor.

	 If you press Enter, a confirmation dialog will appear. You can click Yes and the WDS connection will be cut off immediately.
 Change LAN IP Setting	If there is LAN IP segment conflict in WDS connection, please select that device and click this button to change LAN IP setting.
 Refresh	Click this button to refresh this page.

6.1.9 AP Management

At present, only **AP Status** is available. Click it to check the status of VigorAP managed under current selected network.

Available parameters for this function include:

Items	Description
 Refresh	Click this button to refresh this page.
 Export to CSV	Click this button to save related information of AP status as a CSV file.

 First	When there is more than one page for related information of AP status, click this button to display the first page.
 Previous	When there is more than one page for related information of AP status, click this button to display the previous page.
 Next	When there is more than one page for related information of AP status, click this button to display the next page.
 Last	When there is more than one page for related information of AP status, click this button to display the last page.

6.2 Devices

Most of the Vigor CPEs controlled and managed by VigorACS can be viewed and modified through VigorACS. Click one of the CPEs from the tree view under **Essentials>>Networks and Devices**.

Note: The menu items displayed on menu bar /side bar will be different according to the Vigor router selected. Here, in this section, **Vigor2960** is selected as an example for introducing device management.

Menu Bar

Side Bar

Device: DrayTek_00507F_Vigor2960_00507FFF3900

Your reliable networking solutions partner

Device Information

Status: Normal
Hardware Model: Vigor2960
Firmware Version: 1.3.0_Beta
Hardware Version: 1.0
MAC Address: 00507FFF3900
Serial Number:
Device Name: DrayTek_00507F_
MyVigor License:
Start Date:
End Date:

UpTime: 11 days 18:43:17
CPU: 6%
Memory: 42%
Note 1:
Note 2:
Web: http://172.16.2.4
Proxy: http://172.16.2.4
Network Name: Network View

Network

Link Status	Name	Index	VLAN ID	DHCP
Up	Wan	1	10	172.1
Disable	Wan	2	11	
Up	Lan	1	10	false 192.1
Disable	Lan	2	0	false 0.0.0.

Port Status

Interface	Status	UpTime	Tx Rate	Tx Enal
lan1		0	0	
lan2		0	0	
lan3		0	0	
lan4		0	0	
wan1		0	0	
wan2		0	0	

VoIP Status

Not supported on your device.

Alarm / Note

Device: DrayTek_00507F_Vigor2960_00507FFF3900

Your reliable networking solutions partner

Device Information

Status: Normal
Hardware Model: Vigor2960
Firmware Version: 1.3.0_Beta
Hardware Version: 1.0
MAC Address: 00507FFF3900
Serial Number:
Device Name: DrayTek_00507F_
MyVigor License:
Start Date:
End Date:

UpTime: 11 days 18:43:17
CPU: 6%
Memory: 42%
Note 1:
Note 2:
Web: http://172.16.2.4
Proxy: http://172.16.2.4
Network Name: Network View

Network

Link Status	Name	Index	VLAN ID
Up	Wan	1	10
Disable	Wan	2	11
Up	Lan	1	10
Disable	Lan	2	0

Port Status

Interface	Status	UpTime	Tx Rate
lan1		0	0
lan2		0	0
lan3		0	0
lan4		0	0
wan1		0	0
wan2		0	0

VoIP Status

Not supported on your device.

Alarm / Note

WAN

LAN

Wireless

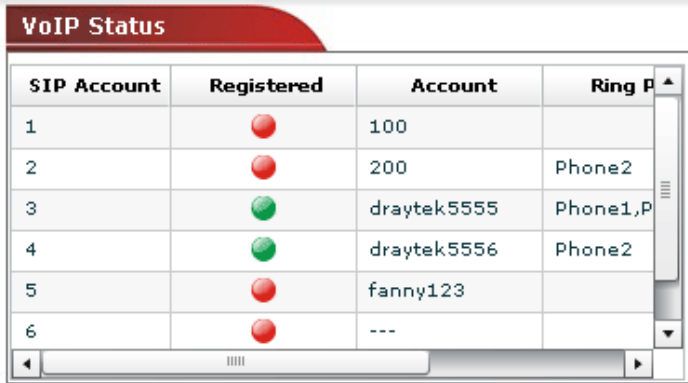
VoIP

Device operation

- Device System Log
- Firmware Status
- Ping/TraceRoute From ACS
- Firmware Upgrade
- Firmware Upgrade Log
- Reboot Device
- Factory Reset Device
- Copy Parameters
- Copy Parameters Log

Statistics

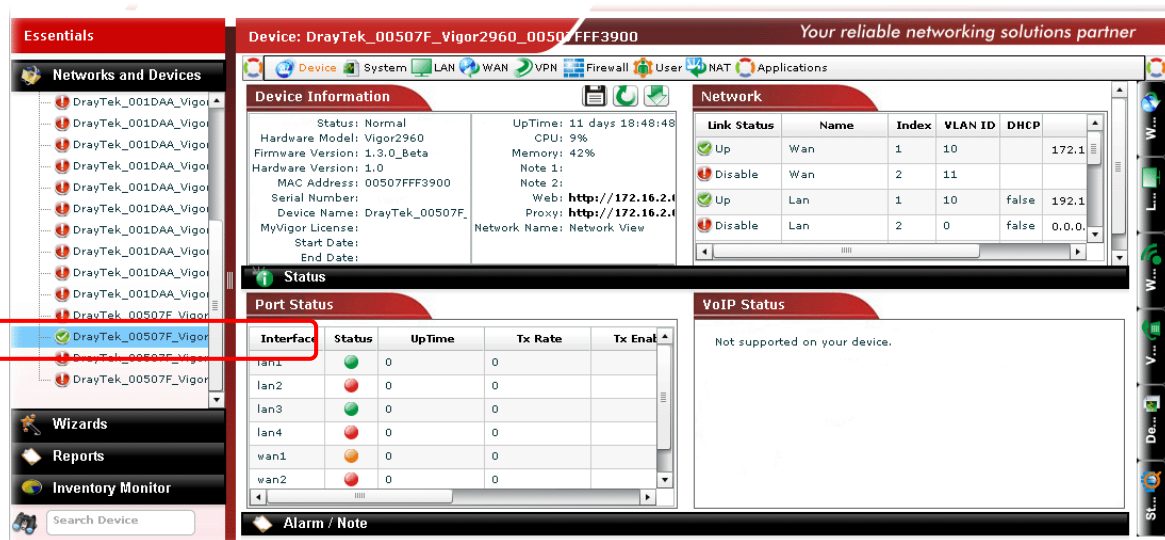
Items	Description
Menu Bar	Display all the available menu items for the device, such as Device, System, LAN, WAN, VPN, Wireless, DSL, Multi-PVC, VoIP, NAT, and etc. Different model of CPE will bring out different menu items.
Side Bar	Only the common used menu items for the selected CPE

	will be displayed. That is, not all the available parameters settings can be seen in this area. The Side Bar can be unfolded whenever you click on any one of the menu items.
Device Information	This area display general information for the selected CPE.  - Click it to backup current configuration for the selected CPE as a file.  - Click it to perform the restoration of the latest configuration file for the selected CPE.  - Click it to download the latest configuration file for the selected CPE.
Port Status	This area will display current status (online/offline, up time and transmission rate) for LAN, WAN, and WLAN of the selected CPE.
Network	This area will display current network configuration, such as VLAN ID setting, DHCP server enabled/disabled, IPv4 address, IPv6 address, proxy enabled/disabled for LAN, WAN and VLAN of the selected CPE.
VoIP Status	If the selected CPE does not support VoIP, you will get a message of “Not supported on your device”. However, if the selected CPE does support VoIP, you will get VoIP Status as the following figure. 

6.2.1 Device Summary

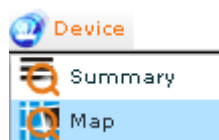


Click one of the CPEs from the tree view under **Essentials>>Networks and Devices**. Then Open **Device>>Summary**. Device details for the selected CPE will be shown with the summary information of system, alarm, network and note. The following example shows the summary of Vigor2960.

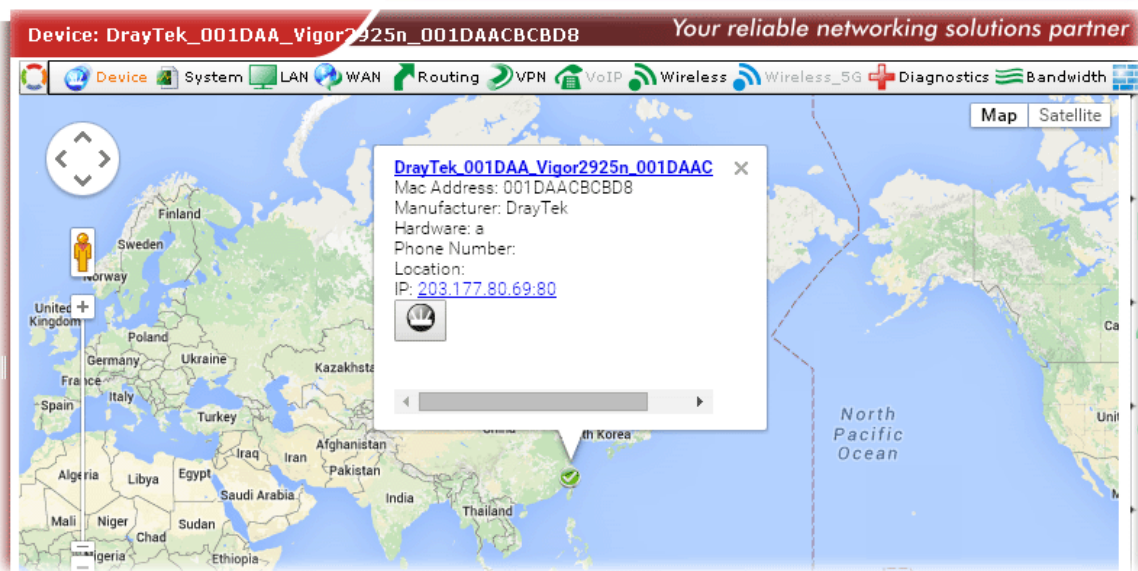


You can **switch into** other page to check additional information, e.g., location of CPE, list of managed CPEs, Web URL to connect CPE and so on. Just move your mouse to **Device** menu and select one of the items from the drop down list.

6.2.2 Device Map



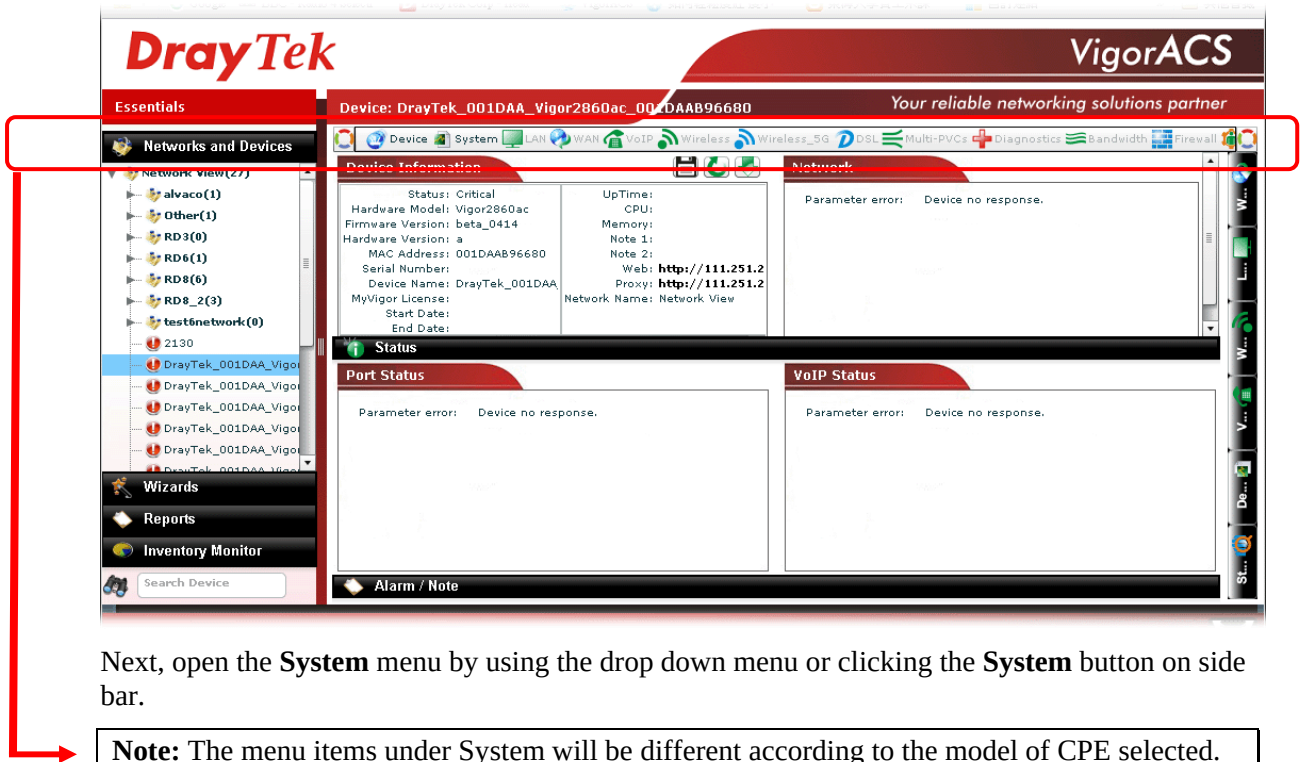
Click this item to display the location of current selected CPE (e.g., Vigor2925n) with a map.



6.2.3 System Management for Selected CPE

VigorACS allows you to view device system log, firmware status, time, TR-069, password setup, syslog setup, statistics, ping/trace route, firmware upgrade, reset/reboot the device, management, copy parameters, CPE notify log, CPE exclude parameters, Login greeting and so on by using **System** menu items.

Click one of the CPEs from the tree view under **Essentials>>Networks and Devices** to display general information for the selected CPE.



The screenshot shows the VigorACS web interface. The top navigation bar includes 'Essentials', 'Networks and Devices', 'Wizards', 'Reports', and 'Inventory Monitor'. The 'Networks and Devices' section is expanded, showing a tree view of devices. A red box highlights the 'System' menu item in the top navigation bar. A red arrow points from the 'System' menu item to a note box.

Note: The menu items under System will be different according to the model of CPE selected.

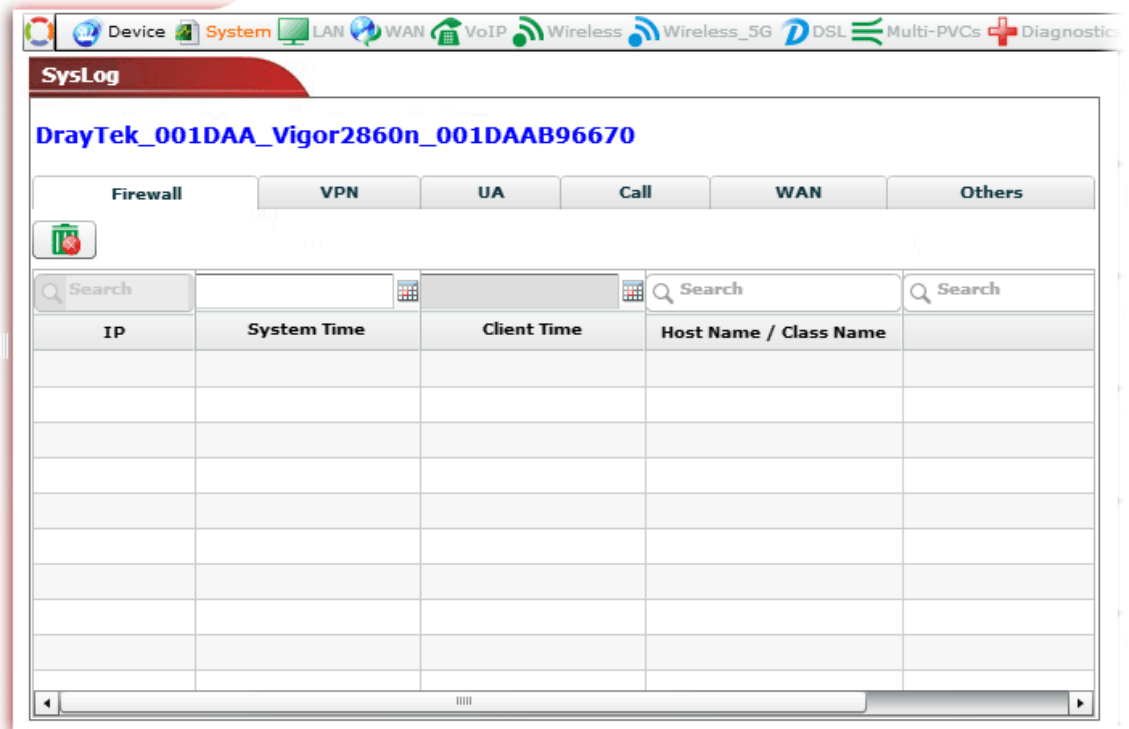
Next, open the **System** menu by using the drop down menu or clicking the **System** button on side bar.

Checking Device SysLog for the Selected CPE

The administrator can check syslog for **selected** CPE. Simply choose **System>>Device System Log**.



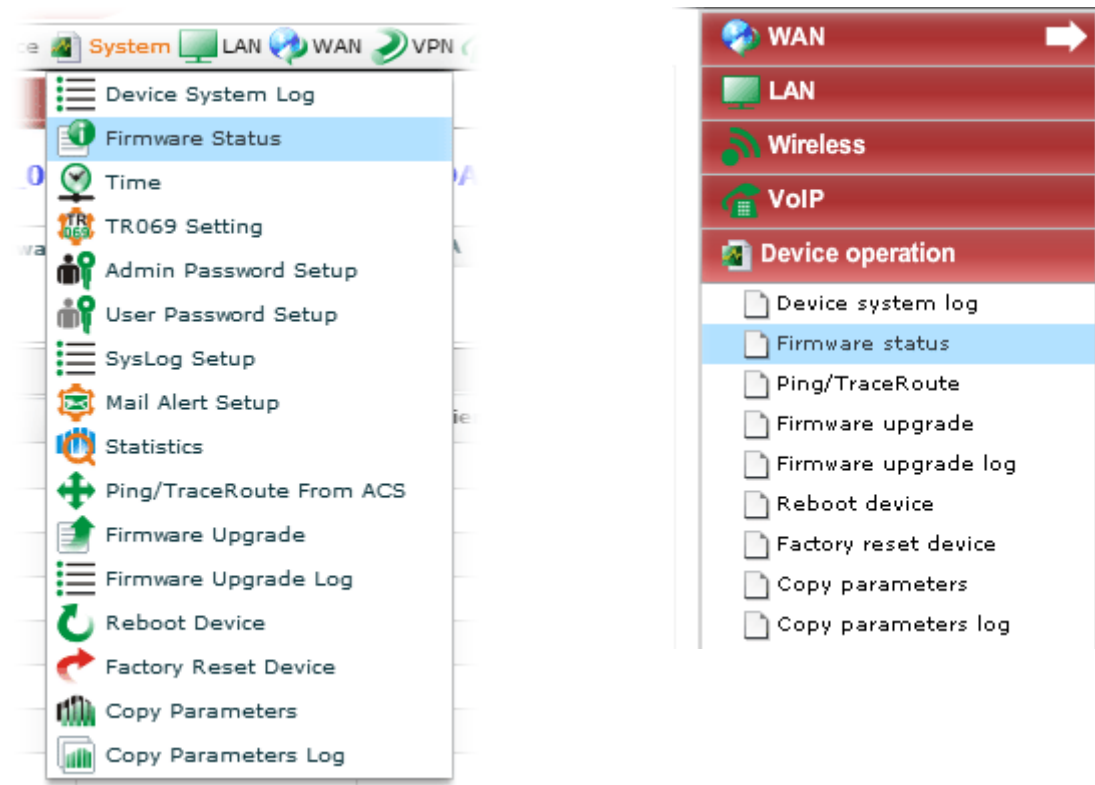
Related page will be shown as follows:



If you want to check syslog for **all devices** which are controlled by VigorACS, please refer to Chapter 6 Log View for more detailed information.

Checking the Firmware Status for the Selected CPE

To get the information of firmware version for the selected CPE, please open **System>>Firmware status**.



A screen of firmware status for the selected CPE will be shown as follows.

Firmware



Index

1

Modem Firmware Version

211011_A Annex_A

Software Version

3.3.6

Manufacturer OUI

00507F

Model Name

Vigor2710Vn

Available parameters for this function include:

Items	Description
Index	Display the index number of the CPE in current network group.
Modem Firmware Version	Display the firmware version for the hardware that the CPE used currently.
Software Version	Display the software version that the CPE used currently.
Manufacturer OUI	Display the characters of OUI. OUI means “organizationally unique identifier” of the device manufacturer.
Model Name	Display the model name of the selected CPE.
 Save parameter settings	Click this button to save the parameters settings.

Specifying the Time Setting for the Selected CPE

To get the information of time setting or modify the time setting for the selected CPE, please open **System>>Time**.

Time




Index 1

NTP Server 1

pool.ntp.org

Current Local Time

2014-09-15T09:01:18

Local Time Zone

+00:00

Local Time Zone Name

Greenwich Mean Time : Dublin ▼

Daylight Savings Used

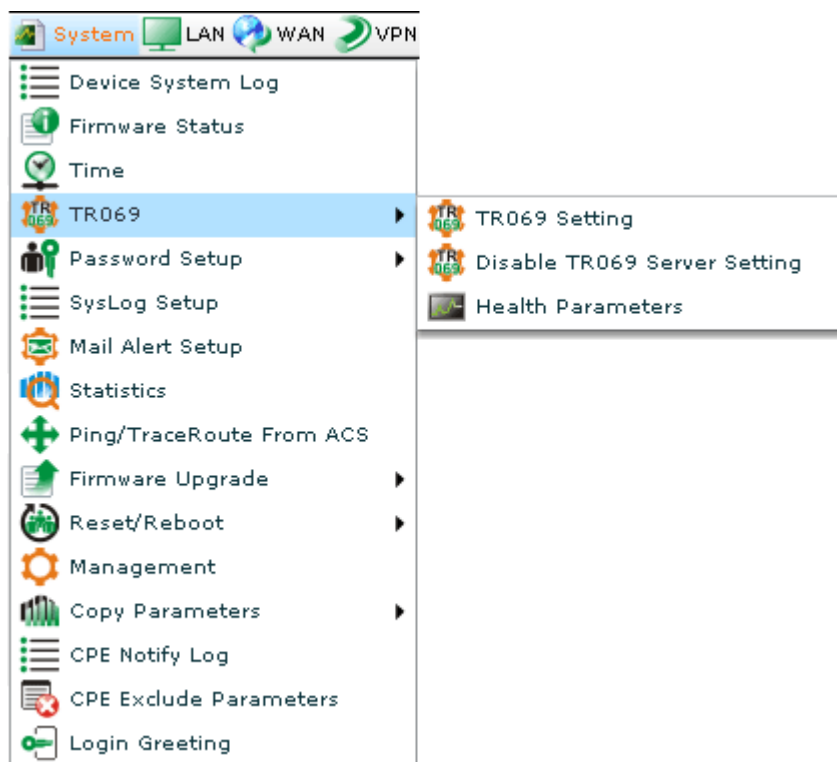
☐

Available parameters for this function include:

Items	Description
Index	Display the index number of the CPE in current network group.
NTP Server 1	Type the web site of the time server.
Current Local Time	Display current time.
Local Time Zone	Type the time zone where the router is located.
Local Time Zone Name	Select the time zone name where the router is located.
Daylight Savings Used.	Check the box to enable the daylight saving. Such feature is available for certain area.

Checking the TR-069 Settings for the Selected CPE

The administrator can view TR-069 settings for the selected CPE.



A screen of TR-069 status for the selected CPE will be shown as follows.

Index	1
ACS Server:URL	http://tim-2930.ath.cx/ACSServer/services/ACSServlet
ACS Server:Username	
ACS Server:Password	
CPE Client:URL	http://61.216.228.23:8069/cwm/CRN.html
CPE Client:Username	vigor
CPE Client:Password	
Periodic Inform:Enable	☒

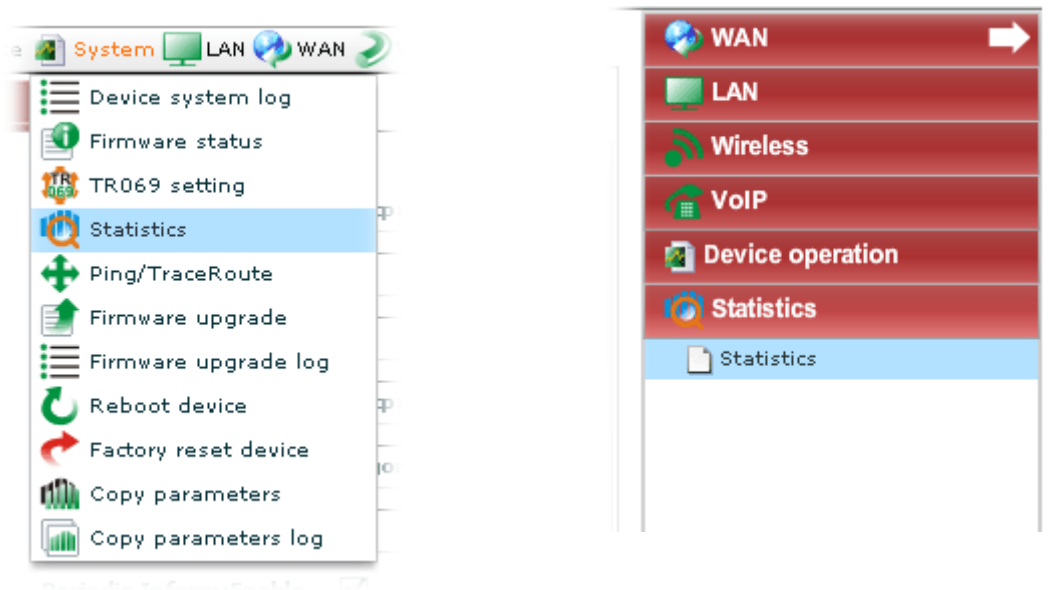
Available parameters for this function include:

Items	Description
Index	Display the index number of the CPE in current network group.
ACS Server: URL/ Username/ Password	The original URL /username/password of VigorACS SI will be displayed in these fields. You can modify the username and password if required.
CPE Client: URL/ Username/ Password	The original URL /username/password of the managed CPE will be displayed in these fields. It is not

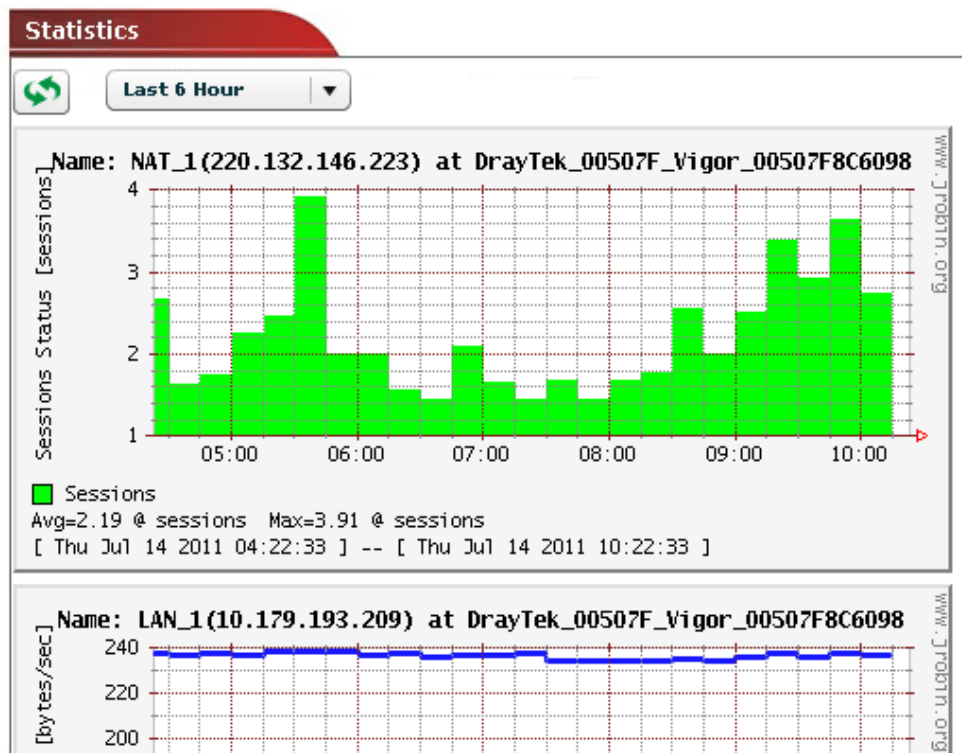
Items	Description
	necessary to change it.
Periodic Inform: Enable	The default setting is Enable (checked). Uncheck the box to close the mechanism of notification.
Periodic Inform: Interval Time	Please set interval time or schedule time for the router to send notification to CPE is Periodic Inform is enabled.
 Save parameter settings	Click this button to save the parameters settings.

Checking the Statistics for the Selected CPE

The administrator can view specified date of statistics for CPE(s).

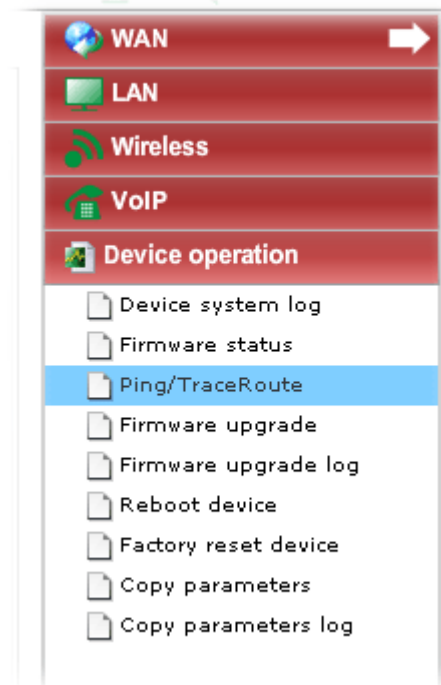
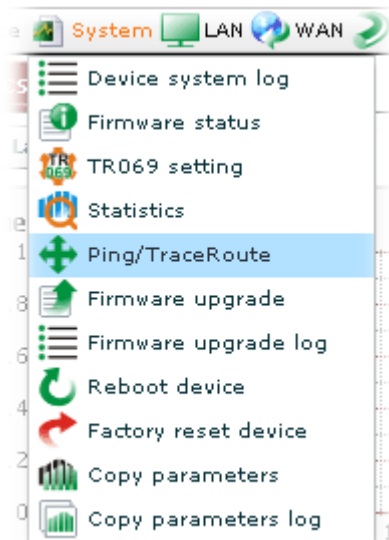


Please open **System>>Statistics**. Such page will display graphics for LAN statistics, WAN Statistics and VPN statistics of the selected CPE.



Pinging or Tracing the Route for the Selected CPE

To trace the route of a host or ping a specific host for the purpose of diagnosis, please open **System>>Ping/TraceRoute**.



This page allows you to specify a host for tracing route or ping.

Available parameters for this function include

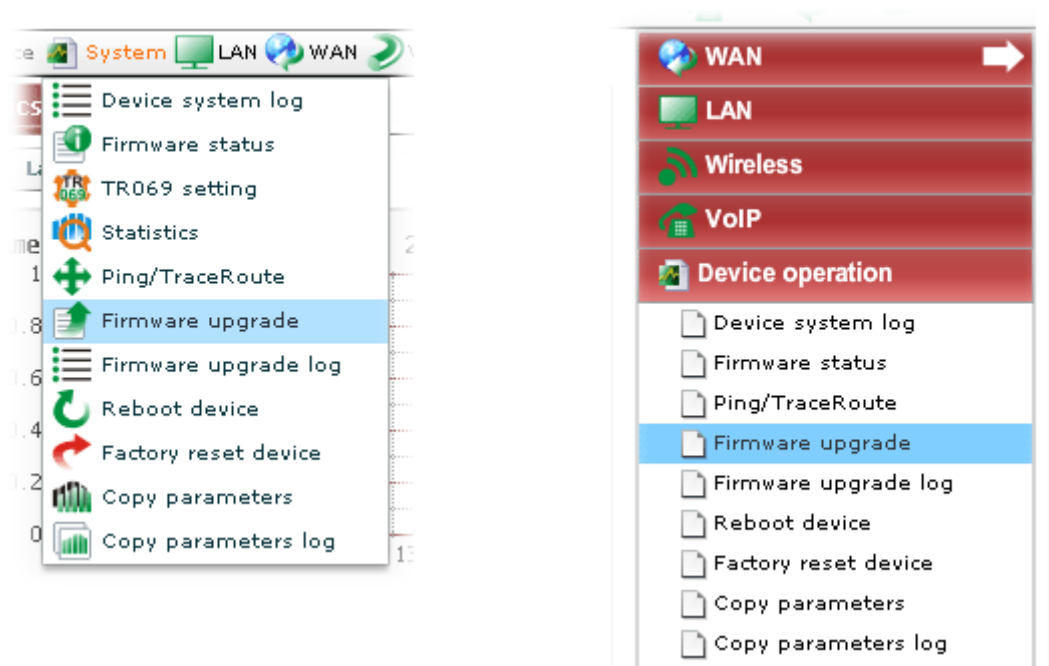
Items	Description
host	Type in the IP address of the Host/IP that you want to ping or trace.
Ping /TraceRoute	Start - Click this button to start the ping work. The result will be displayed on the screen. Stop – Click this button to stop the work of pining or tracing.

Upgrading the Firmware for the Selected CPE

Firmware Upgrade web pages allow you to do firmware upgrade for specified CPE device.

Note: If you want to upgrade the firmware for multiple devices at one time, please go to section **4.2.3** Firmware Upgrade for more detailed information.

Please open **System>>Firmware upgrade**.



A screen of firmware used by current selected CPE will be shown as follows.

[illegible]

Available parameters for this function include:

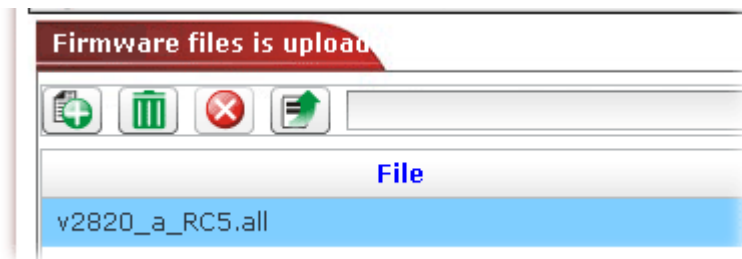
Items	Description
 Add file(s)	Click this button to add the newly firmware driver to VigorACS server. You have to download from DrayTek website first and then click this button for uploading.
 Remove files (s)	Click this button to remove the selected firmware file.
 Cancel upload	Click this button to terminate uploading procedure.
 Upgrade firmware with	Click this button to upgrade the firmware of selected

Items	Description
selected file	CPE. A confirmation dialog box will appear. Click Yes to continue the upgrading process, or click No to cancel this job.  Note: If you do not add any new file to VigorACS server, the confirmation dialog box will not appear.
File	Display current firmware on VigorACS.
Size	Display the file size for the firmware.
Path	Display the location of the firmware.

Performing the Firmware Update

To do the firmware upgrade, please:

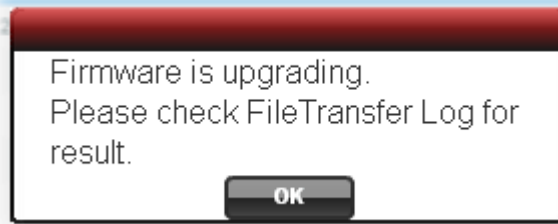
1. Upload the required firmware from vendor for the CPE that you want to upgrade to VigorACS server by clicking **Add** .
2. Choose suitable firmware for the CPE that you want to upgrade. You must specify which firmware to be applied in the CPE device requiring for firmware upgrade. The uploaded firmware will be displayed in the screen as shown below:



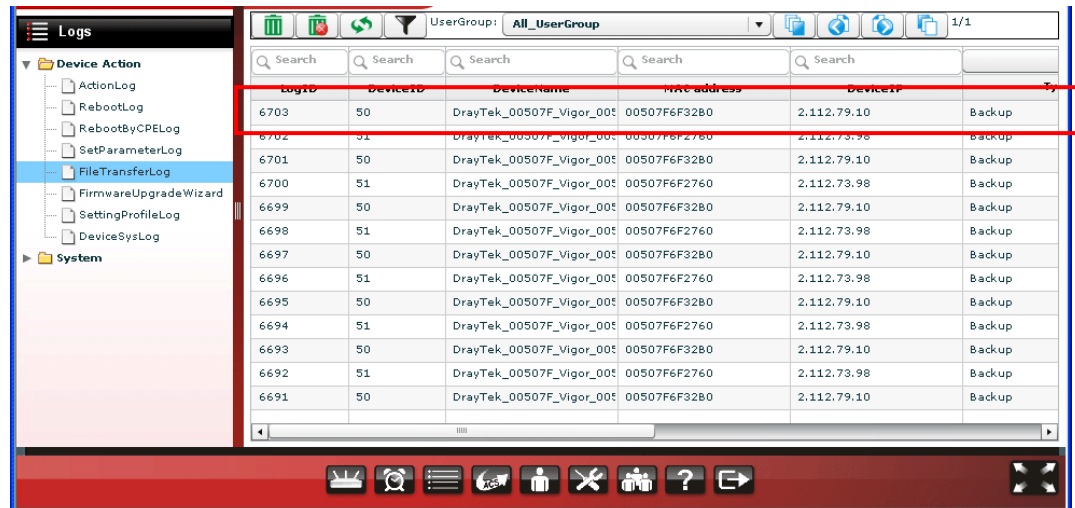
3. When the uploading process is finished, please choose the file and click  to upgrade the firmware with the selected file to the current selected CPE.



4. When the upgrading is completed, the new driver will be shown on the screen.

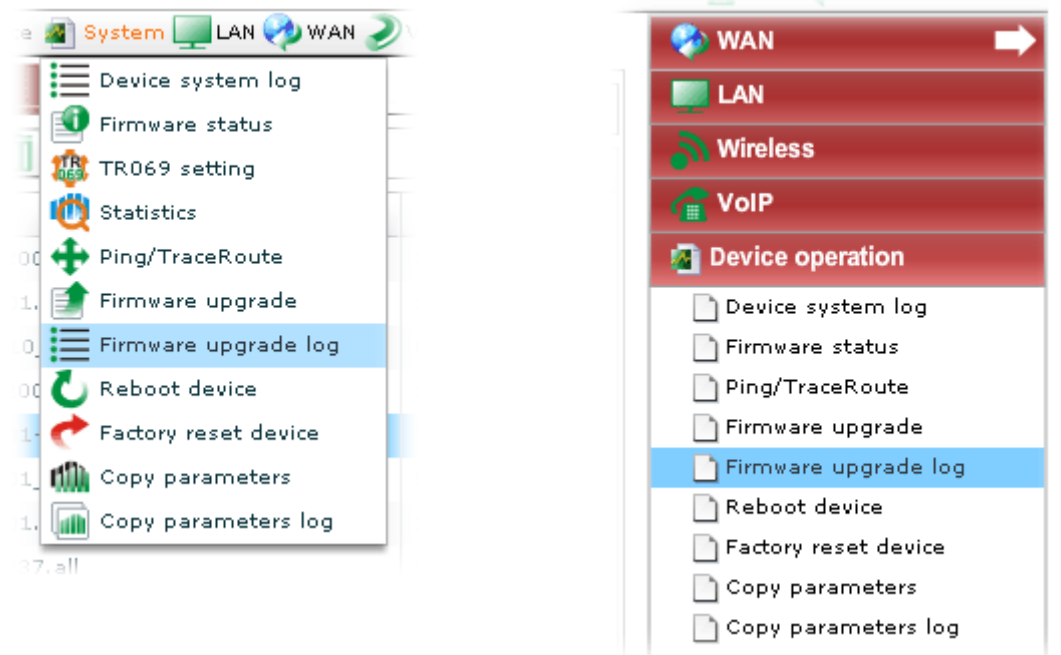


- Click **OK**. Open click the **Log** icon. Under **Device Action**, choose **FileTransferLog**. The new result will be added on the top.



Checking the Firmware Update Log

Please open **System>>Firmware upgrade log** to check the firmware update history.



A screen of firmware upgrade log current selected CPE will be shown as follows.

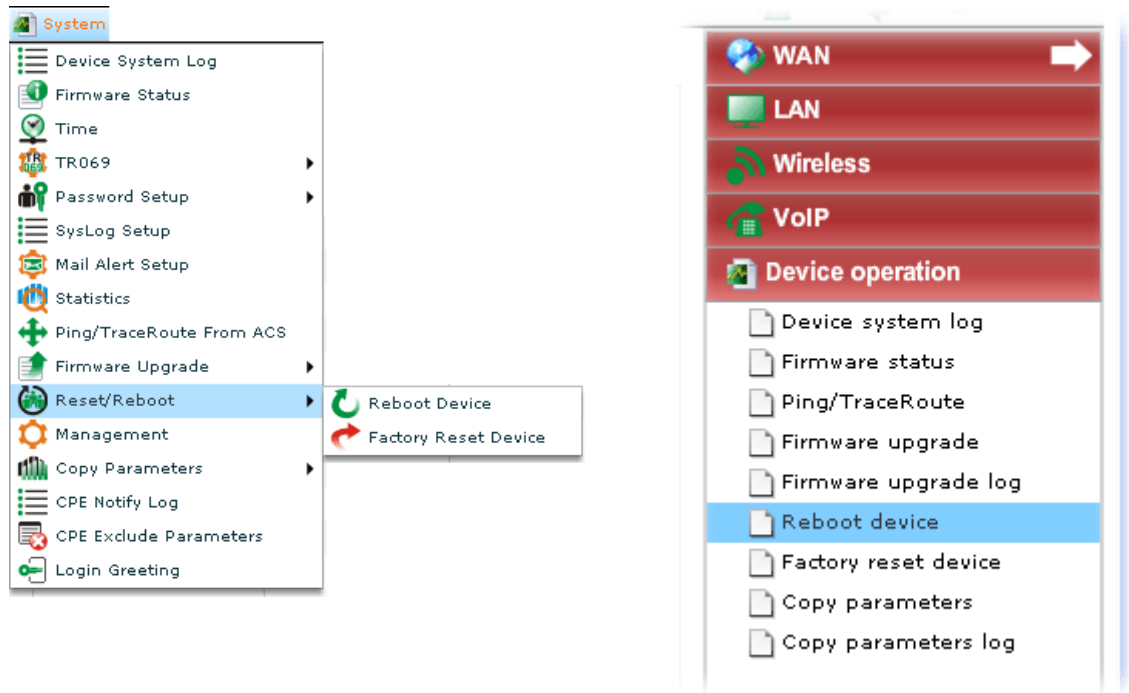


Available parameters for this function include:

Items	Description
 Delete	Click this button to delete a selected record.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 First	When there is more than one page for the firmware upgrade records in this user group, click this button to display the first page.
 Previous	When there is more than one page for the firmware upgrade records in this user group, click this button to display the previous page.
 Next	When there is more than one page for the firmware upgrade records in this user group, click this button to display the next page.
 Last	When there is more than one page for the firmware upgrade records in this user group, click this button to display the last page.
LogID	Display the arrangement number for each firmware upgrade record.
CommandKey	Display the key that VigorACS sends to CPE while performing download/upload job.
Status	Display if the firmware upgrade is successful or not.
Time	Display the time that firmware upgrade is performed.

Rebooting the Selected CPE

When you finish configuration, please open **System>>Reboot device** to make the new settings enabled.

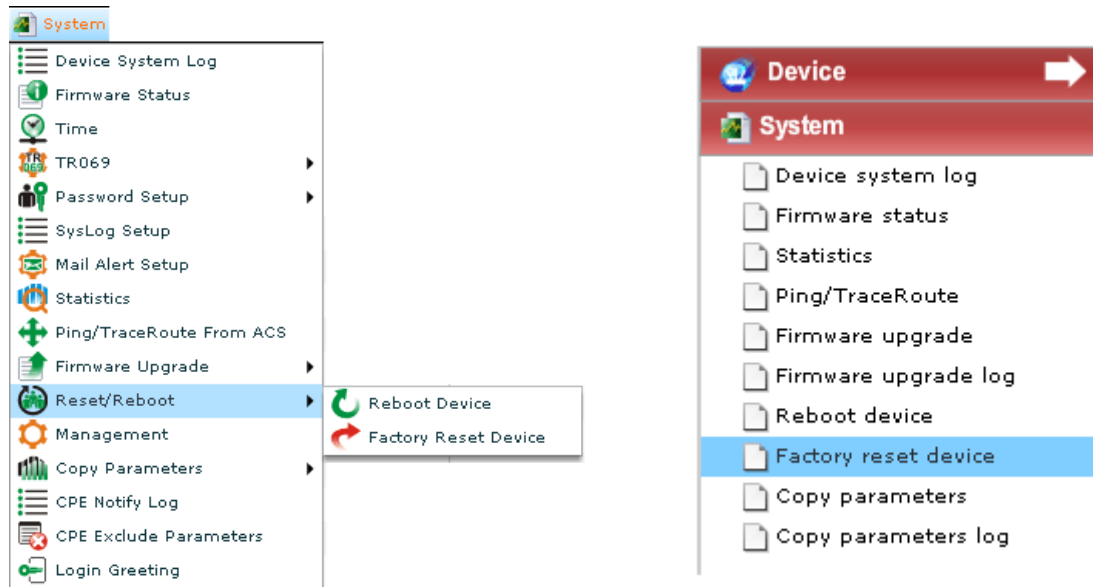


In the confirmation dialog box, click **Yes** to reboot the selected CPE or click **No** to cancel the reboot process.

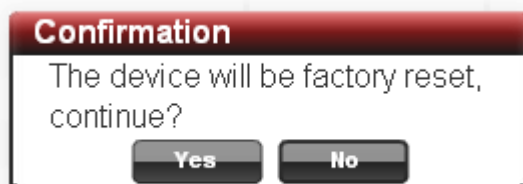


Returning to Factory Default Settings for Selected CPE

If, any time, you want to return to the factory default settings for the selected CPE, choose the device and click **System>>Factory reset device**.

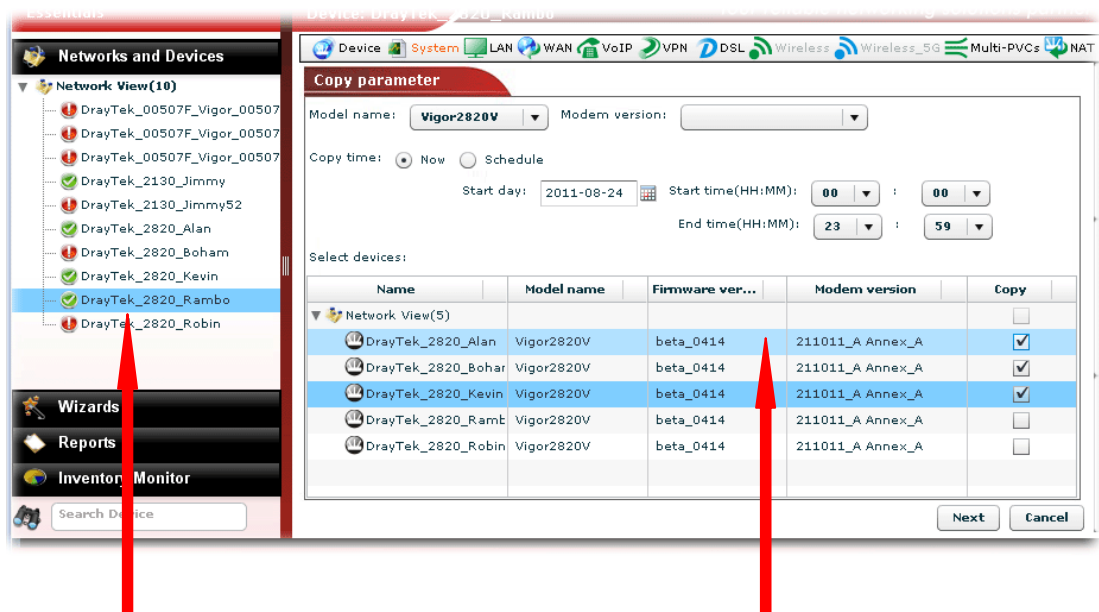


In the confirmation dialog box, click **Yes** to reset the selected CPE or click **No** to cancel the reset process.



Copying Parameters for Selected CPE

Such function allows you to copy parameters from the selected CPE to the devices specified in the of **Copy Parameter** page.

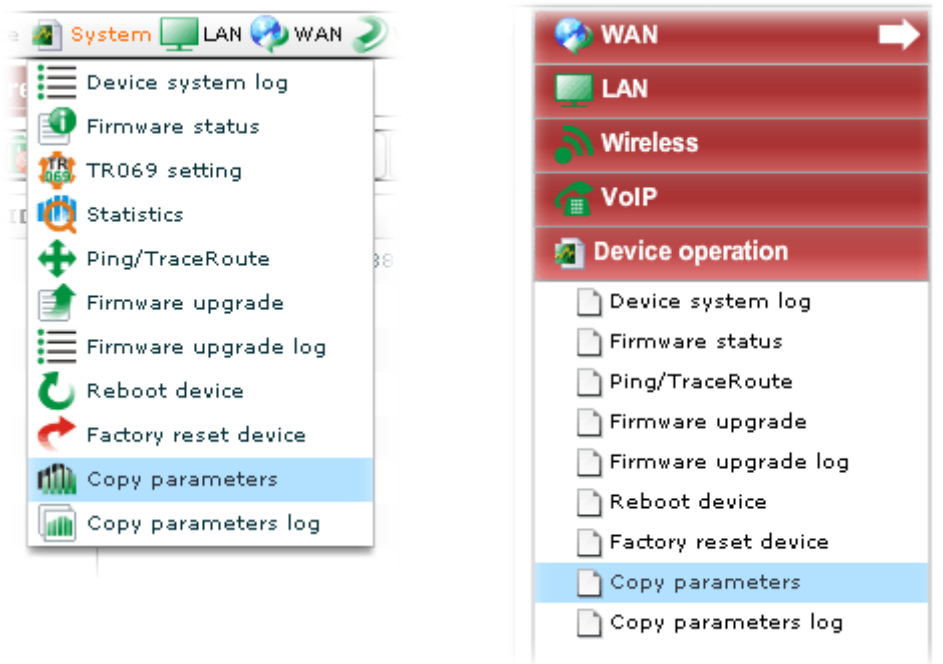


Selected CPE

Devices chosen for applying the parameters coming from the selected CPE

Follow the steps below to perform the operation of **Copy Parameter**.

1. Choose a device from **Networks and Devices**. Next, open **System>> Copying Parameters**.



- The following page will be shown. Set the corresponding settings and select devices from the tree view.

Available parameters for this function include:

Items	Description
Profile	Use the drop down list to choose a existing profile. Delete Profile – If the selected profile is not the one you want, click this button to remove the profile from VigorACS server. Save Profile – If you want to create a new profile for the job, check this box first. The, type a new name in the field of Name.
Model name	Use the drop down list to choose the model to perform the job.
Modem version	Some model might need to choose modem version. If yes, use the drop down list to select the one you need.
Copy time	Now – To perform the job immediately. Schedule – 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. 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 (CPE) that you want to do copying parameters.

Items	Description
Next	Click it to access into next web page. If you do not choose any CPE, such button will not be available.

- After specified the CPE to be applied with the parameters from the selected CPE, click **Next** to access into the following page. In this case, three devices are selected.

Copy parameter

LAN WAN NAT VoIP Multi-PVCs_General Multi-PVCs_ATMQoS Multi-PVCs_Port

Parameter	Parameter	Description
LAN IP Address	LAN IP Address	lan ip address
Subnet Mask	Subnet Mask	subnet mask
	DNS	dns
	DHCP Server Enable	dhcp server enab
	DHCP MinAddress	dhcp minimun ac
	DHCP MaxAddress	dhcp maximun a
	DHCP SubnetMask	dhcp subnet mas

Previous Next Cancel

- From the above page, choose the parameters that you want to copy. In this case, **LAN IP Address** and **Subnet Mask** are selected. Click **Next**. The parameters with values will be displayed on the screen.

Copy parameter

LAN

DrayTek_2820_Alan DrayTek_2820_Boham DrayTek_2820_Kevin

Index	Parameter	Value
1	LAN IP Address	192.168.30.1
1	Subnet Mask	255.255.255.0

Previous Finish Cancel

- Values will be displayed automatically. Such values are from the selected CPE under **Networks and Devices**. Note that the selected devices will be displayed with tabs respectively.

You can click every tab for every device for checking or modifying the parameters and values.
If you want to modify any value, simply move and click your mouse on the value field.

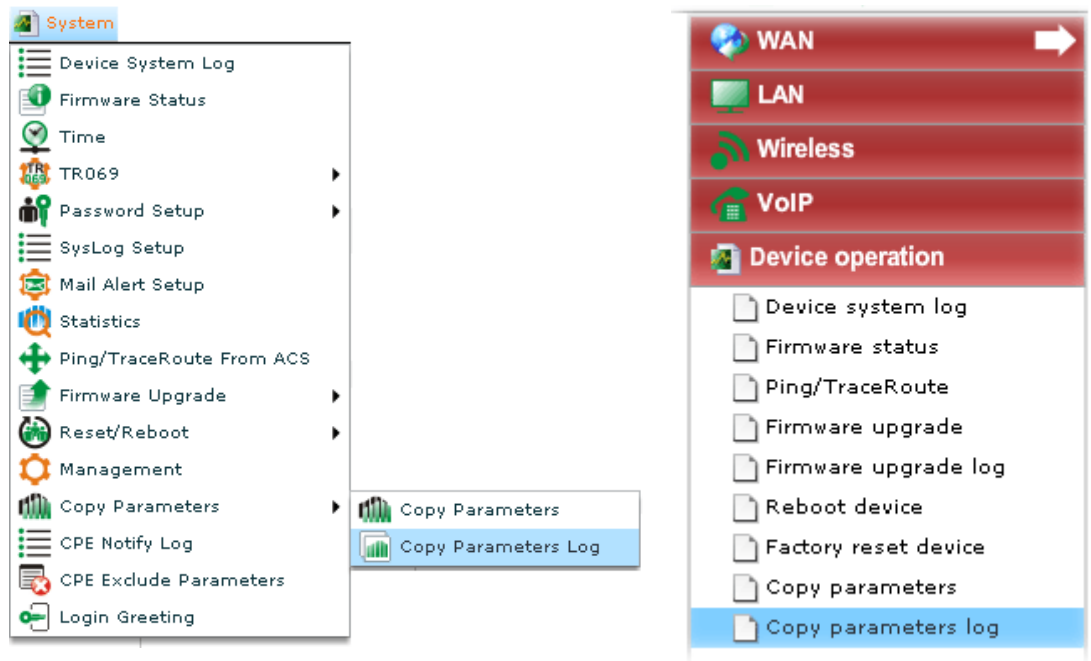
6. If you are satisfied with the settings, click **Finish**. Later, the following dialog will appear.



Checking the Copying Parameters Log

Only the operation that failed to copy parameters will be displayed in this page.

Please open **System>> Copying Parameters log** to check the log.

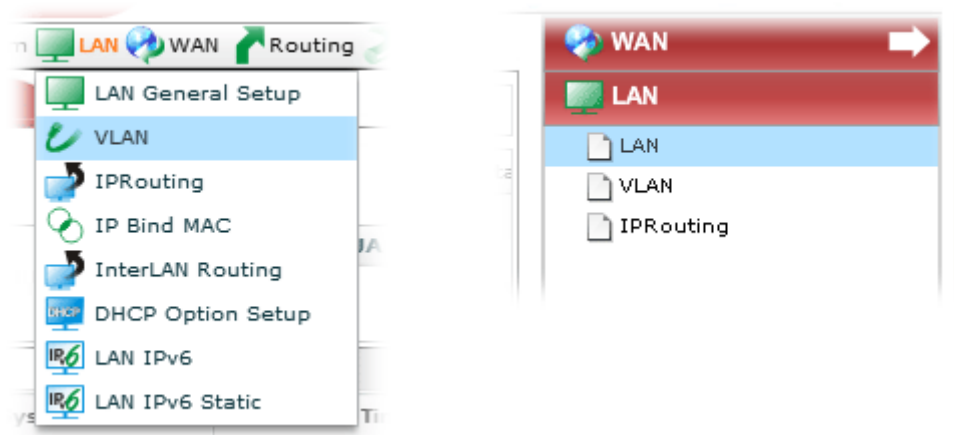


A screen of copy parameters log will be shown as follows:

VigorACS SI User's Guide

6.2.4 LAN Settings for the Selected CPE

The administrator can check and edit LAN settings for the selected **CPE/group** if it is necessary to modify. Simply open **LAN>>LAN**.



The following screen will appear with all of the LAN settings for the selected CPE/group.

Device: DrayTek_00507F_Vigor2960_00507FFF3900 Your reliable networking solutions partner

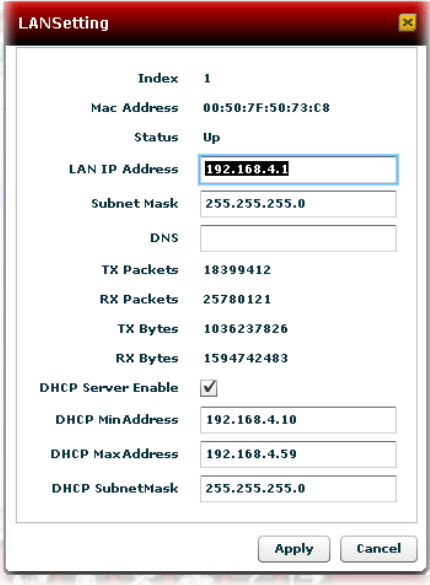
Device System LAN WAN VPN Firewall User NAT Applications

LAN

Index	MAC Address	Enable	VLAN ID	Status	LAN IP Address	Subnet Mask
1	00:50:7f:7c:bb:f1	true	10	Up	192.168.1.3	255.255.255.0
2	00:50:7f:7c:bb:f0	false	0	Disable	0.0.0.0	0.0.0.0
3	00:50:7f:7c:bb:f0	false	0	Disable	0.0.0.0	0.0.0.0
4	00:50:7f:7c:bb:f0	false	0	Disable	0.0.0.0	0.0.0.0
5	00:50:7f:7c:bb:f0	false	0	Disable	0.0.0.0	0.0.0.0
6	00:50:7f:7c:bb:f0	false	0	Disable	0.0.0.0	0.0.0.0
7	00:50:7f:ff:39:00	false	0	Disable	0.0.0.0	0.0.0.0
8	00:50:7f:ff:39:00	false	0	Disable	0.0.0.0	0.0.0.0
9	00:50:7f:ff:39:00	false	0	Disable	0.0.0.0	0.0.0.0

Available parameters for this function include:

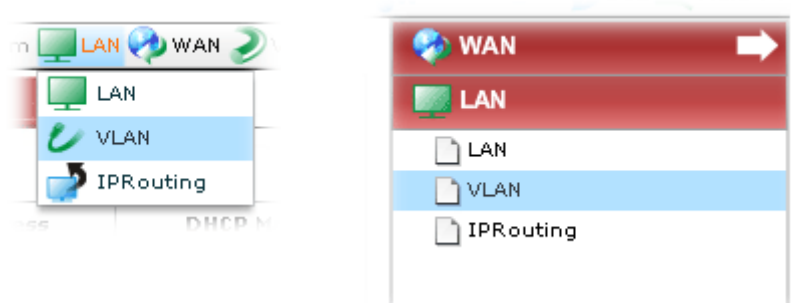
Items	Description
Index	Display the index number of the CPE in current network group.
Mac Address	Display the MAC address of the CPE.
Status	Display current connection status for the selected CPE. "Up" means the CPE is controlled by VigorACS and runs well. "Down" means there is no data transmission/receiving on CPE.
LAN IP Address	Display the IP address of the CPE. Such value can be edited if required.

Items	Description
Subnet Mask	Display the subnet mask of the selected CPE. Such value can be edited if required.
DNS	Display the IP address of DNS server. Such value can be edited if required.
TX/RX Packets	Display the packets of data transmission/receiving.
TX/RX Bytes	Display the size of data transmission/receiving.
DHCP Server Enable	If the DHCP server is enabled, the word of “true” will be shown here. Otherwise, the word of “false” will appear. Such value can be edited if required.
DHCP MinAddress	Display the starting IP address for the range of DHCP server. Such value can be edited if required.
DHCP MaxAddress	Display the ending IP address for the range of DHCP server. Such value can be edited if required.
DHCP SubnetMask	Display the subnet mask for the DHCP server. Such value can be edited if required.
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click this button to open a window for editing the parameters settings of the selected CPE. 

Checking and Editing VLAN Settings for the Selected CPE

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

Note: Only the CPE supporting VLAN feature can be modified by VigorACS. Otherwise, the system will display “Lack of required parameters”.



The following screen will appear with all of the VLAN settings for the selected CPE/group.

Device: 2920_A_00507FC93B24 *Your reliable networking solutions partner*

Device System LAN WAN VPN VoIP Wireless Wireless_5G DSL Multi-PV

LAN_VLAN

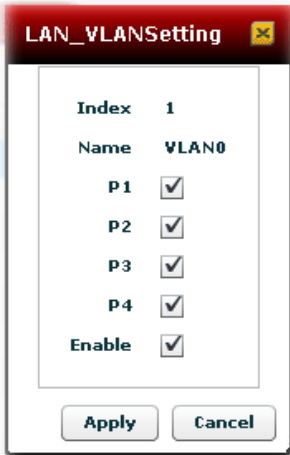
Save Cancel

Index	Name	P1	P2	P3
1	VLAN0	true	true	true
2	VLAN1	false	false	false
3	VLAN2	false	false	false
4	VLAN3	false	false	false

W L W V D S

Available parameters for this function include:

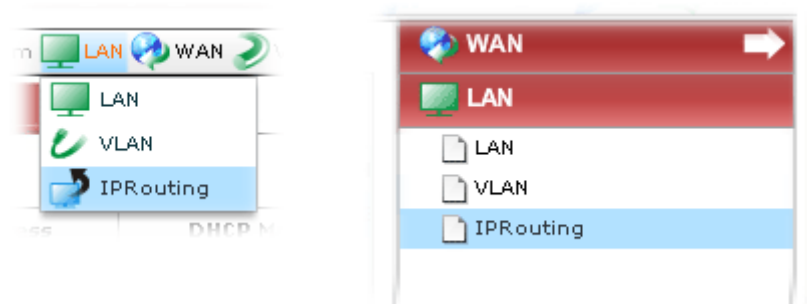
Items	Description
Index	Display the index number of the CPE in current network group.
Name	Display the name of the VLAN group.
P1 – P3	If the LAN port is selected for such VLAN, the corresponding field will display “true”. Otherwise, “false” will be display to indicate such port is not selected for the VLAN group.
 Save parameter setting	Click this button to save the parameters settings.

Items	Description
 Edit	Click this button to open a window for editing the parameters settings of the selected VLAN group. 

Checking and Editing IP Routing Settings for the Selected CPE

If you want to change IP route settings for specified CPE(s), please choose the device. And, open **LAN >>IPRouting**.

Note: Only the CPE supporting IP routing feature can be modified by VigorACS. Otherwise, the system will display “Lack of required parameters”.



The following screen will appear with all of the VLAN settings for the selected CPE/group.

Device: 2920_A_00507FC93B24 Your reliable networking solutions partner

Device System LAN WAN VPN VoIP Wireless Wireless_5G DSL Multi-PVCs Bandw

LAN_IPRouting

Index

1

For IP Routing Usage

☒

IP Address

192.168.99.1

Subnet Mask

255.255.255.0

DHCP:Start IP Address

192.168.99.10

DHCP:IP Pool Counts

5

DHCP:Use LAN Port

☐

DHCP:Use LAN Port P1

☐

DHCP:Use LAN Port P2

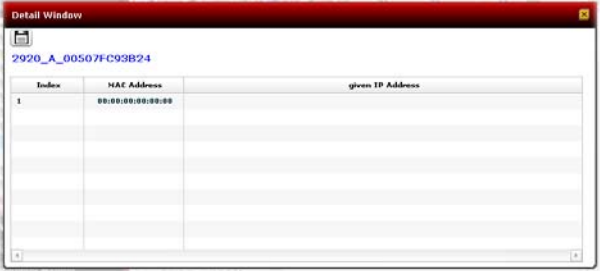
☒

DHCP:Use MAC Address

☐

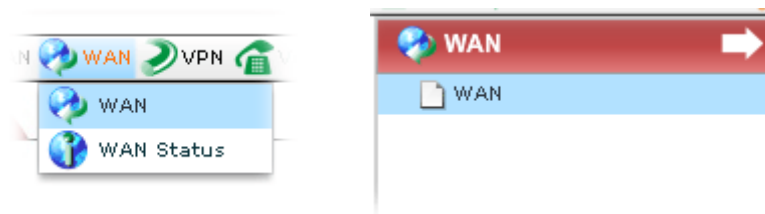
Available parameters for this function include:

Items	Description
Index	Display the index number of the CPE in current network group.
For IP Routing Usage	Check the box to enable such function.
IP Address	The original setting will be shown here. If you want to change it, simply re-type the IP address.
Subnet Mask	The original setting will be shown here. If you want to change it, simply re-type the subnet mask.
DHCP:Start IP Address	Such field defines the starting IP address of DHCP server. If you want to change it, simply re-type the IP address.
DHCP:IP Pool Counts	The original count number will be shown here. If you want to change the total number for IP assignment, simply re-type the value in this field.
DHCP:Use LAN Port/ DHCP:Use LAN Port P1/ DHCP :Use LAN Port P2	Check (or uncheck) the box to change the port usage status.
DHCP :Use MAC Address	Check (or uncheck) the box to use the MAC address for IP routing.
 Save parameter setting	Click this button to save the parameters settings.
 Detail	Such button will bring up another dialog and display detailed information for the selected CPE.

Items	Description
	

6.2.5 WAN Settings for the Selected 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 **WAN >> WAN**.



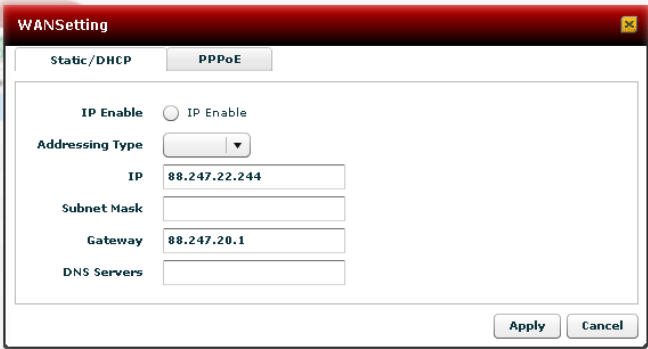
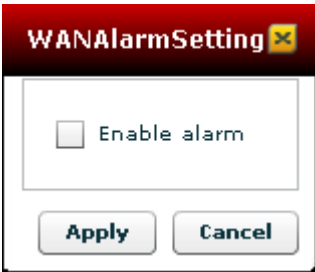
The following screen will appear with all of the WAN settings for the selected CPE/group.



Available parameters for this function include:

Items	Description
Alarm Enable	Display the activation status for alarm mechanism.
Index	Display the index number of the CPE in current network group.
Mac Address	Display the MAC address of the CPE.
Up Time	Display the up time for the connection of the CPE.

Items	Description
Connection Mode	Display the connection mode that such CPE used to access Internet.
IP Enable	Choose True or False to enable/disable IP address on Ethernet port.
Addressing Type	Display the connection type that the CPE used. Available types for such CPE can be seen from the drop down list. You can change the connection type if required.
IP	Display the WAN IP address of the CPE. Such value can be edited if required.
Subnet Mask	Display the subnet mask for the CPE.
Gateway	Display the gateway of the CPE. Such value can be edited if required.
DNS Servers	Display the DNS server used for the CPE.
PPP Enable	Choose True or False to enable/disable PPP connection.
PPP User Name	Display the user name of PPPoE connection.
PPP Password	Display the password of PPPoE connection.
Modem Type	Display the modem type (e.g., DSL, Broadband, etc..) of the CPE.
Link Status	Display current connection status for the selected CPE. "Up" means the CPE is controlled by VigorACS and runs well. "Down" means there is no data transmission/receiving on CPE.
Tx/Rx Bytes	Display the size of data transmission/receiving.
Tx/Rx Packets	Display the packets of data transmission/receiving.
 Save parameter settings	Click this button to save the parameters settings.

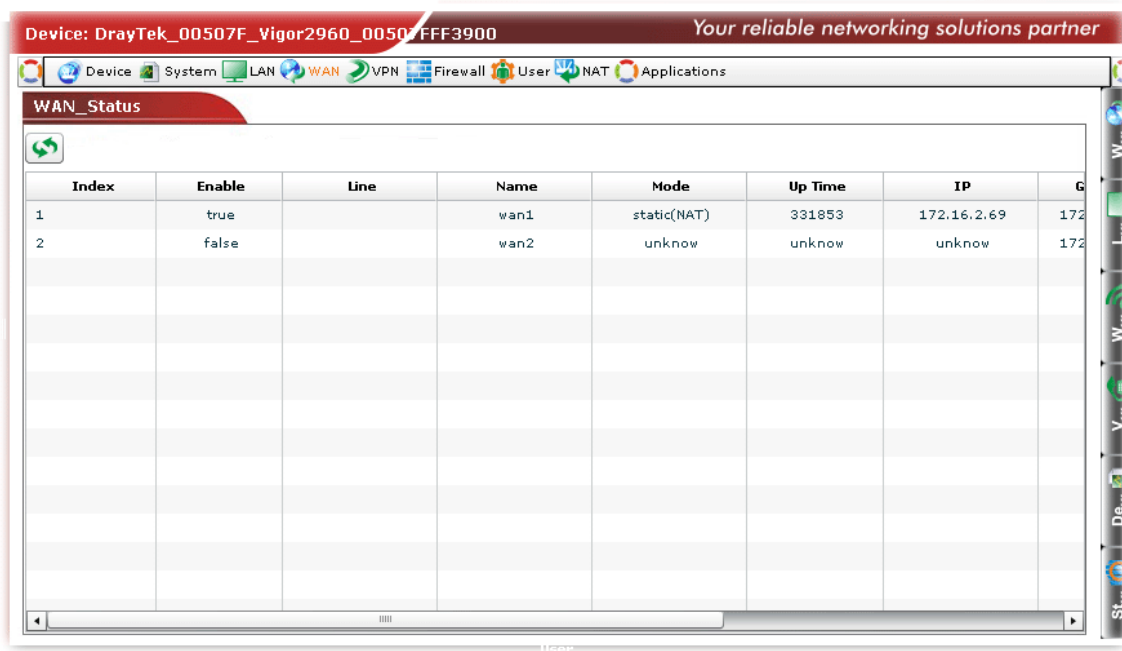
Items	Description
 Edit	Click this button to open a window for editing the parameters settings of the selected CPE.  
 Alarm	Click this button to enable/disable the Alarm mechanism for such WAN. 

Checking WAN Status for the Selected CPE

WAN settings relate to access Internet for CPEs. For checking the status, open **WAN >> WAN Status**.



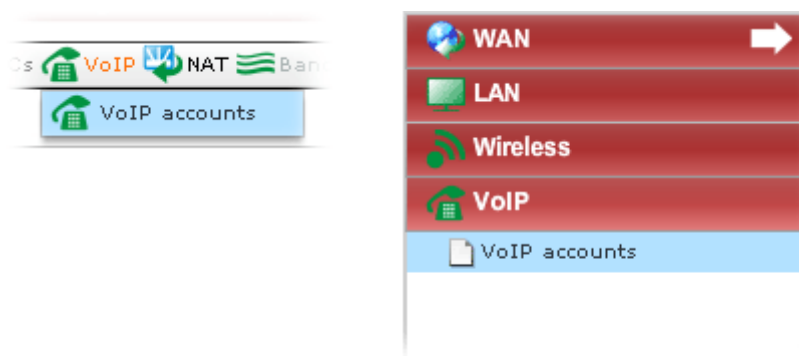
The following screen will appear with all of the WAN settings for the selected CPE/group.



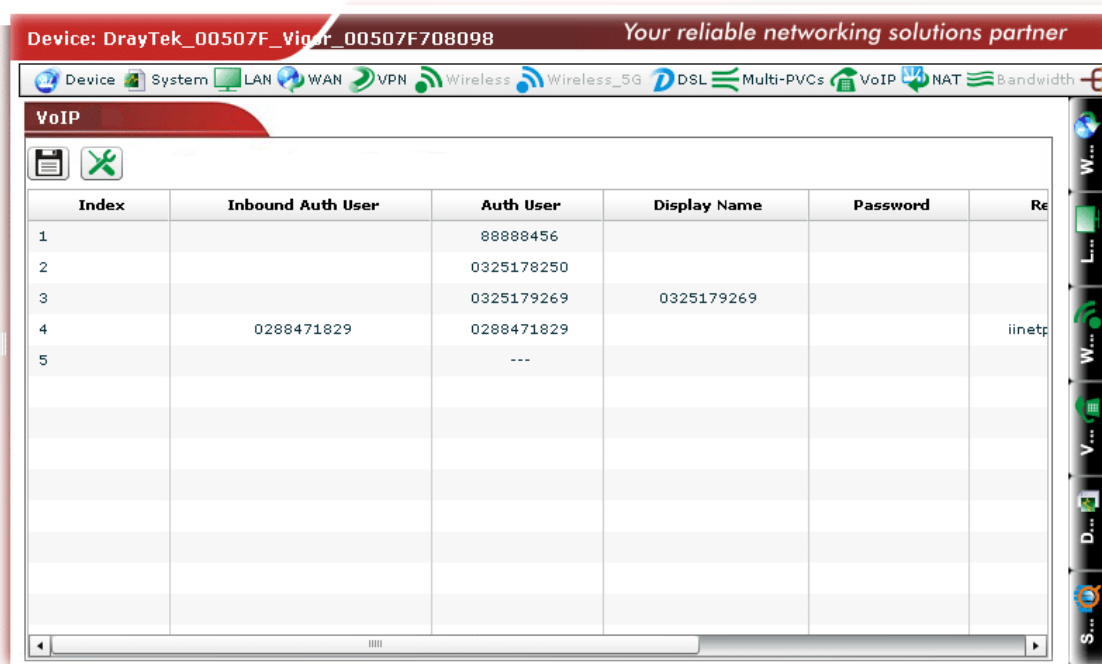
6.2.6 VoIP Settings for the Selected CPE

This page allows you to set VoIP configuration which maps with SIP accounts of the selected device.

Note: If the selected CPE doesn't support VoIP function, such menu will be invalid.



Click **VoIP>>VoIP accounts** to open the following screen.



Available settings for such feature will be shown as follows:

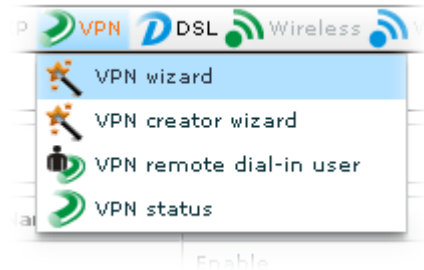
Items	Description
Index	Display the index number of the CPE in current network group.
Inbound Auth User	Display the authentication ID which is specified by the web configuration page of the selected device.
Auth User	Display the account name/account number which is specified by the web configuration page of the selected device.
Display Name	Display the display name which is specified by the web configuration page of the selected device.
Password	Display the password which is specified by the web configuration page of the selected device.
Registrar Server	Display the IP address or domain name of the registrar server for such account.
Proxy Server	Display the IP address or domain name of the proxy server.
Register Via	Display the registration interface for such account.
Ring Port	Display the ring port for such VoIP account.
 Save parameter setting	Click this button to save the parameters settings.

Items	Description
Edit	Click this button to open a window for editing the parameters settings of the selected account Inbound Auth User - Type the authentication ID which is specified by the web configuration page of the selected device. Auth User - Type the account name/account number which is specified by the web configuration page of the selected device. Display Name - Type the display name which is specified by the web configuration page of the selected device. Password –Type the password which is specified by the web configuration page of the selected device. Registrar Server –Type the IP address or domain name of the registrar server for such account. Proxy Server –Type the IP address or domain name of the proxy server. Register Via –Use the drop down list to choose the registration interface (including None, Auto, WAN1, WAN2, LAN_VPN, PVC) for such account. Ring Port - Choose the ring port (including Phone1, Phone2, Phone1, Phone2) for such VoIP account. Apply – Click it to save the settings. Cancel – Click it to exit the screen without saving any settings.

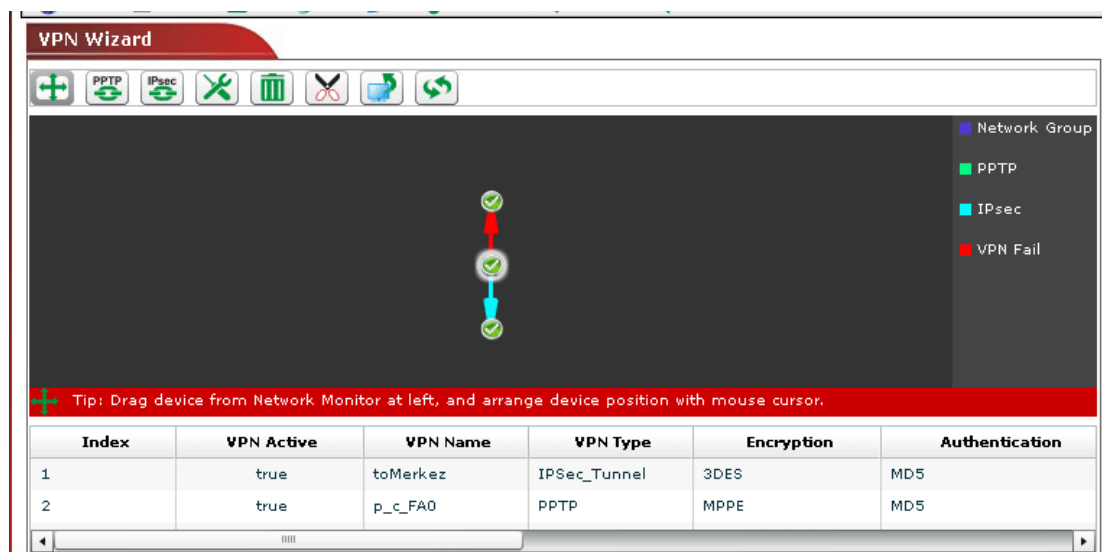
6.2.7 VPN Settings for the Selected CPE

VPN Wizard - Creating VPN Connection between Two CPEs

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

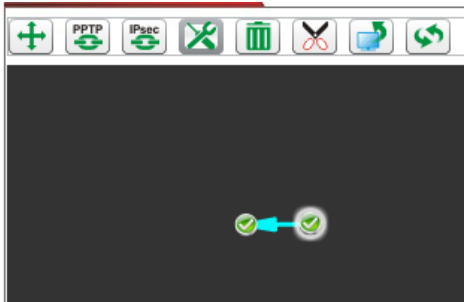
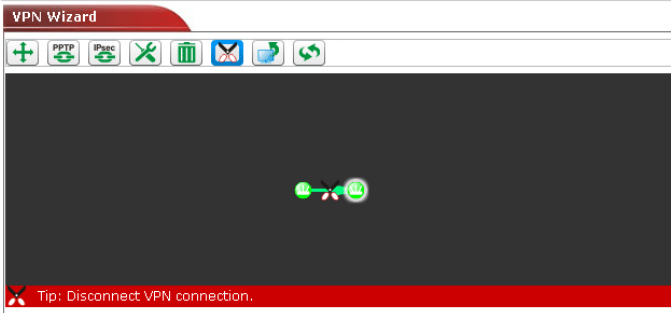


Open **VPN>>VPN wizard**, the following screen will appear.



Available settings for such feature will be shown as follows:

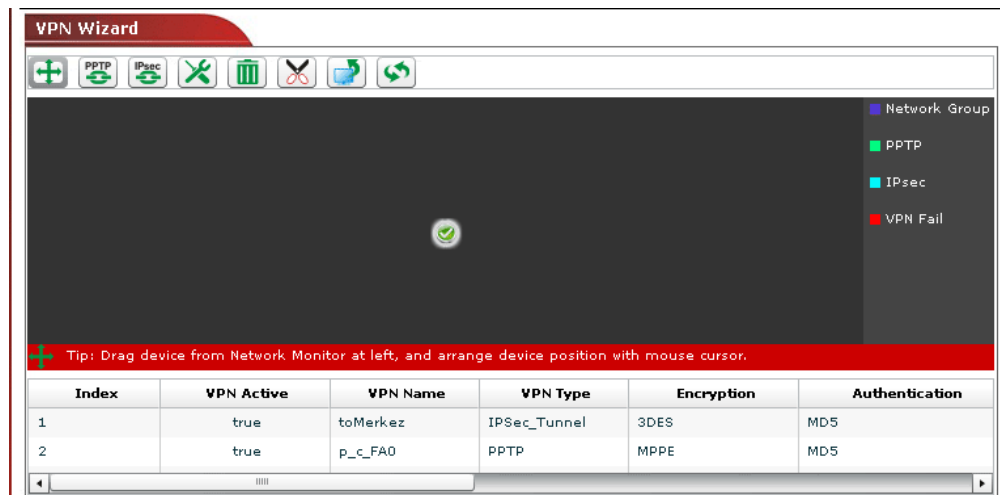
Items	Description
 Add device...	Click this button to add a device for building VPN connection. If you do not click this button first, you can not drag any device from Network View .
 PPTP	To build a quick VPN connection with PPTP , simply click this button first and then drag the device from Network View to the black area.
 IPsec	To build a quick VPN connection with IPsec , simply click this button first and then drag the device from Network View to the black area.
 Advance Connection	To build a VPN connection with detailed configuration, click Advance Connection tool. For detailed information, please refer to the section of Building an Advanced VPN Connection later.

Items	Description
	
 Remove the device....	Click this button to remove the selected device without VPN connection.
 Disconnect	To disconnect a VPN connection, Click this button and move the mouse cursor to the VPN connection that you want to disconnect. Notice that the mouse cursor will be transformed into a scissor.  If you press Enter, a confirmation dialog will appear. You can click Yes and the VPN connection will be cut off immediately. 
 Change LAN IP Setting	If there is LAN IP segment conflict in VPN connection, please select that device and click this button to change LAN IP setting.
 Refresh VPN Wizard	Click this button to reconnect both devices.

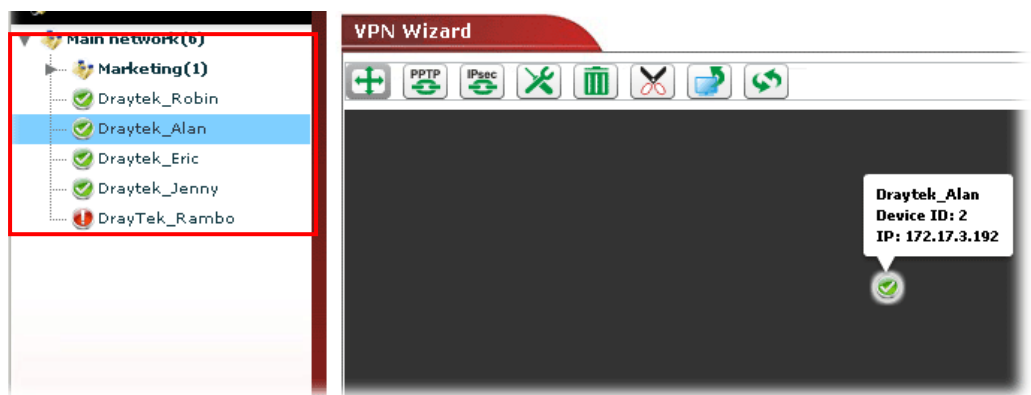
- **Building a Simple VPN Connection**

Please follow the steps to build a simple VPN connection.

10. Open **VPN>>VPN wizard**. You will get the following page. Selected CPE will be displayed in the middle of the screen. There is no VPN connection existed.



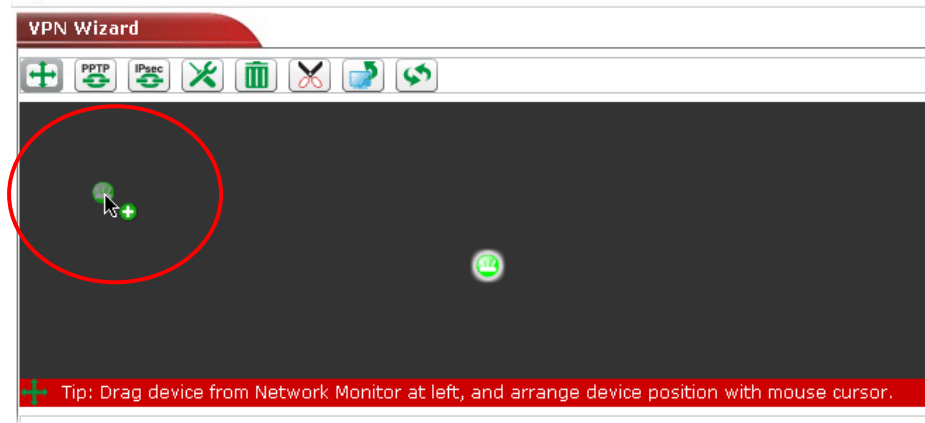
11. Open the **Networks and Devices** and expand the group folder as the following:



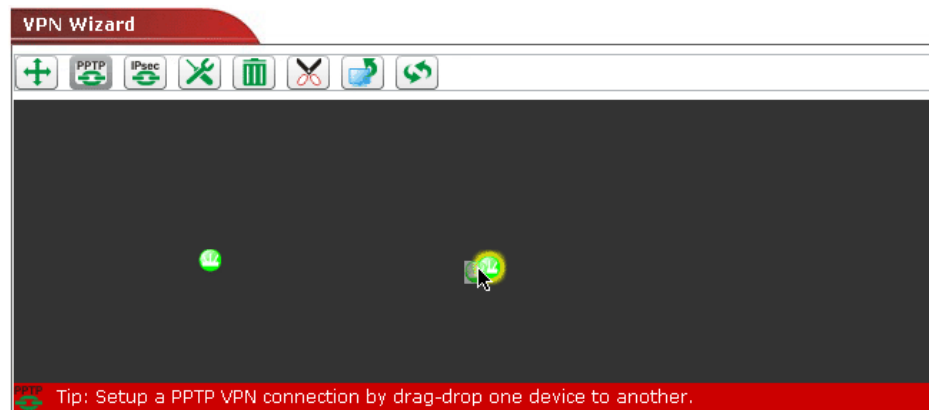
12. Click the **Add device** button.



13. Choose one device from the **Networks and Devices** that you want to build a VPN connection with the current selected device. **Drag** it from the **Networks and Devices** to the page of **Device Details**.



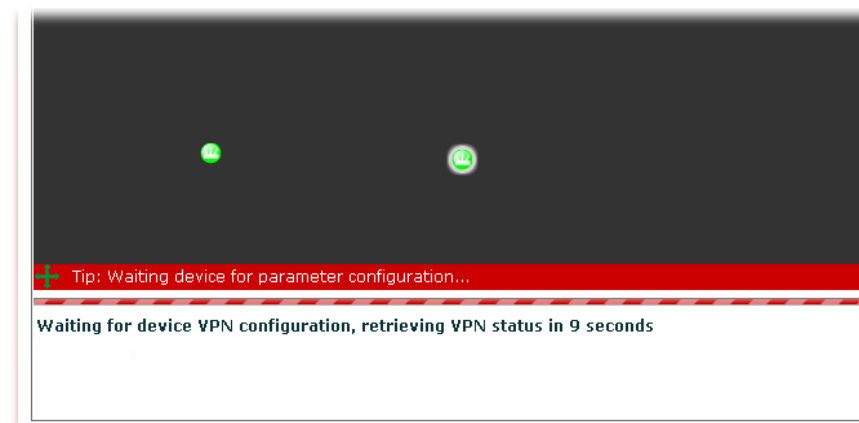
14. If you want to build VPN connection through PPTP or IPSec, click the PPTP or IPSec icon first. Then, drag one of the devices to the other.



15. A confirmation dialog will appear. Click **Yes**.



16. Now, the system will configure parameters automatically between these two devices. Please wait patiently.

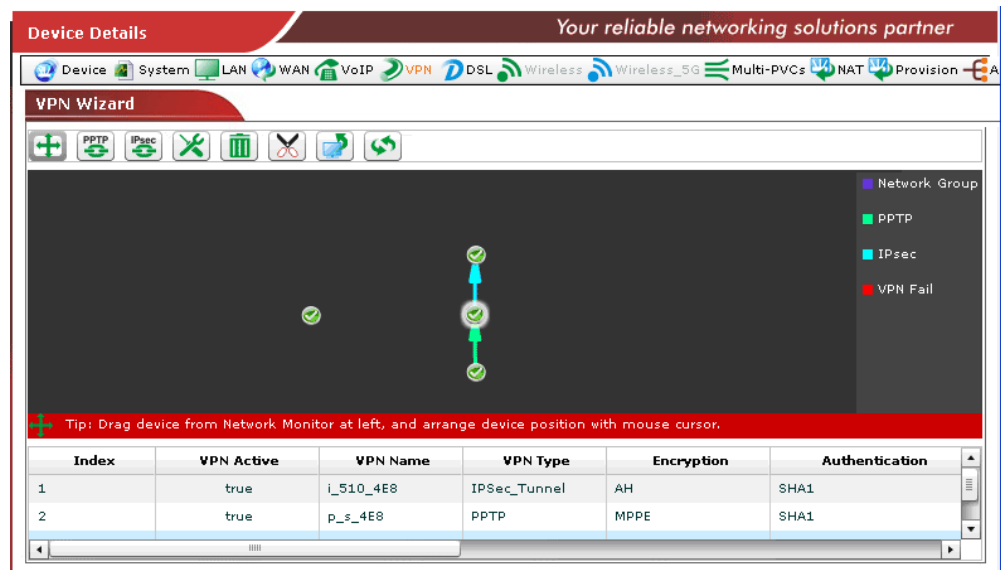


17. When the VPN connection has been done, an arrow will appear and indicate the direction between these two devices. VPN connection information also will be displayed below the black area.
18. Different colors for arrows represent different protocols used in VPN connections. Green means PPTP mode; blue means IPsec mode; and red means the VPN connection is failed.

- **Building an Advanced VPN Connection**

Please follow the steps to build an advanced VPN connection.

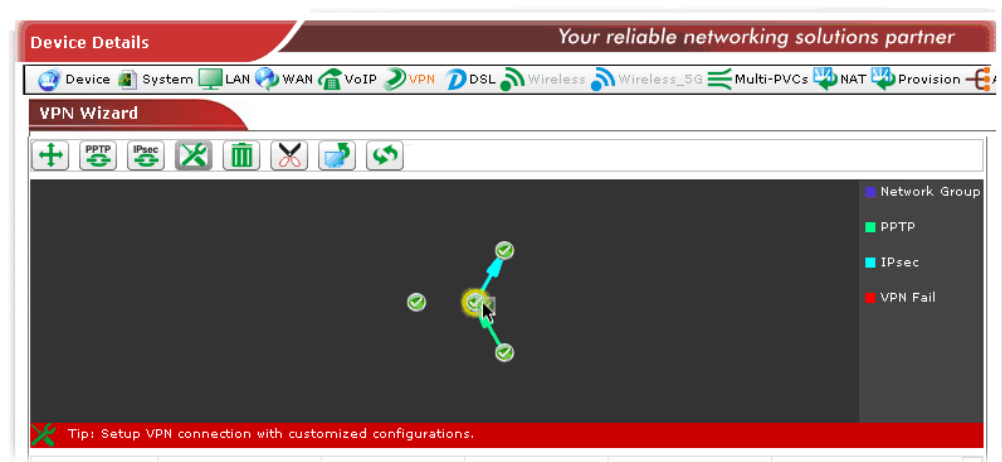
1. Open **VPN>>VPN wizard**. You will get the following page. Selected CPE will be displayed in the middle of the screen. No other device connects to it.



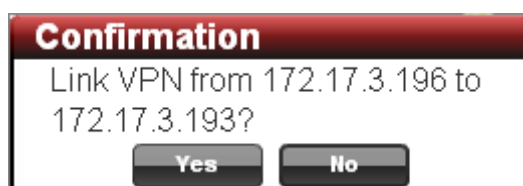
2. Click the **Advance connection** button.



3. To build an advanced VPN connection through PPTP or IPsec, drag the selected CPE s to the one you want to build.



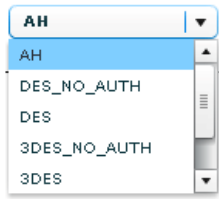
4. A confirmation dialog will appear. Click **Yes**.



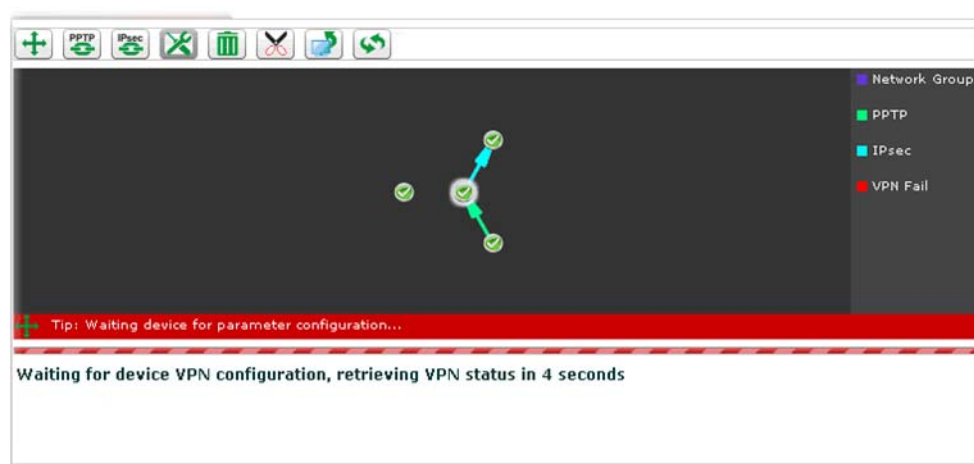
5. A dialog appears as follows. Please set the corresponding parameters and settings manually and click **Connect**.

Available settings for such feature will be shown as follows:

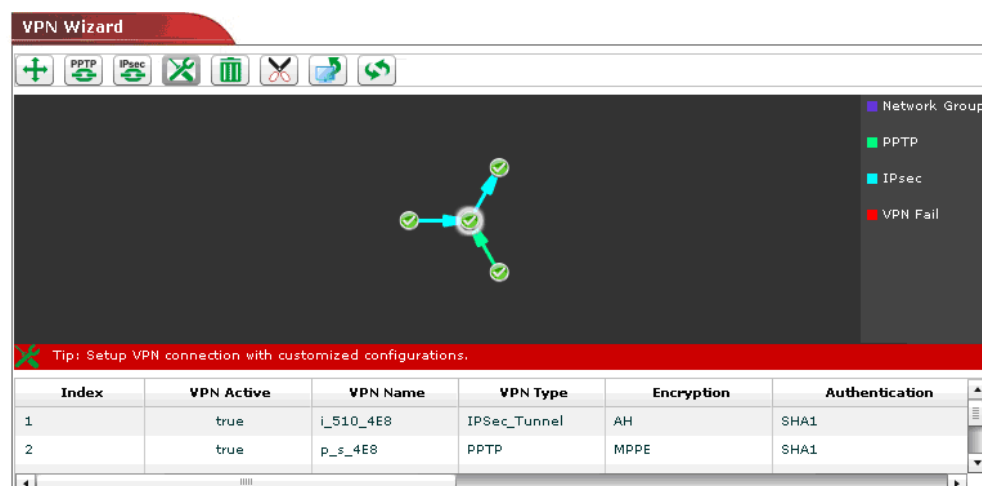
Items	Description
Dial Type	Choose PPTP or IPsec. Relational settings based on the type you choose will be displayed below
VPN Connection Through	Use the drop down list to choose one way for VPN connection. VPN Connection Through: WAN1_First WAN1_First WAN1_Only WAN2_First WAN2_Only
PPTP	When you click PPTP as Dial Type, you have to fill the username and password, choose PPP Authentication and specify if VJ compression should be on or off for such connection.

Items	Description
IPSec	When you click IPSec as Dial Type, you have to type IKE Pre-Shared Key, and choose IPSec Security Method for such connection. IPSec Security Method: 

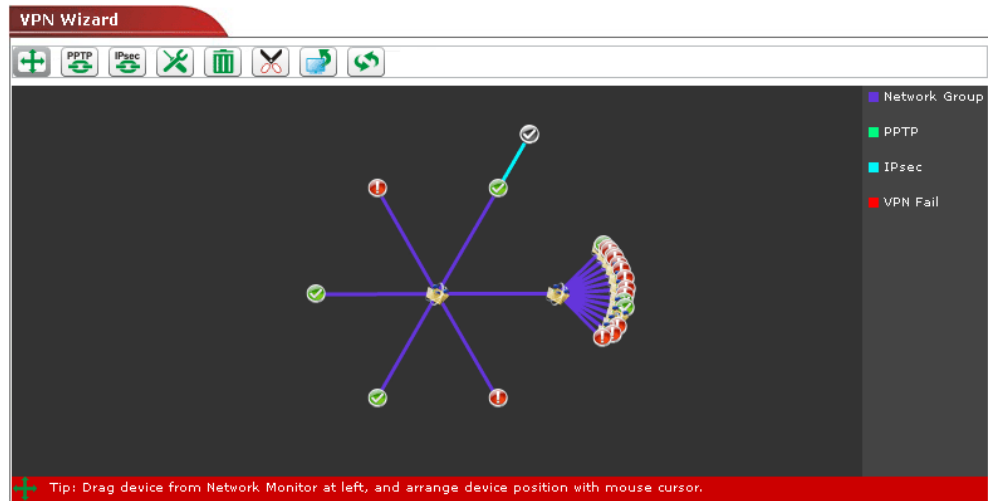
- Now, the system will configure parameters automatically between these two devices. Please wait patiently.



- When the VPN connection has been done, an arrow will appear and indicate the direction between these two devices. VPN connection information also will be displayed below the black area.



Note: 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.



- **Changing LAN IP Setting**

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  **Change LAN IP Setting**. The following dialog will appear.

LAN IP Setting: Draytek_Robin
✕

Device ID: 1

Device IP: 172.17.3.191

LAN IP:

Subnet mask:

DHCP server enable: ☒

Start IP:

End IP:

Gateway:

Force DNS manual setting: ☐

Primary IP:

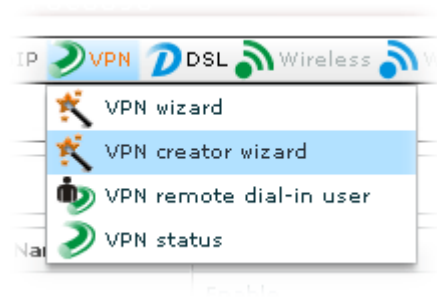
Available settings for such feature will be shown as follows:

Items	Description
Device ID	Display the identification number of the selected device (CPE).
Device IP	Display the WAN IP address of the selected device (CPE).

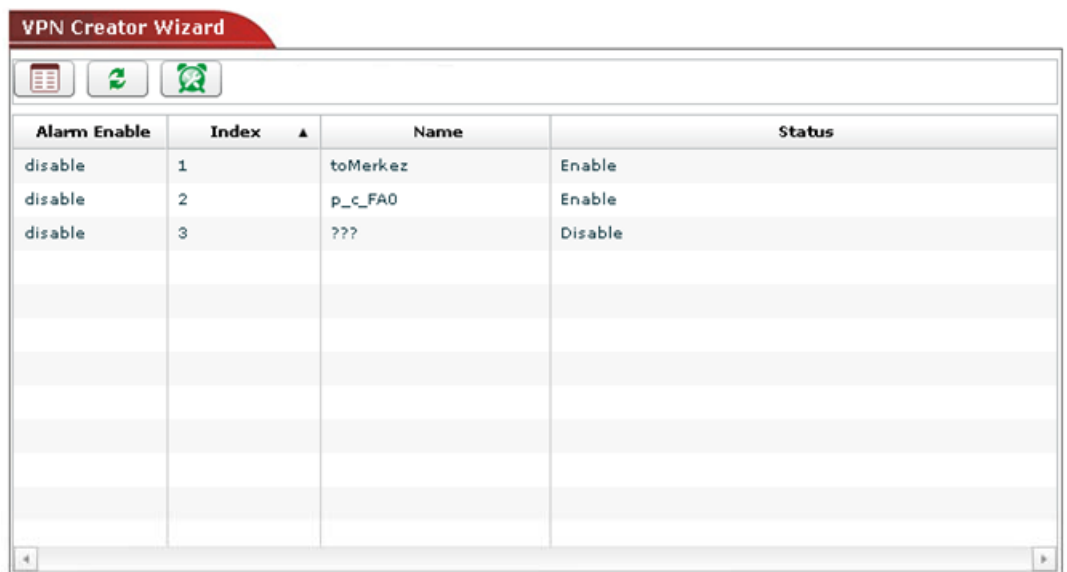
Items	Description
LAN IP	Display the LAN IP address of the selected device. You can change it with another IP address to avoid the conflict.
Subnet mask	Display the subnet mask of the selected device. You can change it if required.
DHCP server enable	DHCP server has been activated. If you uncheck this 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.
Force DNS manual setting	Check this box to force Vigor router using DNS servers in this page instead of DNS servers given by the Internet access server (PPPoE, PPTP, L2TP or DHCP server).
Primary IP (DNS)	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.
Change LAN IP	When you finish the modification, click this button to save the configuration and exit this dialog.

VPN Creator Wizard - Creating LAN to LAN VPN Connection

To create a LAN to LAN connection for the selected CPE, choose **VPN creator wizard**. You can create up to 32 profiles for such CPE.

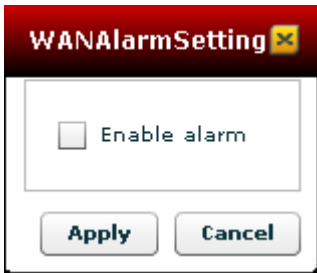


Open **VPN>>VPN creator wizard**, the following screen will appear.



Available settings for such feature will be shown as follows:

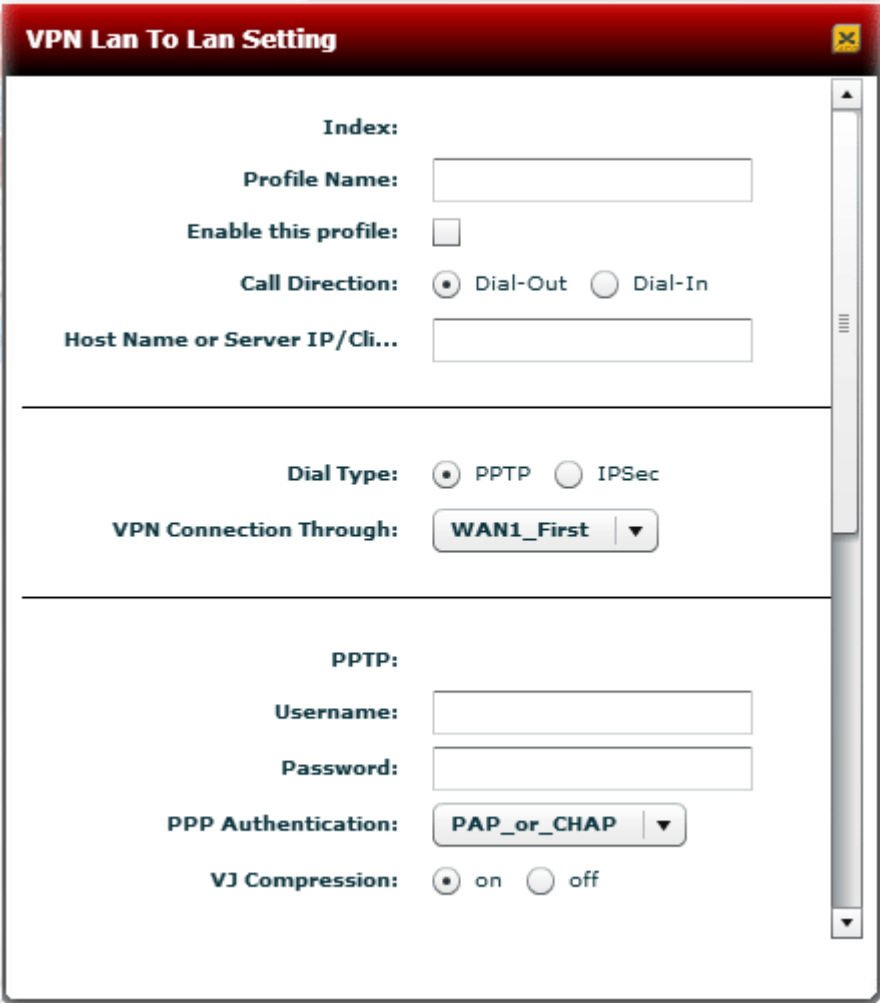
Items	Description
Alarm Enable	Display the activation status for alarm mechanism.
Index	VigorACS SI allows you to create up to 32 index numbers (profiles).
Name	Display the name of the LAN-to-LAN profile.
Status	Display if such profile is enabled or disabled for such CPE.
 Detail	Click this button to edit the selected VPN profile or click it to add a new VPN profile.
 Refresh	Click this button to refresh current page.
 Alarm	Click this button to enable/disable the Alarm mechanism for such WAN.

Items	Description
	

- **Adding/Editing a new LAN-to-LAN VPN Profile**

To add a new LAN-to-LAN VPN profile, simply choose the one with the name (???) and click the **Detail** button .

To modify a VPN profile, choose one of the profile names from the list and click the **Detail** button . The following dialog will appear. You can modify the LAN to LAN settings to fit your necessity.



VPN Lan To Lan Setting

Index:

Profile Name:

Enable this profile: ☐

Call Direction: ☒ Dial-Out ☐ Dial-In

Host Name or Server IP/Cli...

Dial Type: ☒ PPTP ☐ IPSec

VPN Connection Through:

PPTP:

Username:

Password:

PPP Authentication:

VJ Compression: ☒ on ☐ off

Available settings for such feature will be shown as follows:

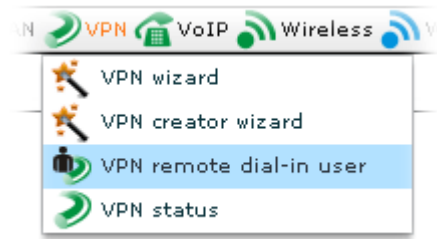
Items	Description
Profile Name	Display the profile name. Modify it if it is required.
Enable this profile	Check the box to enable such profile.
Call Direction	Specify which direction that such profile will use Dial-In or Dial-Out.
Host Name or Server IP /Client IP	Type the IP address for the server / client or the host name.
Dial Type	Click the radio button to specify the dial type.
VPN Connection Through	Use the drop down list to choose one way for VPN connection. VPN Connection Through: WAN1_First ▼ WAN1_First WAN1_Only WAN2_First WAN2_Only

Items	Description
PPTP	When you click PPTP as Dial Type, you have to fill the username and password, choose PPP Authentication and specify if VJ compression should be on or off for such connection.
IPSec	When you click IPSec as Dial Type, you have to type IKE Pre-Shared Key, and choose IPSec Security Method for such connection.
TCP IP Network Settings	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. More->Remote Network – Specify additional IP address and subnet mask for the remote server. More - >Create Phase2 SA Function – Check the box to enable the Phase2 SA function.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

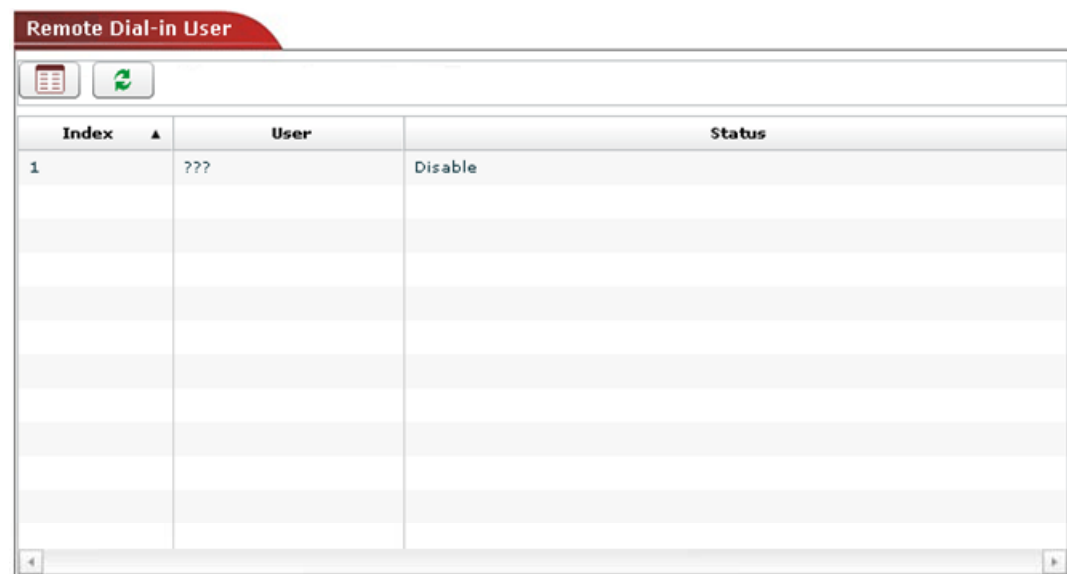
Click **Apply** to save the configuration and exit such window.

Creating 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.



Open **VPN>>VPN remote dial-in user**, the following screen will appear.



Available settings for such feature will be shown as follows:

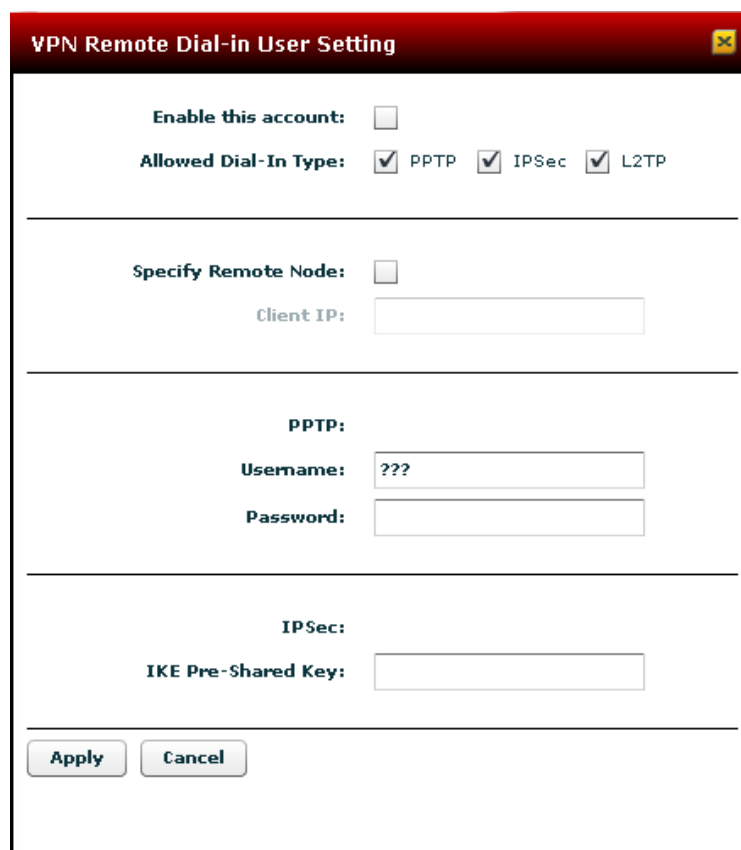
Items	Description
 Detail	Click this button to edit the selected profile or click it to add a new profile.
 Refresh	Click this button to refresh current page.
Index	VigorACS SI allows you to create up to 32 index numbers (profiles).
User	Display the name of the remote dial-in profile.
Status	Display if such profile is enabled or disabled for such CPE.

- **Adding/Editing a new Remote Dial-in User Profile**

To add a new remote dial-in profile, simply choose the one with the name (???) and click the

Detail button .

To modify a selected profile, choose one of the profile names from the list and click the **Detail** button . The following dialog will appear. You can modify the settings to fit your necessity.



The dialog box is titled "VPN Remote Dial-in User Setting". It contains the following fields and controls:

- Enable this account:** A checkbox that is currently unchecked.
- Allowed Dial-In Type:** Three checkboxes: PPTP (checked), IPSec (checked), and L2TP (checked).
- Specify Remote Node:** A checkbox that is currently unchecked.
- Client IP:** A text input field.
- PPTP:**
 - Username:** A text input field containing "???"
 - Password:** A text input field.
- IPSec:**
 - IKE Pre-Shared Key:** A text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

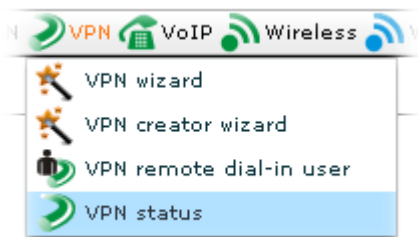
Available settings for such feature will be shown as follows:

Items	Description
Enable this account	Click it to enable such account.
Allow Dial-in Type	Allow the remote dial-in user to make a PPTP/IPSec/L2TP 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.
Client IP	Type the IP address of the remote client that is allowed to pass through VPN connection.
PPTP	Username – This field is applicable when you select PPTP policy above. Password – This field is applicable when you select PPTP policy above.
IPSec	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 .

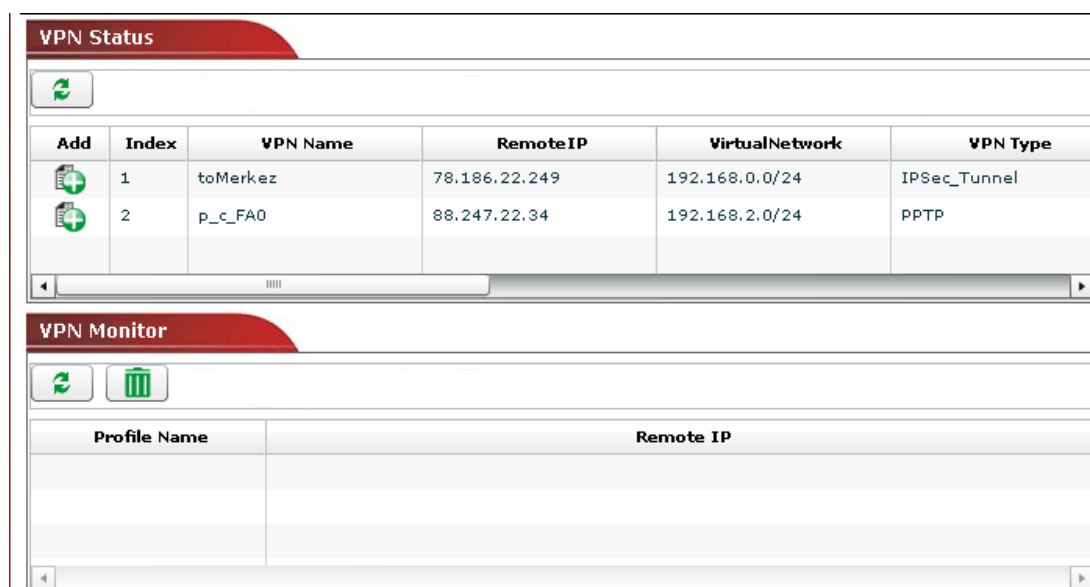
Items	Description
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Checking VPN Connection Status

VPN Status displays VPN name, remote IP address, virtual network address, VPN type, VPN Active, encryption, authentication, transmission packets, transmission bytes, receiving packets, receiving rate, and connection time for the selected CPE.



Open **VPN>>VPN status**, the following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Add to monitor	Make the selected VPN tunnel to be monitored and display in the field of VPN Monitor. Choose any one of the CPEs (or profiles) and click Add to monitor button to make the selected one to be monitored by VigorACS.
Index	Display the number of the VPN tunnel.
VPN Name	Display the VPN profile name that created by using VPN Wizard or VPN creator wizard .
Remote IP	Display the IP address that the VPN tunnel connected.

Items	Description
Virtual Network	Display the private IP address with subnet mask.
VPN Type	Display the connection type used by such VPN tunnel.
VPN Active	Display the status of such VPN tunnel. “ true ” means the VPN tunnel has be connected; “ false ” means the VPN tunnel has be disconnected.
Encryption	Display the method for encryption used by such VPN tunnel.
Authentication	Display the mode for authentication used by such VPN tunnel.
Tx Packets	Display the packet size of the transmitted data.
Tx Bytes	Display the size of the transmitted data.
Rx Packets	Display the packet size of the received data.
Rx Rate	Display the receiving rate for data receiving.
Up Time	Display the connection time for such VPN tunnel.

Monitoring VPN Tunnel

In the **VPN Status** page, basic information for each VPN tunnel will be shown on the screen. However, if you want to check the total traffic of VPN tunnel, you have to do the job of VPN Monitor.

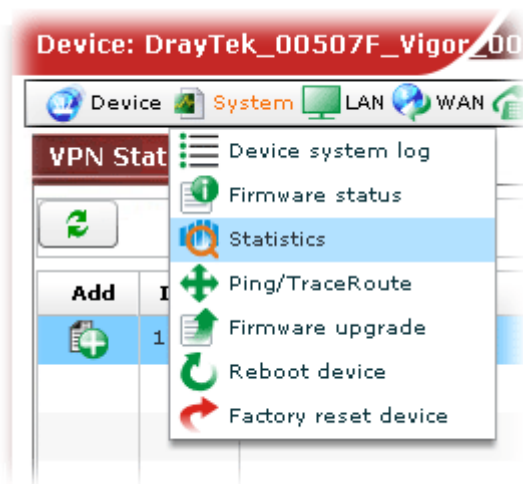
VPN Status						
						
Add	Index	VPN Name	RemoteIP	VirtualNetwork	VPN Type	V
	1	i_4E8_510	172.17.5.192	192.168.20.0/24	IPSec_Tunnel	true
	2	i_4E8_4E0	172.17.5.191	192.168.10.0/24	IPSec_Tunnel	true
	3	i_4E8_620	172.17.5.195	192.168.50.0/24	IPSec_Tunnel	true

VPN Monitor	
	
Profile Name	Remote IP
i_4E8_4E0	172.17.5.191
i_4E8_510	172.17.5.192
i_4E8_620	172.17.5.195

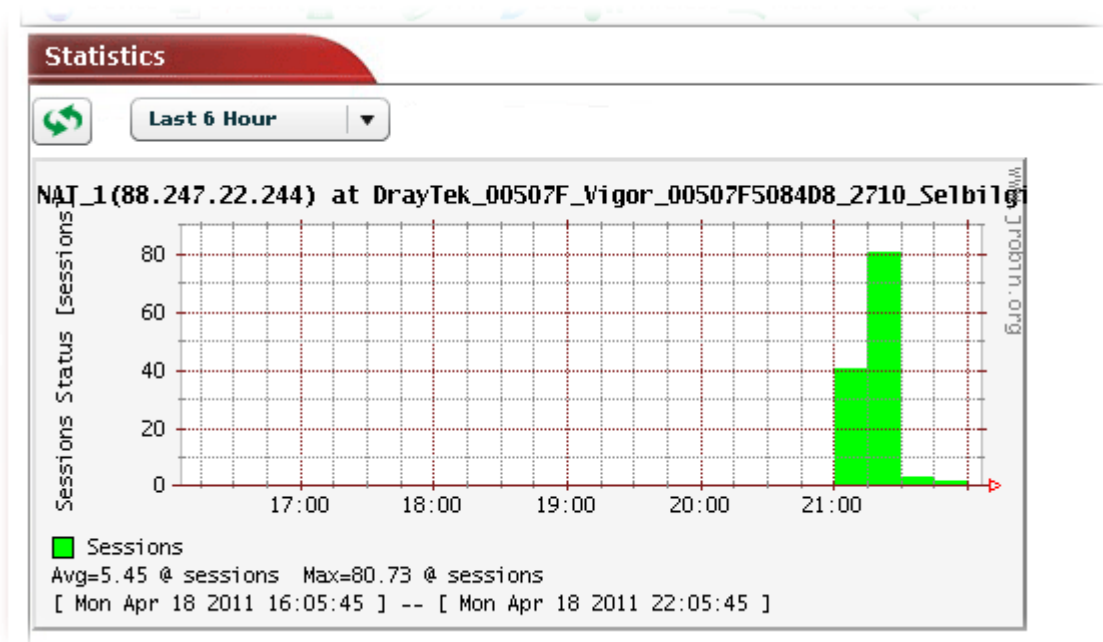
Available settings for such feature will be shown as follows:

Items	Description
Name	Display the name of the profile.
Profile Name	Display the name listed in VPN Name field.
Remote IP	Display the IP address that the VPN tunnel connected.

Choose the VPN tunnel(s) (in this case, p_c_FA0 and toMerkez are selected) that you want to monitor and click the **Add to monitor** icon. Next, open **System >> Statistics**.



The statistics for the above three profiles will be displayed on the screen as shown below.



6.2.8 DSL Settings for the Selected CPE

This page display DSL settings for the selected CPE. You can modify the settings if required.

Note: If the selected CPE is not a DSL router, such menu will be invalid.



Open **DSL>>DSL**, the following screen will appear.

DSL

Index 1

ADSL Status

Up

ADSL Operation Mode

Multimode

Download Speed

7488

Upload Speed

800

SNR Margin

13

Loop Attenuation

190

Protocol

PPPoE

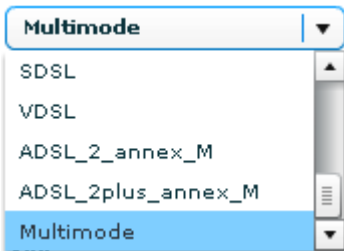
PVC:VPI/VCI

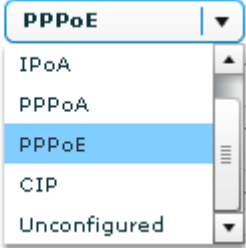
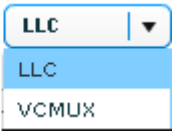
PVC:8/35

User Name

ergpancar@ttnet

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
Index	Display the index number of the CPE in current network group.
ADSL Status	Display current connection status for the selected CPE. “Up” means the CPE is controlled by VigorACS and runs well. “Down” means there is no data transmission/receiving on CPE.
ADSL Operation Mode	Specify the type of DSL module used on the interface associated with connection. 
Download Speed	Display the download speed of the selected CPE.
Upload Speed	Display the upload speed of the selected CPE.
SNR Margin	Display the quality of SNR (signal to noise ratio). The higher the SNR Margin is, the better the connection speed is.
Loop Attenuation	Display the loss of signal over distance. Many factors will influence the value of loop attenuation. The lower the value is, the better the connection speed is.

Items	Description
Protocol	Select an IP mode for the WAN interface of the selected CPE. 
PVC:VPI/VCI	VPI stands for Virtual Path Identifier. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers. VCI stands for Virtual Channel Identifier. It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
User Name	Type a user name for the selected Protocol such as PPPoE, PPPoA and so on.
Password	Type a password for the selected Protocol such as PPPoE, PPPoA and so on.
CRC Errors	Display the CRC (Cycle Redundancy Check) error of your hardware.
ATU CRC Errors	Display the ATU CRC (Cycle Redundancy Check) error of your hardware.
Encapsulating Type	Drop down the list to choose the type provided by ISP.  Available types will be changed according to the model (CPE) you select.

6.2.9 Wireless Settings for the Selected CPE

This page displays wireless settings for the selected CPE. You can modify the settings if required.

Note: If the selected CPE does not support wireless function, such menu will be invalid.



General Setting for Wireless Connection

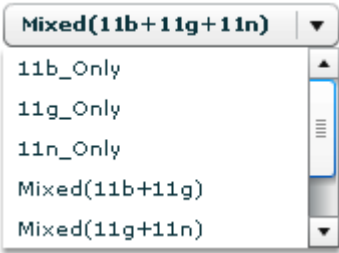
This page allows you to enable the wireless LAN connection for the selected CPE; specify different wireless mode; change wireless channel and invoke the Long Preamble function for the selected CPE.

Open **Wireless>>General**, the following screen will appear.

A screenshot of the 'Wireless_General' settings page. The page has a red header with the title 'Wireless_General'. Below the header, there is a form with the following fields: 'Index' with a value of '1', 'Wireless LAN Enable' with an unchecked checkbox, 'Mode' with a dropdown menu showing 'Mixed(11b+11g+11n)', 'Channel' with a dropdown menu showing 'Channel_6,2437MHz', and 'Long Preamble' with an unchecked checkbox.

Available settings for such feature will be shown as follows:

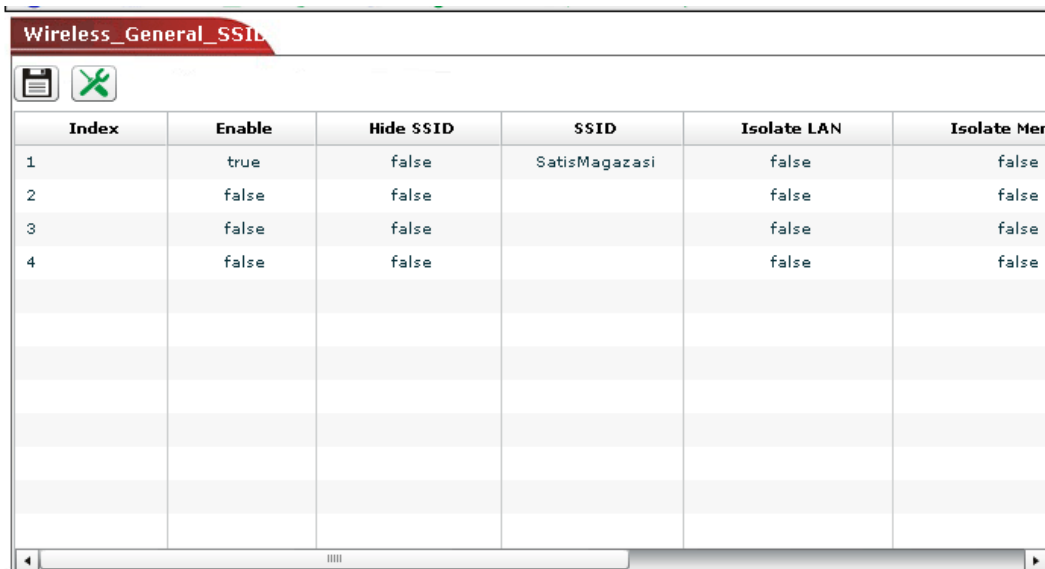
Items	Description
Index	Display the index number of the CPE in current network group.
Wireless LAN Enable	Click it to enable the wireless LAN function for such CPE.
Mode	Choose the wireless mode for such CPE.

Items	Description
	
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.

General SSID Setting for Wireless Connection

This page allows you to configure SSID for the selected CPE.

Open **Wireless>>General SSID**, the following screen will appear.



Index	Enable	Hide SSID	SSID	Isolate LAN	Isolate Men
1	true	false	SatisMagazasi	false	false
2	false	false		false	false
3	false	false		false	false
4	false	false		false	false

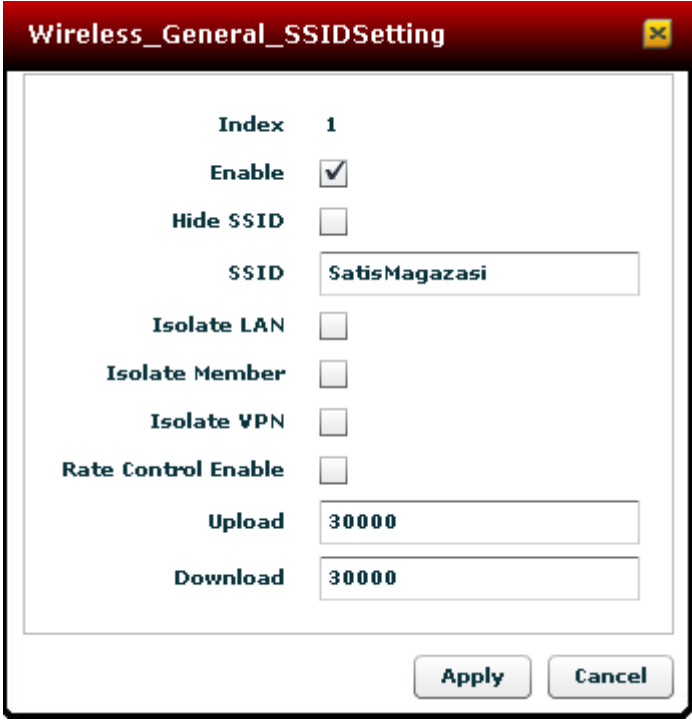
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Enable	Display if such profile is enabled (true) or not (false).
Hide SSID	Display if the SSID of such profile is hidden (true) or not (false).
SSID	Display the SSID of the wireless profile.
Isolate LAN	Display if such function is enabled (true) or not (false).
Isolate Member	Display if such function is enabled (true) or not (false).
Isolate VPN	Display if such function is enabled (true) or not (false).
Rate Control Enable	Display if such function is enabled (true) or not (false).
Upload	Display the transmitting rate for data upload.
Download	Display the transmitting rate for data download.

Editing the SSID Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



The dialog box titled "Wireless_General_SSIDSetting" contains the following settings:

- Index:** 1
- Enable:** ☒
- Hide SSID:** ☐
- SSID:** SatisMagazasi
- Isolate LAN:** ☐
- Isolate Member:** ☐
- Isolate VPN:** ☐
- Rate Control Enable:** ☐
- Upload:** 30000
- Download:** 30000

Buttons: Apply, Cancel

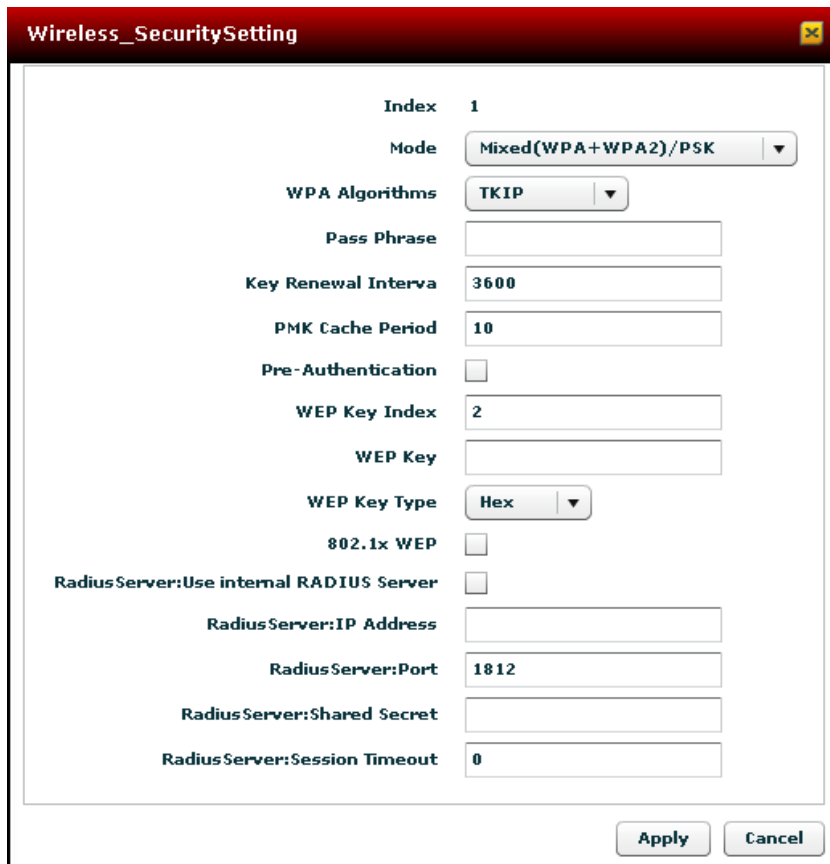
Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the CPE in current network group.
Wireless LAN Enable	Click it to enable this setting.
Hide SSID	Check it to hide the SSID of such wireless profile.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "Draytek. We suggest you to change it.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
Isolate VPN	Check this box to make the wireless clients (stations) with the same SSID not accessing for other VPN.
Rate Control Enable	It controls the data transmission rate through wireless connection. Check the box to enable such function.

Items	Description
	(true) or not (false).
WEP Key Index	Display the number of WEP Key is used.
WEP Key	Display the content of the WEP Key.
WEP Key Type	Display the type of the WEP Key.
802.1x WEP	Display if WEP Encryption is enabled (true) or not (false).
RadiusServer:Use internal RADIUS Server	Display if RADIUS Server is enabled (true) or not (false).
RadiusServer:IP Address	Display the IP address of external RADIUS server.
RadiusServer:Port	Display the UDP port number that the external RADIUS server is using.
RadiusServer:Shared Secret	Display the shared secret that the external RADIUS server and client share.
RadiusServer:Session Timeout	Display maximum time of service provided before re-authentication.

Editing the Security Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



The dialog box titled "Wireless_SecuritySetting" contains the following settings:

- Index:** 1
- Mode:** Mixed(WPA+WPA2)/PSK
- WPA Algorithms:** TKIP
- Pass Phrase:** (empty text field)
- Key Renewal Interval:** 3600
- PMK Cache Period:** 10
- Pre-Authentication:** ☐
- WEP Key Index:** 2
- WEP Key:** (empty text field)
- WEP Key Type:** Hex
- 802.1x WEP:** ☐
- RadiusServer:Use internal RADIUS Server:** ☐
- RadiusServer:IP Address:** (empty text field)
- RadiusServer:Port:** 1812
- RadiusServer:Shared Secret:** (empty text field)
- RadiusServer:Session Timeout:** 0

Buttons: Apply, Cancel

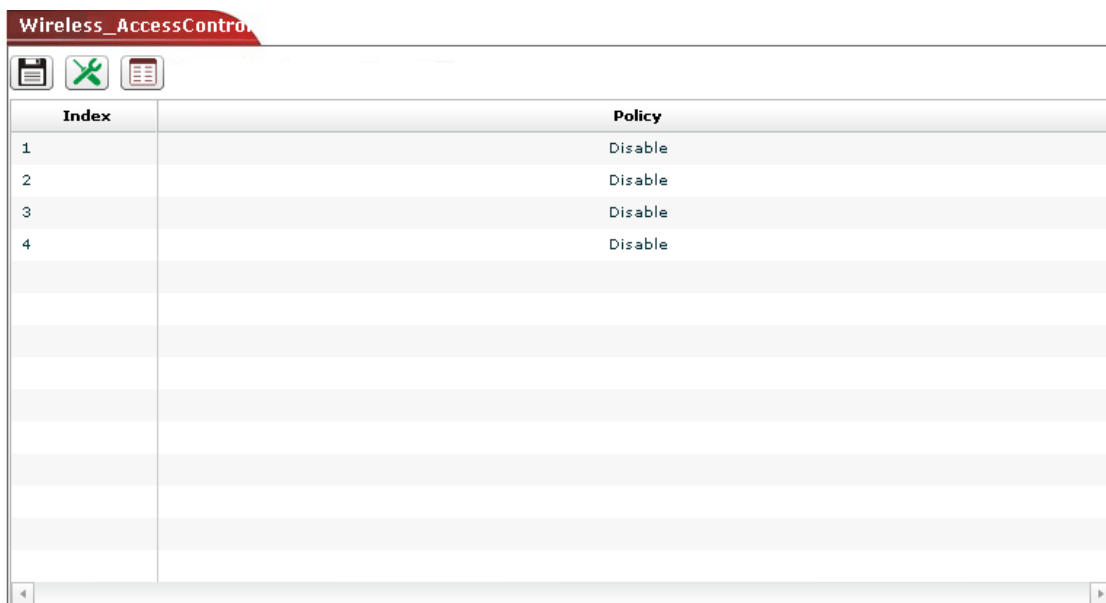
Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Mode	There are several modes provided for you to choose. Disable - The encryption mechanism is turned off. WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key. WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithm	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678. (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK

Items	Description
	mode.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) Check the box to enable IEEE 802.1X Pre-Authentication.
WEP Key Index	Four WEP Keys can be configured for such router. This field is used to indicate which one will be applied. Available numbers are 1 ~ 4.
WEP Key	The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.
WEP Key Type	Choose the type (ASCII or HEX) of the WEP Key.
802.1x WEP	Check the box to enable the WEP Encryption.
RadiusServer:Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box.
RadiusServer:IP Address	Enter the IP address of external RADIUS server.
RadiusServer:Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
RadiusServer:Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
RadiusServer:Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Access Control Setting for Wireless Connection

Display the Access Control settings that Vigor router supports.

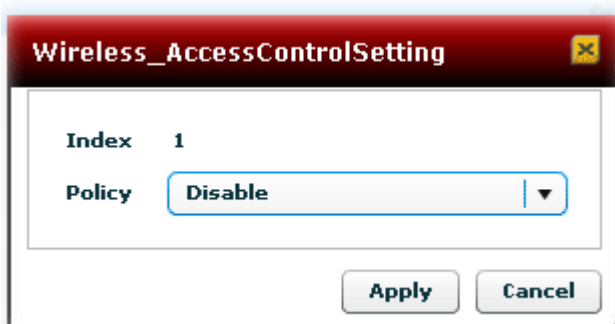


Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
 Detail	Click it to edit the advanced settings of the selected profile.
Index	Display the index number of the profile in current network group.
Policy	Display the selected policy for the wireless control.

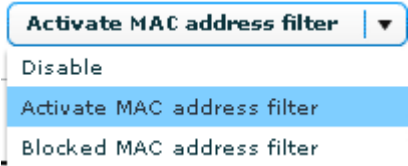
Editing the Access Control Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.

Items	Description
Policy	Determine the policy for the wireless control.  Later, click  to configure advanced settings for the policy.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

WPS Setting for Wireless Connection

Display the WPS settings that Vigor router supports.

[illegible]

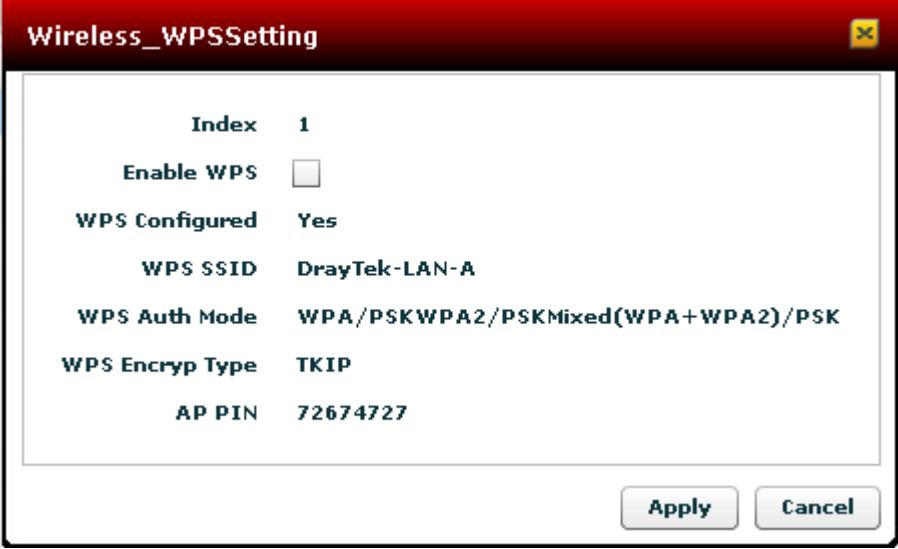
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Enable WPS	Display if the WPS profile is enabled (true) or disabled (false).
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of Vigor router is properly configured, you can see 'Yes' message

Items	Description
	here.
WPS SSID	Display the SSID that such WPS specified.
WPS Auth Mode	Display the authentication modes such router supports.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of Vigor router.
AP PIN	Display the number which is used for remote client entering the registrar's PIN code in remote station to make a network connection.

Editing the WPS Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



The dialog box titled "Wireless_WPSSetting" contains the following settings:

Index	1
Enable WPS	☐
WPS Configured	Yes
WPS SSID	DrayTek-LAN-A
WPS Auth Mode	WPA/PSKWPA2/PSKMixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP
AP PIN	72674727

At the bottom right, there are "Apply" and "Cancel" buttons.

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of Vigor router is properly configured, you can see 'Yes' message here.
WPS SSID	Display the SSID that such WPS specified.
WPS Auth Mode	Display the authentication modes such router supports.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of Vigor router.
AP PIN	Display the number which is used for remote client entering the registrar's PIN code in remote station to make a network connection.

Items	Description
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

AP Discovery Setting for Wireless Connection

Display the AP Discovery settings that Vigor router supports.

Index	SSID	BSSID	RSSI	Channel	Encryption	Auth
1	P874	50:67:f0:1a:0	100%	1		NONE
2	Default_SSID	00:12:34:54:3	86 %	1		NONE
3	DrayTek_kyeh_282C	00:50:7f:6f:83	10 %	1	AES	
4	0024A57217A8-1	00:24:a5:72:1	100%	1		NONE
5	0024A57217A8	00:24:a5:72:1	100%	1		NONE
6	DrayTek	00:50:7f:aa:1	100%	1	AES	
7	FAE-292222220	00:50:7f:c9:3b	100%	4	AES	
8	mis_test	00:12:0e:37:3	44 %	6	TKIP/AES	Mixed
9	DrayTek	00:50:7f:a7:6	24 %	6		NONE
10	DrayTek700-AAA	00:1f:1f:c4:88	100%	6	AES	
11	Dennis_Test	00:50:7f:c3:5f	86 %	6		NONE
12	default	00:1d:7d:34:c	55 %	6		NONE
13	PQA-tang	00:50:7f:ce:b6	70 %	6	TKIP	Mixed
14	DrayTek	00:50:7f:a6:3	100%	6		NONE

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
SSID	Display the SSID of the AP scanned by Vigor router.
BSSID	Display the MAC address of the AP scanned by Vigor router.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by Vigor router.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.

Station List for Wireless Connection

Display the stations connecting to Vigor router.

6.2.10 Wireless 5G Settings for the Selected CPE

At present, VigorAP 800 supports wireless 5G function. You can modify the settings for VigorAP800 via VigorACS SI.

Note: If the selected CPE does not support wireless 5G function, such menu will be invalid.



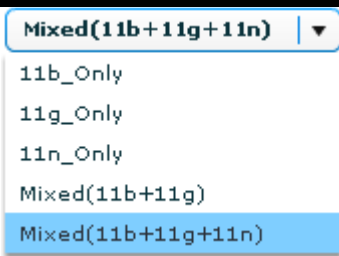
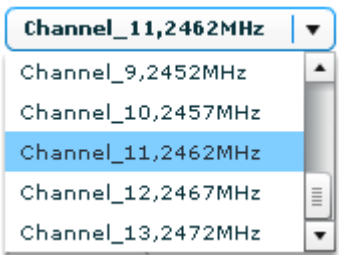
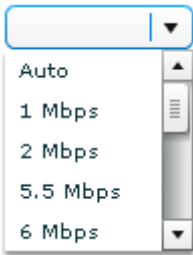
General Setting for Wireless Connection

This page display wireless settings for the selected CPE. You can modify the settings if required.

A screenshot of the 'Wireless_General' settings page in the VigorACS SI interface. The page has a red header with the title 'Wireless_General'. Below the header is a save icon. The main content area contains the following settings: 'Index' set to '1'; 'Enable Wireless LAN' checked; 'Mode' set to 'Mixed(11b+11g+11n)'; 'Enable 2 Subnet (Simulate 2 APs)' checked; 'Channel' set to 'Channel_11,2462MHz'; 'Rate' set to an empty dropdown; 'Tx Burst' checked; 'WMM Capable' checked; and 'Antenna' set to '2T2R'.

Available settings for such feature will be shown as follows:

Items	Description
Save parameter settings	Click this button to save the parameters settings.
Index	Display the index number of the profile in current network group.
Mode	Choose the wireless mode for such CPE.

Items	Description
	
Enable 2 Subnet (Simulate 2 APs)	Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800. If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. 
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate. 
Tx Burst	This feature can enhance the performance in data transmission about 40%* more.
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable radio button.
Antenna	VigorAP 800 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please

Items	Description
	choose 1T1R. 2T2R ▾ 2T2R 1T1R

General SSID Setting for 5G Wireless Connection

This page allows you to configure SSID for the selected CPE.

[illegible]

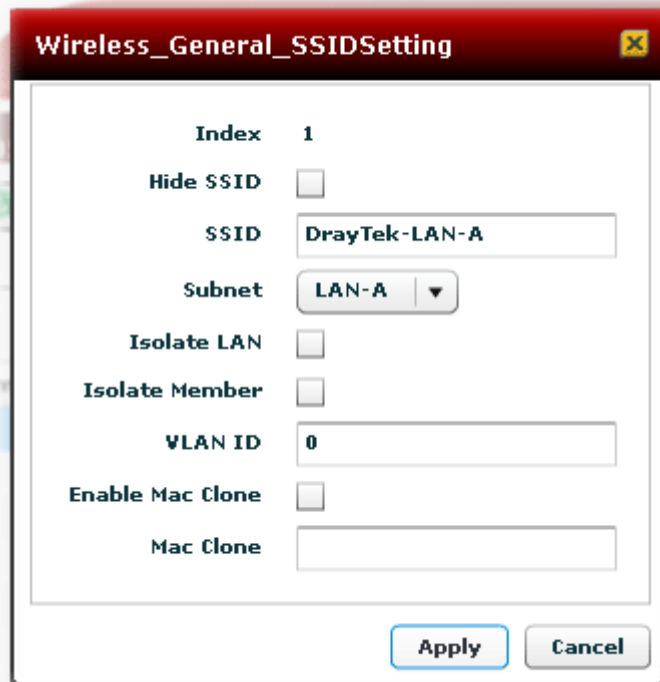
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Hide SSID	Display if the SSID of such profile is hidden (true) or not (false).
SSID	Display the SSID of the wireless profile.
Subnet	Display which subnet is used for the selected CPE.
Isolate LAN	Display if such function is enabled (true) or not (false).
Isolate Member	Display if such function is enabled (true) or not (false).
VLAN ID	Display the VLAN ID of the selected CPE.

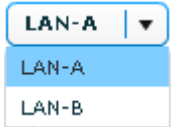
Items	Description
Enable Mac Clone	Display if such function is enabled (true) or not (false).
Mac Clone	Display the MAC address of the selected CPE.

Editing the SSID Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the CPE in current network group.
Hide SSID	Check it to hide the SSID of such wireless profile.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID will be displayed in this field. We suggest you to change it.
Subnet	Choose LAN-A or LAN-B for each SSID. If you choose LAN-A, the wireless clients connecting to this SSID could only communicate with LAN-A. 
Isolate LAN	Check this box to make the wireless clients (stations)

Items	Description
	with the same SSID cannot access wired PCs on LAN. Note: If Isolate LAN is checked, do not type any value for VLAN ID.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.
Enable Mac Clone	Check this box to enable the function.
Mac Clone	Manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Security Setting for 5G Wireless Connection

Display the security settings that Vigor router supports. The administrator can modify and save the changes for the Vigor router remotely by using VigorACS. However, not all of the Vigor routers' wireless security settings can be handled by VigorACS.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.

Items	Description
Mode	Display the mode used by such router.
WPA Algorithms	Display the algorithm used by WPA.
Pass Phrase	Display the Pass Phrase used by such router.
Key Renewal Interval	Display the renewal security time for authentication to the network.
PMK Cache Period	Display the expire time of WPA2 PMK (Pairwise master key) cache.
Pre-Authentication	Display if IEEE 802.1X Pre-Authentication is enabled (true) or not (false).
WEP Key Index	Display the number of WEP Key is used.
WEP Key	Display the content of the WEP Key.
WEP Key Type	Display the type of the WEP Key.
802.1x WEP	Display if WEP Encryption is enabled (true) or not (false).
RADIUS Server: User internal RADIUS Server	Display if RADIUS Server is enabled (true) or not (false).
RADIUS Server: IP Address	Display the IP address of external RADIUS server.
RADIUS Server: Port	Display the UDP port number that the external RADIUS server is using.
RADIUS Server: Shared Secret	Display the shared secret that the external RADIUS server and client share.
RADIUS Server: Session Timeout	Display maximum time of service provided before re-authentication.

Editing the Security Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.

Wireless_5G_SecuritySetting

Index 1

Mode Disable

WPA Algorithms

Pass Phrase

Key Renewal Interval 3600

PMK Cache Period 10

Pre-Authentication

WEP Key Index 1

WEP Key

WEP Key Type Hex

802.1x WEP

RadiusServer:Use internal RADIUS Server

RadiusServer:IP Address

RadiusServer:Port 1812

RadiusServer:Shared Secret

RadiusServer:Session Timeout 0

Apply Cancel

Available settings for such feature will be shown as follows:

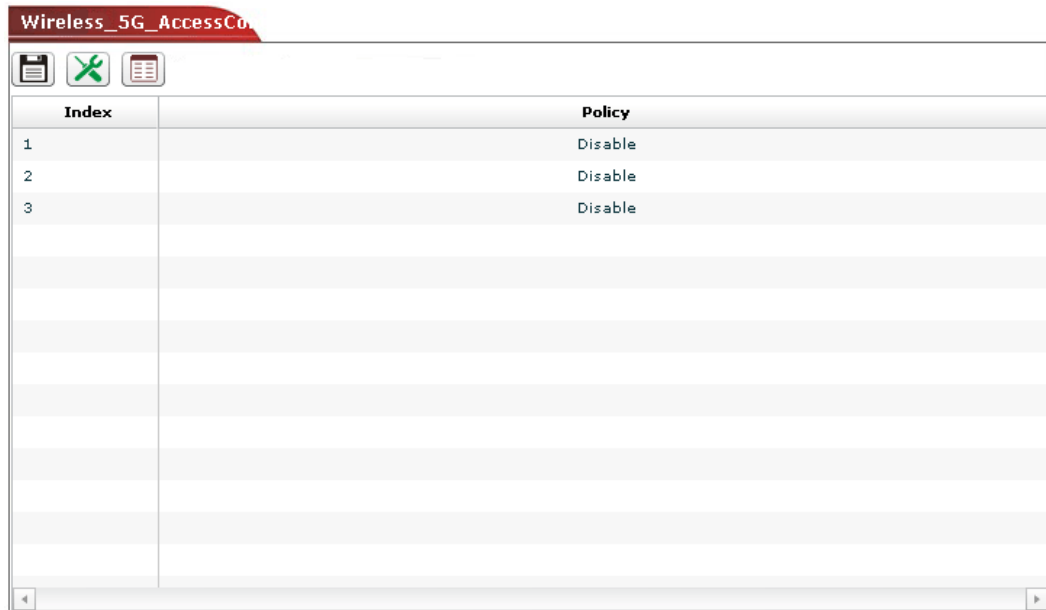
Items	Description
Index	Display the index number of the profile in current network group.
Mode	There are several modes provided for you to choose. Disable - The encryption mechanism is turned off. WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key. WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.

Items	Description
	WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithm	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678. (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) Check the box to enable IEEE 802.1X Pre-Authentication.
WEP Key Index	Four WEP Keys can be configured for such router. This field is used to indicate which one will be applied. Available numbers are 1 ~ 4.
WEP Key	The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level.

Items	Description
	The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.
WEP Key Type	Choose the type (ASCII or HEX) of the WEP Key.
802.1x WEP	Check the box to enable the WEP Encryption.
RadiusServer:Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box.
RadiusServer:IP Address	Enter the IP address of external RADIUS server.
RadiusServer:Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
RadiusServer:Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
RadiusServer:Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Access Control Setting for 5G Wireless Connection

Display the Access Control settings that Vigor router supports.



Available settings for such feature will be shown as follows:

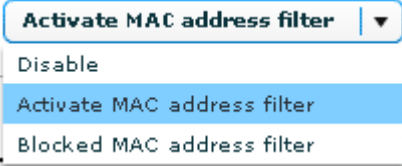
Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
 Detail	Click it to edit the advanced settings of the selected profile. 
Index	Display the index number of the profile in current network group.
Policy	Display the selected policy for the wireless control.

Editing the Access Control Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.



Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Policy	Determine the policy for the wireless control.  Later, click  to configure advanced settings for the policy.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

AP Discovery Setting for 5G Wireless Connection

Display the AP Discovery settings that Vigor router supports.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
SSID	Display the SSID of the AP scanned by Vigor router.
BSSID	Display the MAC address of the AP scanned by Vigor router.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by Vigor router.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.

Station List for 5G Wireless Connection

Display which stations connecting to Vigor router.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
MAC Address	Display the MAC address of the client.
SSID	Display the SSID of the station.
Auth	Display the authentication type which the station uses for connecting the AP.
Encrypt	Display the encryption mode which the station uses for connecting the AP.

6.2.11 Multi-PVCs for the Selected CPE

Note: If the selected CPE does not support Multi-PVCs function, such menu will be invalid.



General Settings for Multi-PVCs

Open **Multi-PVCs>>General**, the following screen will appear.

Multi-PVCs_General					
Index	Enable	VPI	VCI	QoS Type	Protocol
1	true	0	33	UBR	PPPoE
2	true	0	88	UBR	MPoA
3	false	1	43	UBR	PPPoA
4	false	1	44	UBR	PPPoA
5	false	1	45	UBR	PPPoA
6	false	1	46	UBR	PPPoA
7	false	1	47	UBR	PPPoA
8	false	1	48	UBR	PPPoA

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
 Detail	This button is available for Index 3 to Index 5 only. A window with detailed information about the index will be shown on your screen.
Index	Display the index number of the profile in current network group.
Enable	Display if such profile is enabled (true) or not (false).
VPI	Display the VPI value for such profile.
VCI	Display the VCI value for such profile.
QoS Type	Display the QoS type for such profile.
Protocol	Display the protocol for such profile.
Encapsulation	Display the encapsulation type for such profile.
Wancount	Display if such PVC can be configured for WAN interface. When the value is greater than 0, it means WAN settings are available for such PVC.

Editing the General Multi-PVCs Setting

To modify a selected profile, choose one of the profile names from the list and click the **Edit** button . The following dialog will appear. You can modify the settings to fit your necessity.

Multi-PVCs_GeneralSetting

Index 1

Enable ☒

VPI 0

VCI 33

QoS Type UBR ▼

Protocol PPPoE ▼

Encapsulation LLC_SNAP ▼

WanCount 0

Apply Cancel

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable	Check this box to enable the profile.
VPI	VPI stands for Virtual Path Identifier . It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers. Type in the value provided by your ISP.
VCI	VCI stands for Virtual Channel Identifier . It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network. Type in the value provided by your ISP.
QoS Type	Select a proper QoS type for the channel.
Protocol	Select a proper protocol for this channel.
Encapsulation	Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.
WanCount	Display if such PVC can be configured for WAN interface. When the value is greater than 0, it means WAN settings are available for such PVC.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

ATM QoS for Multi-PVCs

This function can display the ATM QoS function settings for the selected CPE.

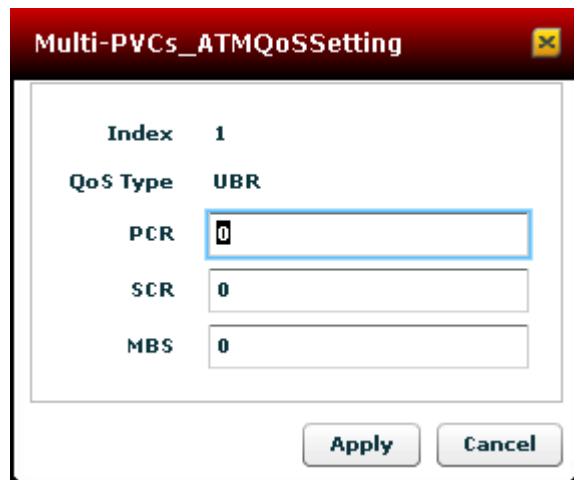
Index	QoS Type	PCR	SCR	MBS
1	UBR	0	0	0
2	UBR	0	0	0
3	UBR	0	0	0
4	UBR	0	0	0
5	UBR	0	0	0
6	UBR	0	0	0
7	UBR	0	0	0
8	UBR	0	0	0

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
QoS Type	Display the QoS type (e.g., UBR, CBR) for the channel.
PCR	Display the value of PCR.
SCR	Display the value of SCR.
MBS	Display the value of MBS.

Editing the ATM QoS for Multi-PVCs Settings

To modify the profile, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



The screenshot shows a dialog box titled "Multi-PVCs_ATMQoSSetting". It contains the following fields and values:

- Index:** 1
- QoS Type:** UBR
- PCR:** 0
- SCR:** 0
- MBS:** 0

At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
QoS Type	Display the type of QoS.
PCR	It represents Peak Cell Rate. The default setting is "0".
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Port-Based Bridge for Multi-PVCs

This function can display the Port-Based Bridge function settings for the selected CPE. There are eight channels that can be configured in this page.

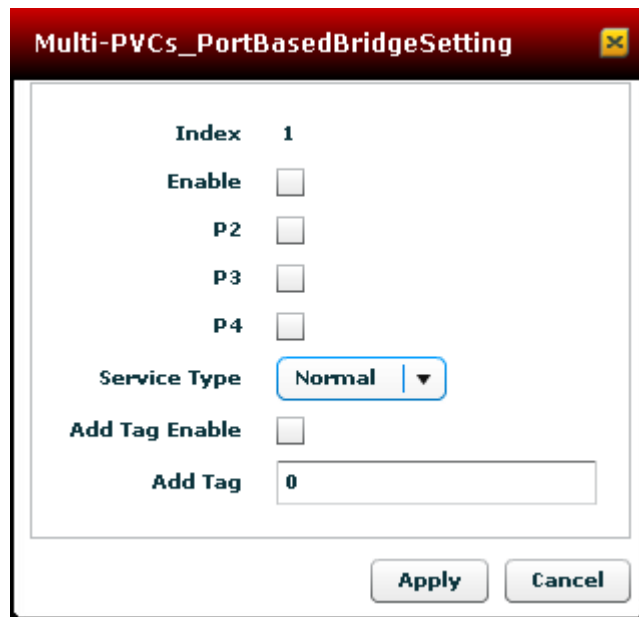
Multi-PVCs_PortBasedB					
					
Index	Enable	P2	P3	P4	Service Type
1	false	false	false	false	Normal
2	false	false	false	false	Normal
3	false	false	false	false	Normal
4	false	false	false	false	Normal
5	false	false	false	false	Normal
6	false	false	false	false	Normal
7	false	false	false	false	Normal
8	false	false	false	false	Normal

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Enable	Display if such profile is enabled (true) or not (false).
P2/P3/P4	Display which LAN port is enabled (true) or disabled (false).
Service Type	Display the service type used for the service of video stream (e.g., IPTV).
Add Tag Enable	Display if such function is enabled (true) or not (false).
Add Tag	Display the number of VLAN ID.

Editing the Port-Based Bridge for Multi-PVCs Settings

To modify the profile, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



Multi-PVCs_PortBasedBridgeSetting

Index 1

Enable ☐

P2 ☐

P3 ☐

P4 ☐

Service Type Normal ▼

Add Tag Enable ☐

Add Tag 0

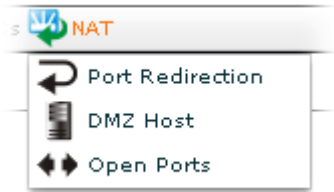
Apply Cancel

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable	Check this box to enable the profile.
P2/P3/P4	Check this box to invoke such LAN port. It means the LAN port 2 to 4. Check the box to designate the LAN port for channel 3 to 8.
Service Type	Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP.
Add Tag Enable	Check this box to enable the function of Add Tag.
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

6.2.12 Configuring NAT Setting for the Selected CPE

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



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. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.

Open **NAT>>Port Redirection**. The following screen will appear with all of the NAT settings for the selected CPE/group.

A screenshot of the NAT Port Redirection configuration interface. It features a table with five columns: Index, Port Redirection, Port Redirection Mode, Service Name, and an empty column. The table contains five rows of data. Above the table are icons for saving (a floppy disk) and editing (a wrench and screwdriver).

Index	Port Redirection	Port Redirection Mode	Service Name	
1	true	Single	kamera1	
2	true	Single	kamera2	
3	true	Single	kamera3	
4	true	Single	kamera4	
5	false	Single		

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the CPE in current network group.
Port Redirection	Display if such profile is enabled (true) or

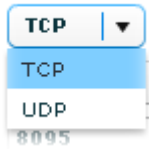
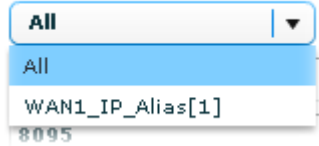
Items	Description
	not (false).
Port Redirection Mode	Display the port redirection mode of the CPE.
Service Name	Display the name of the service for identification.
Protocol	Display the protocol for NAT of the CPE.
WAN IP	Display the WAN IP alias for the device passing through.
Public Port Start	Display which port can be redirected to the specified Private IP and Port of the internal host.
Public Port End	Display the ending port used for such profile.
Private IP Start	Display the private IP address of the internal host providing the service.
Private IP End	Display the IP address as the end of Private IP.
Private Port	Display the private port number of the service offered by the internal host.

Editing the Port Redirection Setting

To modify the profile, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

The screenshot shows a dialog box titled "NATSetting" with a close button in the top right corner. Inside the dialog, the "Index" is set to "1". The "Port Redirection" checkbox is checked. The "Port Redirection Mode" is set to "Single" with a dropdown arrow. The "Service Name" is "kamera1". The "Protocol" is set to "TCP" with a dropdown arrow. The "WAN IP" is set to "All" with a dropdown arrow. The "Public Port Start" is "8095", "Public Port End" is "8095", "Private IP Start" is "192.168.4.96", "Private IP End" is "96", and "Private Port" is "8095". At the bottom, there are "Apply" and "Cancel" buttons.

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the CPE in current network group.
Port Redirection	Move and click your mouse on the field, a check box will appear. Check the box to set “true” mode (means enabled) or uncheck the box to set “false” mode (means disabled).
Port Redirection Mode	Display the port redirection mode of the CPE. Available modes (true/false) for such CPE can be seen from the drop down list. You can change the mode if required.  If you select Range as Port Redirection Mode, please specify the value of Private IP Start and Private IP End.
Service Name	Type a name for the service for identification.
Protocol	Display the protocol for NAT of the CPE. Available settings for such CPE can be seen from the drop down list. You can change the protocol if required. 
WAN IP	Choose WAN IP alias for the device passing through. 
Public Port Start	Specify which port can be redirected to the specified Private IP and Port of the internal host.
Public Port End	If you choose Range as the port redirection mode, please type the required number on this field.
Private IP Start	Specify the private IP address of the internal host providing the service.
Private IP End	If you choose Range as the port redirection mode, you need to specify Private IP End additionally.
Private Port	Specify the private port number of the service offered by the internal host.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

DMZ Host

As mentioned above, **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. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

Open **NAT>>DMZ Host**. The following screen will appear with all of the NAT settings for the selected CPE/group.

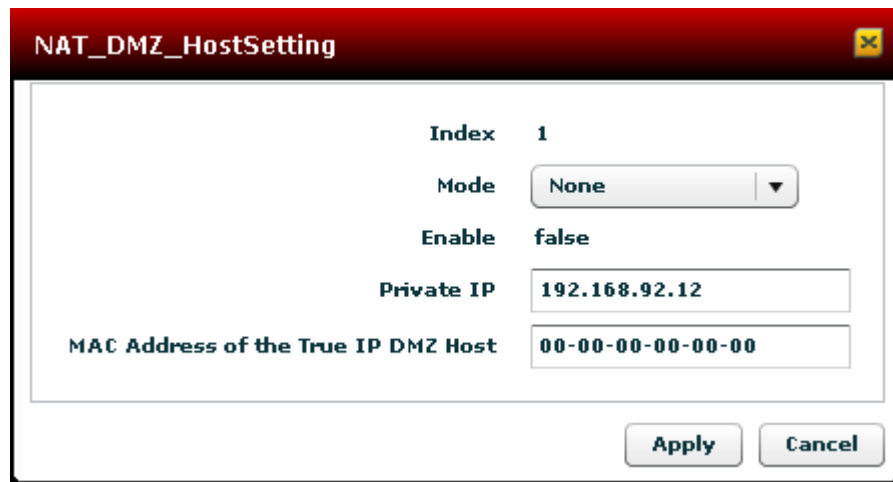
[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the CPE in current network group.
Mode	Display which mode (Private IP or Active_True_IP) is specified for such profile.
Enable	If the DHCP server is enabled, the word of “true” will be shown here. Otherwise, the word of “false” will appear. Such value can be edited if required.
Private IP	Display private IP address of the CPE.
MAC Address of the True IP DMZ Host	Display the MAC address of the CPE.

Editing the DMZ Host Setting

To modify the profile, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



The screenshot shows a window titled "NAT_DMZ_HostSetting" with a red header bar. Inside the window, the following settings are displayed:

- Index**: 1
- Mode**: A dropdown menu currently set to "None".
- Enable**: A checkbox that is currently unchecked, with the label "false" next to it.
- Private IP**: A text input field containing the IP address "192.168.92.12".
- MAC Address of the True IP DMZ Host**: A text input field containing the MAC address "00-00-00-00-00-00".

At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the CPE in current network group.
Mode	Choose None , Private IP or Active_True_IP for typing the related information on the fields listed below.
Private IP	Type the IP address of the DMZ host if you choose Private IP as the Mode.
MAC Address of the True IP DMZ Host	Type the MAC address for the DMZ host if you choose Active_True_IP as the Mode.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Open Ports

Open Ports 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.

Open **NAT>>Open Port**. The following screen will appear with all of the NAT settings for the selected CPE/group.

NAT_Open_Ports					
Index	Enable Open Ports	Comment	WAN Interface	WAN IP	
1	false		WAN1	WAN1_IP_Alias[:]	
2	true	ST7501	WAN1	WAN1_IP_Alias[:]	
3	true	IP7152	WAN1	WAN1_IP_Alias[:]	
4	true	IP7133	WAN1	WAN1_IP_Alias[:]	
5	true	dahua	WAN1	WAN1_IP_Alias[:]	
6	false	idclock	WAN1	WAN1_IP_Alias[:]	
7	true	P27151	WAN1	WAN1_IP_Alias[:]	
8	false		WAN1	WAN1_IP_Alias[:]	

Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings for the profile.
 Edit	Click it to edit the settings of the selected profile.
 Detail	Click it to display a window with detailed information for the selected open ports profile.

Detail Window			
DrayTek_00507F_Vigor_00507FC93B24			
Index	Protocol	Start Port	End Port
1		0	0
2		0	0
3		0	0
4		0	0
5		0	0
6		0	0
7		0	0
8		0	0
9		0	0
10		0	0

Index	Display the index number of the profile in current network group.
Enable Open Ports	Display if such profile is enabled (true) or not (false).
Comment	Display the name for the defined network

Items	Description
	application/service
WAN Interface	Display the WAN interface for the entry.
WAN IP	Display the WAN IP Alias
Local IP Address	Display the private IP address of the local host offering the service.

Editing the Open Ports Setting

To modify the profile, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable Open Ports	Display if such profile is enabled (true) or not (false).
Comment	Make a name for the defined network application/service
WAN Interface	Choose the WAN interface for the entry.
WAN IP	Choose WAN IP address from the drop down list for the entry.
Local IP Address	Type the private IP address of the local host offering the service.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

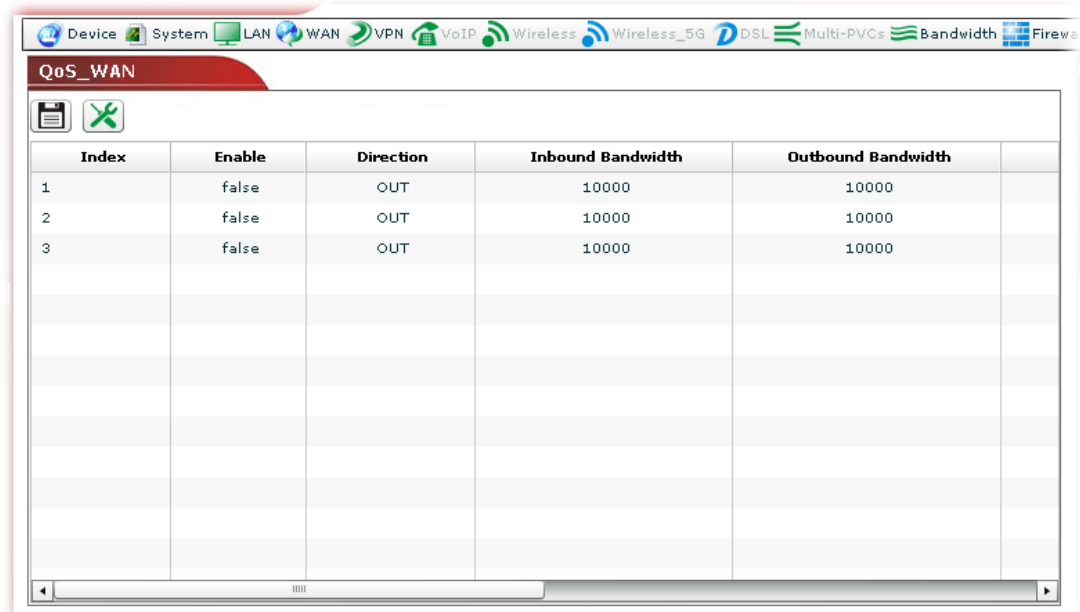
6.2.13 Bandwidth Settings for the Selected CPE

As an administrator, you can configure the bandwidth ratio for QoS of the WAN interface for the selected CPE.



Configuring QoS WAN Setting for the Selected CPE

Open **Bandwidth>>QoS WAN**. The following screen will appear with all of the QoS WAN settings for the selected CPE/group.



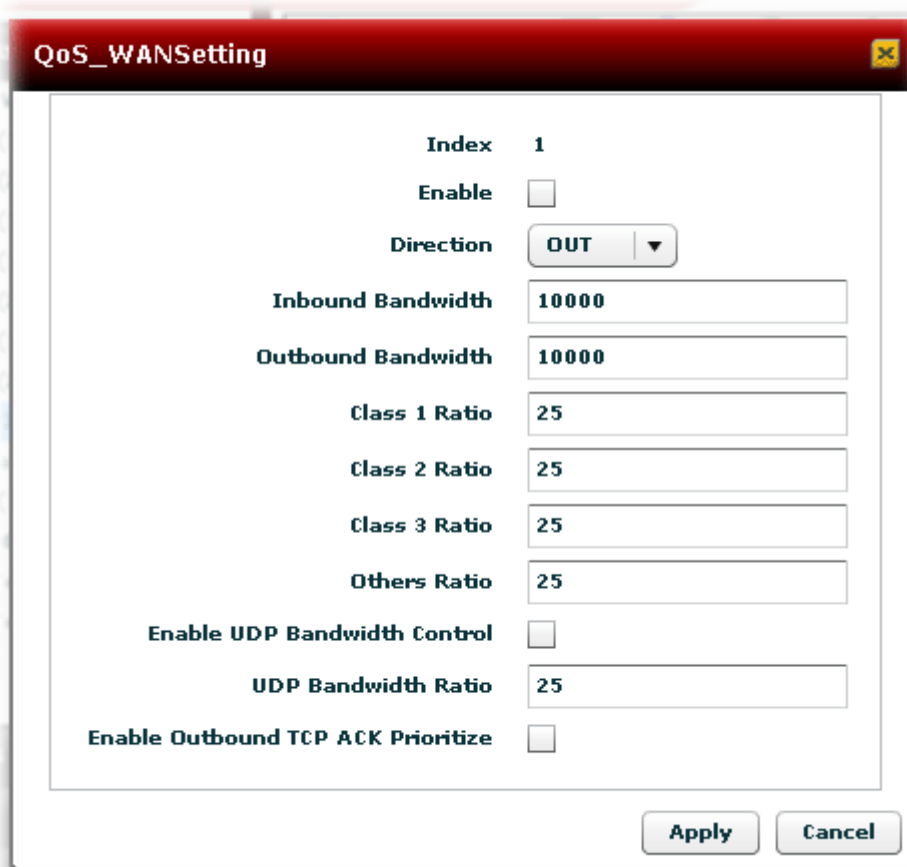
Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable	Display if such profile is enabled (true) or not (false).
Direction	Display the direction (OUT/IN/Both) of such QoS setting.
Inbound Bandwidth	Display the connecting rate of data input for WAN.
Outbound Bandwidth	Display the connecting rate of data output for WAN
Class 1 Ratio/ Class 2 Ratio/ Class 3 Ratio	Display the ratio of bandwidth fo the class rules (up to three) that configured to meet your request.
Others Ratio	Display the ratio of bandwidth reserved for the packets which are not suitable for the user-defined class rules.

Items	Description
Enable UDP Bandwidth Control	Display if the function is enabled (true) or not (false).
UDP Bandwidth Ratio	Display the ratio of bandwidth configured for UDP.
 Save parameter settings	Click this button to save the parameters settings for the profile.
 Edit	Click it to edit the settings of the selected item.

Editing the QoS WAN Setting

To modify the QoS WAN setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



QoS_WANSetting

Index: 1

Enable: ☐

Direction: OUT ▼

Inbound Bandwidth: 10000

Outbound Bandwidth: 10000

Class 1 Ratio: 25

Class 2 Ratio: 25

Class 3 Ratio: 25

Others Ratio: 25

Enable UDP Bandwidth Control: ☐

UDP Bandwidth Ratio: 25

Enable Outbound TCP ACK Prioritize: ☐

Apply Cancel

Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Enable	Check the box to enable QoS WAN setting.
Direction	Define which traffic the QoS Control settings will apply to. IN- apply to incoming traffic only. OUT- apply to outgoing traffic only.

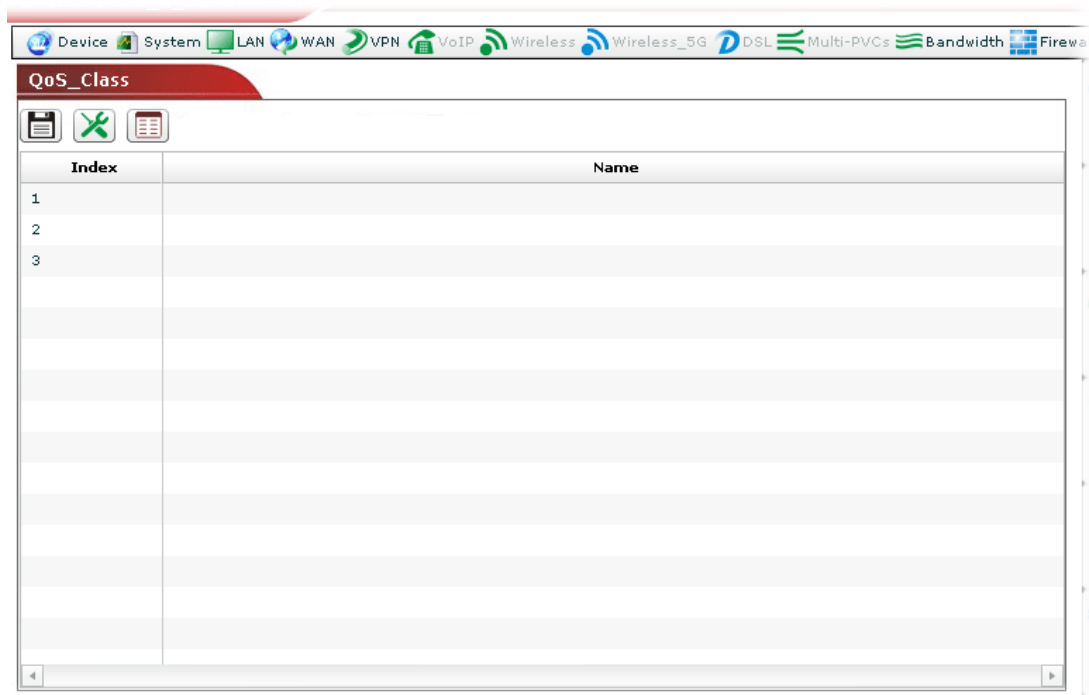
Items	Description
	BOTH- apply to both incoming and outgoing traffic.
Inbound Bandwidth	Set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
Outbound Bandwidth	Set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Class 1 Ratio/ Class 2 Ratio/ Class 3 Ratio/ Others Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed .
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field.
UDP Bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.
Enable Outbound TCP ACK Prioritize	Check this box to push ACK of upload faster to speed the network traffic.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring QoS Class Setting for the Selected CPE

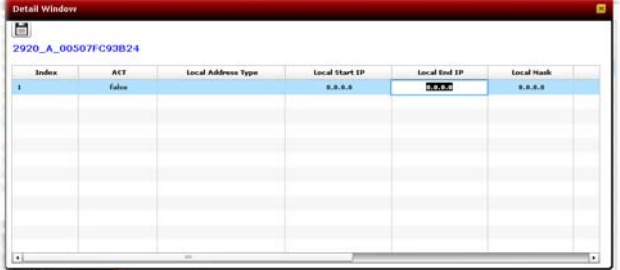
The QoS class rules (Class 1 to Class 3) can be adjusted for your necessity.



Open **Bandwidth>>QoS WAN**. The following screen will appear with all of the QoS class rule settings for the selected CPE/group.

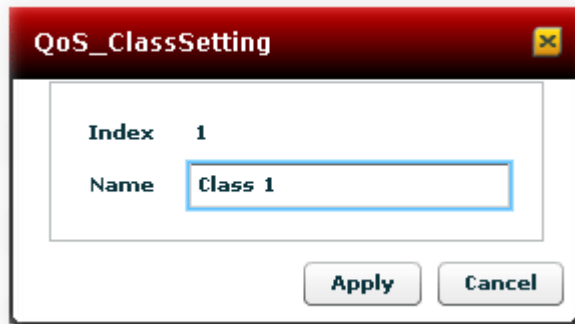


Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Display the name of the QoS Class.
 Save parameter settings	Click this button to save the parameters settings for the profile.
 Edit	Click it to edit the settings of the selected item.
 Detail	Such button will bring up another dialog and display detailed information for the selected CPE.  Move the mouse button to the place below the setting items. Click it to modify the status or settings (local start IP, local end IP, local mask, etc.) for such CPE.

Editing the QoS Class Setting

To modify the QoS Class setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



QoS_ClassSetting

Index 1

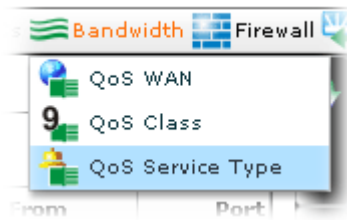
Name Class 1

Apply Cancel

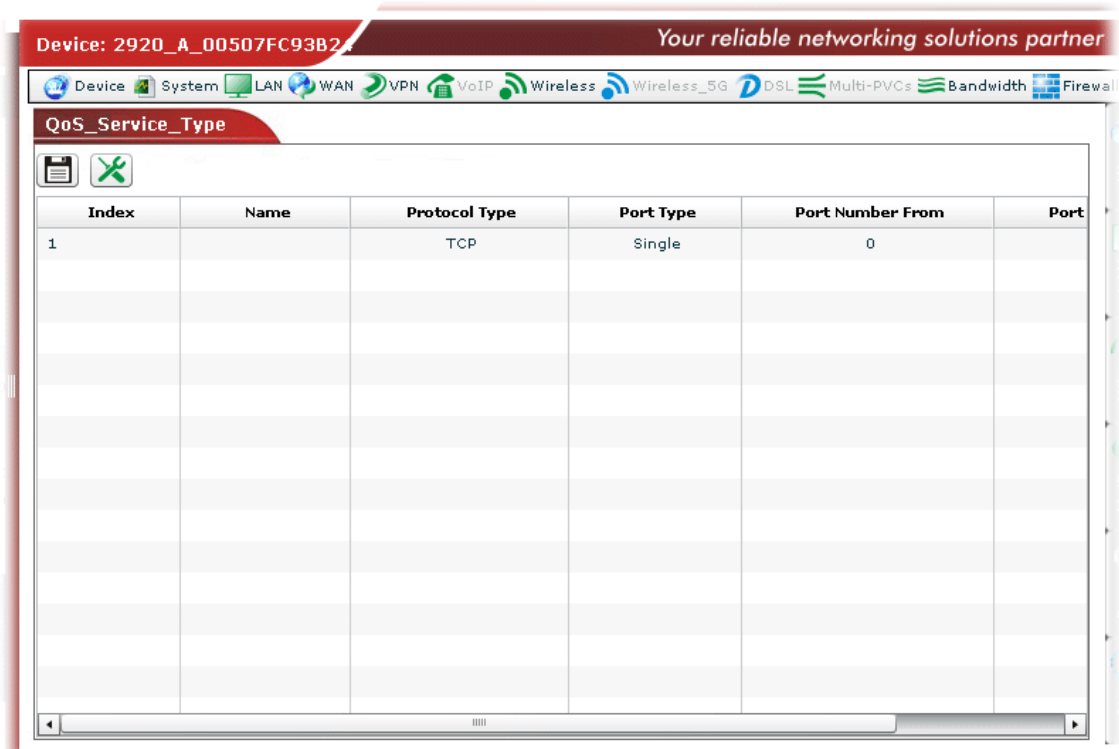
Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Type a name for such class setting.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring QoS Service Type Setting for the Selected CPE



Open **Bandwidth>>QoS WAN**. The following screen will appear with all of the QoS service

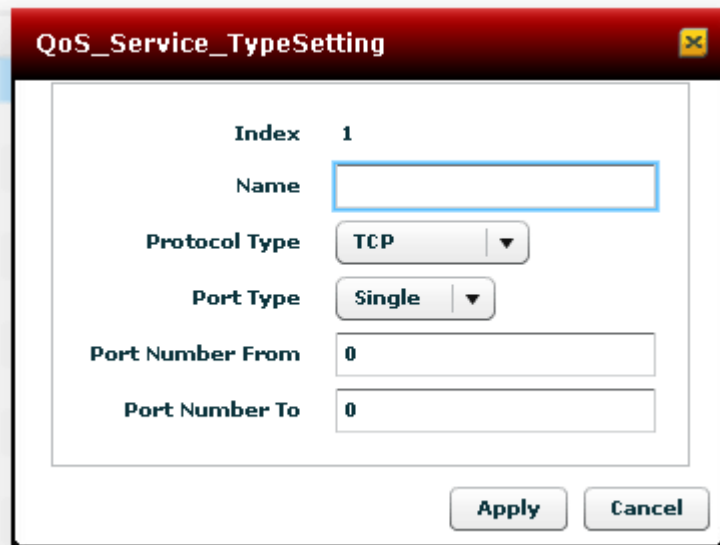


Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Display the name of the QoS Class.
Protocol Type	Display the protocol selected for such service type.
Port Type	Display the port type (single or range) used for such service type.
Port Number From	Display the starting port number.
Port Number To	Display the ending port number.
 Save parameter settings	Click this button to save the parameters settings for the profile.
 Edit	Click it to edit the settings of the selected item.

Editing the QoS Service Type Setting

To modify the QoS service type setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.



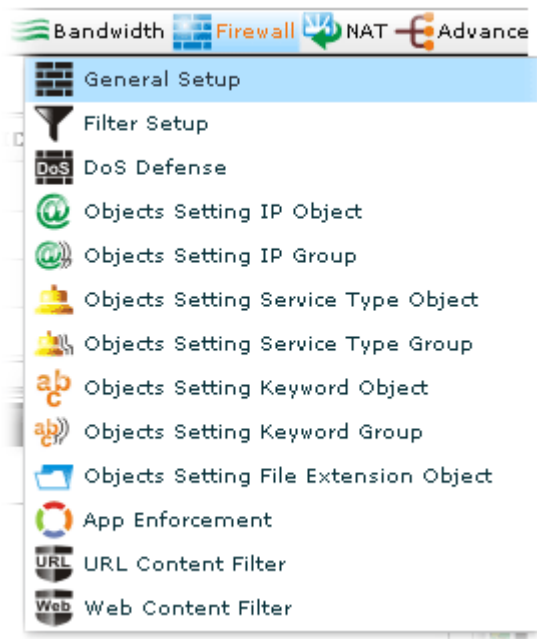
Available settings for such feature will be shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Type a name for the QoS service type.
Protocol Type	Choose the type (TCP, UDP or TCP/UDP) for the new service
Port Type	Click Single or Range as the Type . If you select Range, you have to type in the starting port number and the end porting number on the boxes below.
Port Number From/ Port Number To	Type the same number for starting port and the ending port if you choose Single as the type. For Range, type the different values for these two boxes.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

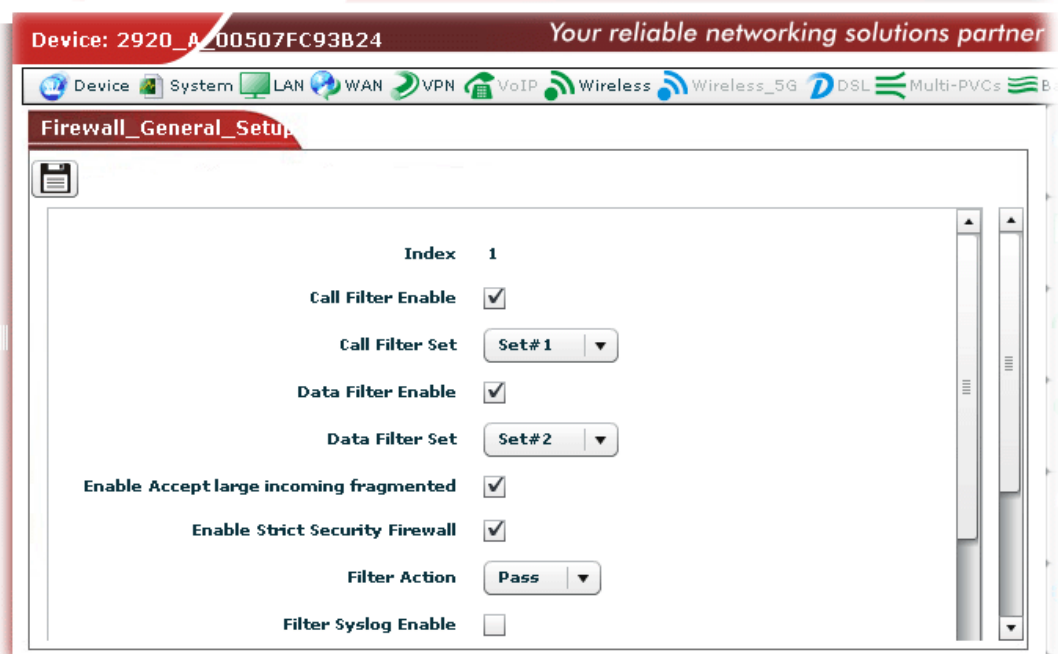
6.2.14 Firewall Settings for the Selected CPE

Configuring General Setup of Firewall for the Selected CPE

General Setup for firewall allows you to adjust settings of IP Filter and common options for the selected CPE.

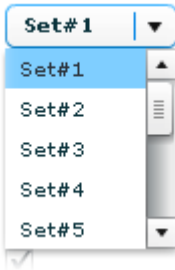
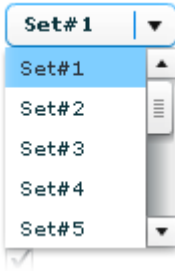


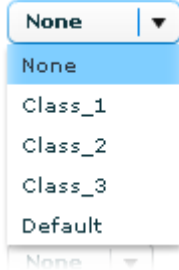
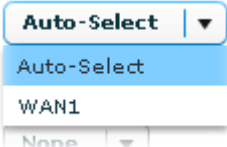
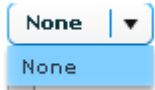
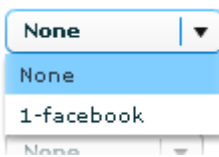
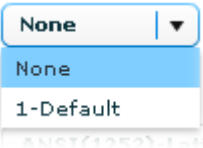
Open **Firewall>>General Setup**. The following screen will appear.

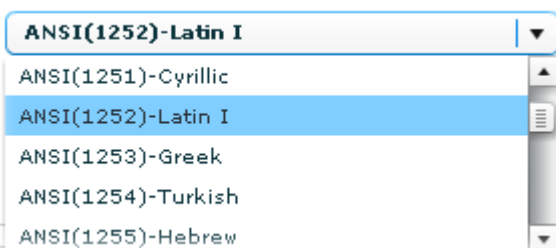


Available settings are shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.

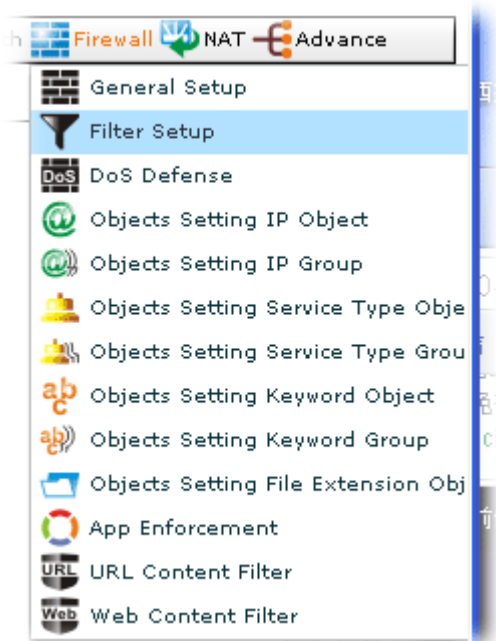
Items	Description
Index	Display the index number of the profile in current network group.
Call Filter Enable	Check Enable to activate the Call Filter function.
Call Filter Set	Assign a start filter set for the Call Filter. 
Data Filter Enable	Check Enable to activate the Data Filter function.
Data Filter Set	Assign a start filter set for the Data Filter. 
Enable Accept large incoming fragmented	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable “ Accept large incoming fragmented ”.
Enable Strict Security Firewall	Check the box to enable such function. All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router if such feature is enabled.
Filter Action	Select Pass or Block for the packets that do not match with the filter rules. 
Filter Syslog Enable	Check the box to make the data filter being sent to Syslog server.
Session Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page.

Items	Description
Session Control Syslog Enable	Check the box to make the session control information being sent to Syslog server.
QoS	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. 
QoS Syslog Enable	Check the box to make the QoS data being sent to Syslog server.
Load-Balance policy	Choose the WAN interface for applying Load-Balance Policy. 
Load-Balance policy Syslog Enable	Check the box to make the load-balance policy being sent to Syslog server.
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. 
APP Enforcement Syslog Enable	Check the box to make the APP enforcement data being sent to Syslog server.
URL Content Filter	
URL Content Filter Syslog Enable	Check the box to make the URL content filter data being sent to Syslog server.
Web Content Filter	Select one of the Web Content Filter profile setting. 
Web Content Filter Syslog	Check the box to make the web content filter data

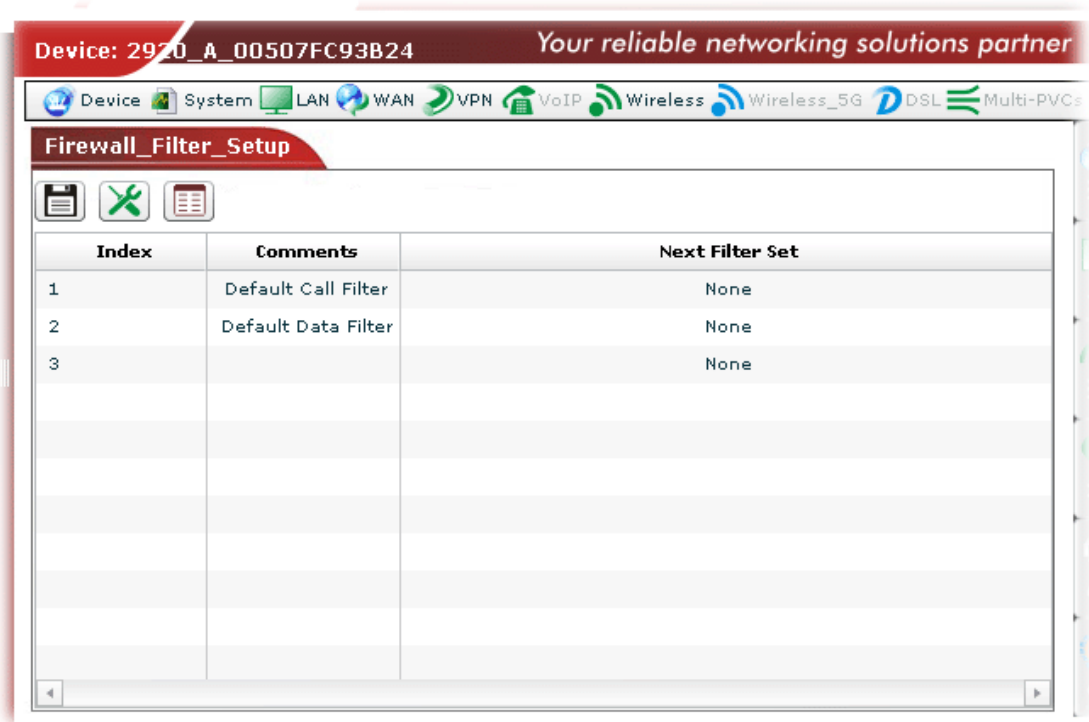
Items	Description
Enable	being sent to Syslog server.
Codepage	It is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. 
Window size	It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.
Session timeout	Setting timeout for sessions can make the best utilization of network resources.

Configuring Filter Setup of Firewall for the Selected CPE

Firewall filter can filter out specific packets that trigger the router to build an unwanted outgoing connection.



Open **Firewall>>Filter Setup**. The following screen will appear.

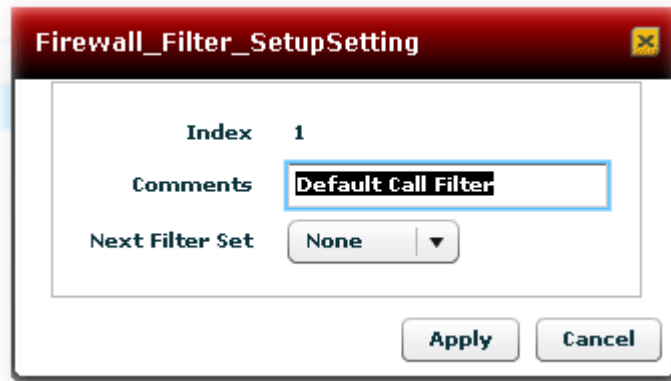


Available settings are shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
 Detail	Click it to edit the advanced settings of the selected profile. 
Index	Display the index number of the profile in current network group.
Comments	Display filter set comments/description.
Next Filter Set	Display the name of the next filter set.

Editing the Filter Setup Setting

To modify the filter setup setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

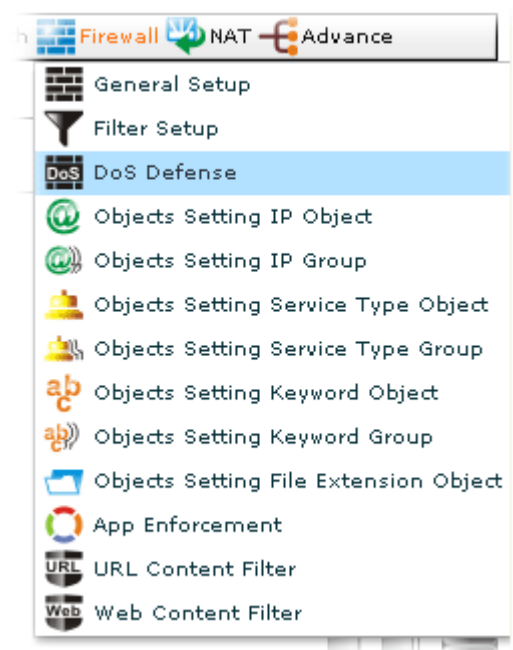


Available settings for such feature will be shown as follows:

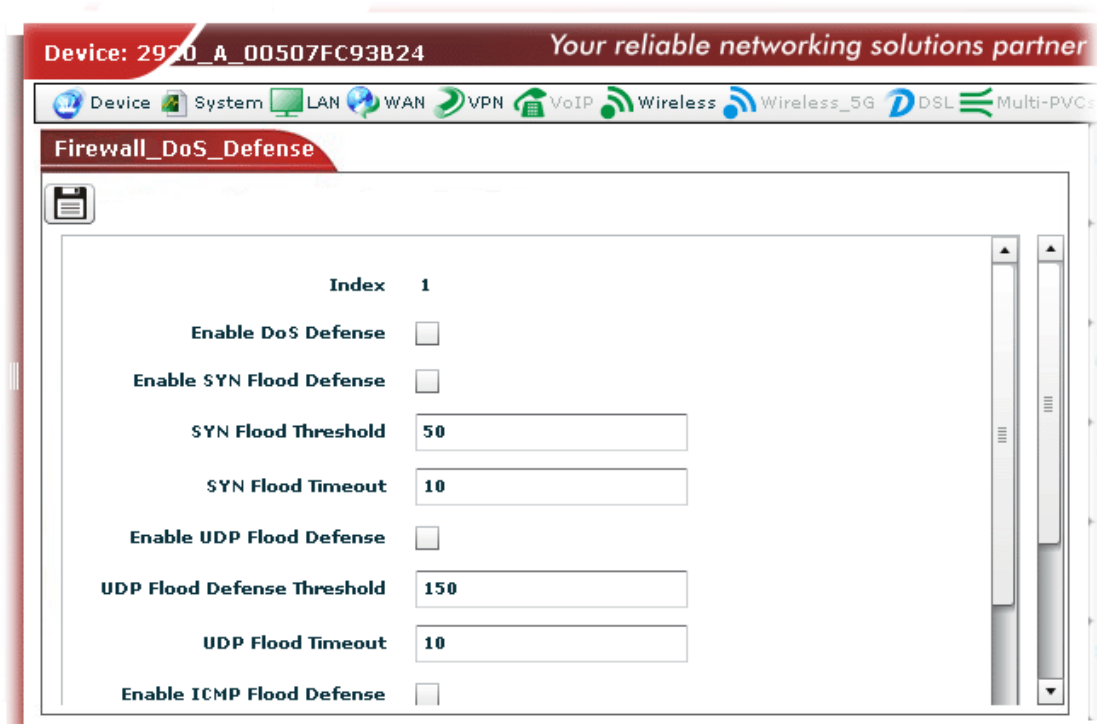
Items	Description
Index	Display the index number of the profile in current network group.
Comments	Enter filter set comments/description. Maximum length is 23-character long.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring DoS Defense of Firewall for the Selected CPE

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



Open **Firewall>>DoS Defense**. The following screen will appear.



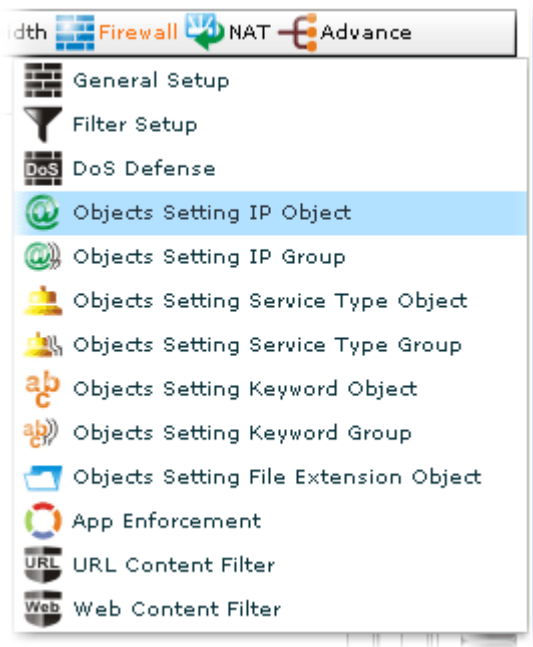
Available settings are shown as follows:

Items	Description
 Save parameter	Click this button to save the parameters settings.

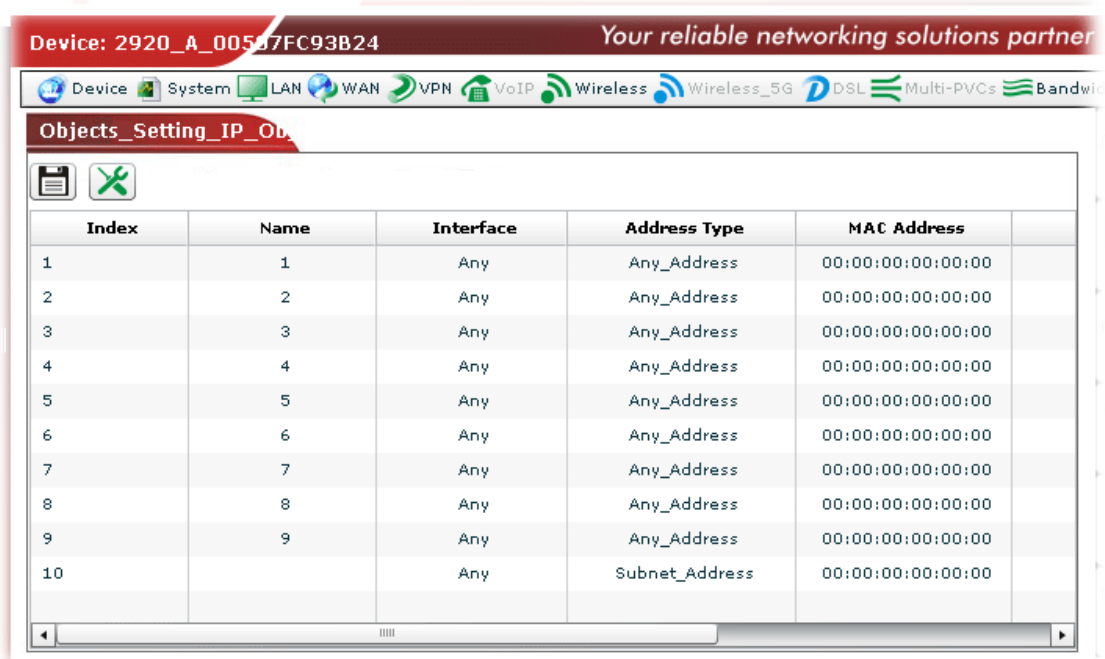
Items	Description
settings	
Index	Display the index number of the profile in current network group.
Enable DoS Defense	Check the box to enable DoS Defense.
Enable SYN Flood Defense	Check the box to enable SYN Flood Defense.
SYN Flood Threshold / SYN Flood Timeout	The goal of the function is to prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP Flood Defense	Check the box to enable UDP Flood Defense.
UDP Flood Defense Threshold/ UDP Flood Timeout	Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP Flood Defense	Check the box to enable ICMP Flood Defense.
ICMP Flood Threshold/ ICMP Flood Timeout	Check the box to activate the ICMP flood defense function. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively
Enable Port Scan Detection	Check the box to enable Port Scan Defense.
Port Scan Threshold	The Vigor router sets the threshold as 150 packets per second.
Block IP Options	Check the box to activate the Block IP options function.
Block TCP Flag Scan	Check the box to activate the Block TCP flag scan function.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks.
Block Tear Drop	Check the box to activate the Block Tear Drop function.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block Ping of Death	Check the box to activate the Block Ping of Death function.
Block Trace Route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block ICMP fragment	Check the box to activate the Block ICMP fragment function.
Block SYN fragment	Check the box to activate the Block SYN fragment function.
Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function.

Configuring IP Object Setting of Firewall for the Selected CPE

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 that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).



Open **Firewall>>Objects Setting IP Object**. The following screen will appear.



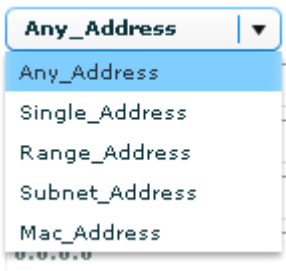
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Name	Display the name of the selected profile.
Interface	Display the interface of the selected profile.
Address Type	Display the address type of the selected profile.
MAC Address	Display the MAC address of the selected profile.
Start IP Address	Display the start IP address of the selected profile.
End IP Address	Display the end IP address of the selected profile.
Subnet Mask	Display the subnet mask of the selected profile.
Invert Selection	Display if the function is enabled (true) or disabled (false).

Editing the IP Object Setting

To modify the IP Object setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

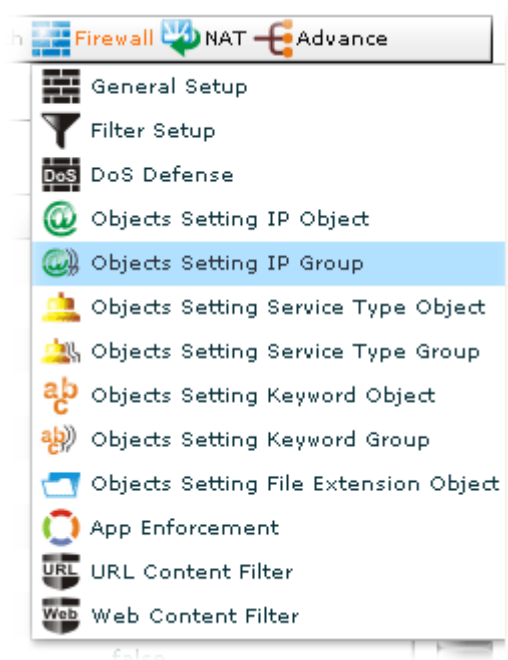
Available settings are shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Interface	Choose an interface you want.
Address Type	Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address. Select Mac Address if this object contains Mac address. 
MAC Address	Type the MAC address of the network card which will be

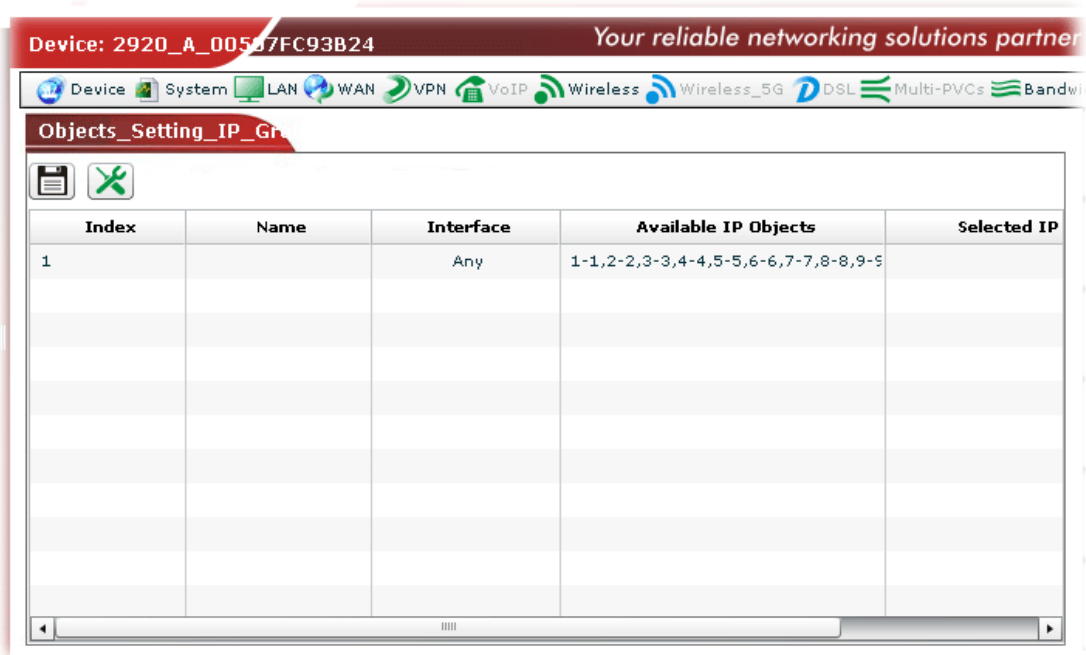
Items	Description
	controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring IP Group Setting of Firewall for the Selected CPE

Several IP objects can be grouped under one IP group profile.



Open **Firewall>>Objects Setting IP Group**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Name	Display the profile name of the IP group.
Interface	Display the interface for the IP group.
Available IP Objects	Display all the available IP objects in this field.
Selected IP Objects	Display the profile name of IP objects under the group.

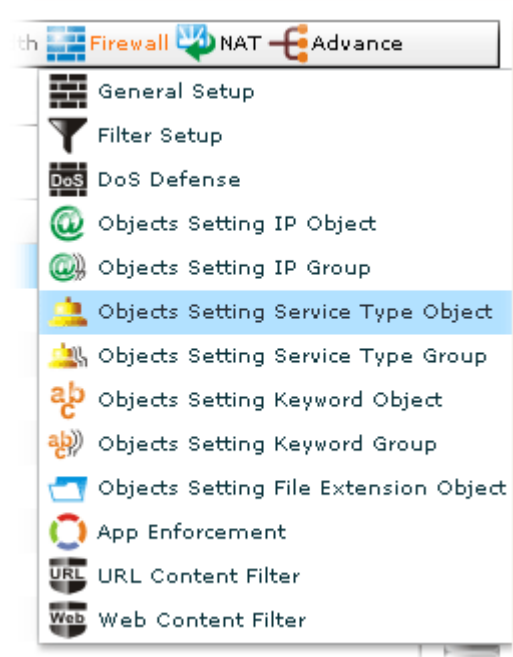
Editing the IP Group Setting

To modify the IP Group setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

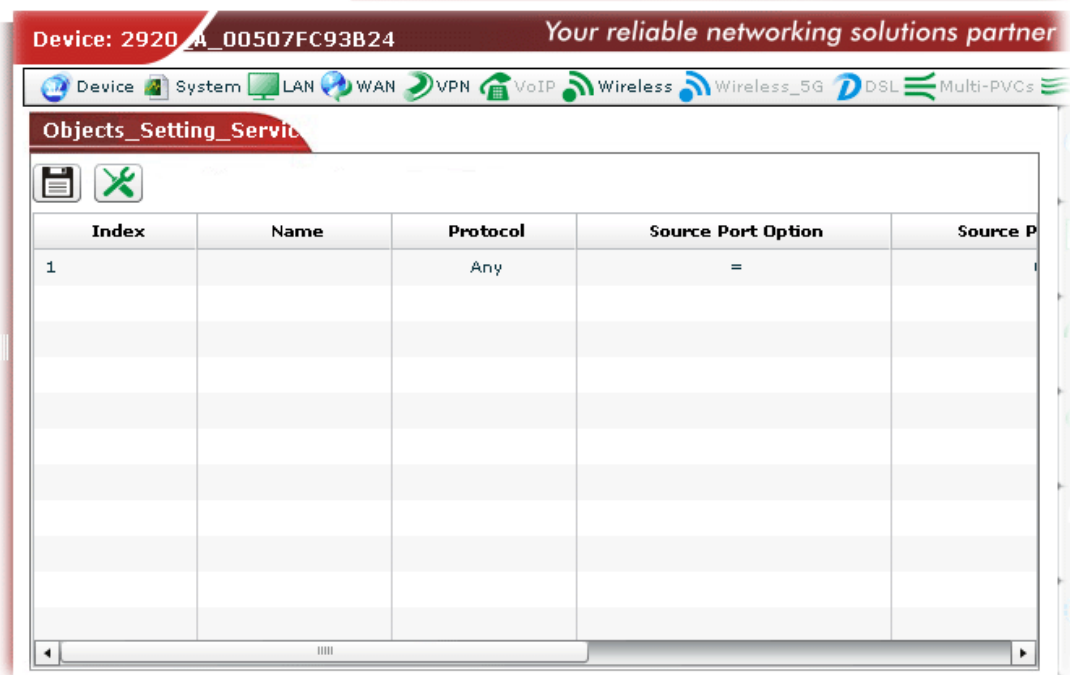
Available settings are shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface will be shown in this box.
Selected IP Objects	Type the profile name of IP objects you want to group in this field.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring Service Type Object Setting of Firewall for the Selected CPE

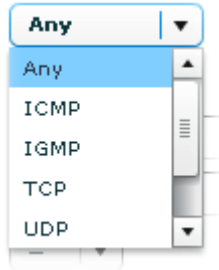


Open **Firewall>>Objects Setting Service Type Object**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Name	Display the name of this profile.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source Port Option / Destination Port Option	Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. (!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) – the port number greater than this value is available. (<) – the port number less than this value is available for this profile.
Source Port From	Display the starting port number of the source.
Source Port To	Display the ending port number of the source.
Destination Port From	Display the starting port number of the destination.
Destination Port To	Display the ending port number of the destination.

Editing the Service Type Object

To modify the service type object setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

Objects_Setting_Service_Type_ObjectSetting

Index: 1

Name:

Protocol: Any

Source Port Option: =

Source Port From: 0

Source Port To: 0

Destination Port Option: =

Destination Port From: 0

Destination Port To: 0

Apply Cancel

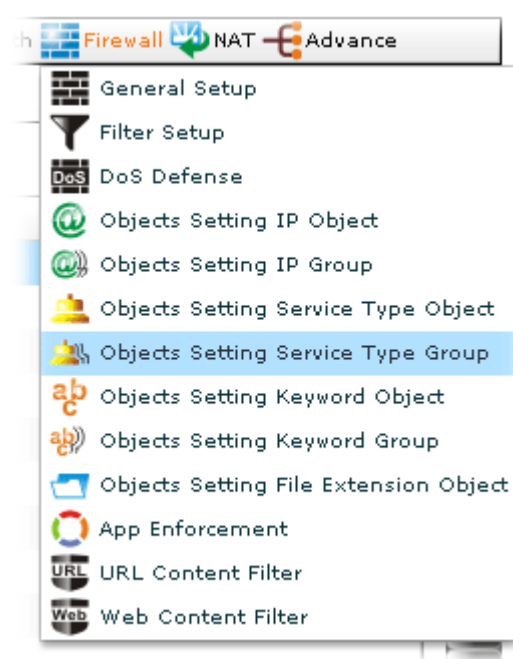
Available settings are shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to.
Source Port Option / Destination Port Option	Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. (!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) – the port number greater than this value is available. (<) – the port number less than this value is available for this profile.
Source Port From	Type a number as starting port.
Source Port To	Type a number as ending port.
Destination Port From	Type a number as starting port.

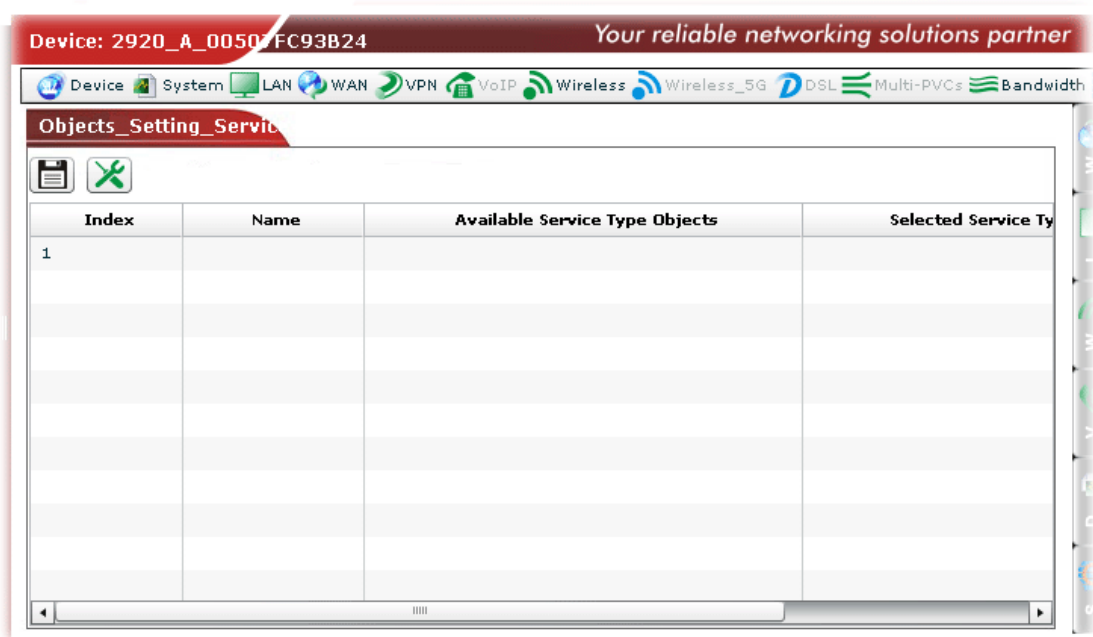
Items	Description
Destination Port To	Type a number as ending port.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring Service Type Group Setting of Firewall for the Selected CPE

Several service type objects can be grouped under one IP group profile.



Open **Firewall>>Objects Setting Service Type Group**. The following screen will appear.



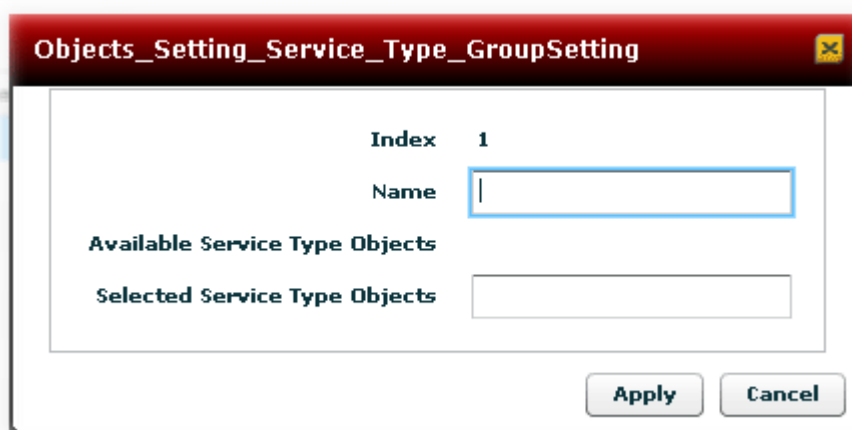
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.

Items	Description
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Name	Display the name of this profile.
Available Service Type Objects	Display all the available service type objects in this field.
Selected Service Type Objects	Display the profile name of service type objects under the group.

Editing the Service Type Group Object

To modify the service type group setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

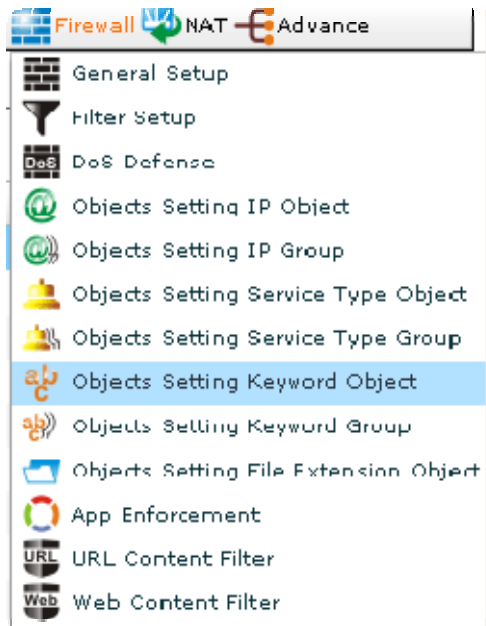


Available settings are shown as follows:

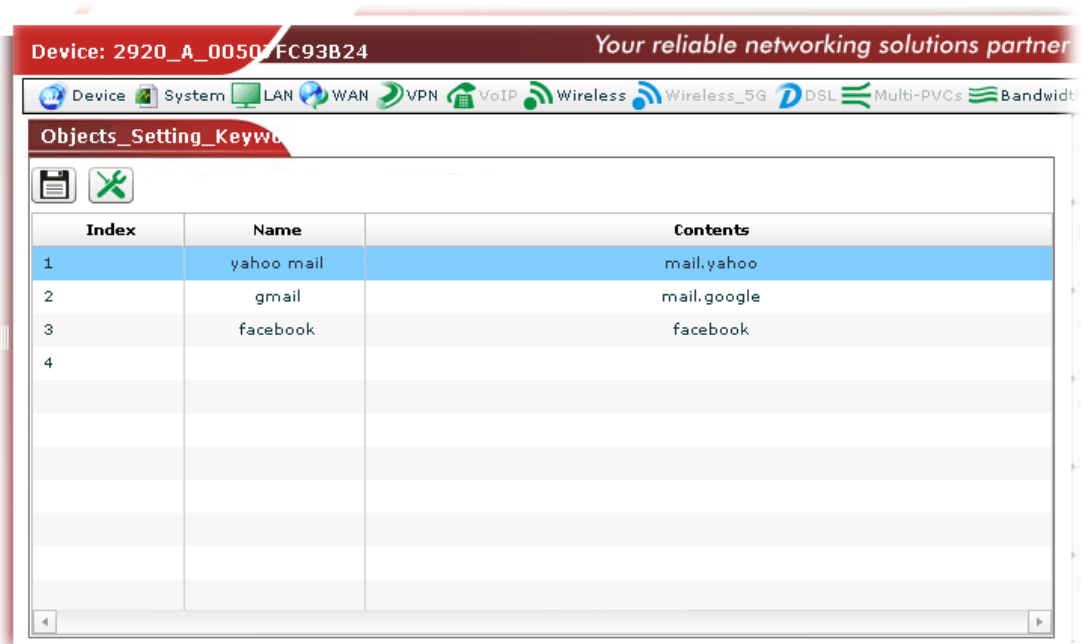
Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service type objects with the specified interface will be shown in this box.
Selected Service Type Objects	Type the profile name of service type objects you want to group in this field.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring Keyword Object Setting of Firewall for the Selected CPE

You can set 200 keyword object profiles for choosing as black /white list used for **URL Content Filter Profile**.



Open **Firewall>>Objects Setting Keyword Object**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Name	Display the name of the profile.
Contents	Display the content of the keyword profile.

Editing the Keyword Object

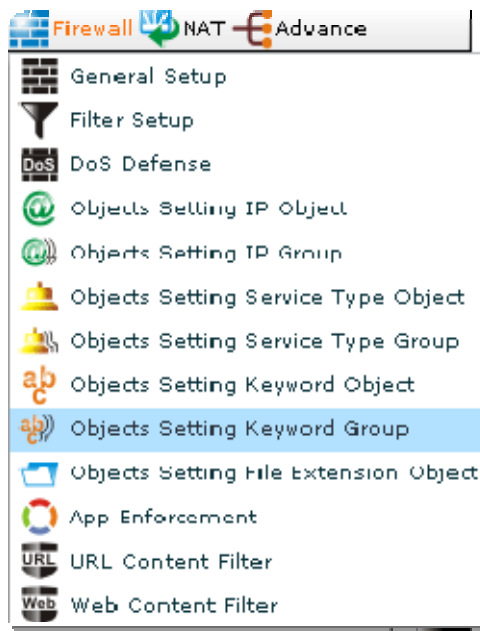
To modify the keyword object setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

Available settings are shown as follows:

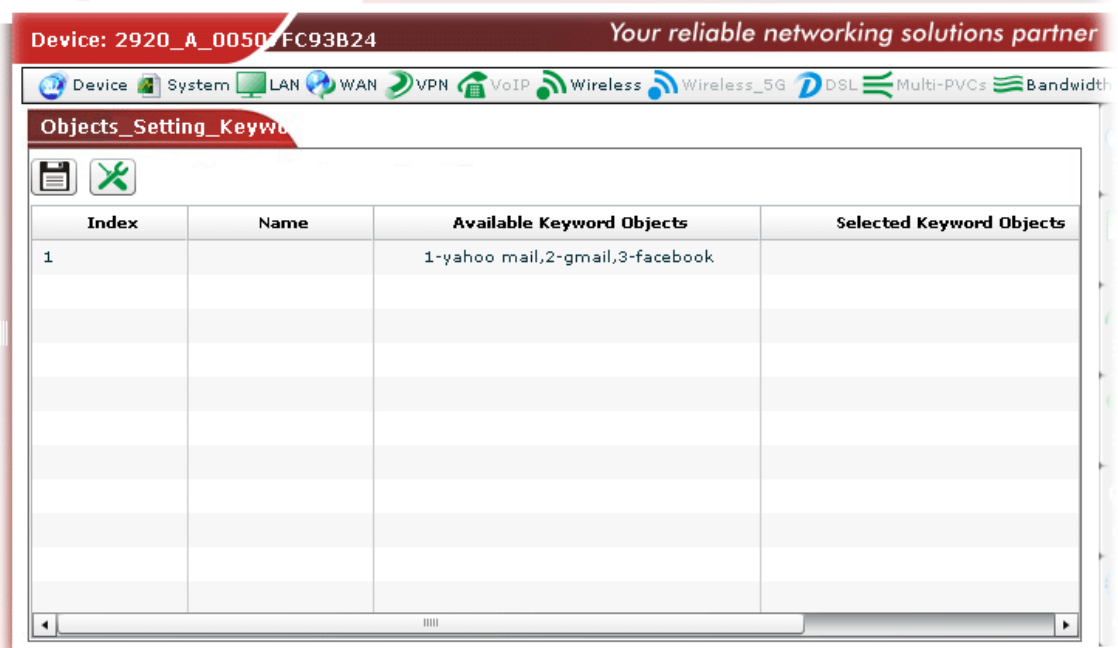
Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Content	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring Keyword Group Setting of Firewall for the Selected CPE

Several keyword group objects can be grouped under one IP group profile.



Open **Firewall>>Objects Setting Keyword Group**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Name	Display the name of this profile.
Available Keyword Objects	Display all the available service type objects in this field.
Selected Keyword Objects	Display the profile name of service type objects under the group.

Editing the Keyword Group

To modify the keyword group setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

Objects_Setting_Keyword_GroupSetting

Index 1

Name

Available Keyword Objects 1-yahoo mail,2-gmail,3-facebook

Selected Keyword Objects

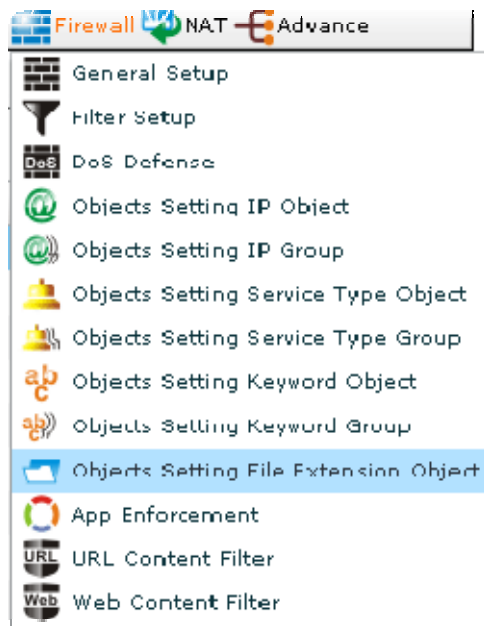
Apply Cancel

Available settings are shown as follows:

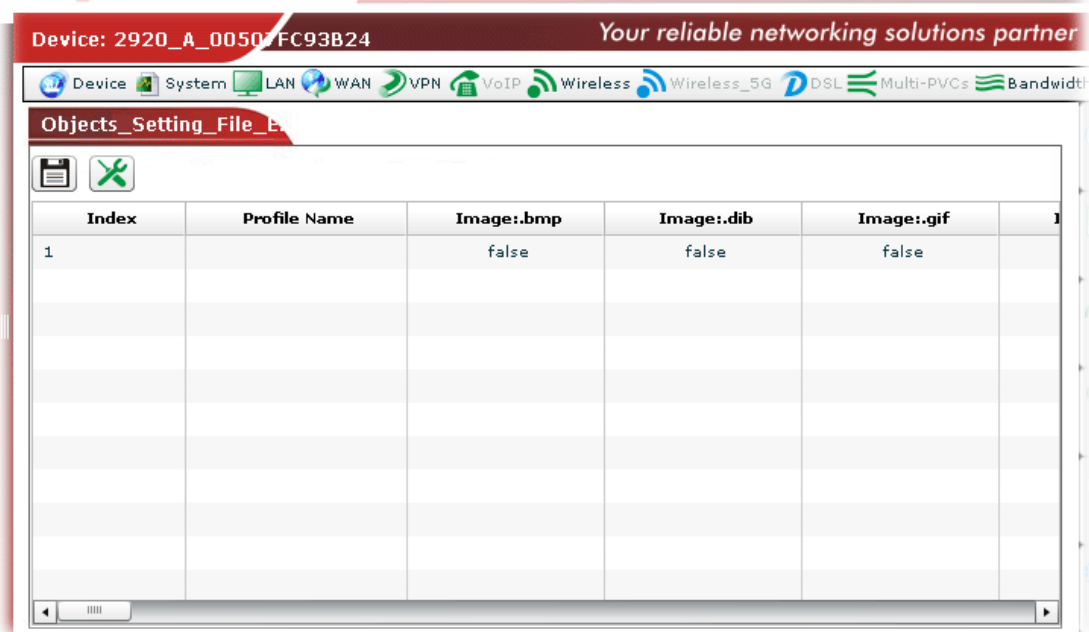
Items	Description
Index	Display the index number of the profile in current network group.
Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Available Keyword Objects	All the available Keyword objects with the specified interface will be shown in this box.
Selected Keyword Objects	Type the name of Keyword objects you want to group in this field.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring File Extension Setting of Firewall for the Selected CPE

All the files with the extension names specified in these profiles will be processed according to the chosen action.



Open **Firewall>>Objects Setting File Extension Object**. The following screen will appear.



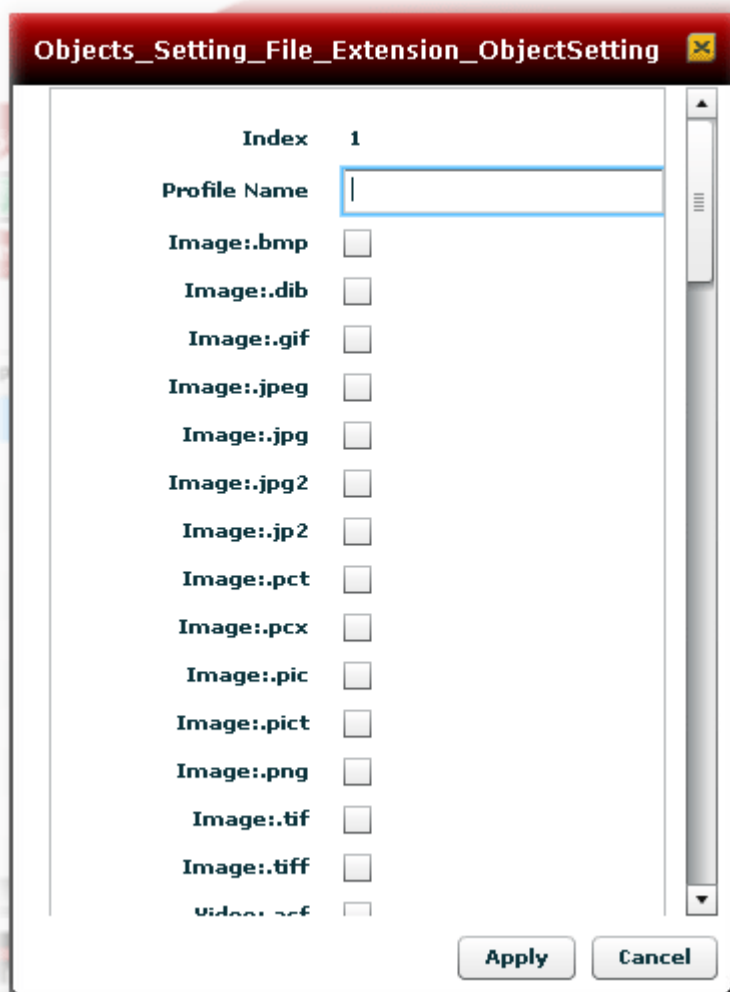
Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Image:.bmp ~ Image:.tiff, Video:.asf ~ Video:.3g2, Audio:.aac ~ Audio:.wma, Java:.class ~ Java:.jtk, ActiveX:.alx ~ ActiveX:.vrm, Compression:.ace ~ Compression:.zip, Execution:.bas ~ Execution:.scr	Display if such file extension is selected (true) or not selected (false) for such profile.

Editing the File Extension Object Setting

To modify the file extension object setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

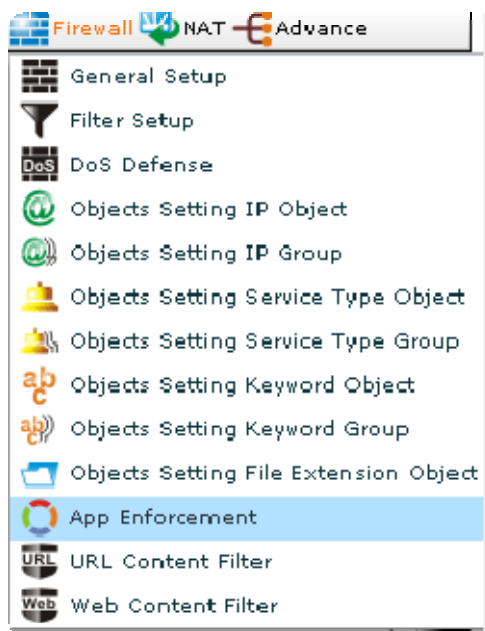


Available settings are shown as follows:

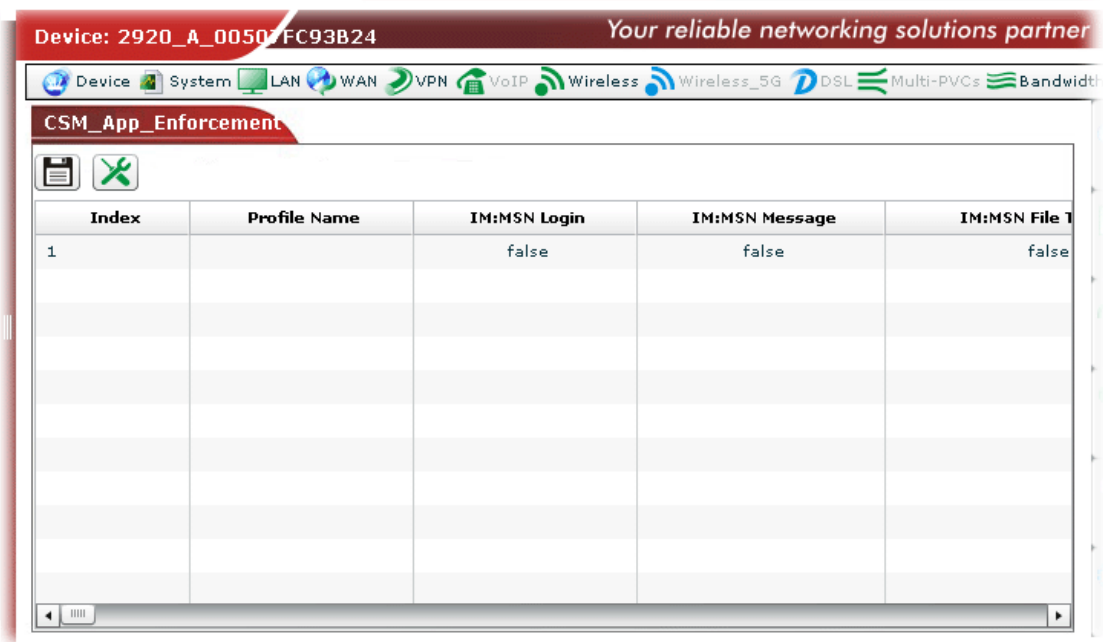
Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Image:.bmp ~ Image.tiff, Execution:.bas ~ Execution:.scr, ...	Check the box of each file extension to make it to be included under the file extension profile. The file extensions specified in this profile will be ignored and not be scanned by Vigor router.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring APP Enforcement Setting of Firewall for the Selected CPE

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



Open **Firewall>>APP Enforcement**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Profile Name	Display the name of the profile.
IM:MSN Login ~ IM:WebIM, P2P:SoulSeek ~ P2P:Kuwo, Protocol:DNS ~ Protocol:Informix, Misc:Tunneling:Socks4/5 ~ Misc:Web HD:OfficeLive	Display if such application is selected (true) or not selected (false) for such profile.

Editing the APP Enforcement Setting

To modify the APP enforcement setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

CSM_App_EnforcementSetting

Index 1

Profile Name

IM:MSN Login ☐

IM:MSN Message ☐

IM:MSN File Transfer ☐

IM:MSN Game ☐

IM:MSN ☐

IM:MSN Other ☐

IM:Yahoo Login ☐

IM:Yahoo Message ☐

IM:Yahoo File Transfer ☐

IM:Yahoo Conference ☐

IM:Yahoo Other ☐

IM:AIM Login ☐

IM:AIM Message ☐

IM:AIM File Transfer ☐

IM:AIM Game ☐

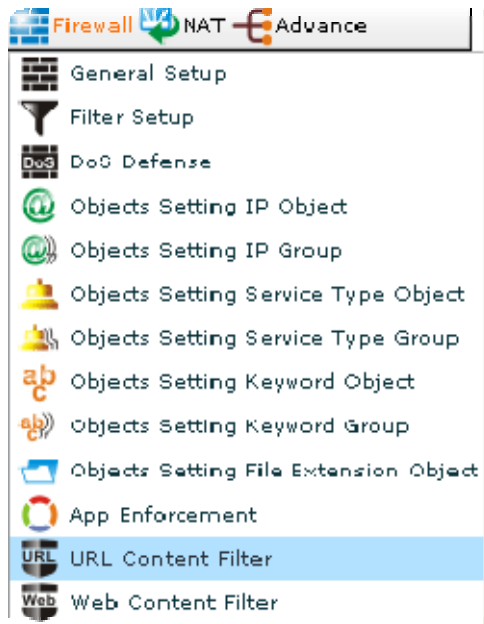
Apply Cancel

Available settings are shown as follows:

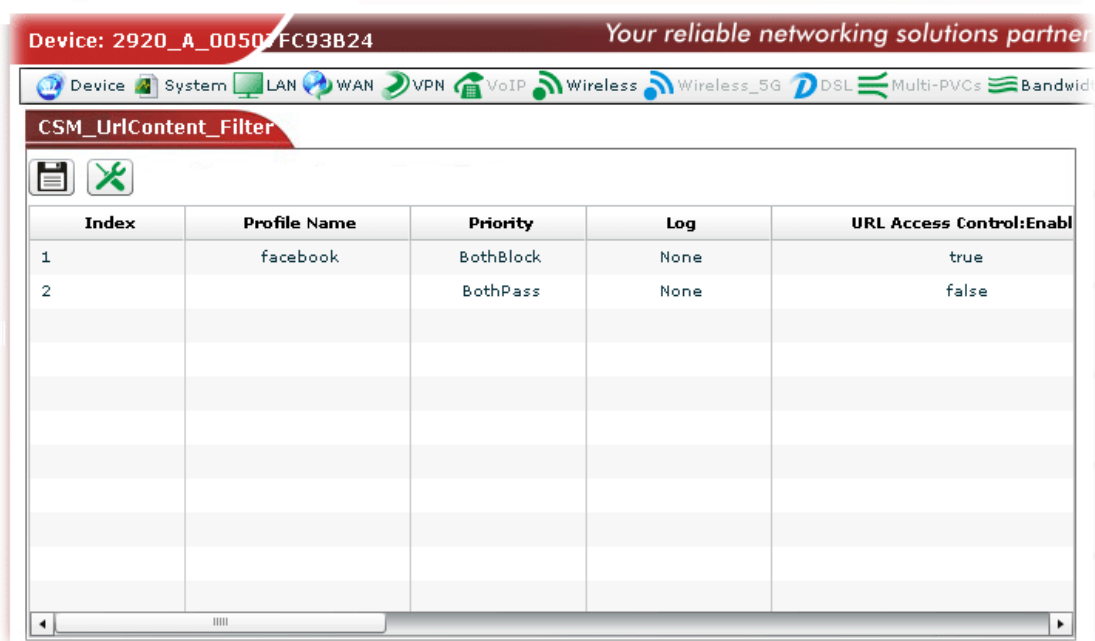
Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
IM:MSN Login ~ IM:WebIM, 5 ~ Misc:Web HD:OfficeLive,.....	Check the box of each APP to make it to be included under the profile. The APP specified in this profile will be ignored and not be scanned by Vigor router.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring URL Content Filter Setting of Firewall for the Selected CPE

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



Open **Firewall>>URL Content Filter**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.
 Edit	Click it to edit the settings of the selected profile.

Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Display the name of the profile.
Priority	Display the action that the CPE will apply.
Log	Display the log with the action recorded for this profile.
URL Access Control:Enable	Display if such function is enabled (true) or disabled (false).
URL Access Control:Prevent web access from IP address	Display if such function is enabled (true) or disabled (false).
URL Access Control:Action	Display the action (Pass or Block) of such feature adopted by this profile.
URL Access Control:Keyword Object1	Display the object profile selected for URL Access Control by this profile.
URL Access Control:Keyword Group1	Display the object group profile selected for URL Access Control by this profile.
Web Feature: Enable	Display if such function is enabled (true) or disabled (false).
Web Feature:Action	Display the action (Pass or Block) of such feature adopted by this profile.
Web Feature:Cookie	Display if such function is enabled (true) or disabled (false).
Web Feature:Proxy	Display if such function is enabled (true) or disabled (false).
Web Feature:Upload	Display if such function is enabled (true) or disabled (false).
Web Feature:File Extension Profile	Display the profile adopted by this profile.

Editing the URL Content Filter Setting

To modify the URL content filter setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

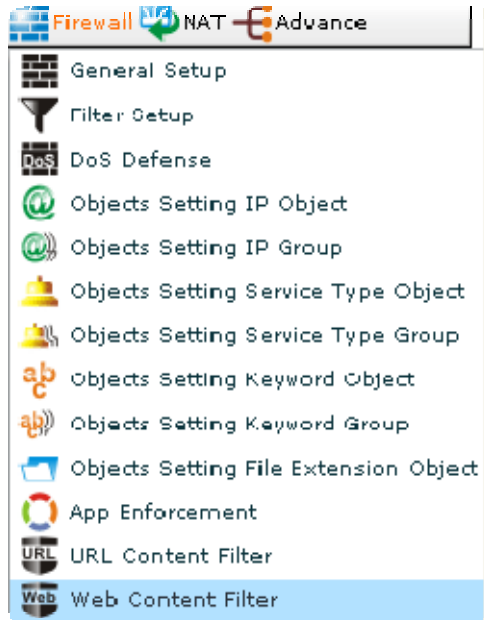
Available settings are shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Priority	It determines the action that this router will apply. Use the drop down list to choose the one you want.
Log	None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog. All – All the actions (Pass and Block) will be recorded in Syslog.
URL Access Control:Enable	Check the box to activate URL Access Control.
URL Access Control:Prevent web access from IP address	Check the box to activate the function of Prevent web access from IP address for URL Access Control.
URL Access Control:Action	Pass - Allow accessing into the corresponding webpage. Block - Restrict accessing into the corresponding webpage. If the web pages do not match with the specified feature set here, it will be processed with reverse action.

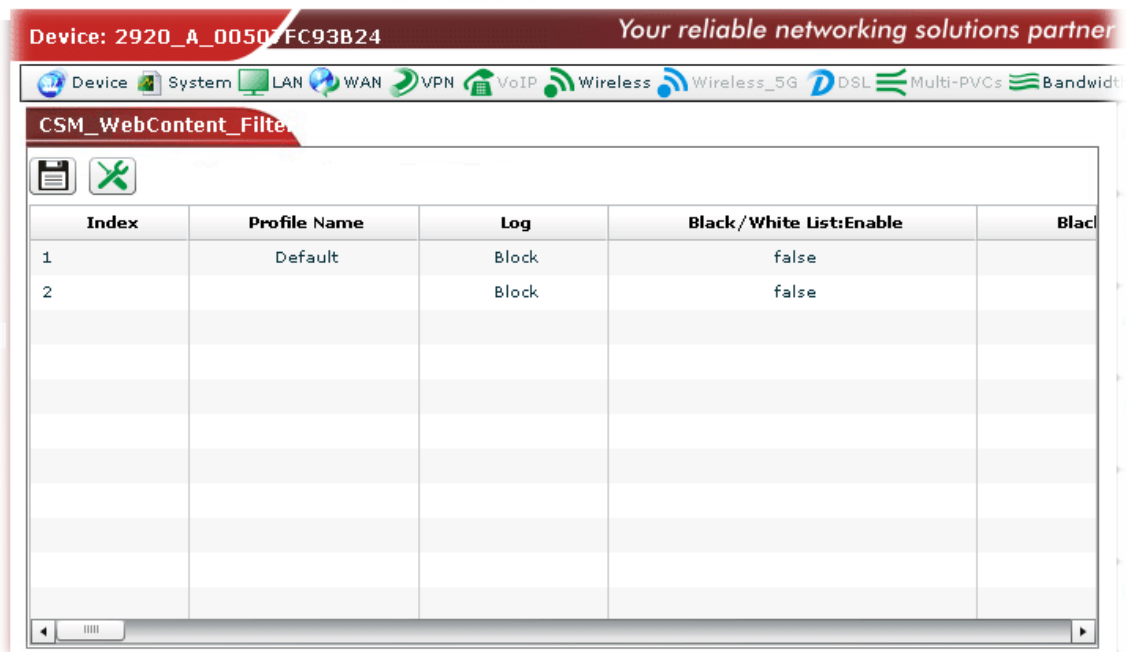
Items	Description
	
URL Access Control:Keyword Object1	Use the drop down list to choose the profile you want.
URL Access Control:Keyword Group1	Use the drop down list to choose the profile you want.
Web Feature: Enable	Check the box to activate Web Feature.
Web Feature:Action	Pass - Allow accessing into the corresponding webpage. Block - Restrict accessing into the corresponding webpage. If the web pages do not match with the specified feature set here, it will be processed with reverse action. 
Web Feature:Cookie	Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
Web Feature:Proxy	Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.
Web Feature:Upload	Check the box to upload data with the limitation of Web Feature.
Web Feature:File Extension Profile	Use the drop down list to choose the profile you want.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

Configuring Web Content Filter Setting of Firewall for the Selected CPE

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. For parents, you can protect your children from viewing adult websites or chat rooms.



Open **Firewall>>Web Content Filter**. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Save parameter settings	Click this button to save the parameters settings.

Items	Description
 Edit	Click it to edit the settings of the selected profile.
Index	Display the index number of the profile in current network group.
Profile Name	Display the name of the profile.
Log	Display the log with the action recorded for this profile.
Black/White List:Enable	Display if such function is enabled (true) or disabled (false).
Black/White List:Action	Display the action (Pass or Block) of such feature adopted by this profile.
Black/White List:Keyword Object 1	Display the keyword object profile selected for this profile.
Black/White List:Keyword Group 1	Display the keyword object group profile selected for this profile.
Action	Display the action (Pass or Block) of such feature adopted by this profile.
Child Protection:Alcohol & Tobacco ~ Child Protection:Child Abuse Images, Other, ...	Display if such application is selected (true) or not selected (false) for such profile.

Editing the Web Content Filter Setting

To modify the Web content filter setting, simply choose the one you want to modify from the list and click the **Edit** button. The following screen will appear.

Available settings are shown as follows:

Items	Description
Index	Display the index number of the profile in current network group.
Profile Name	Retype a name for this profile for modification. Maximum 15 characters are allowed.
Log	None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog. All – All the actions (Pass and Block) will be recorded in Syslog.
Black/White List:Enable	Check the box to activate Black/White List filtering.
Black/White List:Action	Pass - Allow accessing into the corresponding webpage. Block - Restrict accessing into the corresponding webpage. If the web pages do not match with the specified feature set here, it will be processed with reverse action. 

Items	Description
Black/White List:Keyword Object 1	Use the drop down list to choose the profile you want.
Black/White List:Keyword Group 1	Use the drop down list to choose the profile you want.
Action	Pass - Allow accessing into the corresponding webpage. Block - Restrict accessing into the corresponding webpage. If the web pages do not match with the specified feature set here, it will be processed with reverse action. 
Child Protection:Alcohol & Tobacco ~ Child Protection:Child Abuse Images, Other,....	Check the box of each web content category to make it to be included under the profile. The web content category specified in this profile will be ignored and not be scanned by Vigor router.
Apply	Click it to save the settings and exit the screen.
Cancel	Click it to exit the screen without saving any change.

6.3 Wizards

Such page offers several wizards for you to implement the backup, restore, firmware upgrade, system reboot, factory reset for CPE and batch activation of WCF license.

6.3.1 Backup Configuration

It allows you to do backup operation for specified CPEs (devices) immediately or within a specified period.

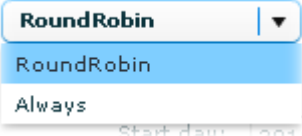
Open **Wizards>>Configuration>>Backup** to display the following page.

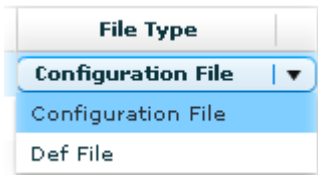
The screenshot shows the DrayTek VigorACS Backup Wizard interface. The left sidebar contains navigation options: Essentials, Networks and Devices, Wizards, Configuration, Backup, Restore, Firmware, Reboot, Factory Reset, My Vigor License, Reports, and Inventory Monitor. The main area is titled 'BackupWizard' and includes the following settings:

- BackupType: RoundRobin (dropdown)
- Period(days): 1 (input field)
- Backup time: Now (radio button selected), Schedule (radio button)
- Start day: 2016-08-03 (calendar icon)
- Start time(HH:MM): 00 : 00 (dropdowns)
- End time(HH:MM): 23 : 59 (dropdowns)

Below these settings is a table titled 'Select devices:' with columns: Name, Model name, Firmware version, Modem version, File Type, and Backup. The table lists various devices and their configurations, including 'Network View(27)', 'alvaco(1)', 'Other(1)', 'RD3(0)', 'RD6(1)', 'RD8(6)', 'RD8_2(3)', and 'test6network(('. Each device has a corresponding 'Configuration File' type and a 'Backup' checkbox.

Available settings for such feature will be shown as follows:

Items	Description
Backup Type	Use the drop down list to choose the backup type for such action. RoundRobin – Choose this type to execute the backup (with global settings). The backup files will be recorded with the filename from 1.cfg to 20.cfg. Only 20 filenames will be kept in the same directory. Always – Choose this type to execute the backup (with global settings) according to the schedule. The backup files will be recorded with the filename one by one (e.g, 1.cfg, 2.cfg,..., 1000cfg,..., 10000cfg,...no limit in file number). All of the backup files will be kept in the same directory. 
Period(days)	Determine the frequency for the configuration backup performed by VigorACS. The default value is 1 day.

Backup time	Now – To perform the firmware backup immediately, choose this one and click Apply. Schedule – To specify a certain time to perform firmware backup, choose this one and specify start day, start time and end time respectively. After finishing the configuration, click Apply. VigorACS will perform firmware backup operation for the selected CPE (s) according to the schedule set here. ● Start day – Use the drop down calendar to specify the day you want to start the firmware backup. ● Start time - Use the drop down menu to specify the hour and minutes you want to start firmware backup. ● End time - Use the drop down menu to specify the hour and minutes you want to finish the firmware backup.
Selected devices	Choose the device that you want to do firmware backup via VigorACS. Specify the File type (Configuration File or Def File) and check the box of Backup. Then click Apply.  If the Backup box the firmware backup is not checked, the backup procedure will not be performed after clicking Apply. Note: Def File means “the default setting file”.
Apply	Execute the action of firmware backup.

6.3.2 Restore configuration

Such page allows you to do firmware restoration for specified CPEs (devices) immediately or within a specified period.

Open **Wizards>>Configuration>>Restore** to display the following page.

Name	Model name	Firmware version	Modem version	File List	Restore
Network View(38)					☐
▶ Carrie(0)					☐
▶ FAE(21)					☐
▶ Jason(3)					☐
▶ Kd5_rd3(3)					☐
▶ MexicoNetwork					☐
▶ NL(4)					☐
▶ Others(0)					☐
▶ RD2(0)					☐
▶ RD3(6)					☐
▶ RD5(0)					☐
▶ RD6(1)					☐

Available settings for such feature will be shown as follows:

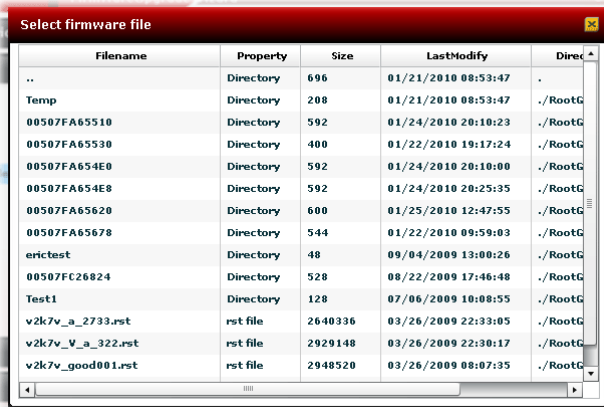
Items	Description
Restore time	Now – To perform the firmware restoration immediately, choose this one and click Apply. Schedule – To specify a certain time to perform firmware restoration, choose this one and specify start day, start time and end time respectively. After finishing the configuration, click Apply. VigorACS will perform firmware restoration operation for the selected CPE (s) according to the schedule set here. ● Start day – Use the drop down calendar to specify the day you want to start the firmware restore. ● Start time - Use the drop down menu to specify the hour and minutes you want to start firmware restore. ● End time - Use the drop down menu to specify the hour and minutes you want to finish the firmware restore.
Selected devices	Choose the device that you want to do firmware restore. Please check the box of Restore , otherwise, the firmware restoration will not be performed after clicking Apply .
Apply	Execute the action of firmware restoration.

6.3.3 Firmware Upgrade for Selected CPE

Firmware upgrade wizard allows you to upgrade firmware for CPEs in specified time or immediately. Open **Wizards>>Firmware>>Firmware Upgrade** to display the following page.

Available settings for such feature will be shown as follows:

Items	Description
Model name	Choose the model name. The related devices will be available for you to choose under Select devices.
Modem version	Display the type (Annex A or Annex B) of the router with type version such as <i>211011_A Hardware: Annex</i> .
Job name	Type the reason to upgrade the firmware. For example, you can type “firewall for protection”. It is just for reference and will not affect the function of firmware upgrade wizard.
Upgrade version	Type the firmware version number for the CPE after finished the firmware upgrade by wizard.
File	Specify a firmware to be used for upgrading the selected CPE(s). Click the blank area to display the following dialog.

	 Double click the item until the <i>rst</i> file is selected.
Upgrade time	Now – To perform the firmware upgrade immediately, choose this one and click Apply. Schedule – To specify a certain time to perform firmware upgrade, choose this one and specify start day, start time and end time respectively. After finishing the configuration, click Apply. VigorACS will perform firmware upgrade operation for the selected CPE (s) according to the schedule set here. ● Start day – Use the drop down calendar to specify the day you want to start the firmware upgrade. ● Start time - Use the drop down menu to specify the hour and minutes you want to start firmware upgrade. ● End time - Use the drop down menu to specify the hour and minutes you want to finish the firmware upgrade.
Selected devices	Choose the device that you want to do firmware backup. Please check the box of Upgrade, otherwise, the firmware upgrade will not be performed after clicking Apply.
Apply	Execute the action of firmware upgrade.

6.3.4 Reboot for Selected CPE(s)

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

Available settings for such feature will be shown as follows:

Items	Description
Period	Determine the frequency for the system reboot performed by VigorACS. The default value is 1 day.
Reboot time	Now – To perform the job immediately. Schedule – 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. ● 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 device(s)	Choose the device that you want to do system reboot. Please check the box of Reboot , otherwise, the system reboot will not be performed after clicking Apply .

Items

Description

Devices:

Name	Model name	Firmware version	Modem version	Reboot
 RD2(0)				☐
 RD3(6)				☐
 RD5(0)				☐
 RD6(0)				☐
 SH(0)				☐
 DrayTek_001D/	Vigor2860n	3.7.4.1_RC1	05-04-04-04-00-01 Annex_A	☒
 DrayTek_00507	Vigor3900	1.0.9_Beta		☐

Apply

Execute the action of firmware upgrade.

6.3.5 Factory Reset for Selected CPE(s)

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

Available settings for such feature will be shown as follows:

Items	Description
Restore time	Now – To perform the job immediately. Schedule – 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. ● 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 device(s)	Choose the device that you want to do factory reset. Please check the box of Reset, otherwise, the factory reset will not be performed after clicking Apply.
Apply	Execute the action of resetting to factory settings.

6.3.6 Batch Activation of MyVigor License for Selected CPE(s)

1. You can activate multiple WCF license(s) for multiple Vigor router(s) at one time. Open **Wizards>>MyVigor License >>Batch Activation** to display the following page.

Name	Model Name	Specify Mail	License Key	License Key	Activate
DrayTek_00507F_Vigor_00507F4	VigorAP 800				☐
DrayTek_00507F_Vigor_00507F5	VigorAP 800				☐
DrayTek_00507F_Vigor_00507F7	Vigor3900	robin_li@draytek.com.tw	954DD-86C66-6D098-6F036		☐
DrayTek_00507F_Vigor_00507F7	Vigor3900				☐
DrayTek_00507F_Vigor_0076204	VigorAP 810				☐
DrayTek_2130	Vigor2130V				☐
provision_test	Vigor2820V			3BFAF-7149F-3957C-626FD	☒

Available settings for such feature will be shown as follows:

Items	Description
UserGroup	Choose the user group for the CPEs required to perform license activation.
UserName	Type the user name which can be used for accessing into MyVigor portal website.
Password	Type the password which can be used for accessing into MyVigor portal website.
Specify Mail	When the license key is expired, the system will send a notification mail to the e-mail address specified here.
Select device(s)	Choose the device that you want to do license activation. Please check the box of Activation , otherwise, the license activation will not be performed after clicking Apply .
License Key	Type the code of the license key in such field.
Activate	Check the box to perform the license activation later.
Next	Click it to open next web page.

- After specifying the required information, click **Next** to get the following page.

BatchActivationWizard Your reliable networking solutions partner

Please go back to confirm your settings again.

MyVigor Account Name: t10414

Mail Address: robin_li@draytek.com.tw

Status	Device Name	MAC Address	License Key Number	Notice
	provision_test	00507FA654E8	38FAF-7149F-3957C-626FD	0000 : Check OK

Previous Finish Cancel

- On the above page, simply check all the information is correct or not. If not, click **Previous** to change the settings.
- If there is no problem, click **Finish**. Now, the system will perform the license activation automatically for lots of CPEs.

6.3.7 Bind with MyVigor Account for Selected CPE(s)

- You can activate the WCF license for Vigor routers at one time. Open **Wizards>>MyVigor License >>Bind With MyVigor Account** to display the following page.

BindAccountWizard Your reliable networking solutions partner

Login Account

UserGroup: RootGroup

UserName: t10414

Password: *****

MyVigor Account Name: robin

MyVigor Account Mail Address: robin_li@draytek.com.tw

Select Devices:

Name	Model Name	MyVigor Account	Mail Address	Activate
DrayTek_00507F_Vigor_00507F487B10	VigorAP 800			☐
DrayTek_00507F_Vigor_00507F522F58	VigorAP 800	robin	robin_li@draytek.com.tw	☐
DrayTek_00507F_Vigor_00507F798528	Vigor3900	robin	robin_li@draytek.com.tw	☐
DrayTek_00507F_Vigor_00507F7883A0	Vigor3900			☐
DrayTek_00507F_Vigor_007620482810	VigorAP 810			☐
DrayTek_2130	Vigor2130V			☐
provision_test	Vigor2820V			☒

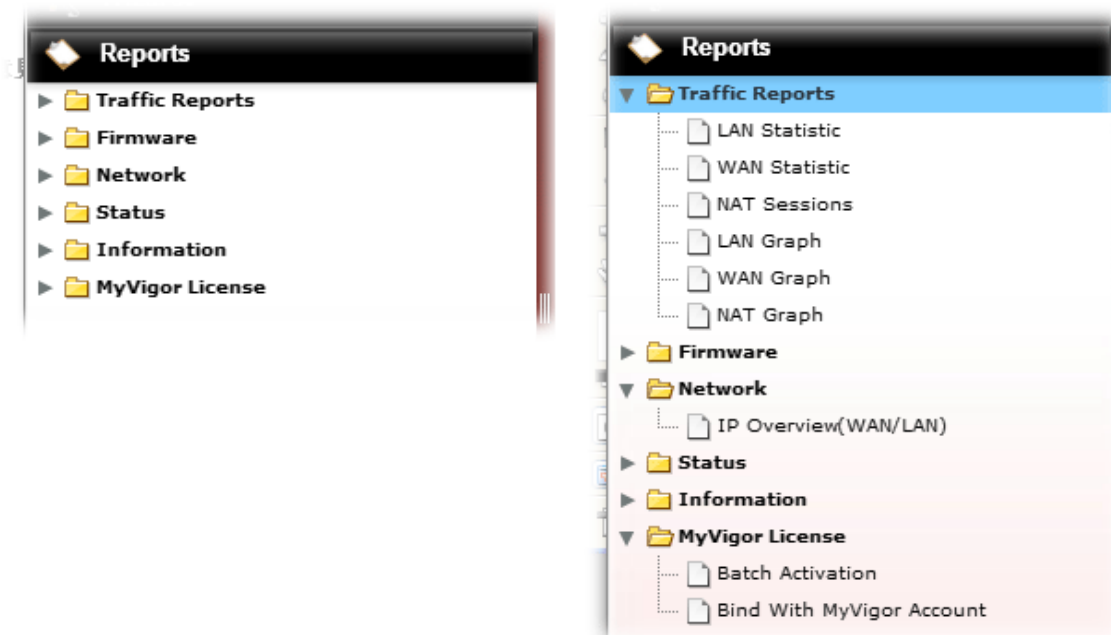
Next Cancel

Available settings for such feature will be shown as follows:

Items	Description
UserGroup	Choose the user group for the CPEs required to perform license activation.
UserName	Type the user name which can be used for accessing into MyVigor portal website.

6.4 Reports

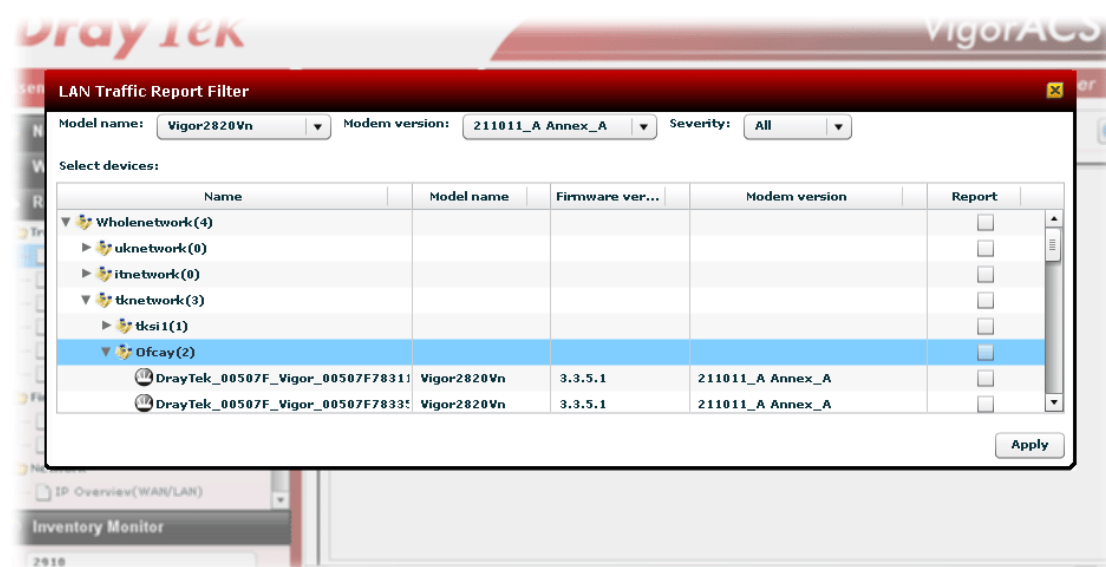
VigorACS allows you to print reports with PDF files. There are several types of reports that you can check and print out. Each type contains several items.



6.4.1 LAN/WAN Statistic

Choose **Traffic Reports**>> **LAN/WAN Statistic** from **Reports**.

Move your mouse to the items you want to print out and click on it. A dialog box will appear. Take **LAN Statistics** as an example.



All the CPEs on the same network group will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

tksi1(1)				
Ofcay(2)				
DrayTek_00507F_Vigor_00507F7831	Vigor2820Vn	3.3.5.1	211011_A Annex_A	☐
DrayTek_00507F_Vigor_00507F7833	Vigor2820Vn	3.3.5.1	211011_A Annex_A	☒
netlinenet(0)				☐
cpmnet(0)				☐
secronnet(0)				☐

Apply

Next, please **Apply**. **VigorACS Report** containing all the records of LAN/WAN configuration for the selected CPE will be shown as the following.

Reports Your reliable networking solutions partner

LAN_Sta...

VigorACS Report

LAN Statistic Report

Device Total Count:1

Device Name	IP	index	TX(B/s)	RX(B/s)
DrayTek_00507F_Vigor_00507F78335	95.9.139.216	1	6.57	63.06

Now, you can print such report as a PDF file or print it out via specified printer.

6.4.2 NAT Sessions

Choose **Traffic Reports>> NAT Sessions** from **Reports**.

Move your mouse to the items you want to print out and click on it. A dialog box will appear.

essentials Reports Your reliable networking solutions partner

NAT Traffic Report Filter

Model name: Modem version: Severity: All

Select devices:

Name	Model name	Firmware ver...	Modem version	Report
Wholenetwork(54)				☐
uknetwork(1)				☐
itnetwork(10)				☐
tknetwork(9)				☐
usanetwork(0)				☐
gmnetwork(0)				☐
bmnetwork(4)				☐
mxnetwork(4)				☐

Apply

All the CPEs on the same network group will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Select devices:

Name	Model name	Firmware ver...	Modem version	Report
▶ acronisnet(0)				☐
▶ armianet(0)				☐
▶ DrayTek_00507F_Vigor_00507FCA4894_	VigorPro 5510	3.3.5	No DSL	☒
▶ DrayTek_00507F_Vigor_00507F5084D8_	Vigor2710Vn	3.3.6	211011_A Annex_A	☒
▶ DrayTek_00507F_Vigor_00507F507FA0_	Vigor2710Vn	3.3.6	211011_A Annex_A	☒
▶ usanetwork(0)				☐
▶ gmnetwork(0)				☐
▶ bmnetwork(4)				☐

Apply

Next, please **Apply**. **VigorACS Report** containing all the records of NAT session for the selected CPE will be shown as the following.

Reports Your reliable networking solutions partner

Page 1 of 1

LAN_Sta... NAT_Ses...

VigorACS Report

NAT Sessions Report

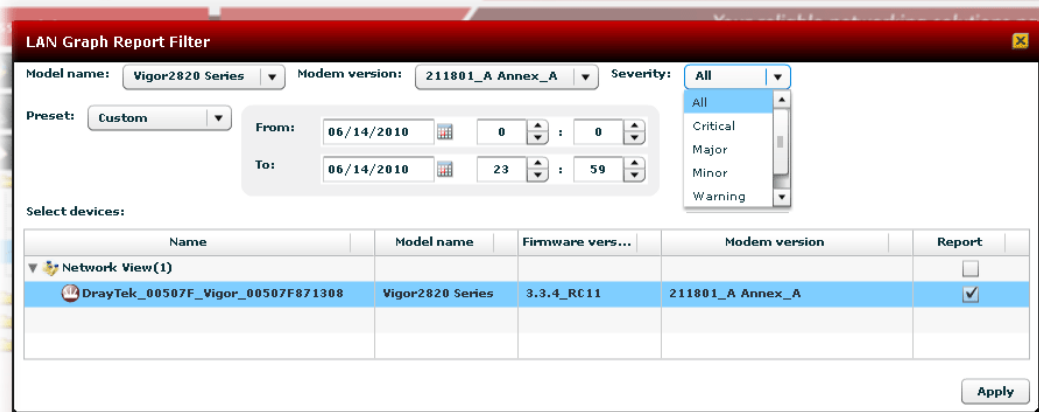
Device Total Count:3

Device Name	IP	index	sessions
DrayTek_00507F_Vigor_00507FCA489	78.186.22.249	1	3
DrayTek_00507F_Vigor_00507F507FA	88.247.22.34	1	0
DrayTek_00507F_Vigor_00507F5084D	88.247.22.244	1	0

6.4.3 LAN/WAN/NAT Graph

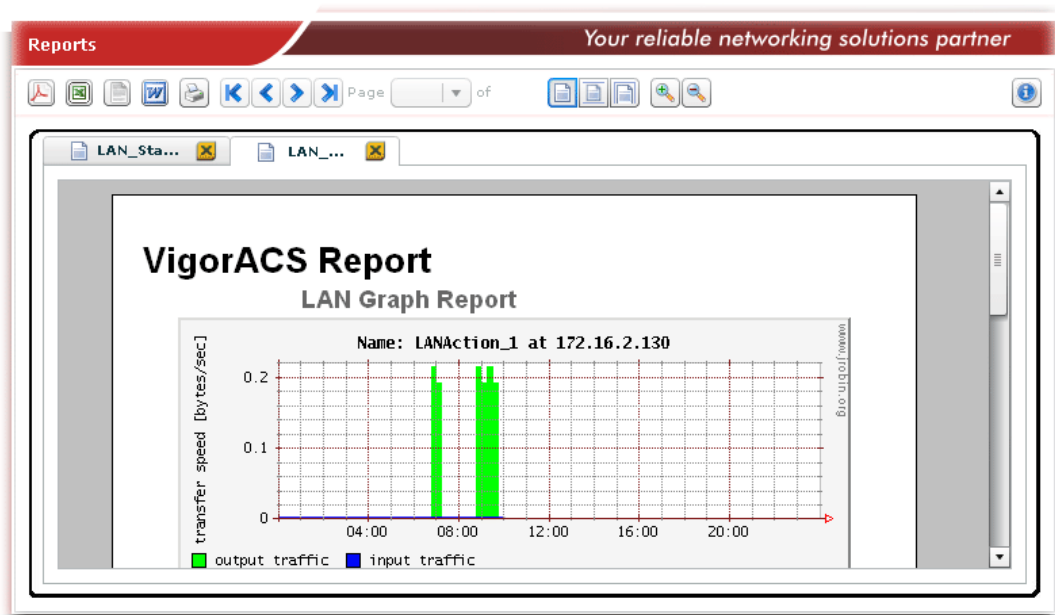
Move your mouse to the items you want to print out and click on it. A dialog box will appear. Take **LAN Graphic** as an example.

Choose **Traffic Reports>> LAN/WAN/NAT Graph** from **Reports**.



All the CPEs on the same network group will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

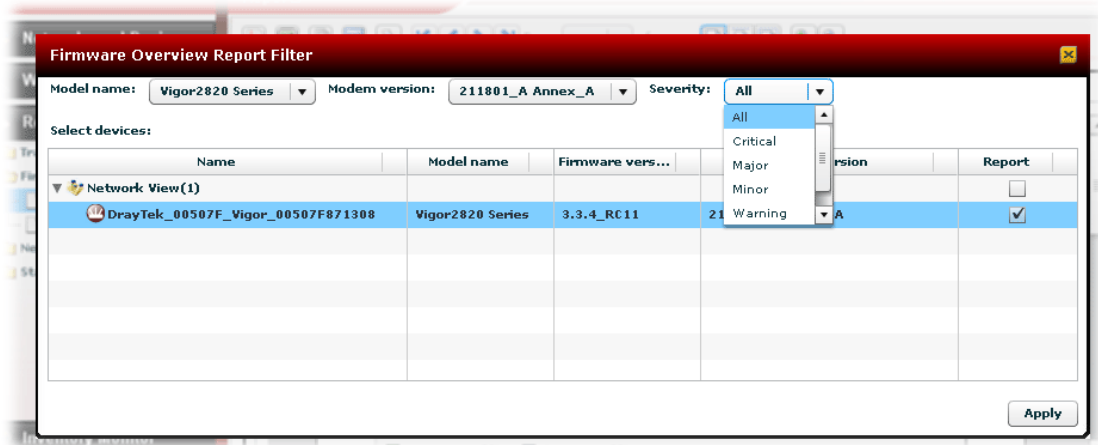
Next, please **Apply**. **VigorACS Report** containing all the LAN/WAN/NAT Graph for the selected CPE will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

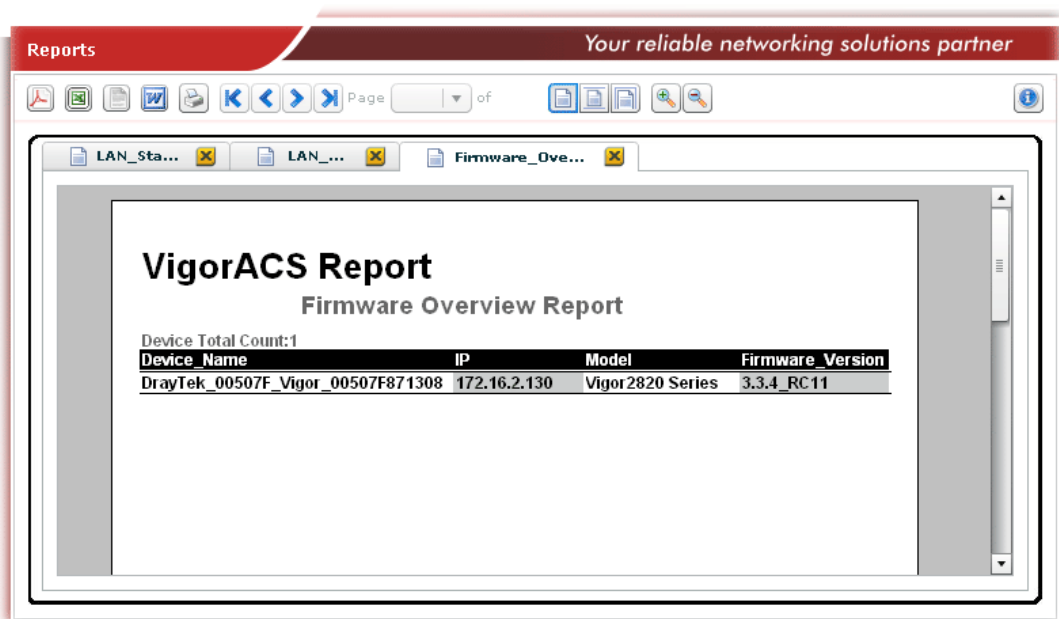
6.4.4 Firmware Overview

Choose **Firmware>>Firmware Overview** from **Reports**. A dialog box will appear.



All the CPEs on the same network group will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

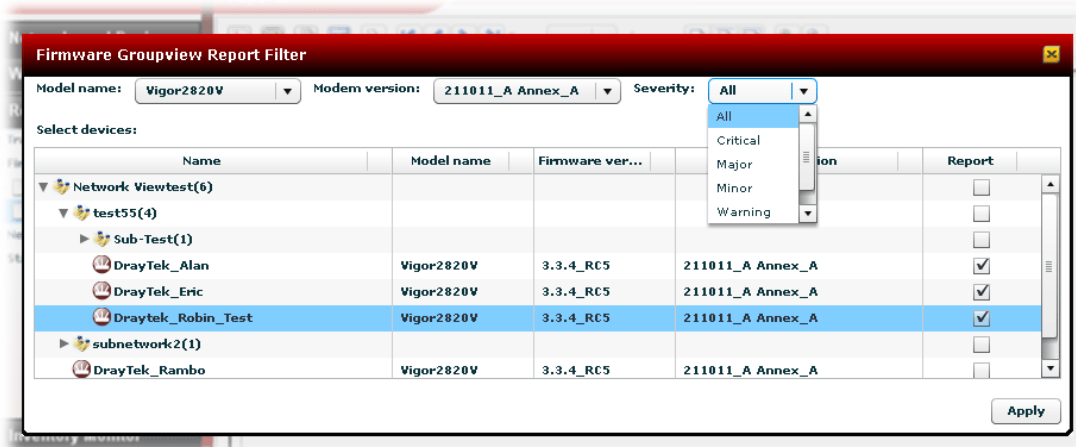
Next, please **Apply**. **VigorACS Report** containing all the records of firmware version ordered with device names for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

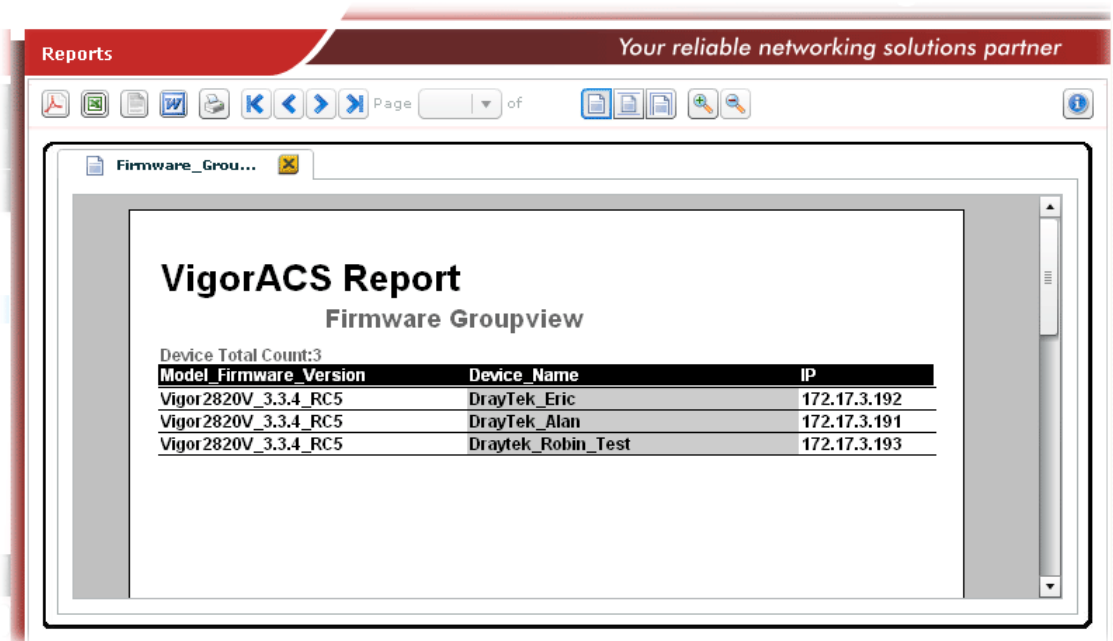
6.4.5 Firmware Groupview

Choose **Firmware >> Firmware Groupview** from **Reports**. A dialog box will appear.



All the CPEs on the same network group will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Next, please **Apply**. **VigorACS Report** containing the records of firmware information ordered with model and firmware version for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

6.4.6 Firmware Upgrade Wizard

Choose **Firmware** >> **Firmware Upgrade Wizard** from **Reports**. A dialog box will appear.

Firmware Upgrade Wizard Overview Report Filter

Model name: Modem version: Severity: Job:

Select devices:

- Vigor2960
- Vigor2860ac
- Vigor2925n
- Vigor2925FVn

	Model name	Firmware version	Modem version	Report
Network				
alvac				
Other(1)				
RD3(0)				
RD6(1)				
RD8(6)				
RD8_2(3)				
test6network(0)				
2130	Vigor2130V	GlasOperator_154.11	No DSL	☐
DrayTek_001DAA_Vigor2860ac_001DAAB9	Vigor2860ac	beta_0414	05-07-01-08-00-01 Annex_A	☐

Apply

All the CPEs which match the conditions specified in Model name, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Next, please **Apply**. **VigorACS Report** containing the records of network IP settings ordered with device names for different CPEs will be shown as the following.

Reports Your reliable networking solutions partner

FirmwareUpgradeWizard_Ove...

VigorACS Report

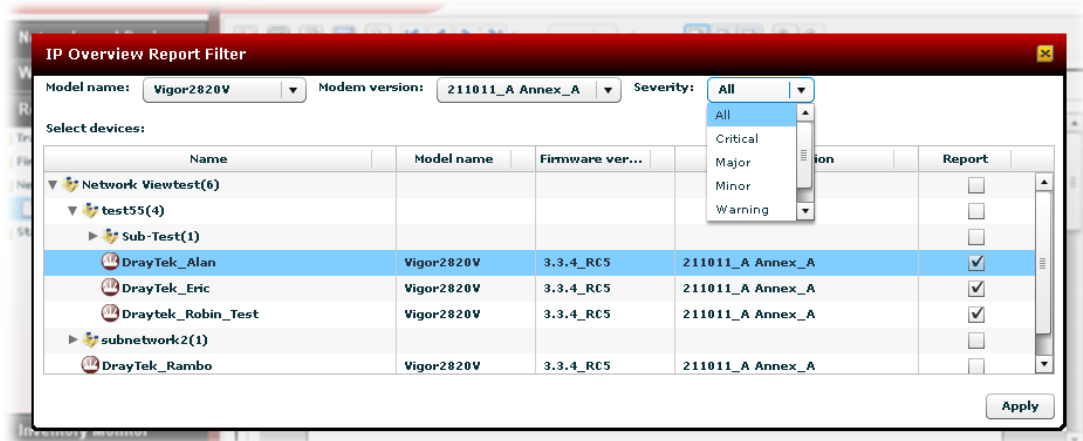
Firmware Upgrade Wizard Overview

Device Total Count:0

Device_Name	MAC/Status	IP/New_Version	Time/Old_Version

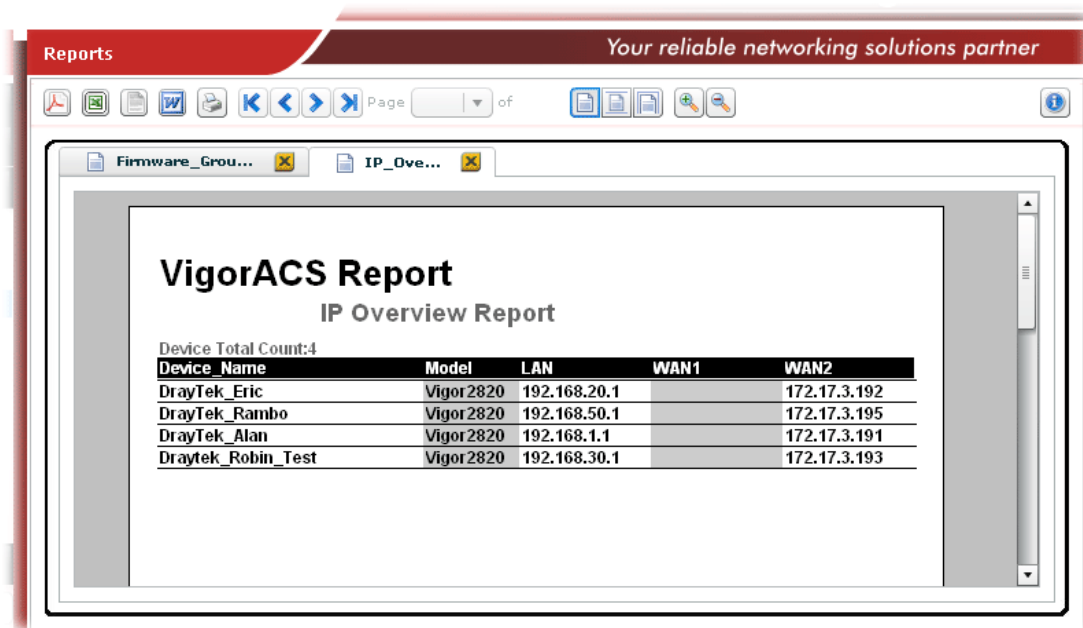
6.4.7 Network IP Overview (WAN/LAN)

Choose **Network>>IP Overview (WAN/LAN)** from **Reports**. A dialog box will appear.



All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

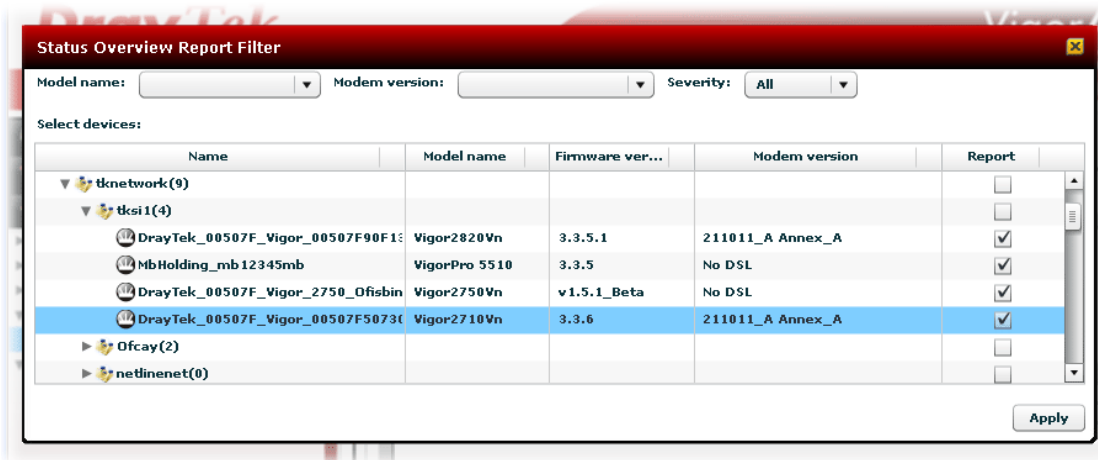
Next, please **Apply**. **VigorACS Report** containing the records of network IP settings ordered with device names for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

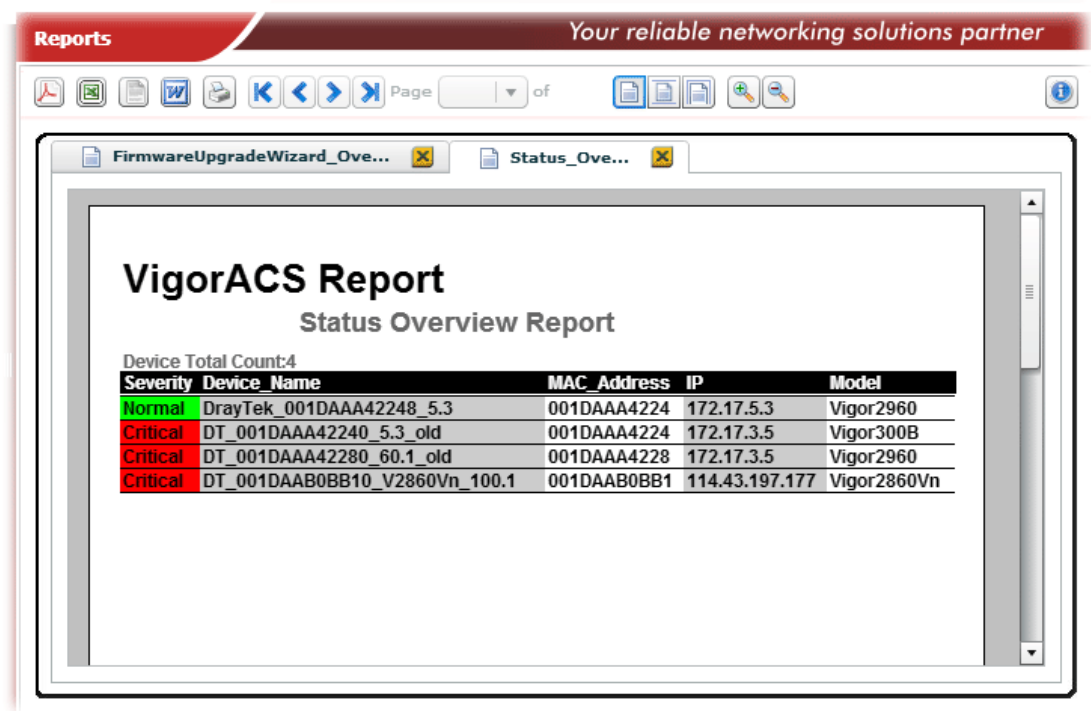
6.4.8 Status Overview / USB Modem Overview / Port Status Overview

Choose **Status>>Status Overview** from **Reports**. A dialog box will appear.



All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

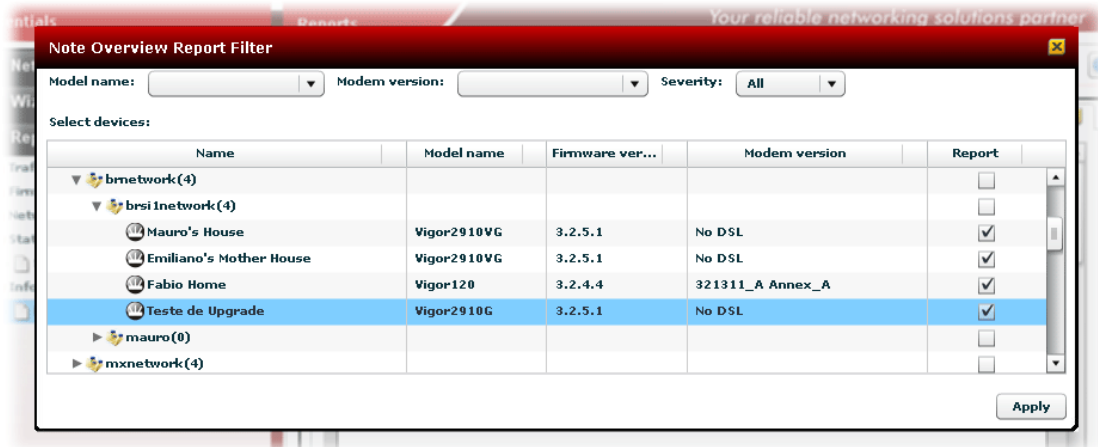
Next, please **Apply**. **VigorACS Report** containing the records of router status ordered with device names for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

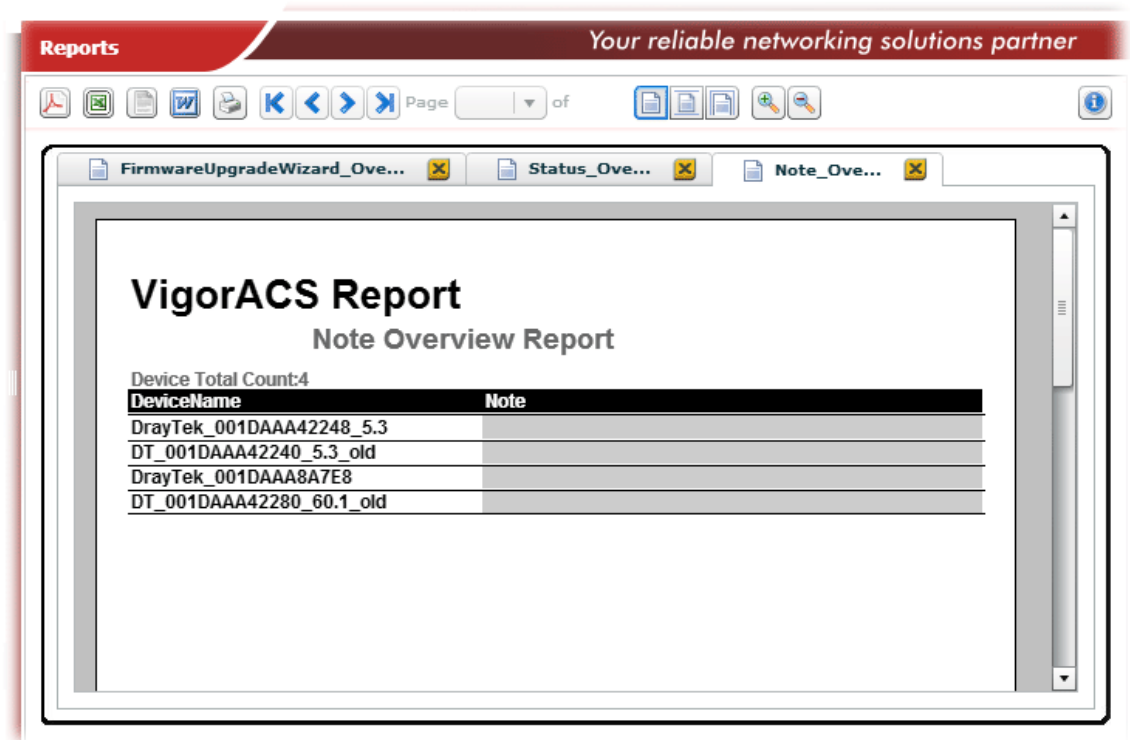
6.4.9 Information Note Overview

Choose **Information>>Note** from **Reports**. A dialog box will appear.



All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

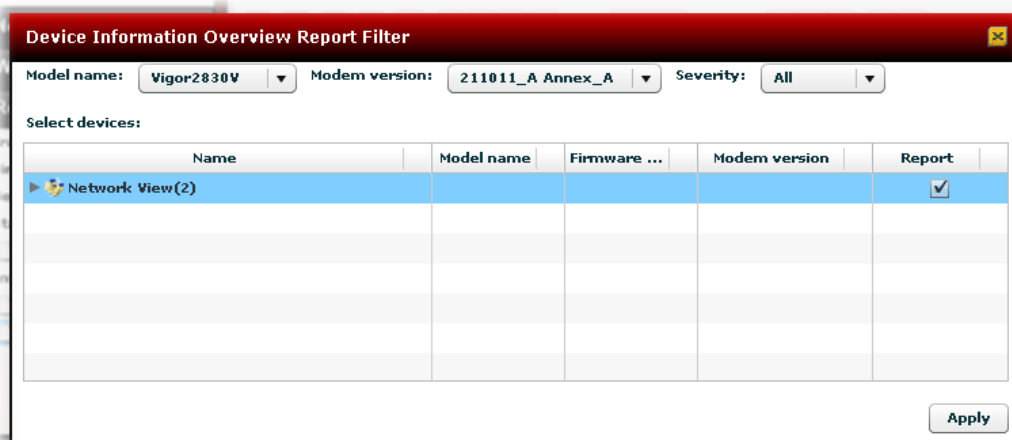
Next, please **Apply**. **VigorACS Report** containing the records of notes ordered with device names for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

6.4.10 Information Device Information Overview / Detail Device Information Overview

Choose **Information>>Device Information** from **Reports**. A dialog box will appear.



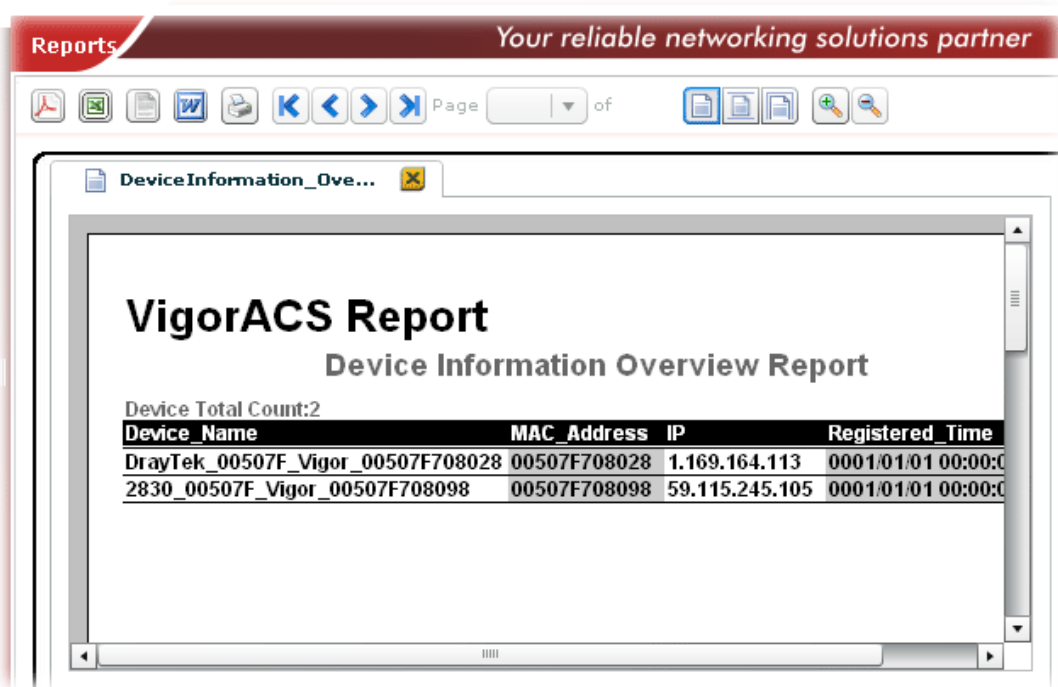
The dialog box titled "Device Information Overview Report Filter" contains the following fields and controls:

- Model name: **Vigor2830V** (dropdown)
- Modem version: **211011_A Annex_A** (dropdown)
- Severity: **All** (dropdown)
- Select devices: A table with columns: Name, Model name, Firmware ..., Modem version, Report.
- An "Apply" button at the bottom right.

Name	Model name	Firmware ...	Modem version	Report
▶ Network View(2)				☒

All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Next, please **Apply**. **VigorACS Report** containing the records of device information ordered with device names for different CPEs will be shown as the following.



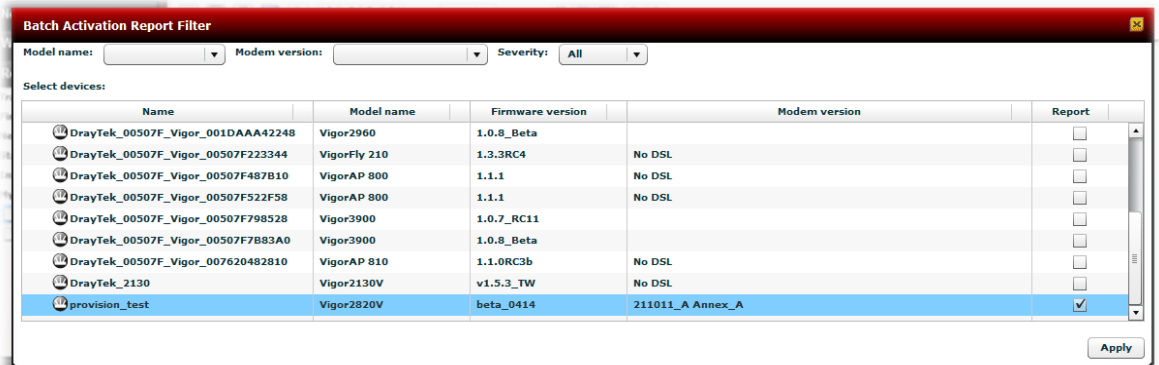
The report is titled "VigorACS Report" and "Device Information Overview Report". It shows a "Device Total Count:2". The table below contains the device information:

Device Name	MAC Address	IP	Registered Time
DrayTek_00507F_Vigor_00507F708028	00507F708028	1.169.164.113	0001/01/01 00:00:00
2830_00507F_Vigor_00507F708098	00507F708098	59.115.245.105	0001/01/01 00:00:00

Now, you can print such report as a PDF file or print it out via specified printer.

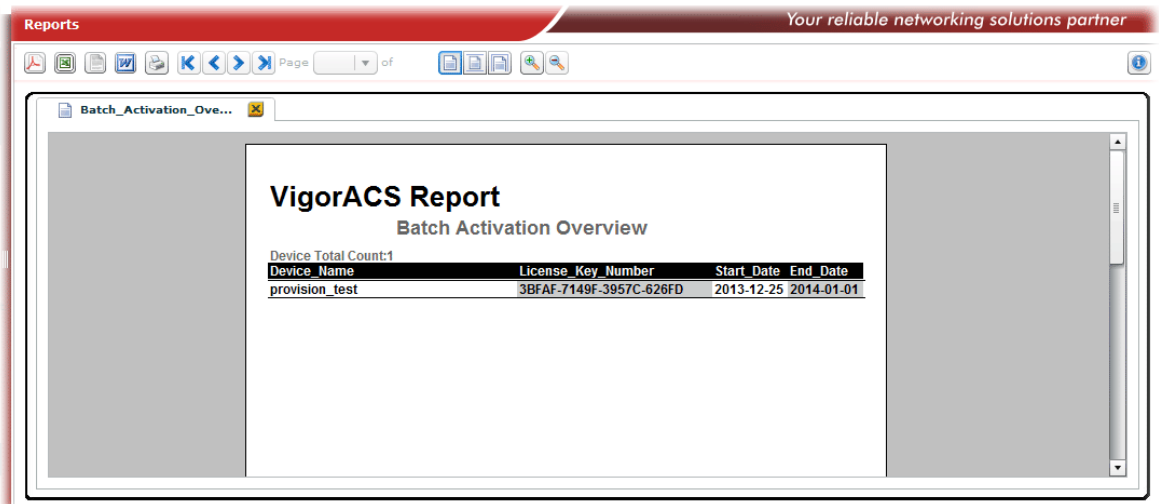
6.4.11 Batch Activation Overview

Choose **MyVigor License>> Batch Activation** from **Reports**. A dialog box will appear.



All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Next, please **Apply**. **VigorACS Report** containing the records of device information ordered with device names for different CPEs will be shown as the following.



Now, you can print such report as a PDF file or print it out via specified printer.

6.4.12 Bind with MyVigor Account Overview

Choose **MyVigor License>>Bind with MyVigor Account** from **Reports**. A dialog box will appear.

Model name: Modem version: Severity:

Select devices:

Name	Model name	Firmware version	Modem version	Report
DrayTek_00507F_Vigor_001DAAA42248	Vigor2960	1.0.8_Beta		☐
DrayTek_00507F_Vigor_00507F223344	VigorFly 210	1.3.3RC4	No DSL	☐
DrayTek_00507F_Vigor_00507F487B10	VigorAP 800	1.1.1	No DSL	☐
DrayTek_00507F_Vigor_00507F522F58	VigorAP 800	1.1.1	No DSL	☐
DrayTek_00507F_Vigor_00507F798528	Vigor3900	1.0.7_RC11		☐
DrayTek_00507F_Vigor_00507F7B83A0	Vigor3900	1.0.8_Beta		☐
DrayTek_00507F_Vigor_007620482810	VigorAP 810	1.1.0RC3b	No DSL	☐
DrayTek_2130	Vigor2130V	v1.5.3_TW	No DSL	☐
provision_test	Vigor2820V	beta_0414	211011_A Annex_A	☒

Apply

All the CPEs which match the conditions specified in Model, Modem version and Severity will be displayed. Please choose the one(s) you want to print out and check the **Report** box.

Reports Your reliable networking solutions partner

Bind_With_MyVigor_Account_Ove...

VigorACS Report

Bind With MyVigor Account

Device Total Count:1

Device Name	Account	Mail
provision_test	robin	robin_li@draytek.com.tw

6.5 Inventory Monitor

Here, VigorACS SI provides another view for displaying the controlled CPEs. In this view, devices will be divided and categorized with the model series, such as Vigor2860 series, Vigor3900 series, and so on.

The screenshot displays the VigorACS SI web interface. On the left is a navigation menu with 'Essentials' at the top, followed by 'Networks and Devices', 'Wizards', 'Reports', and 'Inventory Monitor'. Under 'Inventory Monitor', there is an 'Inventory View' tree showing various device models like 'UnknownModel(3)', 'Vigor2130(1)', 'Vigor2132(1)', 'Vigor2820(6)', 'Vigor2860(4)', 'Vigor2910(3)', 'Vigor2925(2)', 'Vigor2960(2)', and 'VigorAP(5)'. The 'Vigor2960(2)' entry is selected. The main content area is titled 'Device: DrayTek_00507F_Vigor2960_00507FFF3900' and includes a breadcrumb trail: 'Device > System > LAN > WAN > VPN > Firewall > User > NAT > Applications'. The interface is divided into several sections: 'Device Information' (showing status, hardware model, firmware version, MAC address, serial number, device name, license, and up time), 'Network' (a table of link status, name, index, VLAN ID, and DHCP), 'Port Status' (a table of interface status, up time, Tx rate, and Tx enable), and 'VoIP Status' (indicating it is not supported). At the bottom, there is an 'Alarm / Note' section. The right side of the interface features a vertical toolbar with icons for various functions.

Device Information

Status: Normal	UpTime: 13 days 21:16:56
Hardware Model: Vigor2960	CPU: 5%
Firmware Version: 1.3.0_Beta	Memory: 41%
Hardware Version: 1.0	Note 1:
MAC Address: 00507FFF3900	Note 2:
Serial Number:	Web: http://172.16.2.1
Device Name: DrayTek_00507F_Vigor2960	Proxy: http://172.16.2.1
MyVigor License:	Network Name: Network View
Start Date:	
End Date:	

Network

Link Status	Name	Index	VLAN ID	DHCP
Up	Wan	1	10	172.1
Disable	Wan	2	11	
Up	Lan	1	10	false 192.1
Disable	Lan	2	0	false 0.0.0.

Port Status

Interface	Status	UpTime	Tx Rate	Tx Enal
lan1	Up	0	0	
lan2	Down	0	0	
lan3	Up	0	0	
lan4	Down	0	0	
wan1	Up	0	0	
wan2	Down	0	0	

VoIP Status

Not supported on your device.

Alarm / Note

Chapter 7 System Operation

System operation provides system parameters related to VigorACS itself.



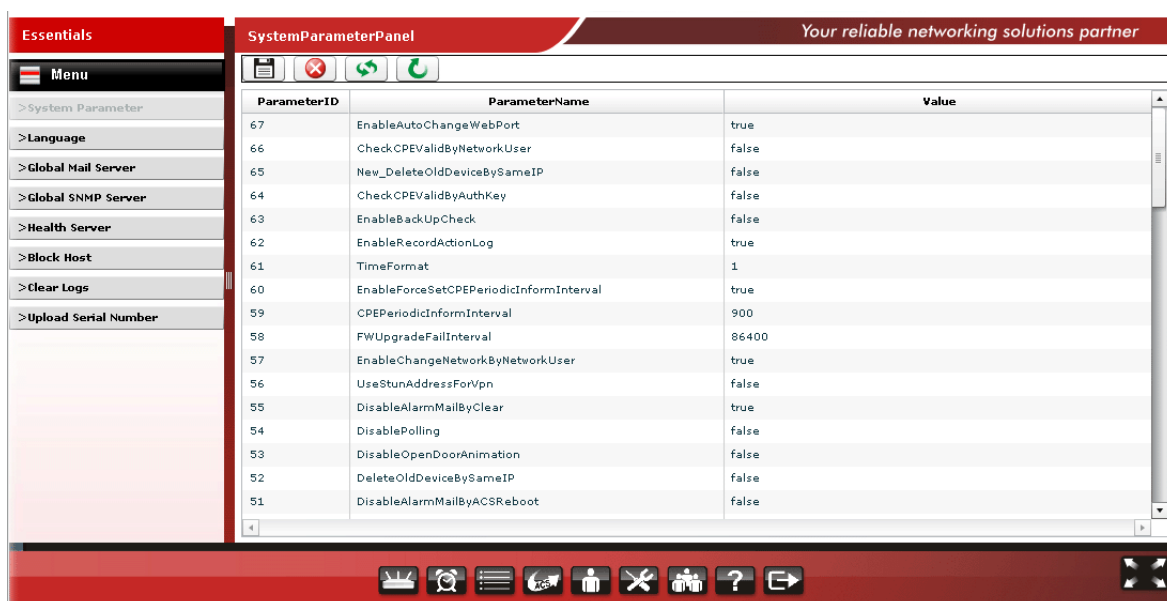
Click the **System** tab to open the following web page.

A screenshot of the VigorACS SystemParameterPanel web page. The page has a red header with the DrayTek logo on the left and 'VigorACS' on the right. Below the header is a navigation menu on the left with options like 'Menu', 'System Parameter', 'Language', 'Global Mail Server', 'Global SNMP Server', 'Health Server', 'Block Host', 'Clear Logs', and 'Upload Serial Number'. The main content area is titled 'SystemParameterPanel' and contains a table of system parameters. The table has three columns: 'ParameterID', 'ParameterName', and 'Value'. The table lists 15 parameters with their IDs, names, and current values. At the bottom of the page is a row of icons representing different system functions: a router, a clock, a list, a person, a wrench, a group of people, a question mark, and a right arrow.

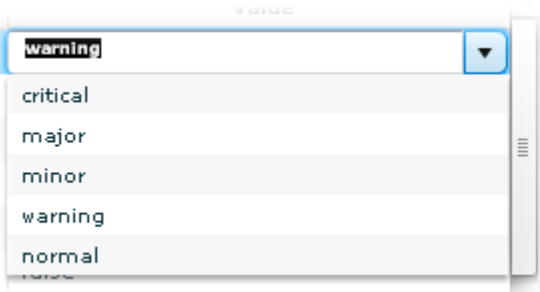
ParameterID	ParameterName	Value
67	EnableAutoChangeWebPort	true
66	CheckCPEValidByNetworkUser	false
65	New_DeleteOldDeviceBySameIP	false
64	CheckCPEValidByAuthKey	false
63	EnableBackUpCheck	false
62	EnableRecordActionLog	true
61	TimeFormat	1
60	EnableForceSetCPEPeriodicInformInterval	true
59	CPEPeriodicInformInterval	900
58	FWUpgradeFailInterval	86400
57	EnableChangeNetworkByNetworkUser	true
56	UseStunAddressForVpn	false
55	DisableAlarmMailByClear	true
54	DisablePolling	false
53	DisableOpenDoorAnimation	false
52	DeleteOldDeviceBySameIP	false
51	DisableAlarmMailByACSReboot	false

7.1 System Parameter Setting

This page displays all of the parameters used by VigorACS and allows you to modify the system parameters slightly.

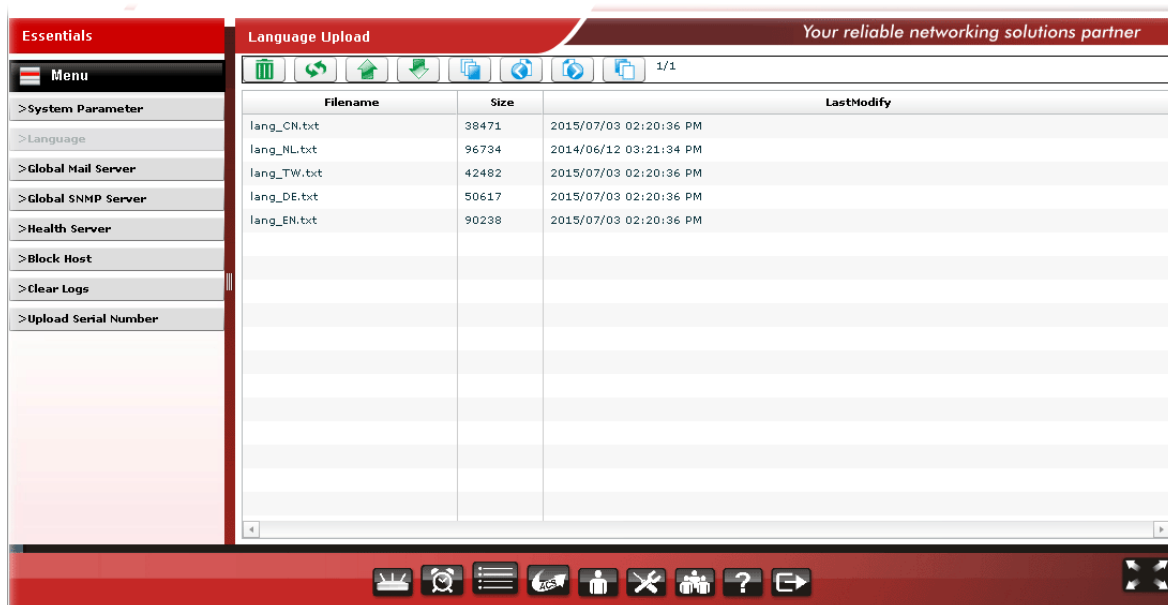


Available settings for such feature will be shown as follows:

Items	Description
 Save	Click this button to save the record.
 Cancel	Click it to exit the screen without saving any change.
 Refresh	Click this button to refresh current page.
ParameterID	Display the sequence number of the parameter.
ParameterName	Display the name of the system parameters.
Value	List the available vales for each parameter. Different parameters have different values including true/false, 0/1, major/minor... and so on. Use the drop down list to choose the value you want. 

7.2 Language Setting

This page allows you to upload the language settings to VigorACS, and choose the language that you want to use for logging onto VigorACS.



Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected language file.
 Refresh	Click this button to refresh uploaded files.
 Upload File	Click this button to upload a language file from your host to VigorACS. The file you upload will be shown on the screen immediately.
 Download File	Click this button to download a language file from VigorACS to your computer.
 First	When there is more than one page for the language files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the language files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the language files in this user group, click this button to display the next page.
 Last	When there is more than one page for the language files in this user group, click this button to display the last page.
Filename	Display the name of the language file.
Size	Display the size of the file.
LastModify	Display the date and time for the last modification.

7.3 Global Mail Server Setting

All of the user groups can apply the mail server settings configured in this page.

Available settings for such feature will be shown as follows:

Items	Description
 Save mail server setting	Click this button to save the record.
 Refresh mail server setting	Click this button to refresh uploaded files.
 Send a test mail	Click this button to send a test mail to the email address specified below.
Enable global mail server	Check this box to enable global settings.
Mail server address	Type the IP address of the SMTP server.
Port	Assign a port for the mail server.
Email address	Assign an IP address for sender.
Email Subject	Specify the subject of the mail server.  - Click this button to open the following dialog. Click the icon under Add to make the selected subject to be added as a Email Subject.

Items	Description
	 - Click this button to reset to default subject items including VigorACS, AlarmLevel, DeviceMAC and AlarmMessage.
Authentication needed	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Security	Choose None / SSL / TLS for the security of the mail transferring.
Alarm Level	Specify the severity level of the mail.

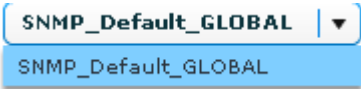
7.4 Global SNMP Server Setting

All of the user groups can apply SNMP server settings configured in this page.

The screenshot shows the 'SNMPServer' configuration page. The left sidebar has a 'Menu' section with the following items: >System Parameter, >Language, >Global Mail Server, >Global SNMP Server, >Health Server, >Block Host, >Clear Logs, and >Upload Serial Number. The main area is titled 'SNMPServer' and contains the following settings:

- Enable global SNMP server: ☐
- SNMP server address:
- Port:
- Community:
- SNMP version:
- SNMP API:
- Alarm Level: ☒ Critical ☒ Major ☒ Minor ☒ Warning ☒ Normal

Available settings for such feature will be shown as follows:

Items	Description
 Save SNMP server setting	Click this button to save the record.
 Refresh	Click this button to refresh uploaded files.
Enable global SNMP server	Check the box to enable SNMP server.
SNMP server address	Type the IP address for the SNMP server.
Port	Type the port number for the 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 .
SNMP version	Choose the version of the SNMP server that you apply to. 
SNMP API	Choose SNMP API from the drop down list. At present, only SNMP_Default_GLOBAL is available. 
Alarm Level	Specify the severity level of the mail.

7.5 Health Server Setting

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

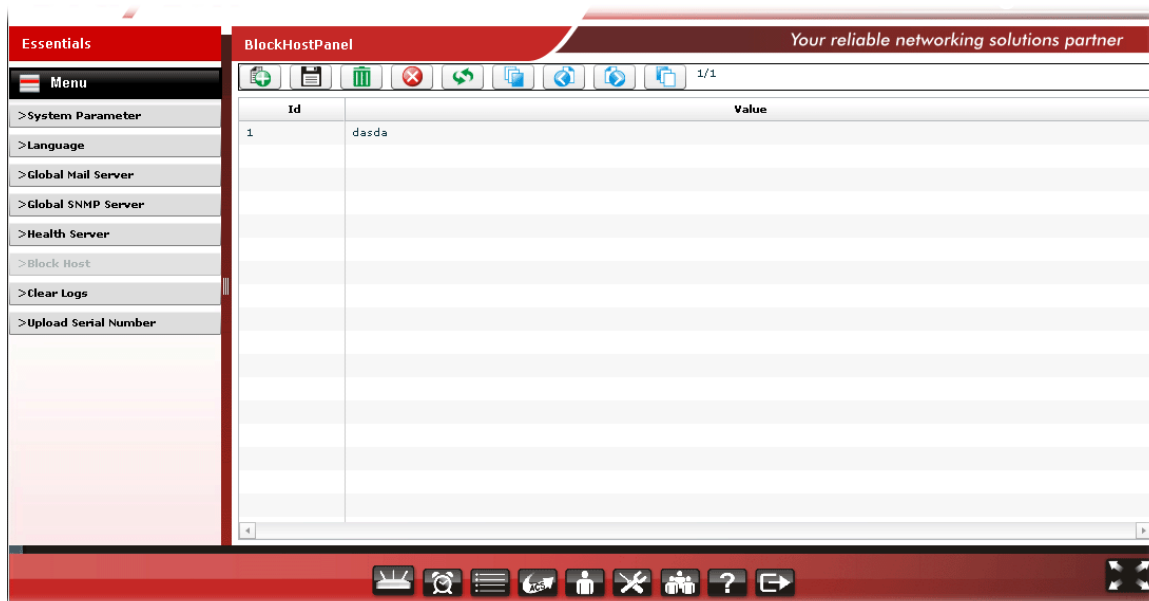
The screenshot shows the 'Health Server' configuration interface. On the left, a sidebar menu lists various system settings, with 'Health Server' currently selected. The main configuration area includes a checkbox to 'Enable health server', a 'URL' field set to '192.168.100.100', a 'User Name' field set to 'admin', a 'Password' field masked with asterisks, and a 'Health API' dropdown menu showing 'Health_Default_GLOBAL'. The interface has a red-themed header and footer with navigation icons.

Available settings for such feature will be shown as follows:

Items	Description
Enable health server	Check the box to enable such feature.
URL	Type the URL or IP address of the third party's server.
User Name	Type the user name for accessing into the third party's server.
Password	Type the password for accessing into the third party's server.
Health API	Use the drop down menu to specify the third party's server.

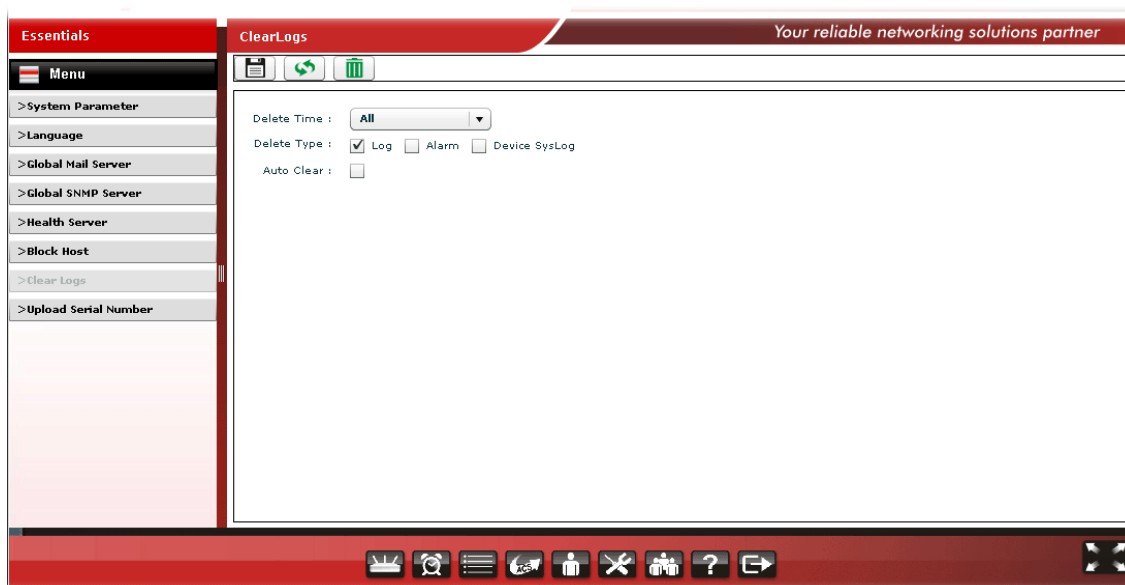
7.6 Block Host Setting

This feature is used to block CPE which is allowed to register to VigorACS.



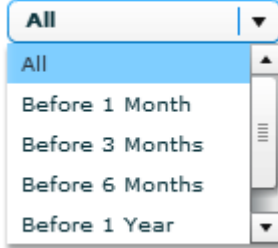
7.7 Clear Logs Setting

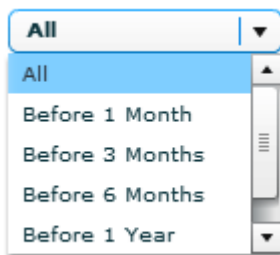
VigorACS will keep log until overload the capacity of hard disk. To avoid such trouble, use Clear Logs to delete the log periodically.



Available settings for such feature will be shown as follows:

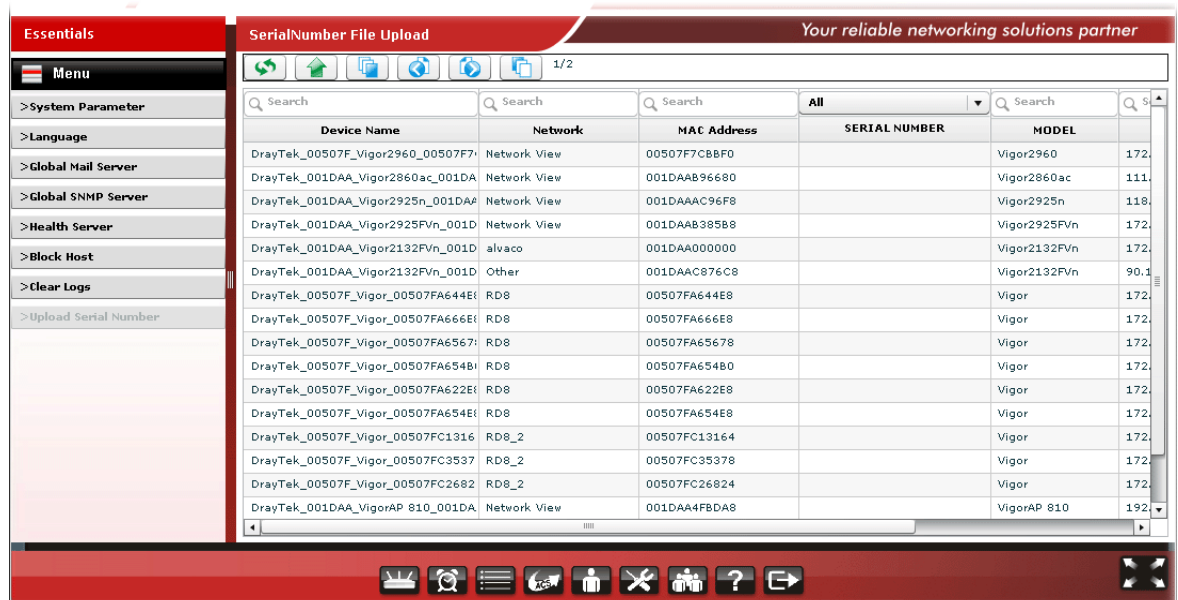
Items	Description
Delete Time	Use the drop down list to specify the timing to delete the log.

Items	Description
	
Delete Type	At present, there are three types that corresponding log can be deleted through such feature.
Auto Clear	Check the box to clear the log automatically.



7.8 Upload Serial Number Setting

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.



Available settings for such feature will be shown as follows:

Items	Description
 Refresh	Click this button to refresh this page.

Items	Description
 Upload File	Click this button 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.
 First	When there is more than one page displayed, click this button to display the first page.
 Previous	When there is more than one page displayed, click this button to display the previous page.
 Next	When there is more than one page displayed, click this button to display the next page.
 Last	When there is more than one page displayed, click this button to display the last page.
Device Name	Display the name of the device.
Network	Display the network of the device classified under VigorACS.
MAC Address	Display the MAC address of the device.
SERIAL NUMBER	Display the serial number of the device.
MODEL	Display the model of the device.
WAN IP	Display the WAN IP address of the device.
LAN IP	Display the LAN IP address of the device.
FW	Display the firmware version used by such device.

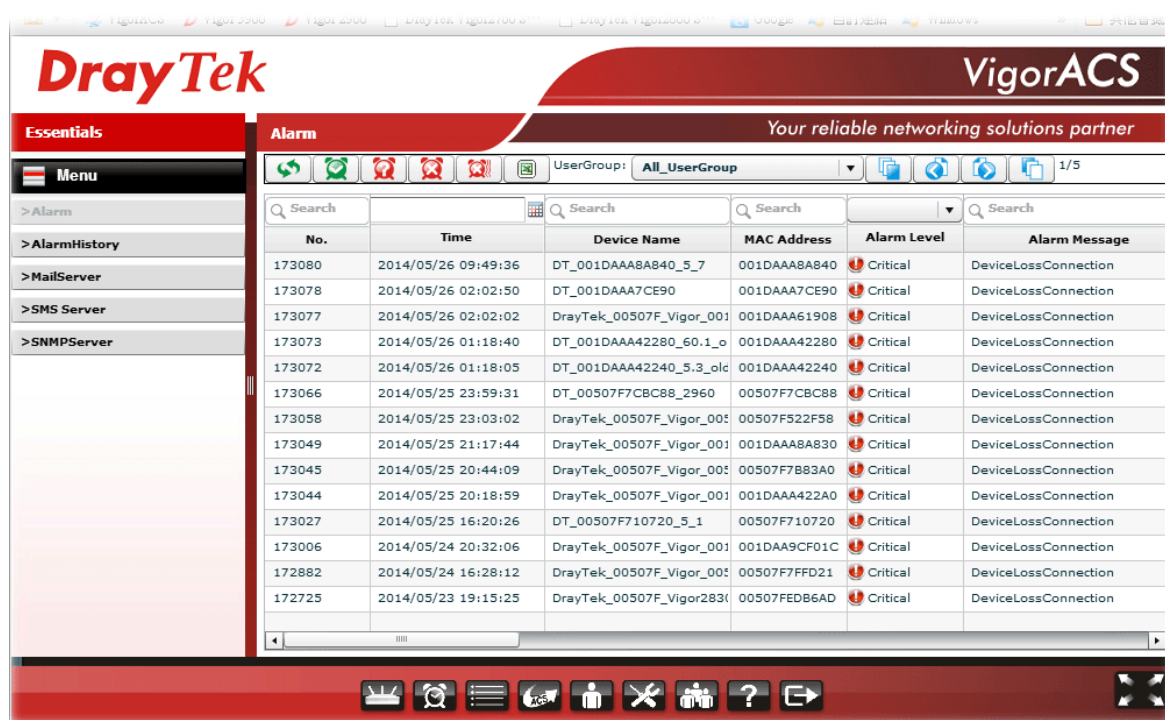
Chapter 8 Alarm Information

To monitor the normal and abnormal actions for CPEs, you will need to set Alarm.



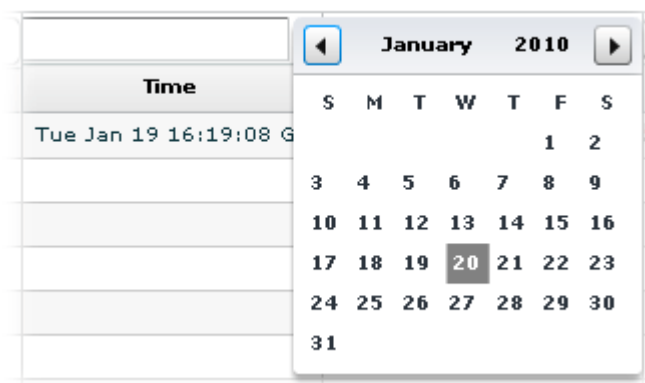
8.1 Alarm

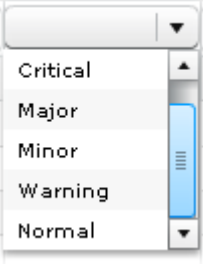
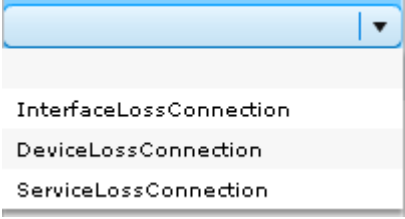
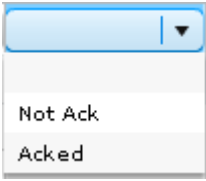
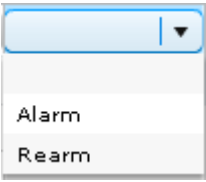
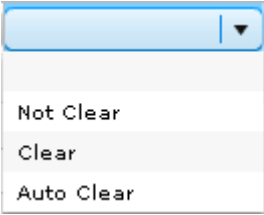
Alarm message will be recorded on VigorACS server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

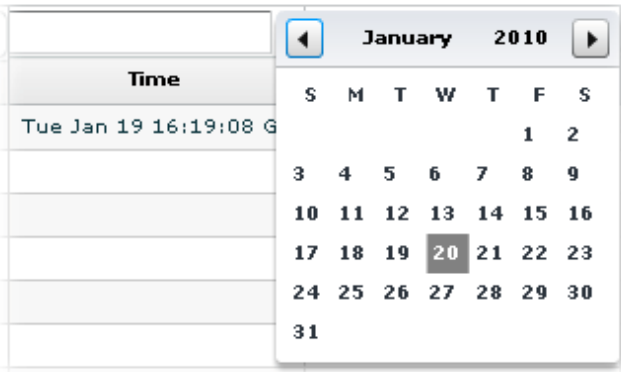
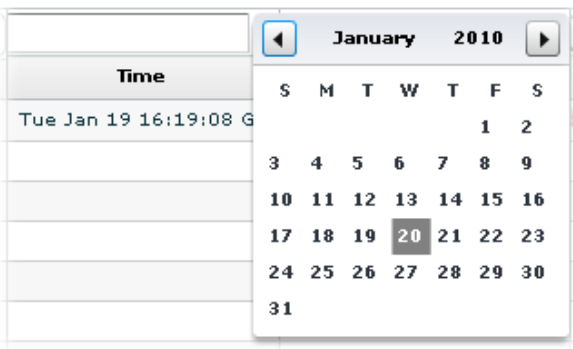
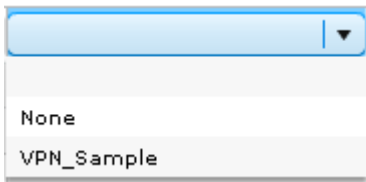


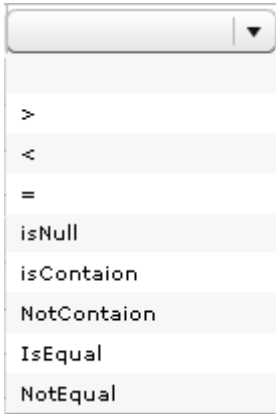
Available settings for such feature will be shown as follows:

Items	Description
Refresh	Click this button to refresh this page.
Ack Alarm	Click this button to make the alarm being captured based on the threshold value and waiting for solving manually.
UnAck Alarm	Disable the Ack Alarm mechanism.
Clear Alarm	Click this button to clear the alarm record which has been solved by VigorACS.
Clear All Alarm	Click this button to clear all of the alarm records which has been solved by VigorACS.

Items	Description
 Export to CSV	Click this button to save alarm log as a CSV file.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the alarm records in this user group, click this button to display the first page.
 Previous	When there is more than one page for the alarm records in this user group, click this button to display the previous page.
 Next	When there is more than one page for the alarm records in this user group, click this button to display the next page.
 Last	When there is more than one page for the alarm records in this user group, click this button to display the last page.
No.	Display the index number of the alarm. It is offered by VigorACS automatically.
Time	Display the time of the alarm recorded. You can use the drop down calendar to inspect other alarms. 
Device Name	Display the name of the CPE which gets trouble.
MAC Address	Display the MAC address of the device.
Alarm Level	Choose one of the alarm levels from the drop down list to display the alarm message with the severity specified.

Items	Description
	
Alarm Message	Display a brief explanation for the alarm sent by VigorACS automatically.
Alarm Type	There are three types of Alarm Type. Choose any one of them to display the alarm message with the type specified. 
Ack Status	Display the status of the records with the type specified here (Not Ack or Acked). 
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. 

Items	Description
Ack Time	Display the record (waiting for solving) based on the date chosen here. 
Ack User	Display the record (waiting for solving) based on the user accounts.
Clear Time	Alarm message record cleared by user will be removed to Alarm History. Choose the date to display the removed record. 
Clear User	Display which user clears such record.
UnAck Time	Display the cancelled job of the record (waiting for solving) based on the date chosen here.
UnAck User	Display which user cancels the job of the record.
Parameter	VigorACS will send the alarm based on the parameter specified here. User will know which parameter got troubles when he/she receives the alarm messages.
Parameter Group	Display the alarm record based on the VPN group selected here. 
Value	Display the threshold value that VigorACS will send alarm message to the CPE.

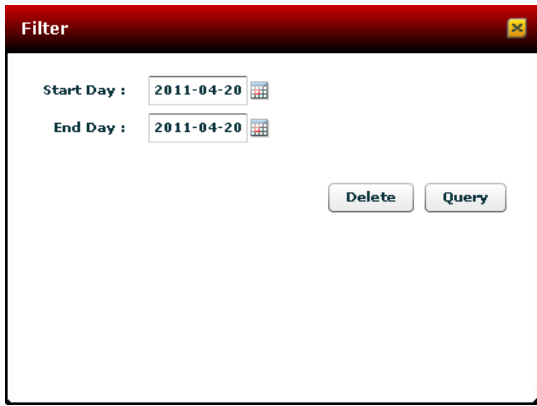
Items	Description
Threshold	Set the condition for data traffic.  > - when the threshold value is greater than the configured value, an alarm message will be sent out. < - when the threshold value is smaller than the configured value, an alarm message will be sent out. = - when the threshold value equals to the configured value, an alarm message will be sent out. isNull - when the threshold value is null, an alarm message will be sent out. isContain - when the threshold value contains the configured value, an alarm message will be sent out. NotContain - when the threshold value does not contain the configured value, an alarm message will be sent out. IsEqual - when the threshold value equals to the configured value, an alarm message will be sent out. NotEqual - when the threshold value does not equal to the configured value, an alarm message will be sent out.
Threshold Value	Set the value to fit the requirement of threshold.
Rearm	For cleaning an alarm record, please configure Rearm value.

8.2 Alarm History

This page will display all the alarm records that have been solved and cleared.

The screenshot displays the AlarmHistory page. On the left is a sidebar with 'Essentials' and 'Menu' sections. The 'Menu' section includes links to 'Alarm', 'AlarmHistory', 'MailServer', 'SMS Server', and 'SNMP Server'. The main area shows a table of alarm records. The table has columns: No., Time, Clear Time, Device Name, MAC Address, and Alarm Level. The records are sorted by No. in descending order. The top record is No. 173085, Time 2014/05/26 14:50:45, Clear Time 2014/05/26 14:51:00, Device Name DrayTek_00507F_Vigor285, MAC Address 00507F5D1630, and Alarm Level Critical. The bottom record is No. 173067, Time 2014/05/26 00:02:30, Clear Time 2014/05/26 00:19:58, Device Name DrayTek_00507F_Vigor_00, MAC Address 001DAAA61908, and Alarm Level Critical. The interface also includes a top navigation bar with 'Your reliable networking solutions partner' and 'UserGroup: All_UserGroup'.

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete a selected record.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried.  The Filter dialog box shows two date pickers: 'Start Day' and 'End Day', both set to '2011-04-20'. There are 'Delete' and 'Query' buttons at the bottom right.
 Export to CSV	Click this button to save alarm log as a CSV file.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.

Items	Description
	
 First	When there is more than one page for the alarm records in this user group, click this button to display the first page.
 Previous	When there is more than one page for the alarm records in this user group, click this button to display the previous page.
 Next	When there is more than one page for the alarm records in this user group, click this button to display the next page.
 Last	When there is more than one page for the alarm records in this user group, click this button to display the last page.

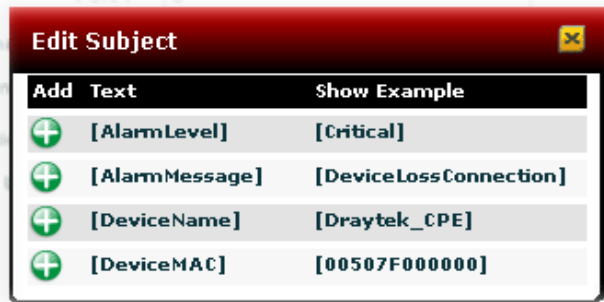
As for detailed information of each item (such as No., Time, Device Name, Alarm Level, Alarm Message....) in Alarm History, please refer to section 8.1.

8.3 Mail Server

VigorACS can notify the user by e-mail whenever an error is detected.

Available settings for such feature will be shown as follows:

Items	Description
 Save mail server setting	Click this button to save the settings configured in this page.
 Refresh mail server setting	Click this button to refresh this page.
 Send a Test Mail	Click this button to send a test mail to the email address specified below.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
Enable email server	Check this box to enable such function.
Mail server address	Type the IP address of the mail server for VigorACS.
Port	Type the port number of the mail server.

Items	Description															
Email address	Type the email address of the mail server.															
Email Subject	Specify the subject of the mail server. The types to be specified contain AlarmLevel, AlarmMessage, DeviceName and DeviceMAC.  - Click this button to open the following dialog. Click the icon under Add to make the selected subject to be added as an Email Subject. <table><tr><th>Add</th><th>Text</th><th>Show Example</th></tr><tr><td></td><td>[AlarmLevel]</td><td>[Critical]</td></tr><tr><td></td><td>[AlarmMessage]</td><td>[DeviceLossConnection]</td></tr><tr><td></td><td>[DeviceName]</td><td>[Draytek_CPE]</td></tr><tr><td></td><td>[DeviceMAC]</td><td>[00507F000000]</td></tr></table>  - Click this button to reset to default subject items including VigorACS, AlarmLevel, DeviceMAC and AlarmMessage.	Add	Text	Show Example		[AlarmLevel]	[Critical]		[AlarmMessage]	[DeviceLossConnection]		[DeviceName]	[Draytek_CPE]		[DeviceMAC]	[00507F000000]
Add	Text	Show Example														
	[AlarmLevel]	[Critical]														
	[AlarmMessage]	[DeviceLossConnection]														
	[DeviceName]	[Draytek_CPE]														
	[DeviceMAC]	[00507F000000]														
Authentication needed	Check this box to activate this function while using e-mail application.															
User Name	Type the user name for authentication.															
Password	Type the password for authentication.															
Security	Choose None / SSL / TLS for the security of the mail transferring.															
Alarm Level	Specify the severity level of the mail.															

8.4 SMS Server

This page allows you to choose which ISP with SMS service you want to use.

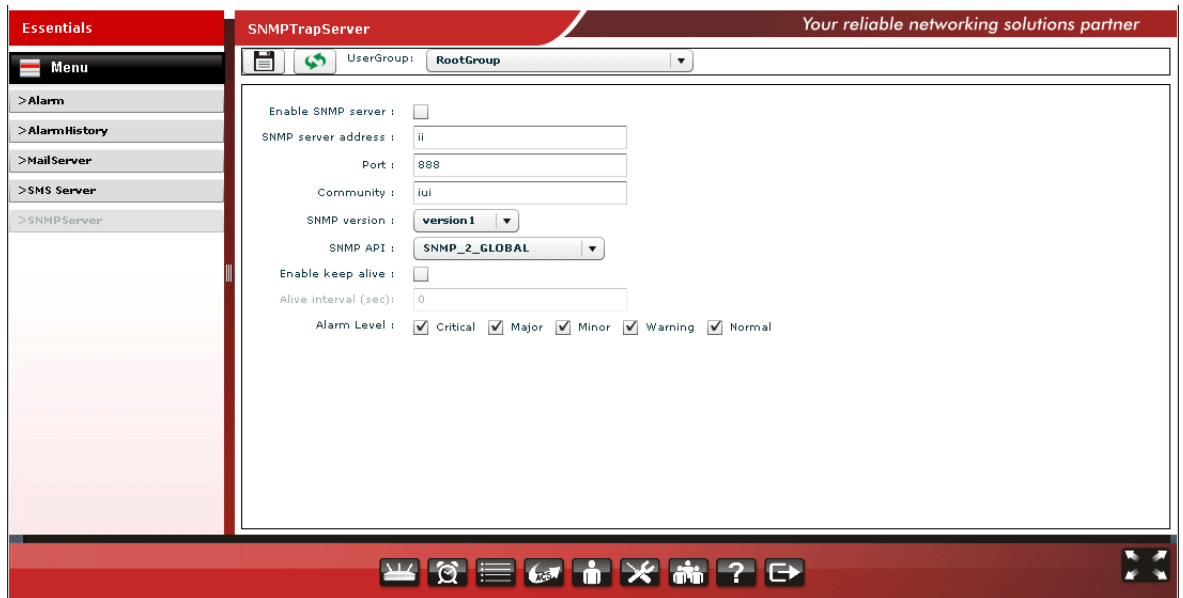
Available settings for such feature will be shown as follows:

Items	Description
 Save SMS server setting	Click this button to save the settings configured in this page.
 Refresh SMS server setting	Click this button to refresh this page.
UserGroup of this SMS server	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
Enable SMS server	Check this box to enable such function.
From Telephone	Type the telephone number of the one who sends the SMS.
User Name	Type a username for authentication.
Password	Type a password for authentication.

Items	Description
SMS API	Use the drop down list to choose the SMS service provider according to the location of the CPE. 
Alarm Level	Specify the severity level of the mail.

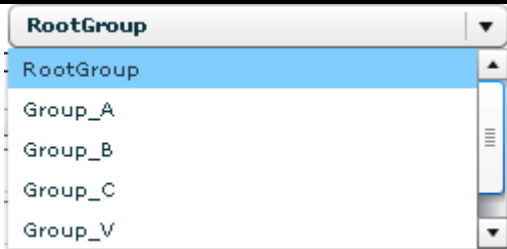
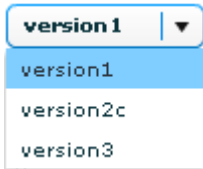
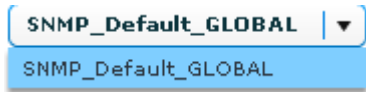
8.5 SNMP Server

This page allows you to manage the settings for SNMP server. When there is alarm detected, VigorACS will transfer the message to the SNMP server specified in this page.



Available settings for such feature will be shown as follows:

Items	Description
 Save SNMP server setting	Click this button to save the settings configured in this page.
 Refresh SNMP server setting	Click this button to refresh this page.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.

Items	Description
	
Enable SNMP server	Check the box to enable SNMP server.
SNMP server address	Type the IP address for the SNMP server.
Port	Type the port number for the 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 .
SNMP version	Choose the version of the SNMP server that you apply to. 
SNMP API	Choose SNMP API from the drop down list. At present, only SNMP_Default_GLOBAL is available. 
Enable keep alive	Check the box to enable the keep alive function.
Alive interval (sec)	Type the interval for the system to keep alive.
Alarm Level	Specify the severity level of the mail.

8.6 Latest Alarms

The latest alarm will be displayed on the home page, tabbed with Latest Alarms. If the area is blank, it means there is no alarm or the alarm has been solved.

Essentials

- Networks and Devices
 - Network View(27)
 - alvaco(1)
 - DrayTek_001DAA_Vigo...
 - Other(1)
 - RD3(0)
 - RD6(1)
 - RD8(6)
 - RD8_2(3)
 - test6network(0)
 - 2130
 - DrayTek_001DAA_Vigo...
 - DrayTek_001DAA_Vigo...
 - DrayTek_001DAA_Vigo...
 - DrayTek_001DAA_Vigo...
- Wizards
- Reports
- Inventory Monitor
- Search Device

Network: Network View *Your reliable networking solutions partner*

Network View VPN Wireless AP Management

Networks And Devices

Managed networks and devices

Total number of networks:7
Alarm networks:5
Total number of devices:27
Number of alarmed devices:25

Unknown Devices

IP Address	Device Name	Device Type	Action
192.168.1...	DrayTek_001D...		+
90.145.22...	DrayTek_001D...		+
118.166.1...	DrayTek_0050...	VigorAP 900	+
172.16.2....	DrayTek_0050...	Vigor2960	+
118.166.1...	2130	Vigor2130V	+
118.166.1...	DrayTek_001D...	Vigor2860Vn	+

Latest Alarms

Level	Time	Device Name	Network	Description	Action
Critical	2016/07/28 05:27:30	DrayTek_001DAA_Vigo...	Network View	DeviceLossConnection	✓ ✗
Critical	2016/07/28 05:27:30	2130	Network View	DeviceLossConnection	✓ ✗
Critical	2016/07/28 05:27:22	DrayTek_00507F_Vigo...	Network View	DeviceLossConnection	✓ ✗
Critical	2016/07/28 05:26:54	DrayTek_00507F_Vigo...	Network View	DeviceLossConnection	✓ ✗
Critical	2016/07/28 05:12:30	DrayTek_00507F_Vigo...	Network View	DeviceLossConnection	✓ ✗
Critical	2016/07/28 05:12:26	DrayTek_001DAA_Vigo...	Network View	DeviceLossConnection	✓ ✗

This page is left blank.

Chapter 9 Log View

Log provides administrator records for action, downloading, rebooting, parameter values, object adding and deleting executed by VigorACS.



When you choose this function, the following screen will appear with all the information offered by VigorACS. Please click any one of the links on the left side. The detailed information will be shown on the right side box.

DrayTek VigorACS
Your reliable networking solutions partner

ActionLog

UserGroup: All_UserGroup 1/673

Log ID	Action	Device ID	Device Name	MAC Address	Device IP	Action ID	Time
10102	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9990	2016/08/01 02:01:05 P
10101	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9989	2016/08/01 01:10:16 P
10100	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9988	2016/08/01 01:08:56 P
10099	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9987	2016/08/01 00:57:46 P
10098	AddObject	25	DrayTek_00507F_Vigor296	00507FFF3900	172.16.2.69	8	2016/08/01 00:02:41 P
10097	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9986	2016/08/01 10:23:29 A
10096	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9985	2016/08/01 09:24:57 A
10095	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9984	2016/07/30 09:24:54 A
10094	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9983	2016/07/30 09:24:42 A
10093	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9982	2016/07/29 11:24:15 P
10092	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9981	2016/07/29 11:11:40 P
10091	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9980	2016/07/29 10:59:52 P
10090	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9979	2016/07/29 10:43:59 P
10089	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9978	2016/07/29 06:04:12 P
10088	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9977	2016/07/29 06:03:49 P

9.1 Device Action

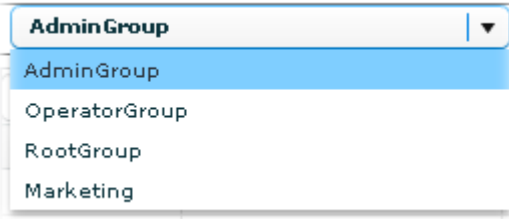
9.1.1 Action Log

Such page displays all the actions executed by VigorACS for your reference.

ActionLog		Your reliable networking solutions partner					
		UserGroup: All_UserGroup				1/673	
Log ID	Action	Device ID	Device Name	MAC Address	Device IP	Action ID	Time
10102	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9990	2016/08/01 02:01:05 P
10101	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9989	2016/08/01 01:10:16 P
10100	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9988	2016/08/01 01:08:56 P
10099	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9987	2016/08/01 00:57:46 P
10098	AddObject	25	DrayTek_00507F_Vigor296	00507FFF3900	172.16.2.69	8	2016/08/01 00:02:41 P
10097	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9986	2016/08/01 10:23:29 A
10096	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9985	2016/08/01 09:24:57 A
10095	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9984	2016/07/30 09:24:54 A
10094	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9983	2016/07/30 09:24:42 A
10093	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9982	2016/07/29 11:24:15 P
10092	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9981	2016/07/29 11:11:40 P
10091	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9980	2016/07/29 10:59:52 P
10090	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9979	2016/07/29 10:43:59 P
10089	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9978	2016/07/29 06:04:12 P
10088	Inform	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10	9977	2016/07/29 06:03:49 P

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. Filter Start Day : 2011-04-20 End Day : 2011-04-20 Delete Query
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window.

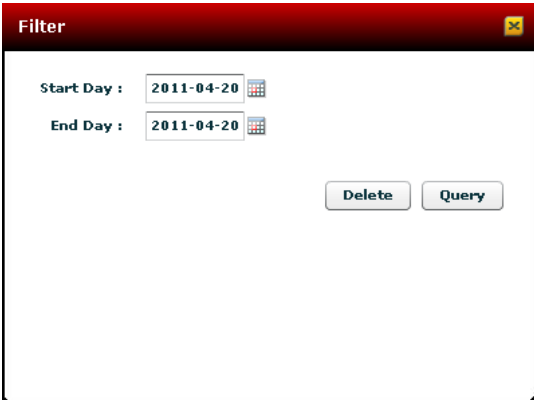
	
 First	When there is more than one page for the Action Log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the Action Log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the Action Log in this user group, click this button to display the next page.
 Last	When there is more than one page for the Action Log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Action	Display the action done by VigorACS to certain device.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the CPE.
MAC Address	Display the MAC address of the CPE.
Device IP	Display the WAN IP address of the CPE.
Action ID	Display the identification number of the action.
Time	Display the time that such action is done.

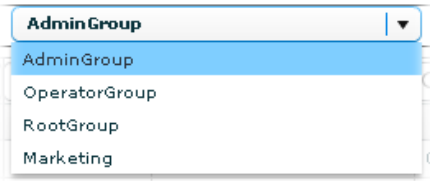
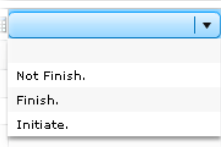
9.1.2 Reboot Log

Such page displays all the reboot actions initiated by VigorACS for your reference.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window.

Items	Description
	
 First	When there is more than one page for the Reboot Log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the Reboot Log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the Reboot Log in this user group, click this button to display the next page.
 Last	When there is more than one page for the Reboot Log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the CPE.
MAC Address	Display the MAC address of the CPE.
Device IP	Display the WAN IP address of the CPE.
User ID	Display which user reboots the device.
CommandKey	Display the key that VigorACS sends to CPE while performing download/upload job.
CurrentTime	Display current time.
Status	If you do not specify the condition, the server will display information for all of the CPEs which are rebooting, finish rebooting or are initiating. 

9.1.3 RebootByCPELog / ResetSystemPasswordLog

Such page displays all the reboot / reset actions initiated by CPE controlled under VigorACS for your reference.

Log ID	Device ID	Device Name	MAC Address	Device IP	CommandKey	CurrentTime
6363	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 02:01:05 PM
6362	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 01:10:15 PM
6361	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 01:08:56 PM
6360	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 00:57:46 PM
6359	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 10:23:29 AM
6358	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/08/01 09:24:56 AM
6357	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/30 09:24:54 AM
6356	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 11:24:15 PM
6355	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 11:11:40 PM
6354	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 10:59:52 PM
6353	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 10:43:59 PM
6352	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 06:04:12 PM
6351	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 06:03:49 PM
6350	31	DrayTek_001DAA_VigorAP	001DAA268D1C	192.168.1.10		2016/07/29 05:53:28 PM
6349	25	DrayTek_00507F_Vigor296	00507FFF3900	172.16.2.69		2016/07/28 05:11:58 PM

Available settings for such feature will be shown as follows:

Items	Description
Delete	Click this button to delete the selected log.
Delete All	Click this button to delete all of the records.
Refresh	Click this button to refresh this page.
Filter	Click this button to specify which records within certain period will be deleted or queried.
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window.

Items	Description
	
 First	When there is more than one page for the Reboot By CPE Log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the Reboot By CPE Log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the Reboot By CPE Log in this user group, click this button to display the next page.
 Last	When there is more than one page for the Reboot By CPE Log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
User ID	Display the user name that creates such profile.
Device Name	Display the name of the CPE.
MAC Address	Display the MAC address of the CPE.
Device IP	Display the WAN IP address of the CPE.
CommandKey	Display the key that VigorACS sends to CPE while performing download/upload job.
CurrentTime	Display current time.

9.1.4 SetParameterLog

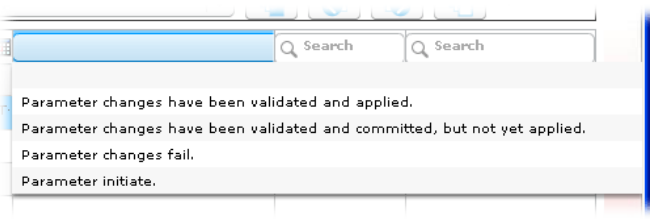
Such page displays all the values of parameters of CPE devices controlled by VigorACS for your reference.

SetParameterValuesLog				Your reliable networking solutions partner			
UserGroup: All_UserGroup				1/7			
Log ID	Device ID	Device Name	MAC Address	Device IP	User ID	ParameterKey	Created
98	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
97	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
96	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
95	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
94	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
93	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
92	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
91	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
90	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
89	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
88	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
87	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
86	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
85	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1
84	20	DrayTek_00507F_VigorAP 9	00507F043044	192.168.1.10	root	ManualSet	2016/06/1

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. Filter Start Day : 2011-04-20 End Day : 2011-04-20 Delete Query

Items	Description
 Detail	Such button will bring up another dialog and display detailed information for the selected CPE. 
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window. 
 First	When there is more than one page for the set parameter log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the set parameter log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the set parameter log in this user group, click this button to display the next page.
 Last	When there is more than one page for the set parameter log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the CPE.
MAC Address	Display the MAC address of the CPE.
Device IP	Display the WAN IP address of the CPE.
User ID	Display the user name that creates such profile.
ParameterKey	Display the key that VigorACS sends to CPE while performing parameter configuration.
Create Time	Display the time that the parameters created.
Finish Time	Display the time that the parameters enabled.

Items	Description
Status	VigorACS can display if the parameters configured for CPEs are successful or failed under four different conditions. Choose any one of them to display the status for your necessity. 
Fault Code	Display a code which is sent by CPE device to VigorACS when VigorACS server fails to perform the job of parameter configuration.
Fault String	Display the error message which is sent by CPE device to VigorACS when VigorACS server fails to perform the job of parameter configuration.

9.1.5 FileTransferLog

This page displays the record for firmware upload and download configuration for all CPEs controlled by VigorACS.

FileTransferLog

Your reliable networking solutions partner

UserGroup: All_UserGroup

1/1

Search

LogID

Search

DeviceID

Search

DeviceName

Search

MAC address

Search

DeviceIP

Ty

6707

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6706

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6705

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6704

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6703

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6702

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6701

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6700

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6699

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6698

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6697

50

DrayTek_00507F_Vigor_005

00507F6F32B0

2.112.79.10

Backup

6696

51

DrayTek_00507F_Vigor_005

00507F6F2760

2.112.73.98

Backup

6695

50

DrayTek_00507F_Vigor_005

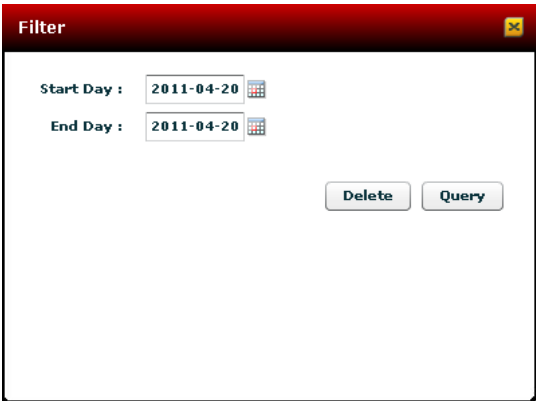
00507F6F32B0

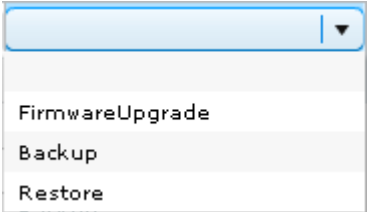
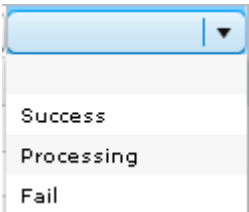
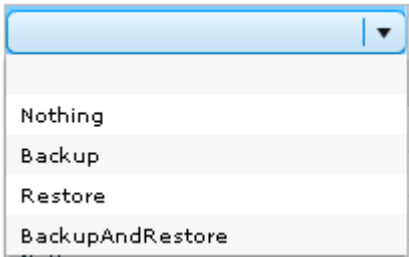
2.112.79.10

Backup

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.

Items	Description
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window. 
 First	When there is more than one page for the Log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the Log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the Log in this user group, click this button to display the next page.
 Last	When there is more than one page for the Log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
DeviceName	Display the name of the device.
MAC Address	Display the MAC address of the device.
DeviceIP	Display the WAN IP address of the device.

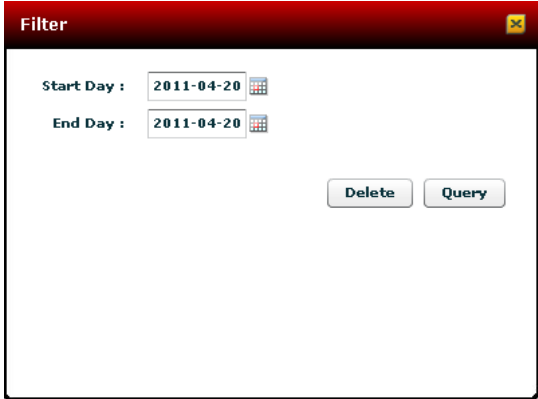
Items	Description
Type	Display the file transfer type (firmware upgrade, backup or restore) for the specified CPE. If you do not specify the condition, the server will display information for all of the CPEs which have done firmware upgrade, backup and restore configurations. 
Status	Display the result (success, processing or fail) for the file transfer action. If you do not specify the condition, the server will display information of the backup and restore no matter the job is successful, processing or failed. 
Event	Display the job (nothing, backup, restore or backup and restore) that the selected CPE is performing. You can specify which event to be displayed on the window. Simply choose any one of the event from the drop down list. If you choose Nothing, no record will be shown. 
FirmwareUpgradeID	Display the identification number of the firmware upgrade profile.
CommandKey	Display the key that VigorACS sends to CPE while performing download/upload job.
Count	Display the times of firmware upgrade for such device.
Time	Display the time that such log is done.

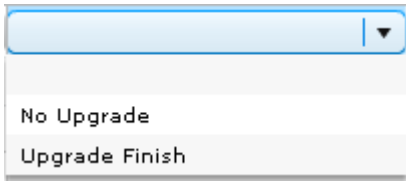
9.1.6 FirmwareUpgradeWizard

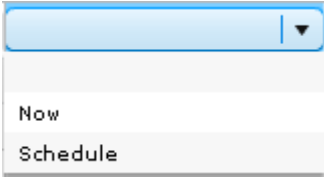
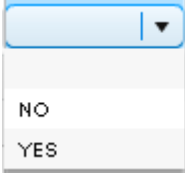
This page displays the record for firmware upgrade done by using wizard.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
 Detail	Such button will bring up another dialog and display detailed information for the selected CPE.

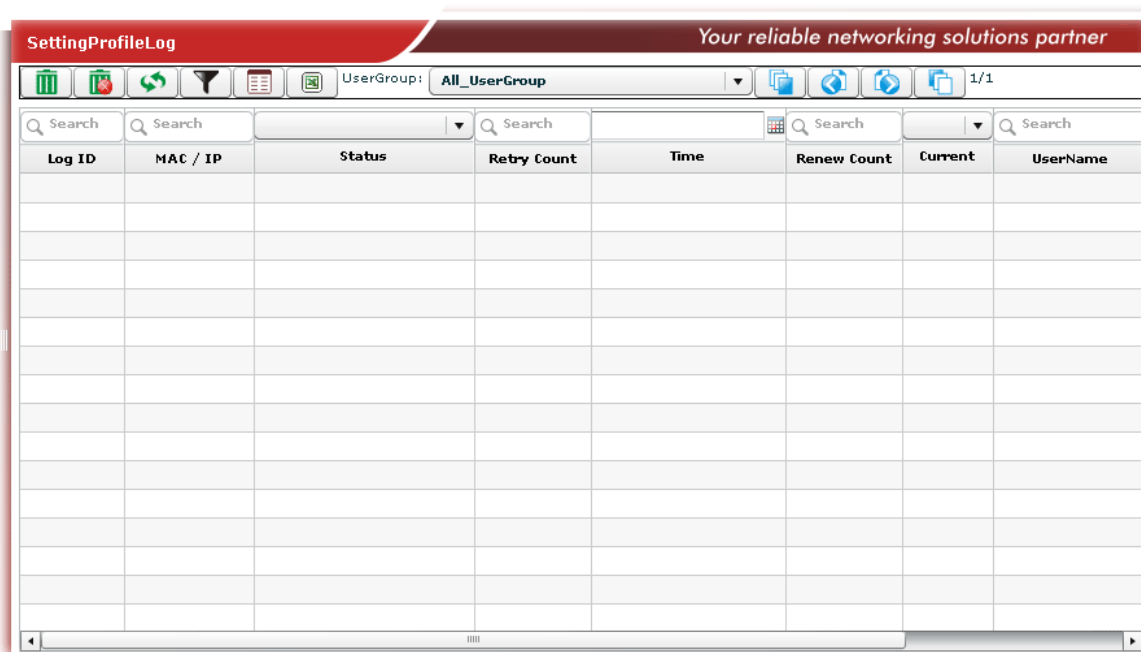
	
UserGroup	Use the drop down list to choose a user group. CPEs under such group will be displayed on the window. 
 First	When there is more than one page for the Log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the Log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the Log in this user group, click this button to display the next page.
 Last	When there is more than one page for the Log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the device.
Time	Specify one day (by using the calendar icon) to display the records of that time.
Status	Choose from the drop down menu to display the records of upgrade finished or no upgrade. 

Time Type	Display the log of certain time (now or schedule). 
Start Day	Display the firmware upgrade starting date that is configured in firmware upgrade profile.
Start Time	Display the firmware upgrade starting time that is configured in firmware upgrade profile.
End Time	Display the firmware upgrade ending time that is configured in firmware upgrade profile.
Upgrade File	Display the file name of the firmware used to upgrade for the selected CPE.
Current	Display if such log has been processed or not. If yes, please choose NO ; if not, please choose YES . 
UserName	Display the user name that creates such profile.

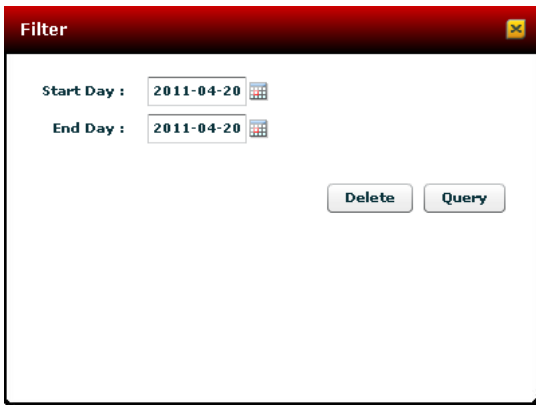
9.1.7 SettingProfileLog

After uploading the profile to the selected CPE, VigorACS will search from the database to find the proper configuration to the specified CPE when it tries to connect to VigorACS server. If the specified CPE receives the configuration, it will return confirmation information to VigorACS server.

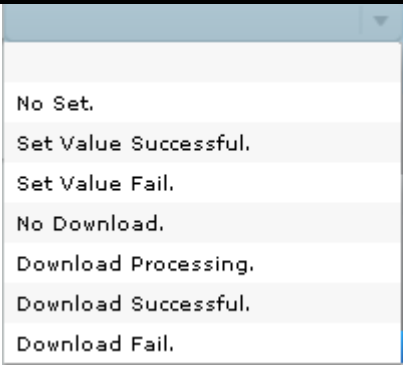
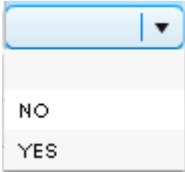
This page will list **current** status of the returning message of the CPE to VigorACS server.



Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
 Detail	Click this button to open a window with detailed information for checking the parameter settings of the selected log.

Items	Description
	
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the setting profile log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the setting profile log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the setting profile log in this user group, click this button to display the next page.
 Last	When there is more than one page for the setting profile log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
MAC / IP	Display the MAC address of the CPE.
Status	Specify the condition listed below. If you do not specify the condition, the server will display all of the information for the profile uploaded.

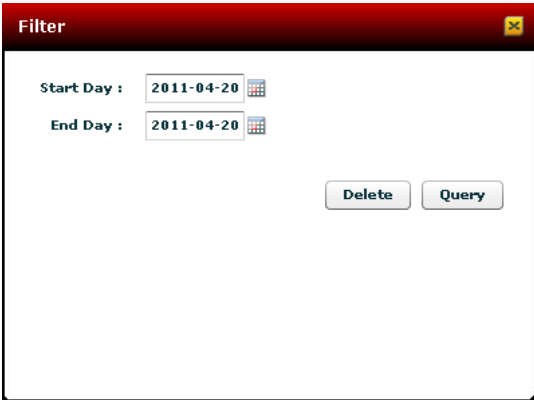
Items	Description
	
Retry Count	Display the time that VigorACS tries to set parameters to the selected CPE.
Time	Display the time recorded for the log.
Renew Count	Display how many times that such profile is uploaded.
Current	Display if such log has been processed or not. If yes, please choose NO; if not, please choose YES. 
UserName	Display the user name that creates such profile.
Action	Choose to begin or stop using such profile.
File Id	Display the file ID number of the uploaded profile.

9.1.8 DeviceSysLog

Such page displays the system log of connected CPEs.

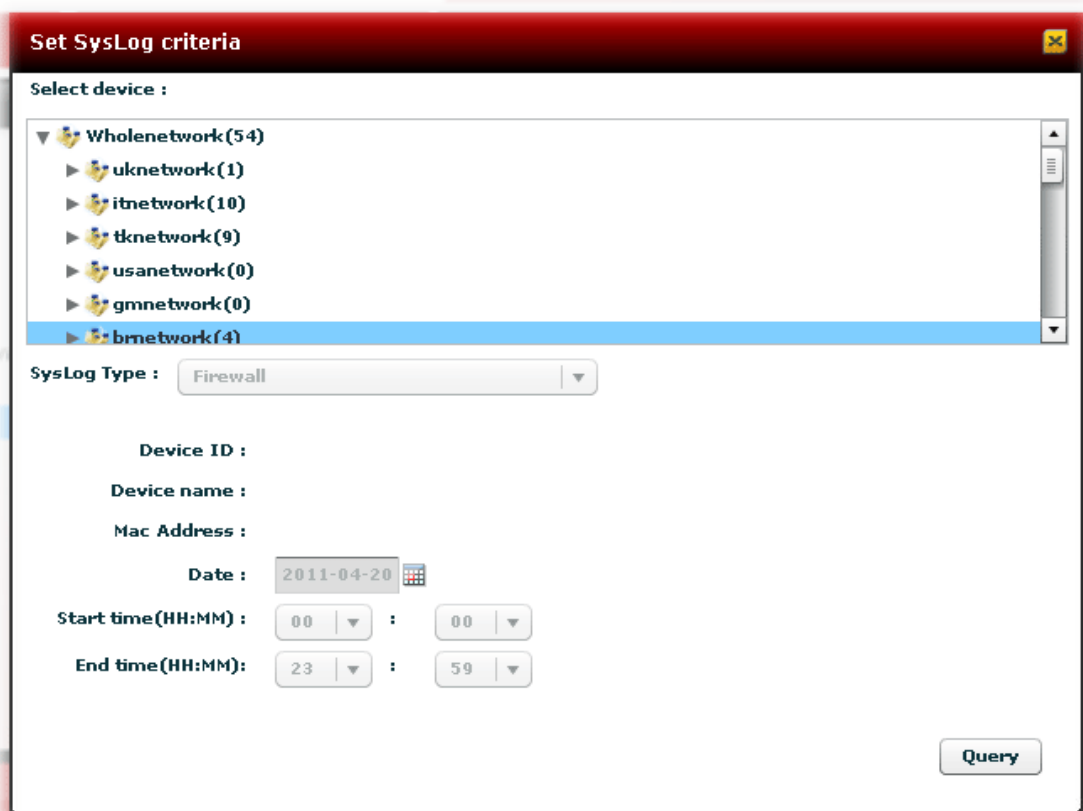
[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Set SysLog Criteria	Click this button to query syslog for certain CPE.
 Delete All	Click this button to delete all of the records.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
 First	When there is more than one page for the device system log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the device system log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the device system log in this user group, click this button to display the next page.

Items	Description
 Last	display the next page.
Log ID	When there is more than one page for the device system log in this user group, click this button to display the last page.
IP	The number displayed here is specified by VigorACS automatically.
System Time	Display the WAN IP address of the CPE.
Client Time	Display the time when the function is executed for the CPE.
Host Name / Class Name	Display the time of CPE when it sends system log out.
Message	Display the name of the host sent by CPE.
	Display a brief description for such log.

To view syslog information of specified CPE, please click  **Set SysLog Criteria** button first. The following dialog will appear.



Set SysLog criteria

Select device :

- ▼ Wholenetwork(54)
 - ▶ uknetwork(1)
 - ▶ itnetwork(10)
 - ▶ tknetwork(9)
 - ▶ usanetwork(0)
 - ▶ gmnetwork(0)
 - ▶ **bnetwork(4)**

SysLog Type : Firewall ▼

Device ID :

Device name :

Mac Address :

Date : 2011-04-20 

Start time(HH:MM) : 00 : 00

End time(HH:MM): 23 : 59

Query

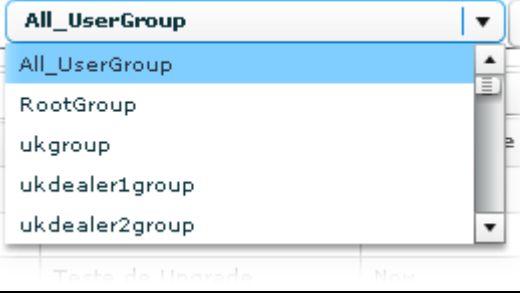
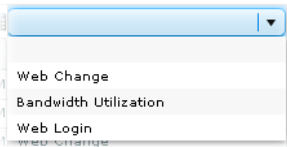
9.1.9 CPENotifyLog

Such page displays the

Log ID	Device ID	Device Name	MAC Address	Device IP	User Name	User IP	Value	
154	29	DrayTek_001DAA_Vigor286	001DAAB0BC30	172.17.5.148	Admin	172.17.5.146	LAN >>> LAN Po	2016/0
153	29	DrayTek_001DAA_Vigor286	001DAAB0BC30	172.17.5.148	Admin	172.17.5.146	LAN >>> LAN Po	2016/0
152	29	DrayTek_001DAA_Vigor286	001DAAB0BC30	172.17.5.148	Admin	172.17.5.146	LAN >>> LAN Po	2016/0
151	29	DrayTek_001DAA_Vigor286	001DAAB0BC30	172.17.5.148	Admin	172.17.5.146	System Mainten.	2016/0
150	29	DrayTek_001DAA_Vigor286	001DAAB0BC30	172.17.5.148	Admin	172.17.5.146	System Mainten.	2016/0
149	3	DrayTek_001DAA_Vigor286	001DAAB96680	111.251.239.16	admin	192.168.1.10	[Web]WebUI log	2016/0
148	3	DrayTek_001DAA_Vigor286	001DAAB96680	111.251.239.16	Admin	192.168.1.50	Wireless LAN(2.4	2016/0
147	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
146	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
145	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
144	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
143	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
142	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
141	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0
140	24	DrayTek_001DAA_Vigor286	001DAAA62650	172.17.3.83	admin	192.168.1.24	[Web]WebUI log	2016/0

Available settings for such feature will be shown as follows:

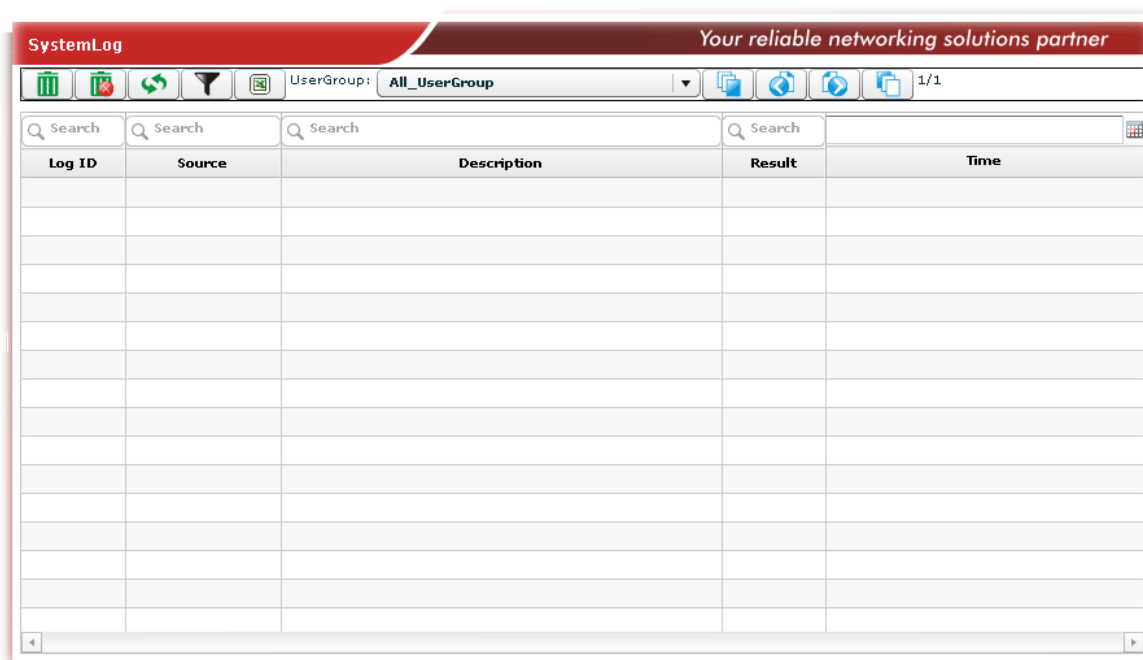
Items	Description
Delete	Click this button to delete the selected log.
Delete All	Click this button to delete all of the records.
Refresh	Click this button to refresh this page.
Filter	Click this button to specify which records within certain period will be deleted or queried.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.

Items	Description
	
 First	When there is more than one page for the device system log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the device system log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the device system log in this user group, click this button to display the next page.
 Last	When there is more than one page for the device system log in this user group, click this button to display the last page.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the device.
MAC Address	Display the MAC address of the device.
Device IP	Display the WAN or LAN IP address of the CPE.
User Name	Display the user account that a remote user used to access into that CPE.
User IP	Display the IP address (LAN or WAN) of the remote end which accesses into the CPE.
Value	Display the modification information for the device.
Notify Time	Display when the log is generated.
Type	Display the property (such as web change, bandwidth utilization and web login) of the log.  Web Change – Someone changes settings of CPE. Bandwidth Utilization – The status of bandwidth usage. Web Login - Someone accesses into CPE.

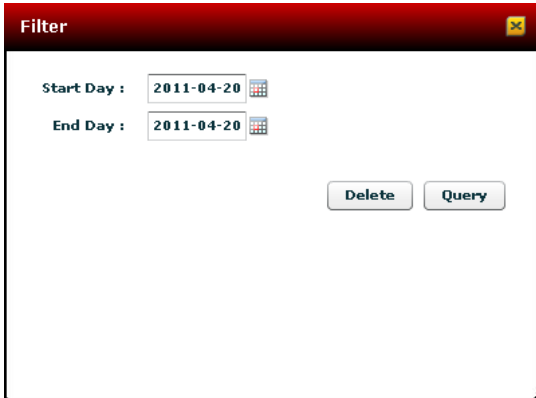
9.2 System

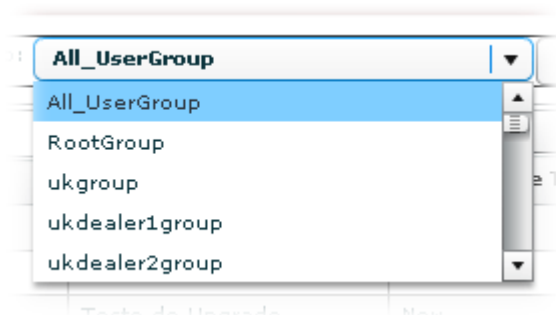
9.2.1 System Log

VigorACS will record the modification or changes of the CPE(s) done by VigorACS. For example, CPE will be attributed to another network, name of CPE will be changed or location of CPE on Google map will be modified, and etc. Refer to the following example:



Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the system log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the system log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the system log in this user group, click this button to display the next page.
 Last	When there is more than one page for the system log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Source	Display the device name.
Description	Display a brief explanation for the change to the CPE.
Result	Success - the change or modification succeeds and is recorded. Fail – the change or modification fails and is recorded.
Time	Display the time recorded for the log.

9.2.2 LoginLog

VigorACS will record the login information for every login user. Refer to the following example:

LoginLog		Your reliable networking solutions partner			
		UserGroup: All_UserGroup		1/28	
Q Search	Q Search	Q Search			
Log ID	User Name	Login IP	Login Time	Logout Time	Status
420	root	172.16.3.130	2016/08/01 10:49:08 AM		Success.
419	root	118.166.175.221	2016/08/01 10:17:10 AM		Success.
418	root	172.16.3.130	2016/07/28 04:53:55 PM		Success.
417	root	172.16.3.130	2016/07/28 04:53:55 PM		Success.
416	root	172.16.3.130	2016/07/28 04:43:05 PM		Success.
415	root	172.16.3.130	2016/07/28 04:11:25 PM		Success.
414	root	172.16.3.130	2016/07/28 04:10:40 PM		Success.
413	root	220.132.109.131	2016/07/26 03:02:46 PM		Success.
412	root	220.132.109.131	2016/07/26 03:02:31 PM		Success.
411	root	172.16.2.221	2016/07/26 02:59:30 PM		Success.
410	root	220.132.109.131	2016/07/26 02:32:41 PM		Success.
409	root	220.132.109.131	2016/07/26 01:59:09 PM		Success.
408	root	220.132.109.131	2016/07/26 01:04:41 PM		Success.
407	root	220.132.109.131	2016/07/26 01:04:31 PM		Fail.
406	root	220.132.109.131	2016/07/26 01:03:44 PM		Fail.

Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. Filter Start Day : 2011-04-20 End Day : 2011-04-20 Delete Query

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the login log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the login log in this user group, click this button to display the previous page.
 Next	When there is more than one page for the login log in this user group, click this button to display the next page.
 Last	When there is more than one page for the login log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
User Name	Display the user name that the user adopts for accessing into VigorACS.
Login IP	Display the public IP address of the user.
Login Time	Display the time that the user accesses into VigorACS.
Logout Time	Display the time that the user exits VigorACS.
Status	Display the status (success or fail) that the user access into VigorACS.

9.2.3 DeviceInformationLog

This page displays the general information of CPE registered to VigorACS SI.

DeviceInformationLog		Your reliable networking solutions partner		
  UserGroup: All_UserGroup     1/2				
Device ID	Device Name	MAC Address	Device IP	Registered Time
153	DrayTek_001DAA_Vigor_00	00:1d:aa:00:00	61.216.231.25	2012/05/07 19:13:28
151	DrayTek_00507F_Vigor_005	00507FAFB3A0	59.115.247.206	2012/04/26 18:46:43
149	2910_00507F_Vigor_00507	00507F267257	192.168.91.1	2012/04/25 13:35:28
148	DrayTek_00507F_Vigor_005	00507F77D0E8	61.216.232.88	2012/04/18 14:14:53
147	DrayTek_00507F_Vigor_005	00507FCB8C654	192.168.93.50	0/12/30 00:00:00
146	DrayTek_00507F_Vigor_005	00507F7FFB41	37.46.160.162	0/12/30 00:00:00
140	2710_00507F_Vigor_00507	00507FA05138	59.115.241.116	0/12/30 00:00:00
139	DrayTek_00507F_Vigor_005	00507F9FAE98	1.169.165.67	0/12/30 00:00:00
133	2830_00507F_Vigor_00507	00507F708098	59.115.240.18	0/12/30 00:00:00
131	DrayTek_00507F_Vigor_005	00507FC8432C	192.168.92.2	0/12/30 00:00:00
130	DrayTek_00507F_Vigor_005	00507FCC1AB4	114.44.48.170	0/12/30 00:00:00
129	DrayTek_00507F_Vigor_005	001D000000DC	1.169.156.19	0/12/30 00:00:00
116	AP800_A_00507F_Vigor_005	00507F522F58	192.168.92.2	0/12/30 00:00:00
80	2920_A_00507FC93B24	00507FC93B24	1.169.159.46	0/12/30 00:00:00

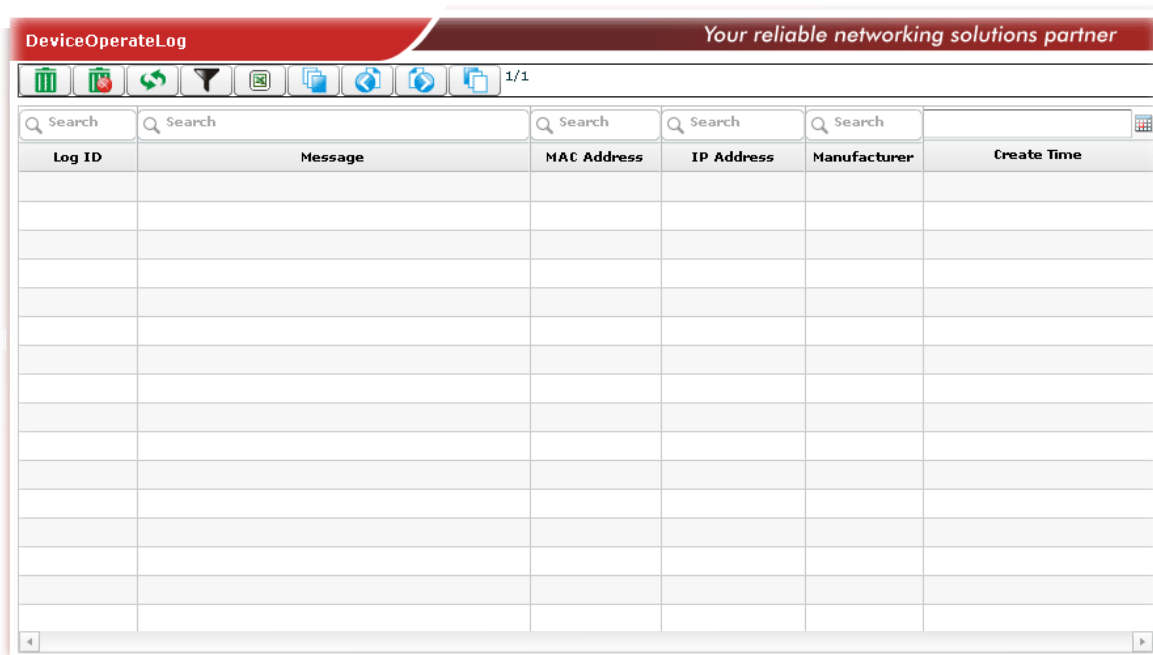
Available settings for such feature will be shown as follows:

Items	Description
 Refresh	Click this button to refresh this page.
 Export to CSV	Click this button to export the all the logs as an Excel file.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the device operate log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the device operate log in this user group, click this button to display the previous

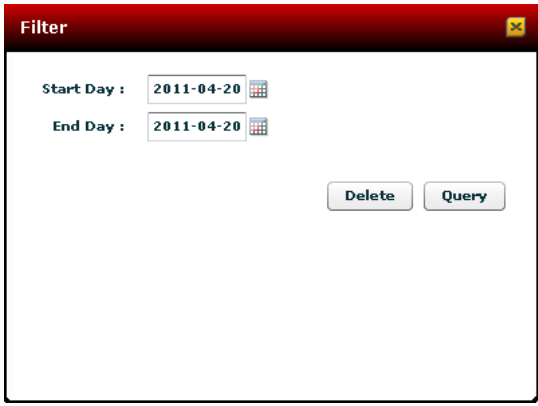
Items	Description
	page.
 Next	When there is more than one page for the device operate log in this user group, click this button to display the next page.
 Last	When there is more than one page for the device operate log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Device ID	The number displayed here is specified by VigorACS automatically.
Device Name	Display the name of the CPE.
MAC Address	Display the MAC address of the CPE.
Device IP	Display the IP address of the CPE.
User ID	Display the user name that creates such profile.
Time	Display the time that such CPE registers to VigorACS SI.
Status	Display current status (register to VigorACS or deleted by VigorACS) of such CPE.

9.2.4 DeviceOperateLog

This page displays the log about which CPE connects to VigorACS successfully or unsuccessfully.



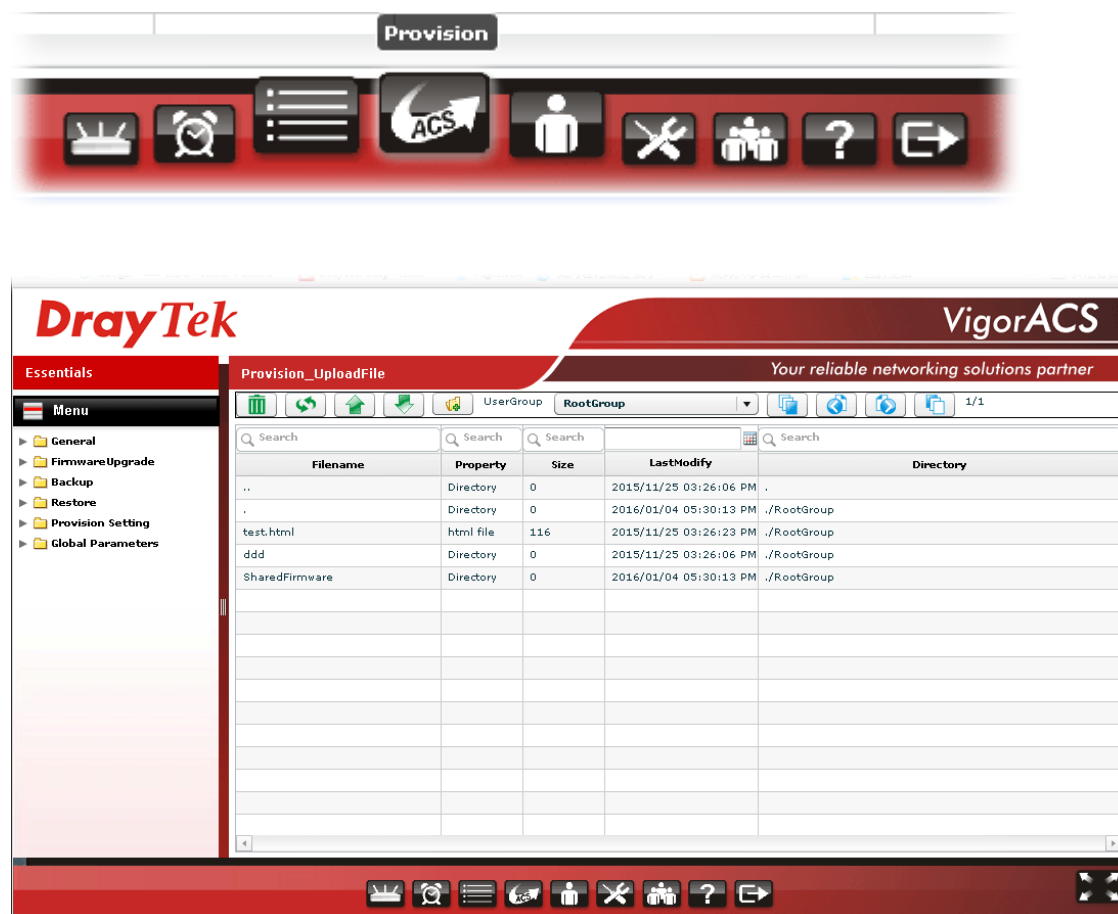
Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected log.
 Delete All	Click this button to delete all of the records.
 Refresh	Click this button to refresh this page.
 Filter	Click this button to specify which records within certain period will be deleted or queried. 
 First	When there is more than one page for the device operate log in this user group, click this button to display the first page.
 Previous	When there is more than one page for the device operate log in this user group, click this button to display the previous page.

Items	Description
 Next	When there is more than one page for the device operate log in this user group, click this button to display the next page.
 Last	When there is more than one page for the device operate log in this user group, click this button to display the last page.
Search	Click this box to type the search condition and press Enter . The server will display the data based on your request.
Log ID	The number displayed here is specified by VigorACS automatically.
Message	Display related information for the CPE.
MAC Address	Display the MAC address of the CPE.
IP Address	Display the IP address of the CPE.
Manufacturer	Display the manufacturer for the CPE.
Create Time	Display the time that the operation created.

Chapter 10 Provision Configuration

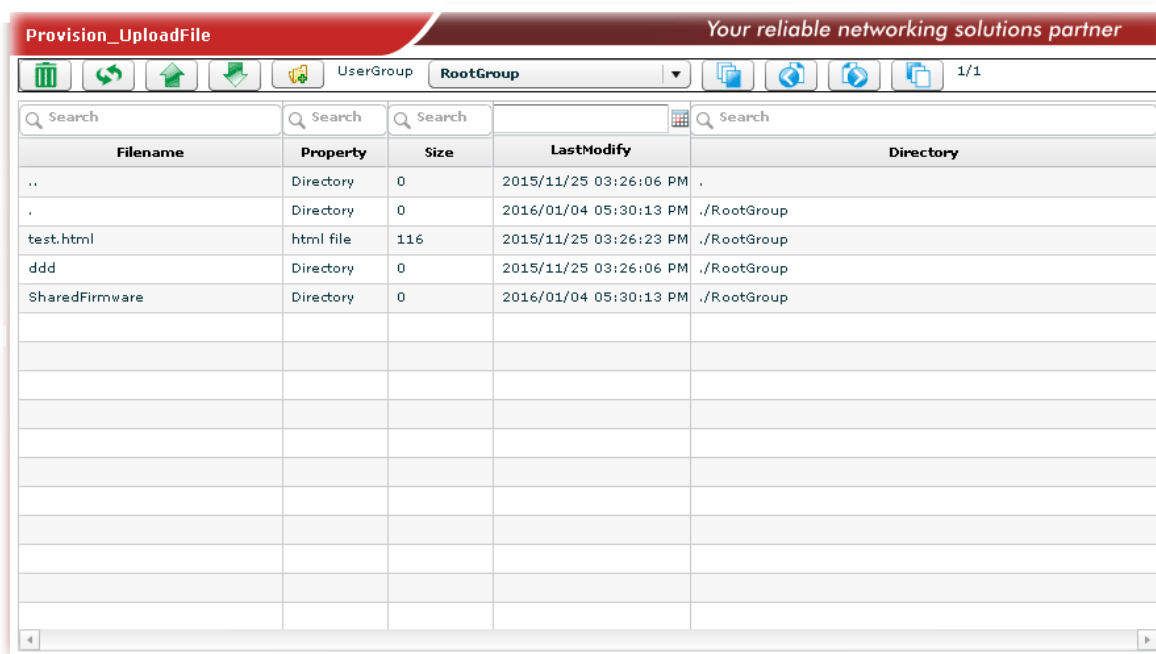
Provision functions allow users to set provision profiles for applying in numerous TR-069 CPEs instead of configuring settings for each CPE one by one.



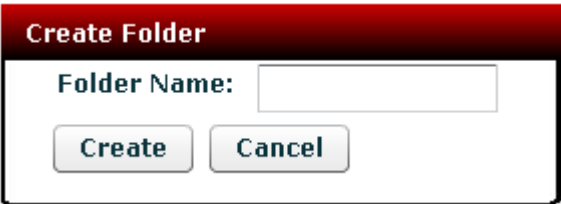
10.1 General Setting

10.1.1 Upload File

Upload File function allows users to upload the file to VigorACS, including configuration and firmware image files.



Available settings for such feature will be shown as follows:

Items	Description
 Delete	Click this button to delete the selected provision file.
 Refresh	Click this button to refresh uploaded files.
 Upload File	Click this button to upload a provision file from your host to VigorACS. The file you upload will be shown on the screen immediately.
 Download File	Click this button to download a file from VigorACS to your computer.
 Create Folder	Click this button to create a new folder for storing and managing the uploaded files. It will be displayed under filename field.  Type the name for the new folder and click Create. The new folder will be displayed on the screen.

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the upload files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the upload files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the upload files in this user group, click this button to display the next page.
 Last	When there is more than one page for the upload files in this user group, click this button to display the last page.
Filename	Display the name of the download/upload file or created folder.
Property	Display whether this is a folder or a file. If it is a folder, it will display "Directory", otherwise, it will display extension name of the file.
Size	Display the file size of the file or folder.
LastModify	Display the latest time the file has been modified.
Directory	Display the relative path of this file/folder.

10.1.2 Trigger

This page allows administrator to set special time to trigger the provision for firmware upgrade. You can specify a name for it.

Available settings for such feature will be shown as follows:

Items	Description
 Add firmware upgrade trigger	Click this button to create a new trigger profile for firmware upgrade, backup and restore.
 Save trigger setting	Click this button to save the trigger settings after finish the configuration.
 Delete firmware upgrade trigger	Click this button to delete the selected trigger.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 

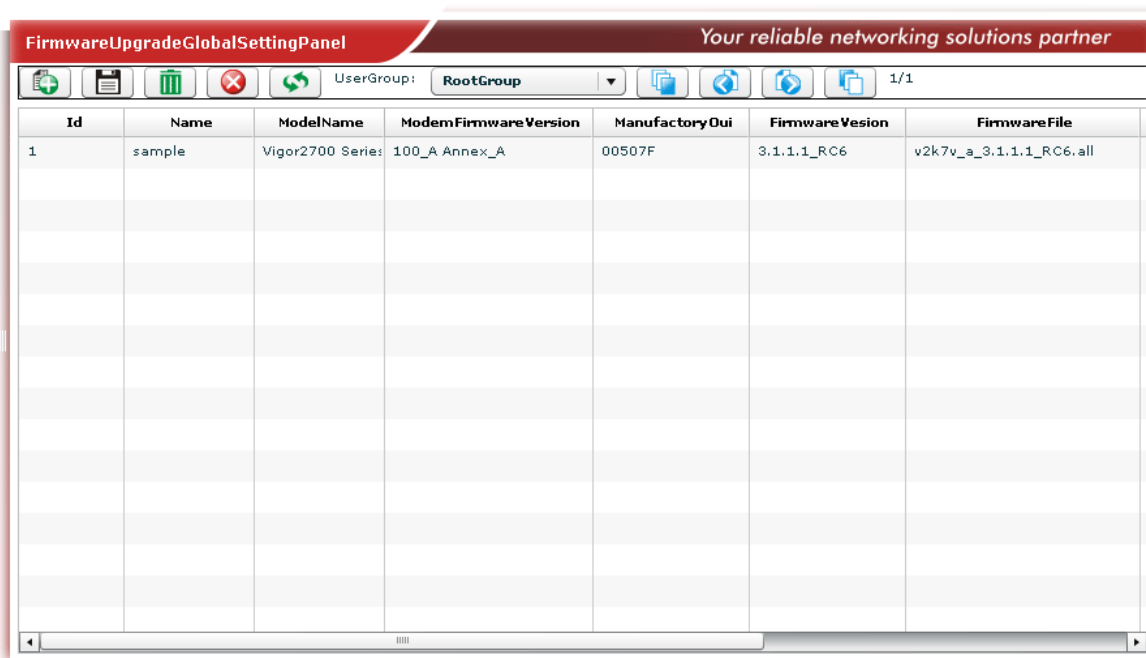
Items	Description
 First	When there is more than one page for the triggered files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the triggered files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the triggered files in this user group, click this button to display the next page.
 Last	When there is more than one page for the triggered files in this user group, click this button to display the last page.
Triggername	Type a special and easy to identify name for the time trigger. After you click  Save , the new name will be displayed on the screen.
DayType	Choose Any to activate such trigger every day. Choose Schedule to activate such trigger according to the date and time set in this page.
StartDay	Use the pop-up calendar window to set the starting day for CPE firmware update. Move your mouse cursor to choose one day and click the mouse. The selected date will be shown on the entry box.
CheckEndDay	Check this box to let VigorACS check the end of the schedule automatically. YES means the trigger will not be activated after the end day. No means the trigger will be activated everyday to execute the provision.
EndDay	Use the pop-up calendar window to set the ending day for CPE firmware update. Move your mouse cursor to choose one day and click the mouse. The selected date will be shown on the entry box.
TimeType	Choose Any to activate such trigger for the next time CPE sends information to VigorACS. In default, CPE sends information to VigorACS every 15 minutes. Choose Schedule to activate such trigger according to the date and time set in this page.
StartTime(HH:MM)	Type the start time (HH:MM) in this filed for such trigger.
EndTime(HH:MM)	Type the end time (HH:MM) in this filed for such trigger.
CreateTime	Display the time of such time trigger created.
CreateUser	Display the name of the user/administrator who made such time triggering.

10.2 FirmwareUpgrade

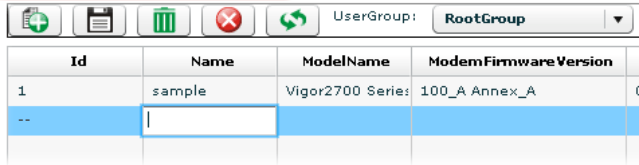
10.2.1 UpgradeSetting

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.

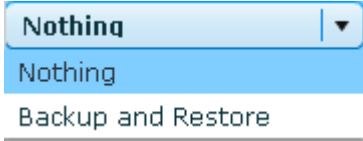
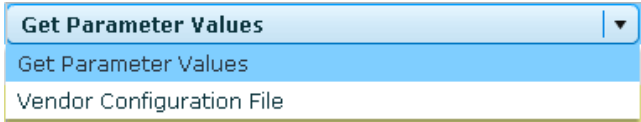
When VigorACS server receives information from CPE about firmware upgrade, it will check if the received model name, modem firmware version, parameters of manufacturer OUI and software version correspond to the information recorded in VigorACS server. If everything can match but software version not,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



Available settings for such feature will be shown as follows:

Items	Description
 Add firmware upgrade global setting	Click this button to add global setting name on the screen. 
 Save firmware upgrade global setting	Click this button to save the configuration.
 Delete firmware upgrade global setting	Click this button to delete the selected parameter.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page.

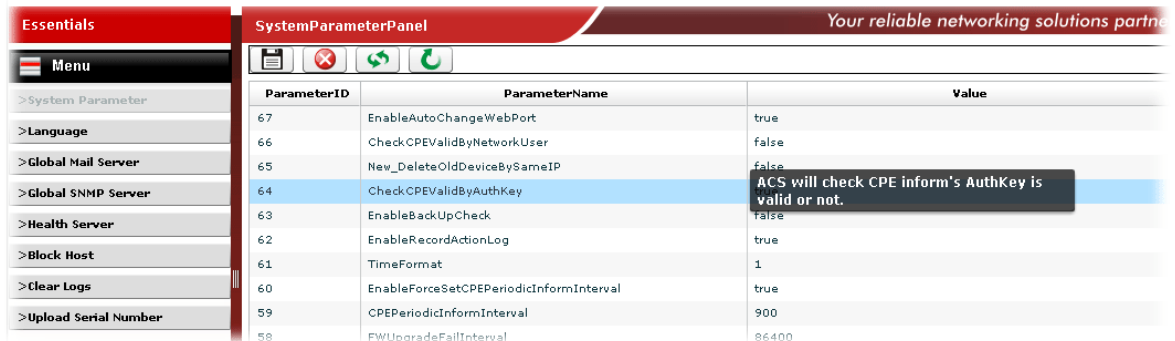
Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the global setting files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the global setting files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the global setting files in this user group, click this button to display the next page.
 Last	When there is more than one page for the global setting files in this user group, click this button to display the last page.
Id	Display the number of the global setting.
Name	Type a name for such global setting profile.
ModelName	Type the model of the CPE device that needs to upgrade firmware.
ModemFirmwareVersion	Type the firmware version of the CPE device, e.g., Annex A, Annex B and etc. Note: Before performing firmware upgrade for the CPE, VigorACS will check if the received model name, modem firmware version, parameters of manufacturer OUI and software version match with the information recorded in VigorACS server or not. If you type “*” in this filed, the modem firmware version will not be regarded as a comparison condition in the process of firmware upgrade. It will be ignored.
ManufactoryOui	Type the characters of OUI. OUI means “organizationally unique identifier” of the device manufacturer. Note: Before performing firmware upgrade for the CPE, VigorACS will check if the received model name, modem firmware version, parameters of manufacturer OUI and software version match with the information recorded in VigorACS server or not. If you type “*” in this filed, the manufacturer OUI will not be regarded as a comparison condition in the process of firmware upgrade. It will be ignored.

Items	Description
SoftwareVersion	Type the version of the firmware.
FirmwareFile	Double click this file to open a dialog for choosing one provision file created in section 7.1.1 UploadFile for this profile. 
TriggerName	Choose one of the trigger profiles from the drop down list.
Status	Click Disable to give up the upgrade procedure or click Enable to activate the upgrade procedure after clicking Save .
Event	While upgrading firmware for CPE device, the required parameters (e.g, WAN, LAN, VPN...) on CPE device can be backup in VigorACS server and can be restored in the future if required. Please choose the one you need.  Nothing – All the parameters configured in CPE device will not be saved / restored and will be written after VigorACS server executes firmware upgrade for it. Backup and Restore – All the parameters configured in CPE device will be saved and restored in a place before VigorACS server executes firmware upgrade for it.
EventType	If you choose Backup and Restore as the event selection, you have to specify event type additionally.  Get Parameter Values – Generally, VigorACS server will scan all the parameters configured in CPE device while connecting CPE device. You can choose this item to use current configured parameters obtained from CPE device as the basis for parameters backup and restore. Vendor Configuration File – Choose this time to use the parameters recorded in cfg file of CPE device as the basis for back and restore.

After you finished all of the settings, remember to click  **Save** to save your record.

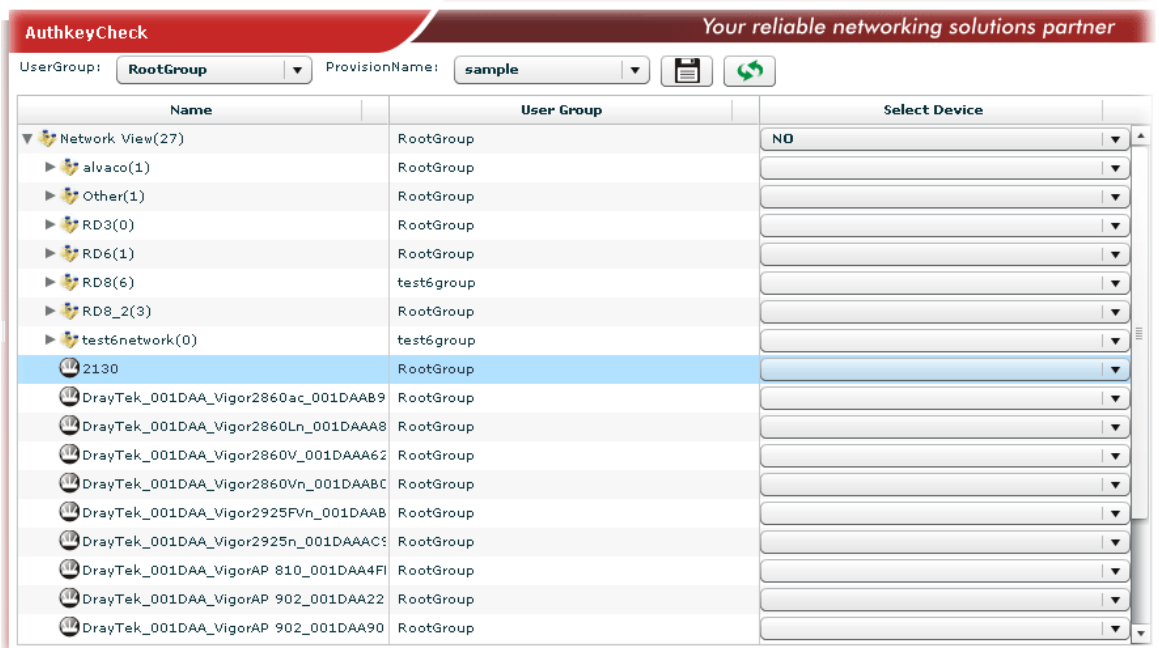
10.2.2 AuthkeyCheck

To avoid hacker's attack via Vigor device (router or AP), special authentication key is used for communication between Vigor device and VigorACS SI. When the value of "CheckCPEValidAuthKey" in **System Parameter** is set as "true", VigorACS will verify all of the Vigor devices via authentication key issued by DrayTek to ensure the network security.



In general, newest released firmware for DrayTek device contains "AuthKey". Therefore, the network administrator shall determine which CPE device required to execute firmware upgrade for owing the "AuthKey".

The following page is used to specify which CPE device required to execute firmware upgrade for having AuthKey.



Available settings for such feature will be shown as follows:

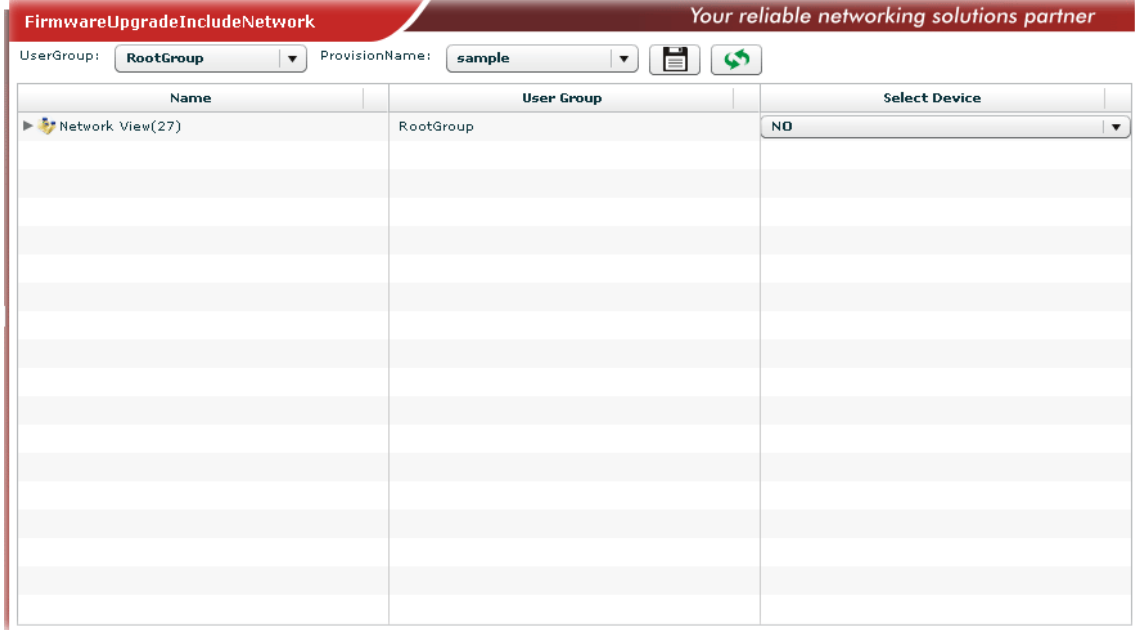
Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.

	 All the devices controlled under the group will be shown on the screen.
ProvisionName	Use the drop down list to choose a global setting profile for firmware upgrade.
 Save	Click this button to save the configuration.
 Refresh	Click this button to refresh current page.
Name	Display the CPEs with the authority of the selected group.
User Group	Display the user group for the selected device.
Select Device	YES – If the device does not have Authkey, choose YES to carry out firmware upgrade for that device automatically when it tries to communicate with VigorACS. NO – If the device has Authkey, it is not necessary to perform firmware upgrade.

After you finished all of the settings, remember to click  **Save** to save your record.

10.2.3 IncludeList

This page displays the quantities of profiles created in FirmwareUpgrade_GlobalSetting. You can specify which CPE device required to execute firmware upgrade.

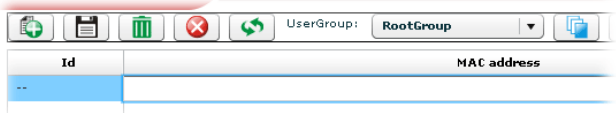


Available settings for such feature will be shown as follows:

10.2.4 ExcludeList

Not all the CPEs controlled by VigorACS need to upgrade firmware at any time. VigorACS 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 do firmware upgrade for the specified CPE, simple open this page and remove the item.

Available settings for such feature will be shown as follows:

Items	Description
 Add excluded device	Click this button to add CPEs which will not be upgraded.  Type the MAC address of the CPE that does not need to do firmware upgrade.
 Save exclude setting	Click this button to save the configuration.
 Delete exclude device	Click this button to delete the selected parameter.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.

Items	Description
	
 First	When there is more than one page for the excluded setting files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the excluded setting files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the excluded setting files in this user group, click this button to display the next page.
 Last	When there is more than one page for the excluded setting files in this user group, click this button to display the last page.
Id	Display the number of the firmware upgrade.
MAC address	Display the MAC address of the

10.2.5 RemoteFileList

This page displays the firmware of CPE which is located / stored in FTP server.

Remote FTP File		Your reliable networking solutions partner		
		UserGroup	RootGroup	
Filename	Property	Size	LastModify	Directory
..	Directory	0		.
.	Directory	0		.
2011 databook	Directory	4096	03/01/2011 09:00:00	.
ACS SI	Directory	4096	06/15/2010 00:00:00	.
DSLVIgor_USB_MODEM	Directory	4096	08/24/2008 00:00:00	.
Declaration of Conformity	Directory	4096	03/18/2010 00:00:00	.
Document	Directory	4096	02/03/2009 00:00:00	.
France	Directory	4096	08/24/2008 00:00:00	.
ISDNVigor128	Directory	4096	08/24/2008 00:00:00	.
MiniVigor128	Directory	4096	08/24/2008 00:00:00	.
Signature	Directory	4096	05/21/2010 00:00:00	.
Vigor N61	Directory	4096	08/28/2008 00:00:00	.
Vigor120	Directory	4096	06/15/2010 00:00:00	.
Vigor120 V2	Directory	4096	12/17/2009 00:00:00	.

Available settings for such feature will be shown as follows:

Items	Description
 Refresh	Click this button to refresh current page.
 Download File	Click this button to download a file from VigorACS to your computer.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
Filename	Display the name of the download/upload file or created folder.
Property	Display whether this is a folder or a file. If it is a folder, it will display "Directory", otherwise, it will display extension name of the file.
Size	Display the file size of the file or folder.
LastModify	Display the latest time the file has been modified.
Directory	Display the relative path of this file/folder.

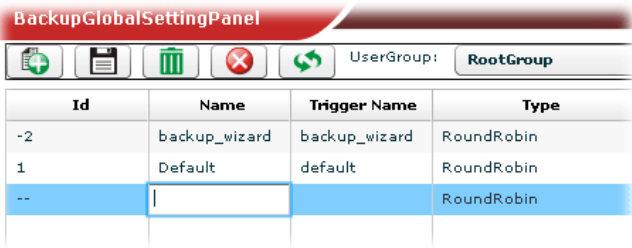
10.3 Backup

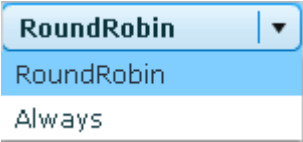
10.3.1 BackupSetting

Such page can determine the trigger time and method for firmware backup. Profiles configured here can be selected in the page of **Backup>>BackupSetting**.

[illegible]

Available settings for such feature will be shown as follows:

Items	Description
 Add backup global setting	Click this button to add a new backup profile with global settings.  Type a new name in the blank box; specify a trigger name and type by using the drop down list; type the period value and give a brief description.
 Save backup global setting	Click this button to save the backup profile.
 Delete backup global setting	Click this button to delete the selected backup profile.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the global setting files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the global setting files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the global setting files in this user group, click this button to display the next page.
 Last	When there is more than one page for the global setting files in this user group, click this button to display the last page.
Id	Display the number of the global setting.
Name	Type a name the global setting.
Trigger Name	Choose one of the trigger profiles from the drop down list.
Type	Choose the type for the configuration backup.  RoundRobin – Choose this type to execute the backup (with global settings). The backup files will be recorded with the filename from <i>1.cfg</i> to <i>20.cfg</i>. Only 20 filenames will be kept in the same directory. Always – Choose this type to execute the backup (with global settings) according to the schedule. The backup files will be recorded with the filename one by one (e.g. <i>1.cfg</i>, <i>2.cfg</i>, ..., <i>1000cfg</i>, ..., <i>10000cfg</i>, ...no limit in file number). All of the backup files will be kept in the same directory.
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.
Description	Type a brief description for profile.

10.3.2 Backup

Such page can determine which device or network will be applied with backup profiles.

[illegible]

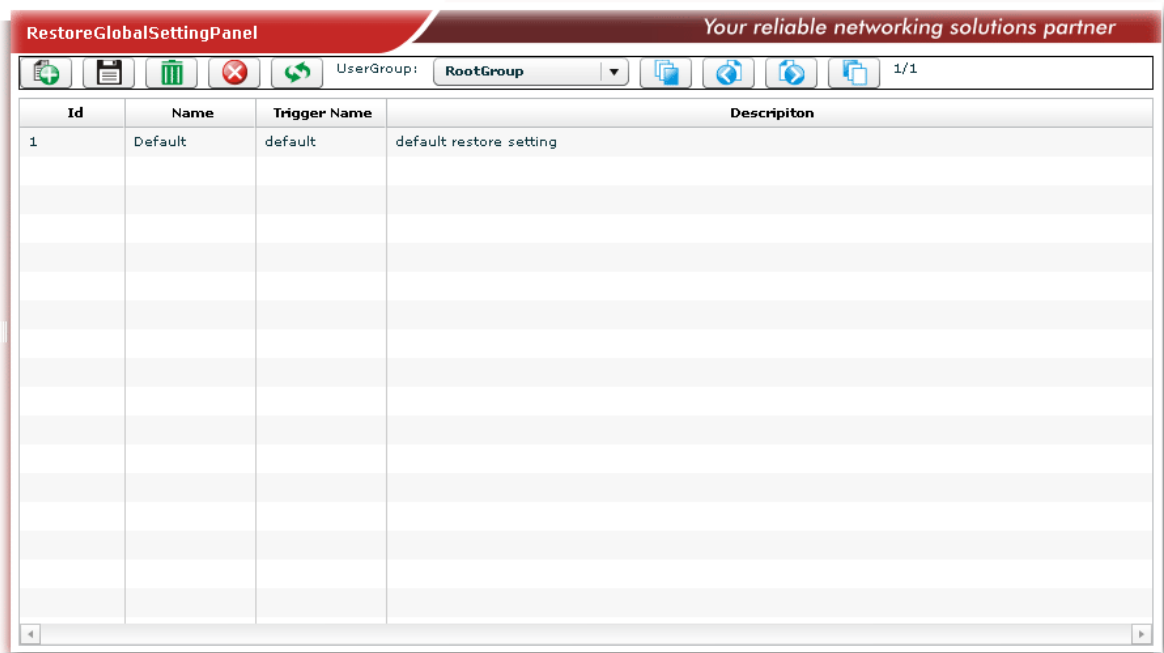
Available settings for such feature will be shown as follows:

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.  Later, the corresponding devices will be shown in this page.
 Save	Click this button to save the backup profile.
 Refresh	Click this button to refresh current page.
Name	Display the CPEs with the authority of the selected group.
User Group	Display the user group for the selected device.
Profile Id	Choose a profile (with global settings) defined in GlobalSetting (section 7.6.1) to be applied in such selected CPE.

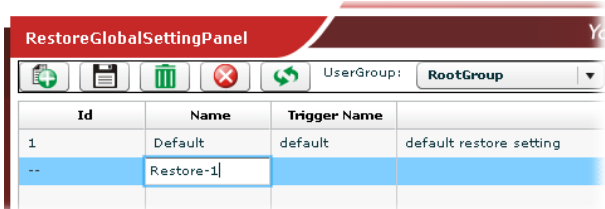
10.4 Restore

10.4.1 RestoreSetting

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



Available settings for such feature will be shown as follows:

Items	Description
 Add restore global setting	Click this button to add a new restore profile with global settings. To configure a profile with global settings, please refer to 7.1.2 Trigger for detailed information. 
 Save restore global setting	Click this button to save the restore profile.
 Delete restore global setting	Click this button to delete the selected restore profile.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page.

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 First	When there is more than one page for the global setting files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the global setting files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the global setting files in this user group, click this button to display the next page.
 Last	When there is more than one page for the global setting files in this user group, click this button to display the last page.
Id	Display the number of the global setting.
Name	Type a name for such record.
Trigger Name	Choose one of the trigger profiles from the drop down list.
Description	Type a brief description for such profile.

10.4.2 Restore

Such page can determine which device or network will be applied with restore profiles.

Available settings for such feature will be shown as follows:

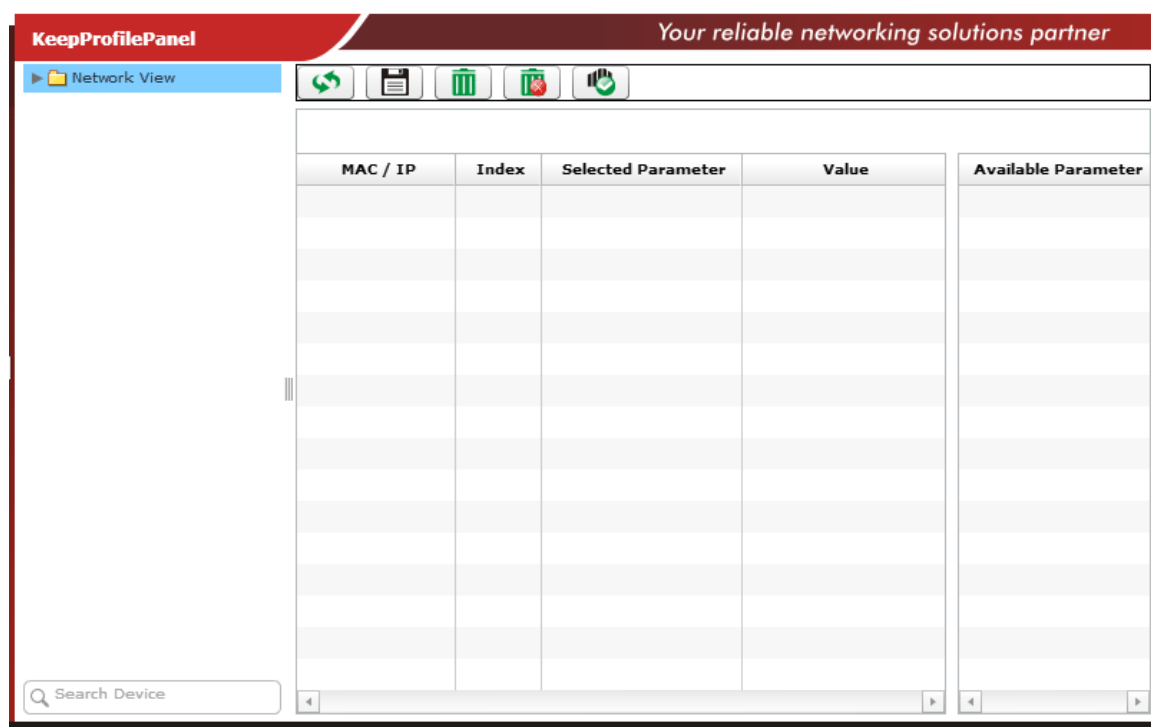
Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.  Later, the corresponding devices will be shown in this page.
 Save	Click this button to save the restore profile.
 Refresh	Click this button to refresh current page.
Name	Display the names of CPEs with the authority of the selected group.
User Group	Display the user group for the selected device.
Status	Check this box to execute file 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

Items	Description
	file restoration of the selected CPE.
Restore Profile	Use the drop down list to choose one of the time profiles (with global settings, section 7.1.2) to be applied for the file restoration of the selected CPE.

10.5 Provision Setting

10.5.1 KeepProfile Setting

Some ISPs do not wish CPE client changing the parameters of CPE device. If the parameters of CPE device were modified by the users, VigorACS (the administrator) server could use the parameters listed in this web page to **restore the original parameters**.

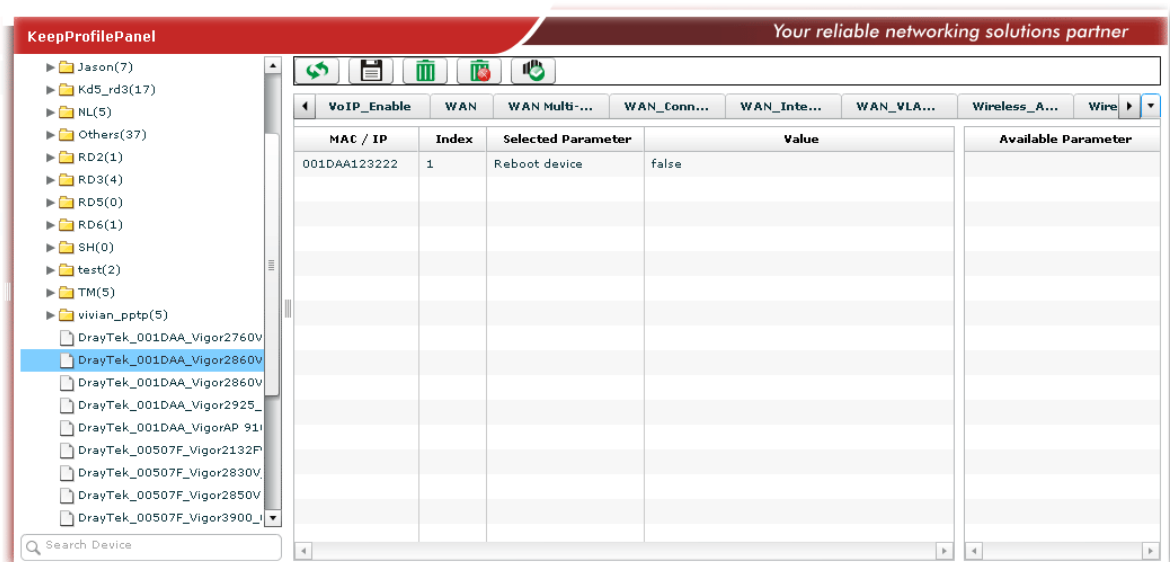


Available settings for such feature will be shown as follows:

Items	Description
 Refresh	Click this button to refresh current page.
 Save	Click this button to save the configuration.
 Delete	Click this button to delete the selected parameter.
 Delete All	Click this button to delete all of the parameters.
 Complete Parameter	Click this button to open KeepProfilePanel Detail Table for adding new user-defined parameter with value for the selected device.

Items	Description
	
MAC Address	Display the MAC address for the selected CPE.
Index	Display the index number for the parameter.
Parameter	Display the parameter name that you want to configure.
Value	Based on the parameters selected above, type the required value for the selected device.

Settings will be shown on the right side. **Reboot, LAN, WAN, VPN, NAT, VoIP, Firmware** tabs and others (**displayed based on the CPE you choose**) will appear for you to click to configure. In the field of **Available Parameter**, all the available parameters for the selected tab will be displayed.



Note: Available parameters tabs will be different according to the CPE selected and the firmware used by that CPE. In addition, you can click the arrows on top-right to scroll the setting tabs to find the one you want to configure.



Here, we take the **WAN** settings (for Vigor2860) as an example:

WAN Settings

To configure the WAN settings, please double click on the parameter in the right side. Then, MAC Address and the selected parameter with value will be shown on the right side.

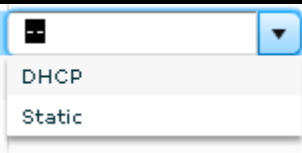
MAC / IP	Index	Selected Parameter	Value	Available Parameter
				IP
				Addressing Type
				Gateway
				PPP User Name
				PPP Password
				IP Enable
				PPP Enable
				Subnet Mask
				DNS Servers
				VLAN ID
				Port
				VLAN Tag Insertion
				Tag Value
				Priority

To edit the value for the selected parameter, move the mouse cursor to the box under value and click it. An entry box will appear for you to type the value for that parameter. After typing the value, click the **Save** button to save it.

MAC / IP	Index	Selected Parameter	Value	Available Parameter
001DAA123222	1	IP		IP
				Addressing Type
				Gateway
				PPP User Name
				PPP Password
				IP Enable
				PPP Enable
				Subnet Mask
				DNS Servers
				VLAN ID
				Port
				VLAN Tag Insertion
				Tag Value
				Priority

Available parameters for WAN include:

Items	Description
IP	Type the WAN IP address for the selected CPE.
Addressing Type	Choose the type from the drop down list for WAN settings.

Items	Description
	
Gateway	Type the gateway for the selected CPE.
PPP User Name	Type the user name offered by ISP for PPP connection.
PPP Password	Type the password offered by ISP for PPP connection.
IP Enable	Choose True to enable settings for DHCP or Static IP connection.
PPP Enable	Choose True to enable settings for PPP connection.
Subnet Mask	Type the subnet mask for the selected CPE if IP Enabled is set to "True".
DNS Servers	Type the IP address of DNS Server for the selected CPE.
VLAN Tag Insertion	Type "enable" or "disable" to enable/disable such function.
Tag Value	Type the value as the VLAN ID number. The range is form 0 to 4095.
Priority	Type the packet priority number for such VLAN. The range is from 0 to 7.

Note: For detailed explanation for each parameter, refer to User's Guide of Vigor router if required.

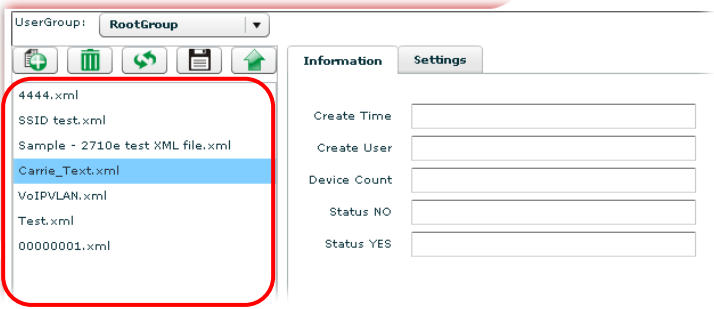
After finished the configuration, click **Save** to save the settings. Then, the parameter information for the selected router (CPE) that you modified in such page is changed.

10.5.2 SettingProfile

This page allows you to **create** provision profiles for CPEs. Important information (such as Create Time, Create User, Device Count, Status NO and Status YES) for the provision will be shown under **Information** tab. If you want to modify the settings (such as MAC/IP, Reboot, Name, Network, Status and etc.), simply click the **Settings** tab.

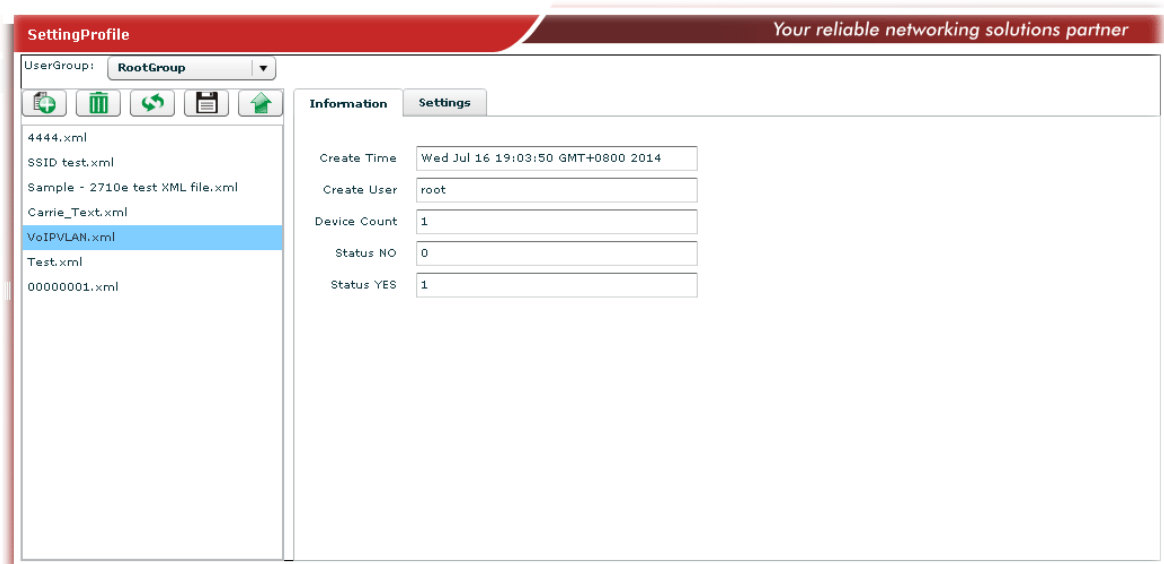
Available settings for such feature will be shown as follows:

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.
Add Profile	Click this button to add a new provision file. When the following dialog appears, simply type a name for the profile in the field of File Name and click Create. The new profile name will be shown on the field beneath

	the Add Profile button.  Next, you can configure the settings for the new created profile, e.g., adding new devices.
 Delete Profile	Click this button to delete the selected profile.
 Refresh	Click this button to refresh current page.
 Deploy Profile	Click this button to transfer the configuration to the VigorACS server. Usually, settings profiles are stored in the memory. When you press the Deploy Profile button, that profile will be applied to the CPEs.
 Upload file	Click this button to upload a user defined XML file to VigorACS SI server. Such file can be used for configuring the parameters for CPE.

Information Tab

It displays the basic information of the selected provision profile created including create time, create user, device count, status on/off and so on.



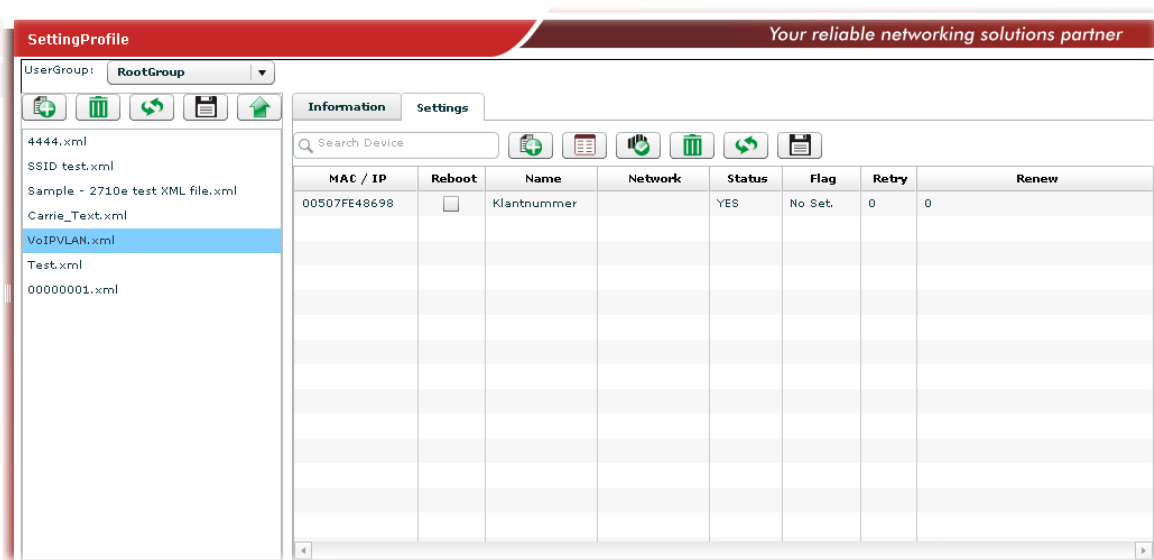
Available settings for such feature will be shown as follows:

Items	Description
Create Time	Display the creation time of the selected provision file.
Create User	Display the user group for the selected provision file.

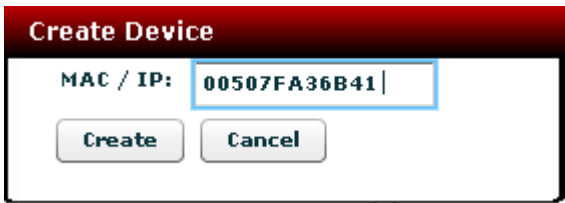
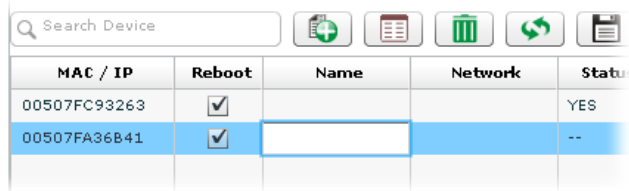
Device Count	Display the number of devices apply such provision file.
Status NO	Display the number of devices which are inactive now.
Status YES	Display the number of devices which are active.

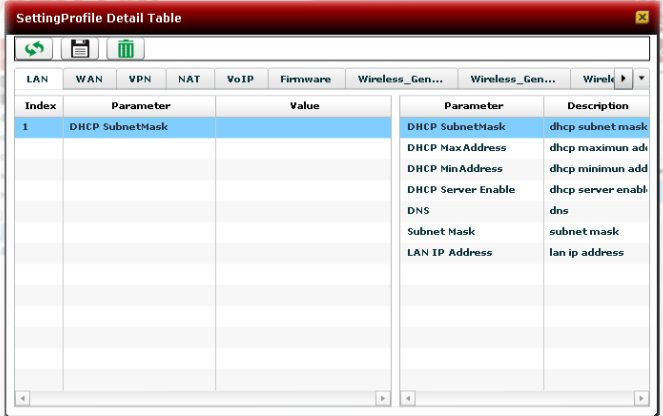
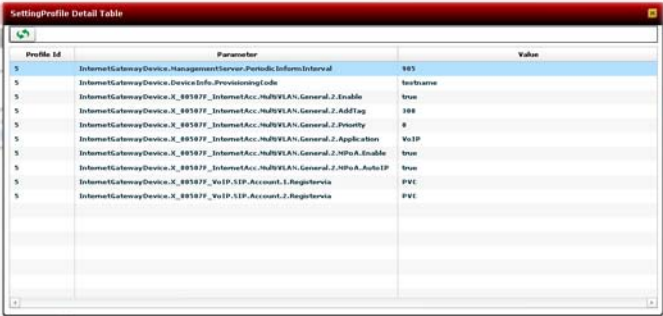
Settings Tab

To configure the settings for the selected provision profile, please click **Settings** tab. The following screen will appear.



Available settings for such feature will be shown as follows:

Items	Description
 Add Device	Click this button to add CPEs to current selected provision profile. When the following dialog appears, simply type MAC address of the device in the field of MAC/IP and click Create.  The new added device will be shown on the screen. Next, you can configure the settings for the new device, e.g., name of the device, specify the user group, and etc.  If you want to set more settings, click the Detail Setting icon.
 Detail Setting	Click this button to open Detail Setting window to add, modify and view the whole settings (e.g., WAN, LAN,

	NAT, VoIP, Firewall, Wireless...) for the selected provision profile.  Note: Each parameter configured in Detail Setting can be found in Complete Parameters window, too.
 Complete Parameters	The pop-up window displays parameters configured in Detail Setting. The difference is that full name of the configured parameter can be seen on the window. It is convenient for people who want to edit the parameters by modifying the parameter directly. 
 Delete Device	Click this button to delete the selected parameter.
 Refresh	Click this button to refresh current page.
 Save Profile	Click this button to save the configuration.
MAC / IP	Display the MAC address or IP Address of CPE.
Reboot	Check this box to reboot the CPE automatically after finishing the profile settings.
Name	Set the name of the CPE. The name of the CPE will be changed with the one set here when it connects to VigorACS for next time.
Network	Set the network of the CPE. The CPE will be moved and grouped under the network specified here when it connects to VigorACS for next time.
Status	YES- means such profile has been configured. NO- means such profile has not been configured.

Flag	Display the setting result of the profile.
Retry	If the provision profile is applied to CPE but failed, VigorACS will try to configure the settings again. The number of the retry time will be 3, at most.
Renew	Display the times that this profile has been modified.

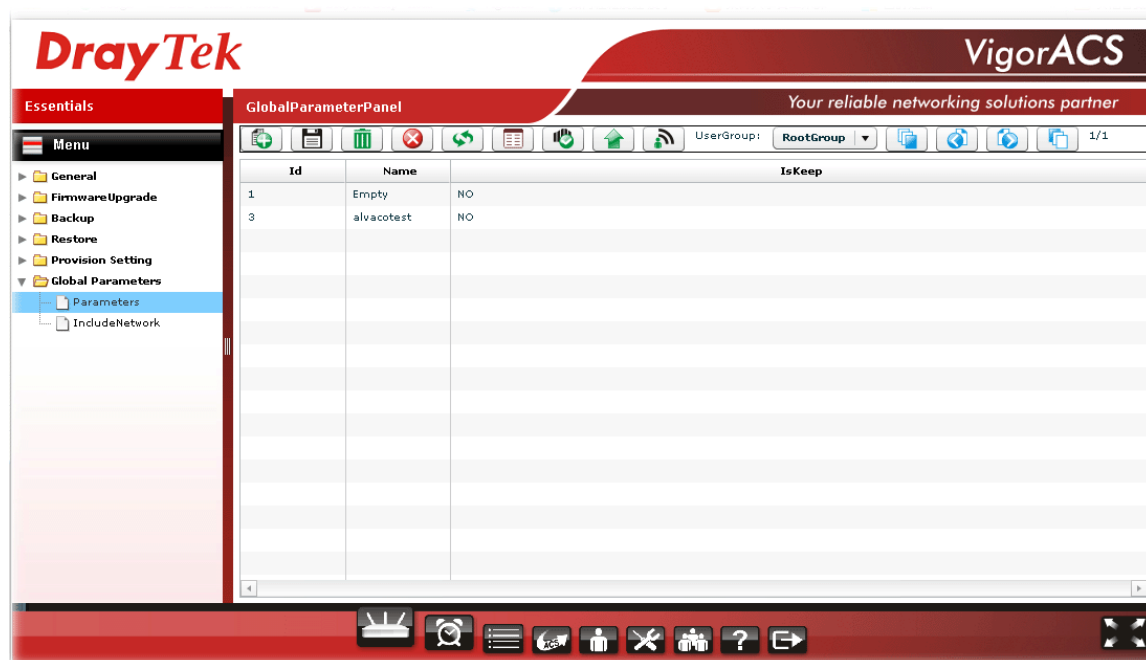
10.6 Global Parameters

Through **Global Parameters>>IncludeNetwork**, the 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.

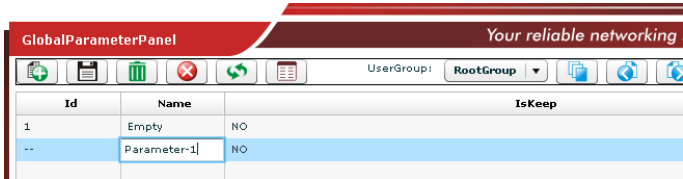
10.6.1 Parameters

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

Through Primary Setting, Advanced Setting and AP Wizards, general profiles with parameters can be configured for applying onto lots of selected CPE/AP devices at one time.



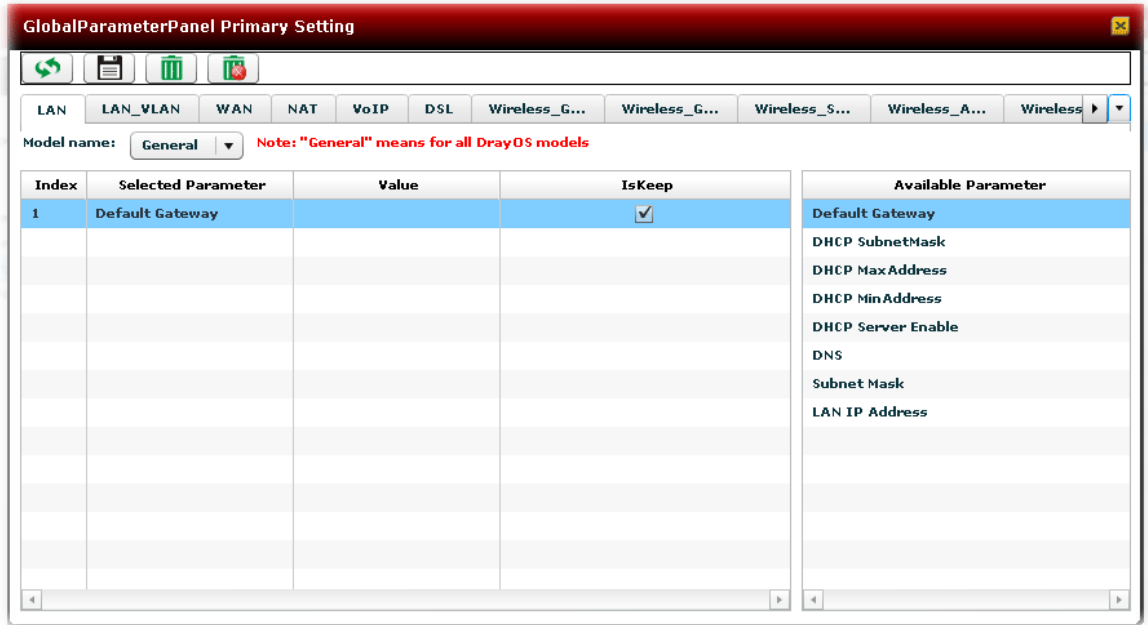
Available settings for such feature will be shown as follows:

Items	Description
 Add global parameter	Click this button to add a new global parameter profile name. Type a new name in the blank box. 
 Save global parameter setting	Click this button to save the restore profile.

Items	Description
 Delete global parameter	Click this button to delete the selected restore profile.
 Cancel	Click this button to cancel the operation.
 Refresh	Click this button to refresh current page.
 Primary Setting	Click this button to view and modify the whole settings (e.g., WAN, LAN, NAT, VoIP, Firewall, Wireless...) for the selected device manually.
 Complete Parameter	The pop-up window displays parameters configured in Primary Setting /APM Wizard. The difference is that full name of the configured parameter can be seen on this window. It is convenient for people who want to edit the parameters by modifying the parameter directly.
 Upload file	Click this button to upload a user defined XML file to VigorACS SI server. Such file can be used for configuring the parameters for CPE.
 APM Wizard	Click this button to configure wireless parameters for VigorAP devices.
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to view the files stored under the user group. Use the drop down list to specify the authority for the selected group.
 First	When there is more than one page for the global parameter files in this user group, click this button to display the first page.
 Previous	When there is more than one page for the global parameter files in this user group, click this button to display the previous page.
 Next	When there is more than one page for the global parameter files in this user group, click this button to display the previous page.
 Last	When there is more than one page for the global parameter files in this user group, click this button to display the last page.
Id	Display the number of the profile.
Name	Type the name for the global parameter profile, which will be applied in GlobalParameter_Includenetwork.
IsKeep	Choose YES to make such profile being kept.

Primary Setting

Choose one of the parameters profiles listed on the page and click  **Primary Setting** button to view and modify the whole settings. Use the arrow buttons () to scroll the menu bar and click the menu item you want. Then available parameters for that menu item will be displayed on the field of Available Parameters.



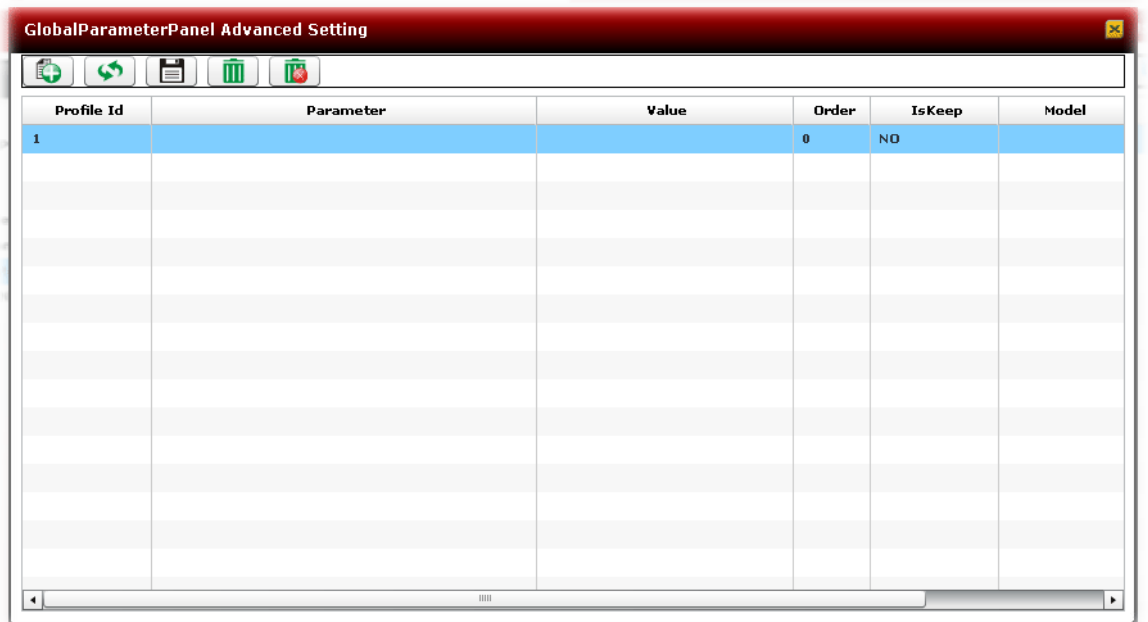
The screenshot shows the 'GlobalParameterPanel Primary Setting' window. It features a top menu bar with tabs: LAN, LAN_VLAN, WAN, NAT, VoIP, DSL, Wireless_G..., Wireless_G..., Wireless_S..., Wireless_A..., and Wireless. Below the menu bar, there is a 'Model name:' dropdown set to 'General' and a note: 'Note: "General" means for all DrayOS models'. The main area contains two tables. The left table has columns: Index, Selected Parameter, Value, and IsKeep. The right table has a column: Available Parameter.

Index	Selected Parameter	Value	IsKeep
1	Default Gateway		☒

Available Parameter
Default Gateway
DHCP SubnetMask
DHCP MaxAddress
DHCP MinAddress
DHCP Server Enable
DNS
Subnet Mask
LAN IP Address

Complete Parameter

Choose one of the parameters profiles listed on the page and click  **Complete Parameter** button. A pop-up window displays parameters configured in **Primary Setting** /APM Wizard. In addition, it allows you to view and add advanced parameters for CPEs/APs.

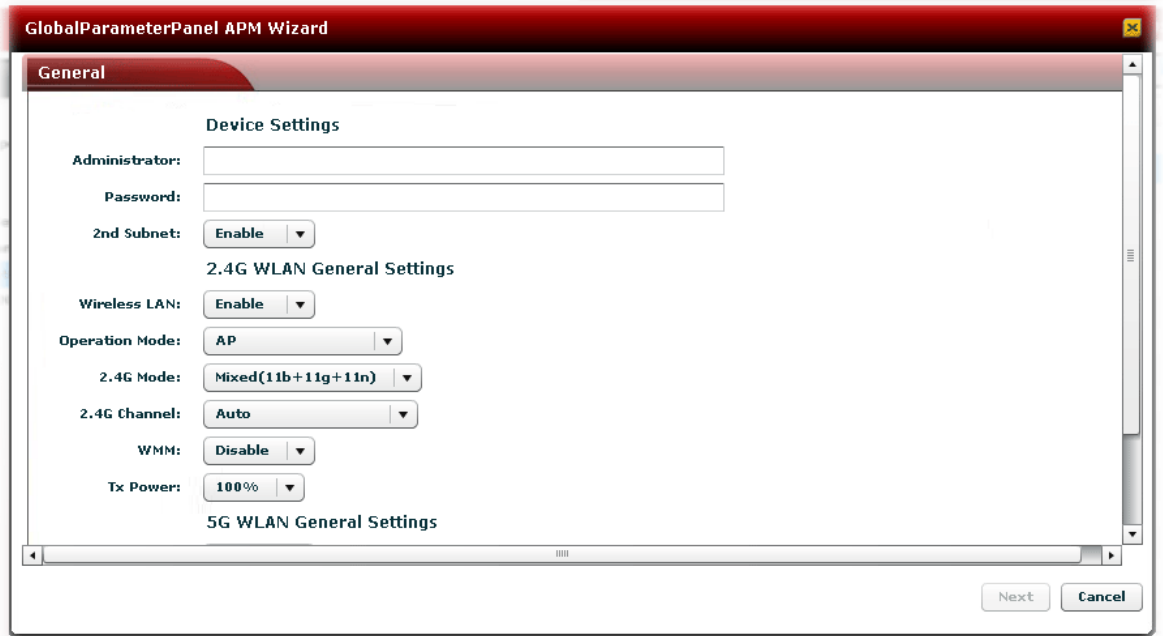


The screenshot shows the 'GlobalParameterPanel Advanced Setting' window. It features a top menu bar with tabs: LAN, LAN_VLAN, WAN, NAT, VoIP, DSL, Wireless_G..., Wireless_G..., Wireless_S..., Wireless_A..., and Wireless. Below the menu bar, there is a 'Model name:' dropdown set to 'General' and a note: 'Note: "General" means for all DrayOS models'. The main area contains a table with columns: Profile Id, Parameter, Value, Order, Is Keep, and Model.

Profile Id	Parameter	Value	Order	Is Keep	Model
1			0	NO	

APM Wizard

Choose one of the parameters profiles listed on the page and click  **APM Wizard** button. The following window will appear which allows you to create or view wireless network connection parameters for VigorAP devices.



GlobalParameterPanel APM Wizard

General

Device Settings

Administrator:

Password:

2nd Subnet: ▼

2.4G WLAN General Settings

Wireless LAN: ▼

Operation Mode: ▼

2.4G Mode: ▼

2.4G Channel: ▼

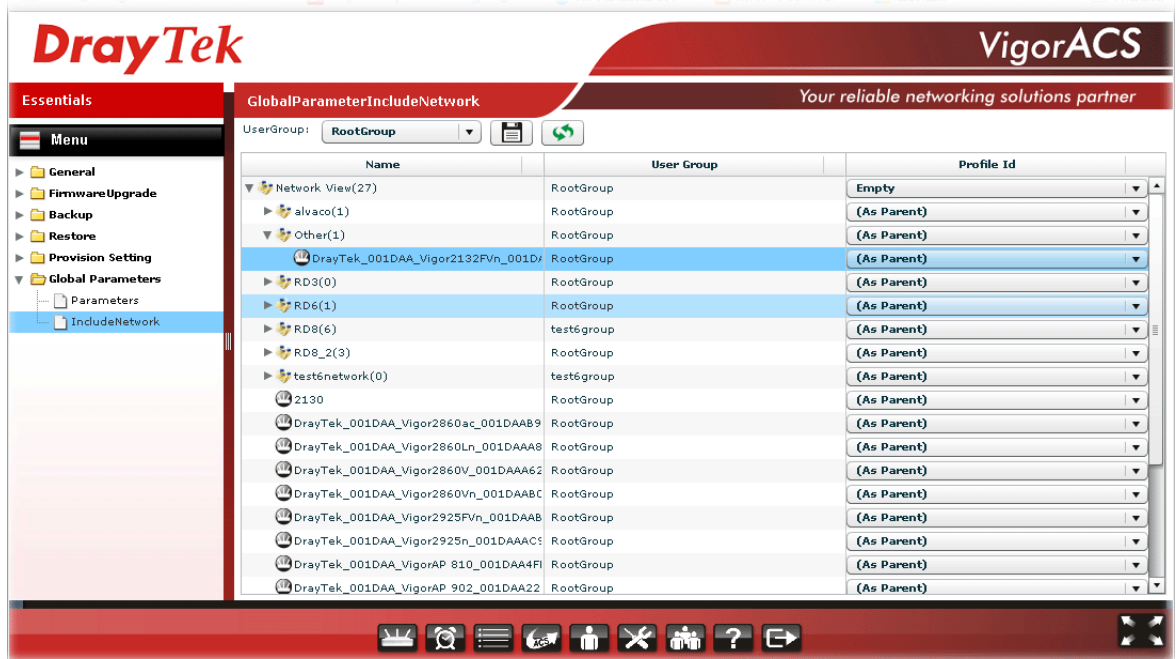
WMM: ▼

Tx Power: ▼

5G WLAN General Settings

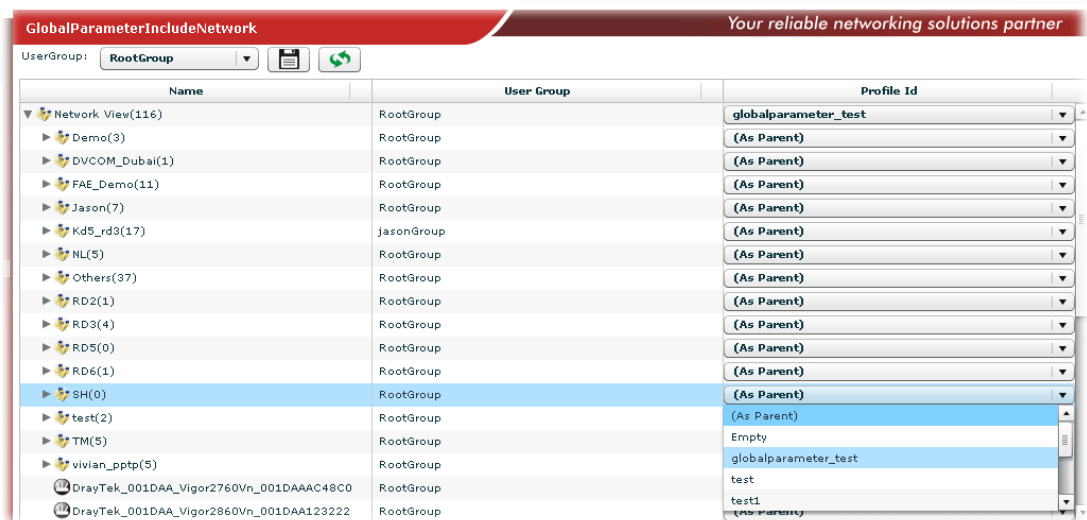
10.6.2 IncludeNetwork

If you have created several parameters profiles in **Global Parameters>>Parameters**, you can specify which CPE/AP device to be applied with the new created profile. If you do not specify any profile for the connected CPE/AP device, the default profile configuration is “Empty” (displayed in the field of Profile ID). No parameters will be applied to the connected CPE/AP device.



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 of Network View. Use the drop down list of **Profile Id** to specify the global parameter profile required for that CPE/AP.



Available settings for such feature will be shown as follows:

Items	Description
UserGroup	If there are many user groups with different authorities for the user account you use to access into VigorACS, you can use the drop down menu to choose one of the user groups to

Items	Description
	view the files stored under the user group. Use the drop down list to specify the authority for the selected group. 
 Save	Click this button to save the restore profile.
 Refresh	Click this button to refresh current page.
Name	Display the CPE/AP with the authority of the selected group.
User Group	Display the user group for the selected device.
Profile Id	Choose a profile (with global settings) defined in GlobalSetting (section 7.3.1) to be applied in such selected CPE/AP. (As Parent)- Choose the same setting as the previous layer.

Chapter 11 Help for License

Help page displays version information for VigorACS SI, as well as license key information and license agreements. Besides, it provides a channel to get new license from MyVigor website.

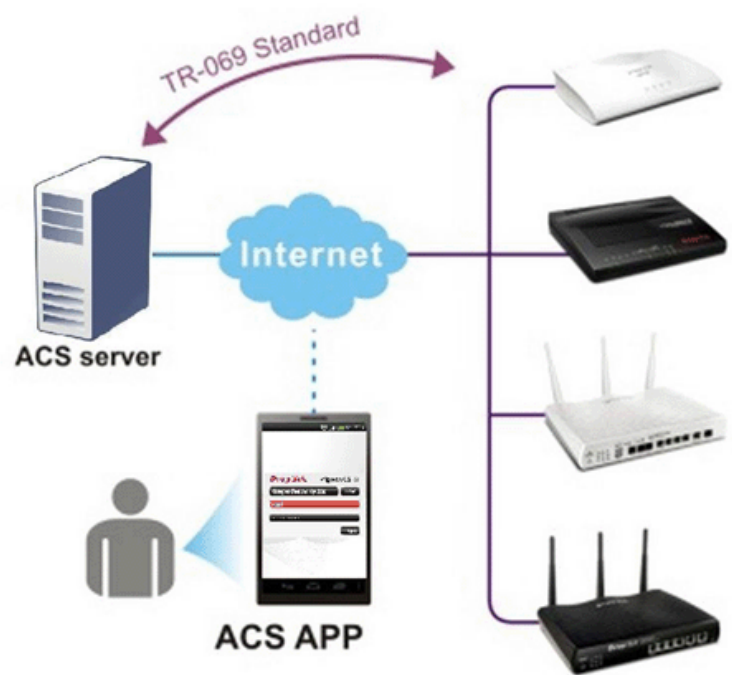


11.1 About VigorACS

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.



11.2 License Key Information

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

The screenshot shows the VigorACS SI web interface. The top header features the DrayTek logo on the left and the VigorACS logo on the right, with the tagline "Your reliable networking solutions partner". Below the header, a red navigation bar contains the "Essentials" menu and the "License Key Information" tab. The left sidebar shows a "Menu" with options: "> About VigorACS", "> License Key Information", and "> License Agreements". The main content area displays the "License Key Information" page, which includes a refresh button and a key-value list:

License Id:	00001ef
Start Date:	2012-02-23
Expire Date:	2012-12-31
Max Node:	1000
Trial license:	Yes

At the bottom of the interface is a red bar with various system icons and a maximize button.

11.3 License Agreements

This page displays relational license information required by VigorACS SI.

The screenshot shows the VigorACS SI web interface with the "License Agreements" tab selected. The left sidebar is identical to the previous screenshot. The main content area displays the "License Agreements" page, which includes the text "ACS use following library and license agreement." and "LGPL V3". Below this, there are three tables listing libraries and their license pages:

Name	Author	License Page
Blazeds		opensource.adobe.com/wiki/display/blazeds/License
JasperReports		www.gnu.org/copyleft/lesser.html
JDIC		www.gnu.org/copyleft/lesser.html

Below the first table, there is a section for "LGPL V2.1" with another table:

Name	Author	License Page
JRobin API		oldwww.jrobin.org/license.html
JBoss-4.0.4.GA		docs.jboss.org/jbossas/admindevel326/html/apa.html
Hibernate		www.hibernate.org/356.html
SendTrap		sendtrap.sourceforge.net/license.txt

Below the second table, there is a section for "Apache License, Version 2.0" with a third table:

Name	Author	License Page

The interface also includes a red bar at the bottom with system icons and a maximize button.

This page is left blank.

Part III Application

This page is left blank.

Chapter 12 Tutorials

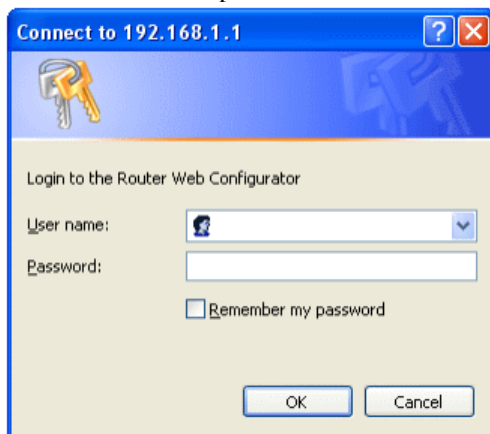
This chapter offers several examples for using VigorACS.

12.1 How to Manage CPE through VigorACS

12.1.1 Set ACS URL on CPE

To manage CPEs through VigorACS, you have to set ACS URL on CPE first and set username and password for VigorACS.

1. Connect one CPE (e.g., Vigor2910 series).
2. Open a web browser (for example, **IE**, **Mozilla Firefox** or **Netscape**) on your computer and type **http://192.168.1.1**.
3. Please type username and password on the window. If you don't know the correct username and password, please consult your dealer to get them. In this section, we take the figures displayed on Windows as examples.



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

System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server	
URL	http://172.17.3.185:80/ACSServer/services/ACSServlet
Username	acs
Password	*****
CPE Client	
☒ Enable ☐ Disable	
URL	http://172.16.3.229:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	*****

Periodic Inform Settings

☐ Disable ☒ Enable	
Interval Time	900 second(s)

OK

- If the connected CPE needs to be authenticated, please set URL as the following and type username and password for ACS server:

http://{IP address of VigorACS}:80/ACSServer/services/ACSServlet

- If the connected CPE does not need to be authenticated please set URL as the following:
http://{ IP address of VigorACS}:80/ACSServer/services/UnAuthACSServlet
 - If the connected CPE needs to be authenticated and the data transmission between CPE and VigorACS needs to be encrypted (SSL), please set URL as the following:
https://{IP address of VigorACS}:443/ACSServer/services/ACSServlet
 - If the connected CPE needs not to be authenticated but the data transmission between CPE and VigorACS needs to be encrypted (SSL), please set URL as the following:
https://{IP address of VigorACS}:443/ACSServer/services/UnAuthACSServlet
5. Fill Username and Password for VigorACS Server for authentication. Please type as the following:
Username: *acs*
Password: *password*
 6. For the username and password of CPE client, it is not necessary for you to type them. Refer to section 3.2 for detailed information.

12.1.2 Invoke Remote Management for CPE

You have to make sure that the CPE device you want to connect supports VigorACS features. Please consult your dealer if you have no idea in it.

1. Suppose WAN IP of CPE device has been setup successfully. And you can access into Internet without difficulty.
2. Login the device by web.
3. Go to **System Maintenance>>Management Setup**.

Check **Enable remote firmware upgrade (FTP)** and **Allow management from the Internet** to set management access control.

System Maintenance >> Management

Management Setup

Management Access Control

☒ Allow management from the Internet

☐ FTP Server

☒ HTTP Server

☒ HTTPS Server

☒ Telnet Server

☐ SSH Server

☒ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1		
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)

SSH Port (Default: 22)

SNMP Setup

☐ Enable SNMP Agent

Get Community

Set Community

Manager Host IP

Trap Community

Notification Host IP

Trap Timeout seconds

OK

12.1.3 Enable WAN Connection on CPE

You have to make sure the CPE device you want to connect has configured properly, and are able to access Internet.

1. Login the device by web.
2. Go to **Internet Access>>MPoA**.
3. Click **Enable** for MPoA.
4. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.

WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client)
☒ Enable ☐ Disable

ISDN Dial Backup Setup
Dial Backup Mode: None

Keep WAN Connection
☐ Enable PING to keep alive
PING to the IP:
PING Interval: 0 minute(s)

WAN Connection Detection
Mode: ARP Detect
Ping IP:
TTL:

MTU: 1442 (Max:1500)

RIP Protocol
☐ Enable RIP

WAN IP Network Settings WAN IP Alias
☐ Obtain an IP address automatically
☒ **Specify an IP address**
IP Address: 172.16.3.229
Subnet Mask: 255.255.0.0
Gateway IP Address: 172.16.3.4

DNS Server IP Address
Primary IP Address:
Secondary IP Address:

☒ Default MAC Address
☐ Specify a MAC Address
MAC Address: 00 . 50 . 7F . DD . 15 . 19

OK Cancel

Note: Reboot the CPE device and re-log into VigorACS SI. CPE which has registered to VigorACS will be captured and displayed on the home page of VigorACS SI.

12.1.4 Connect to ACS Server through PVC Channel

1. Login the device by web.
2. Go to **Internet Access>>MPoA**.
3. Click **Enable** for MPoA.
4. Choose 1483 Bride IP LLC as encapsulation. And set VPI and VCI with 8 and 35.
5. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.

Internet Access >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Mode
☒ Enable ☐ Disable

DSL Modem Settings
 Multi-PVC channel:
 Encapsulation:
 VPI:
 VCI:
 Modulation:

RIP Protocol
☐ Enable RIP

Bridge Mode
☐ Enable Bridge Mode

WAN IP Network Settings
☐ Obtain an IP address automatically
 Router Name:
 Domain Name:
 *: Required for some ISPs
☒ Specify an IP address
 IP Address:
 Subnet Mask:
 Gateway IP Address:
☒ Default MAC Address
☐ Specify a MAC Address
 MAC Address:

- Go to **Internet Access>>Multi-PVCs**. Enable Channel 3 WAN check box and set VPI and VCI as 9 & 36.

Multi-PVCs

Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.	☒	8	35	UBR	MPoA	1483 Bridged IP LLC
2.	☒	8	38	UBR	MPoA	1483 Bridged IP LLC
3.	☒ WAN	9	36	UBR	PPPoA	VC MUX
4.	☐ WAN	1	44	UBR	PPPoA	VC MUX
5.	☐ WAN	1	45	UBR	PPPoA	VC MUX
6.	☐	1	46	UBR	PPPoA	VC MUX
7.	☐	1	47	UBR	PPPoA	VC MUX
8.	☐	1	48	UBR	PPPoA	VC MUX

Note: VPI/VCI must be unique for each channel!

OK Clear Cancel

- Click **WAN** link to open the following page for configuring in details.

WAN for Router-borne Application:

☒ Enable ☐ Disable

DSL Modem Settings
 VPI:
 VCI:
 QoS Type:
 Protocol:
 Encapsulation:

PPPoE/PPPoA Client
ISP Access Setup
 ISP Name:
 Username:
 Password:
 PPP Authentication:
☒ Always On
 Idle Timeout: second(s)

IP Address From ISP
 Fixed IP: ☒ Yes ☐ No (Dynamic IP)

MPoA (RFC1483/2684)
☐ Obtain an IP address automatically
 Router Name:
 Domain Name:
 *: Required for some ISPs
☒ Specify an IP address
 IP Address:
 Subnet Mask:
 Gateway IP Address:
 DNS Server IP Address:

8. Set **WAN for Router-borne Application** as **Management**. And set VPI and VCI with 9 & 36. Choose **MPoA** as the protocol and choose **1483 Bridge IP LLC** as Encapsulation. Finally set a static IP address. Click **Ok**.
9. Open **System Maintenance >>TR-069**. Choose **PVC** for ACS Server On. Type correct URL for the ACS server. Type username and password for ACS Server.

ACS and CPE Settings

ACS Server On PVC

ACS Server

URL http://172.17.3.165:8080/ACSServer/services/ACSServlet

Username acs

Password *****

CPE Client

URL http://172.17.3.162/cwm/CRN.html

Port 80

Username vigor

Password *****

10. Click **OK** to save the settings. Now, reboot the CPE device and re-log into VigorACS SI. CPE which has registered to VigorACS will be captured and displayed on the home page of VigorACS SI.

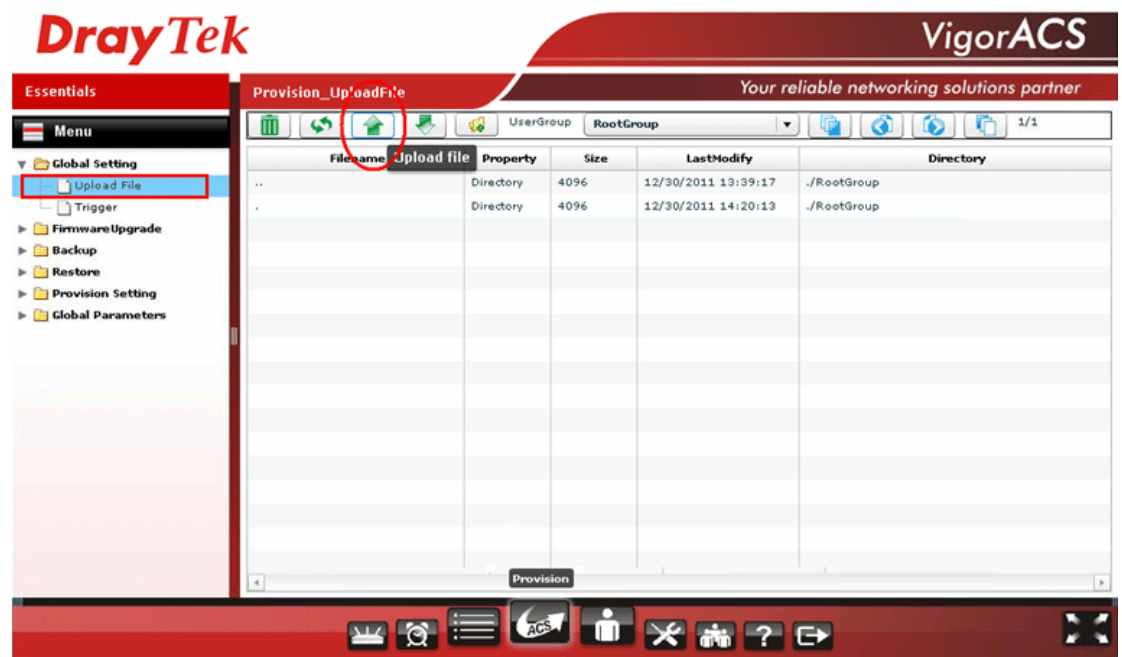
12.2 How to upgrade CPE firmware by using VigorACS SI Provision

I. Import firmware file to VigorACS SI server

There are two ways to import firmware file to VigorACS server:

Upload to VigorACS server from your PC

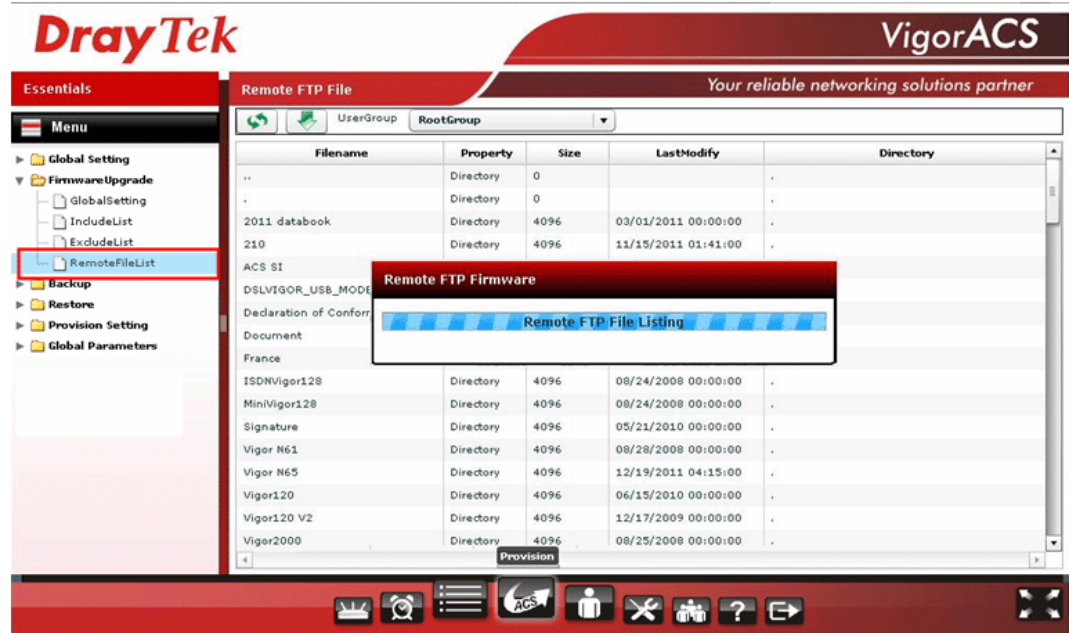
1. The newest firmware file (e.g., V3.3.7 in this case) is located on your PC. You can upload it from your PC to VigorACS SI. Just click the **Provision** tab. From the menu tree view on the right side, click the grey triangle near to **Global Setting** to unfold it.



2. Then click **Upload File** to choose the file to be uploaded to VigorACS SI server.

Download from our FTP site

1. The newest firmware file (e.g., V3.3.7 in this case) is located on FTP site. You can download it from the FTP to VigorACS SI. Just click the **Provision** tab. From the menu tree view on the right side, click the grey triangle near to **FirmwareUpgrade** to unfold it.

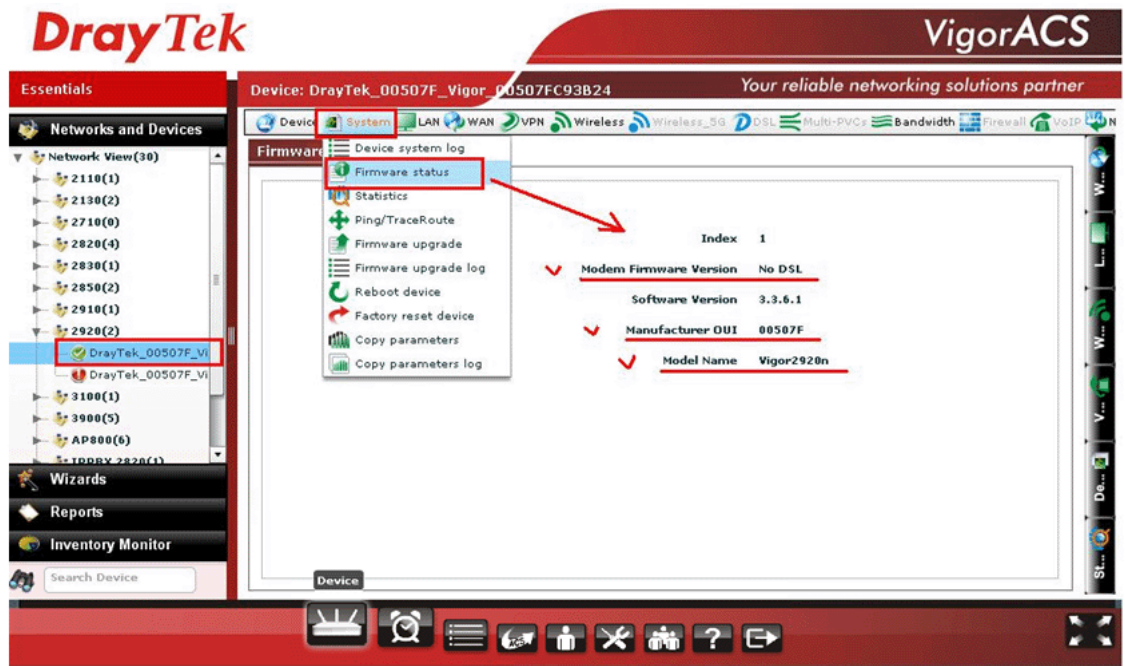


2. Then click **FirmwareUpgrade** to choose the file to be downloaded and uploaded to VigorACS SI server.

II. Check the firmware status of the CPE you want to upgrade

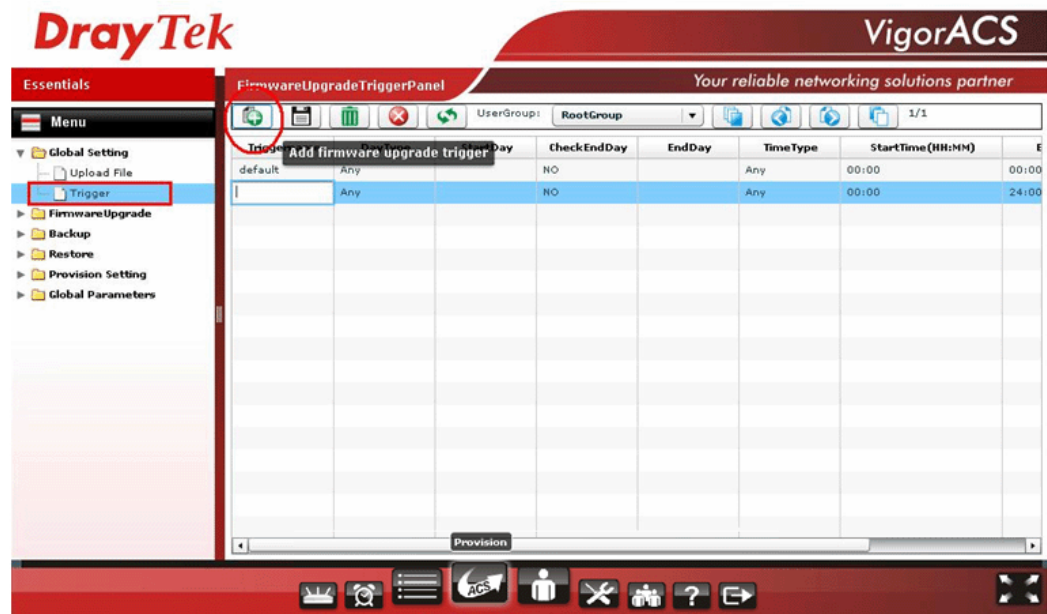
Now you can check the firmware information of the CPE that you want to upgrade. Click the **Device** tab. Open **System >> Firmware status**. Write down the following items:

- Modem Firmware Version
- Manufacturer OUI
- Model Name



III. Set a new trigger profile

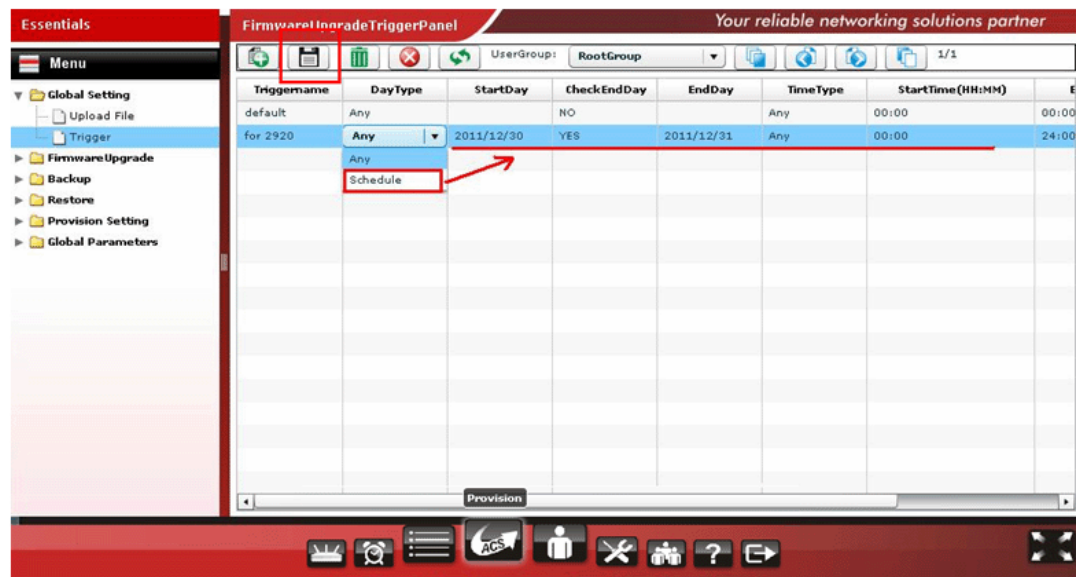
1. Click the **Provision** tab. Open **Global Setting >> Trigger** to add a new trigger profile.



2. Click the Add firmware upgrade trigger button.
3. For the **DayType**, you can choose **Any** or **Schedule** for your necessity. Then, click **Save** to save the settings.

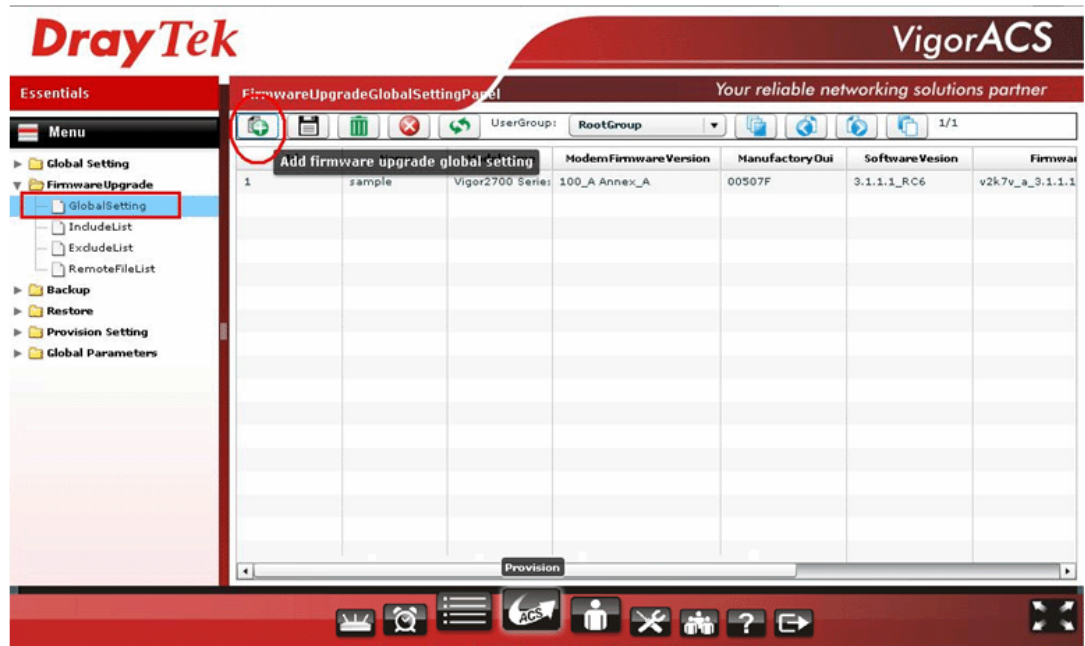
Any – firmware upgrade will be done whenever VigorACS SI server gets the inform packet from the CPE.

Schedule -VigorACS SI server gets the inform packet from CPE based on the time settings.

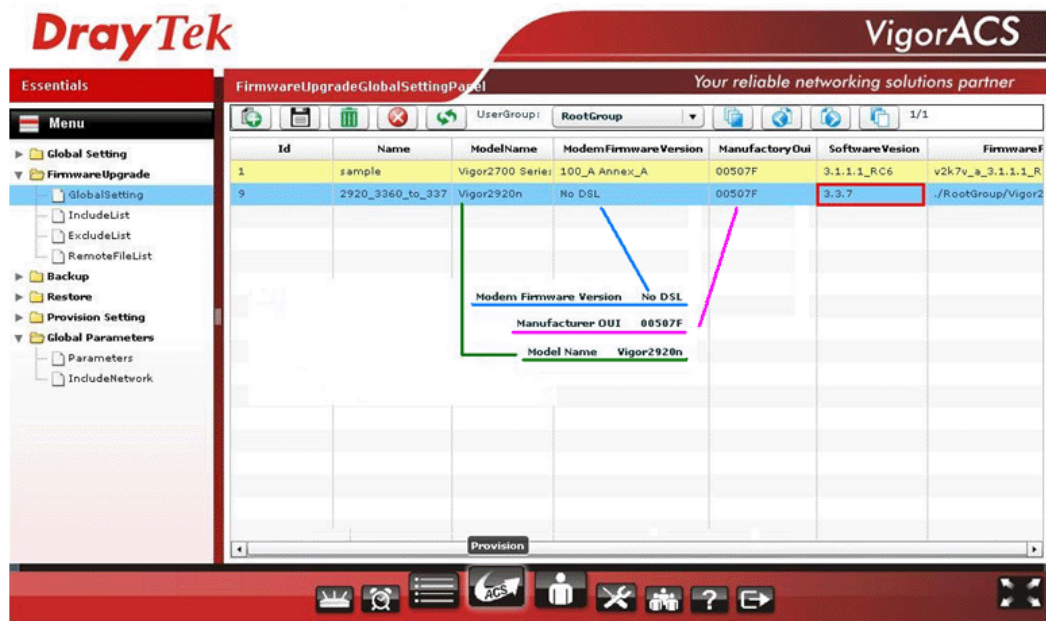


IV. Set a new firmware upgrade profile

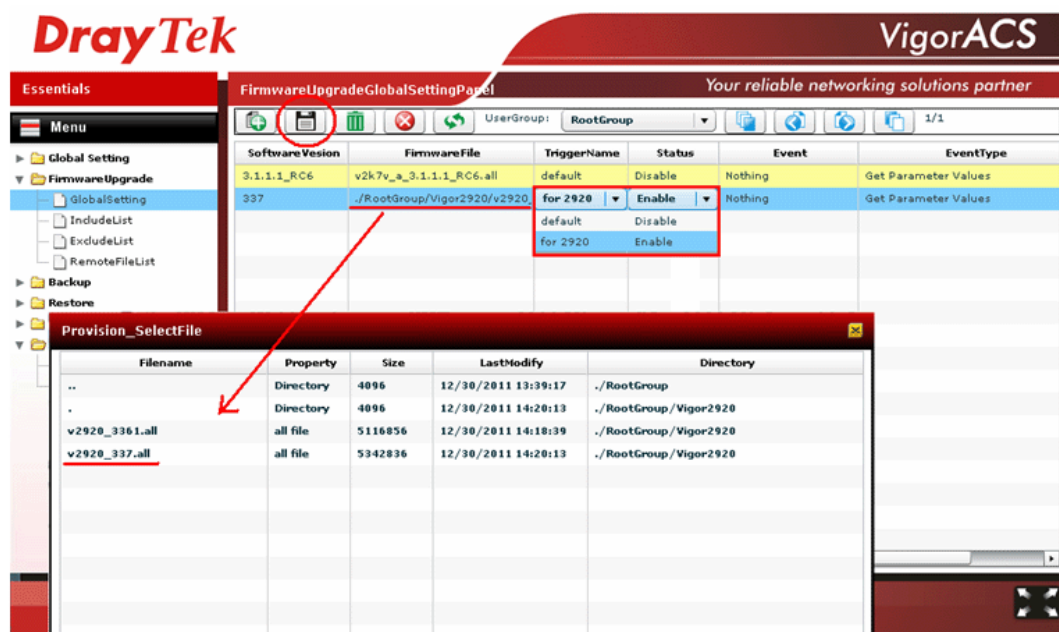
1. Click the **Provision** tab. Open **FirmwareUpgrade** >> **GlobalSetting** to add a new upgrade profile.



2. Click the **Add firmware upgrade global setting** button.
3. Type a name for such profile (e.g., 2920_336_to337) and configure the Model Name, Modem Firmware Version and Manufacturer OUI obtained from **System** >> **Firmware status** in the step above.

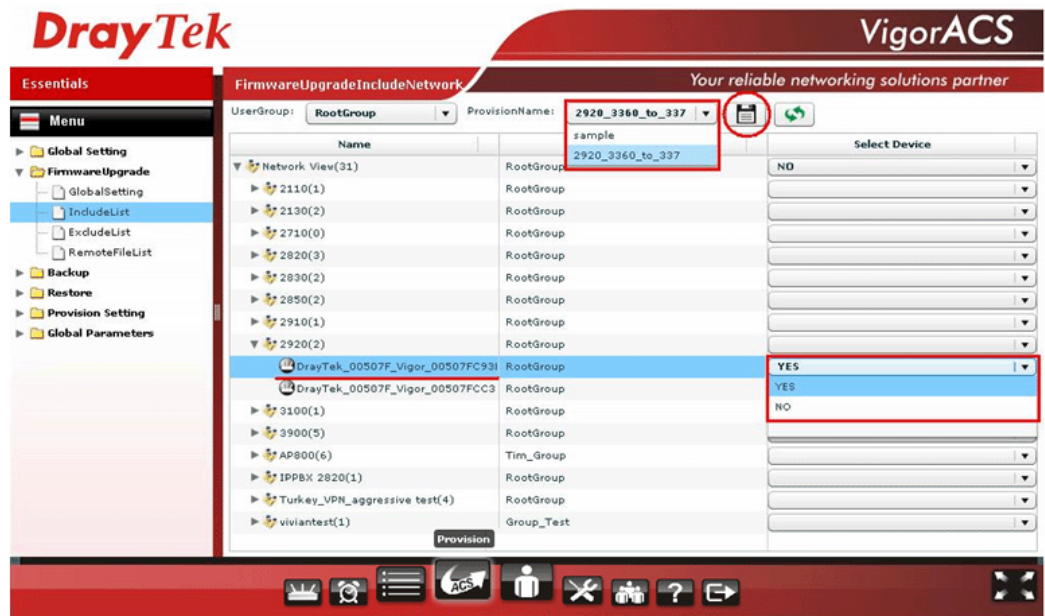


4. Type the version number (e.g., 3.3.7 in this case) for **SoftwareVersion** the same as the firmware version (e.g., V3.3.7 mentioned above in this case) that you want to upgrade to. Otherwise VigorACS SI server will keep trying to upgrade the CPE's firmware to this version.
5. Select the firmware file and the trigger profile. Remember to enable them. Then, click **Save** to save the settings.



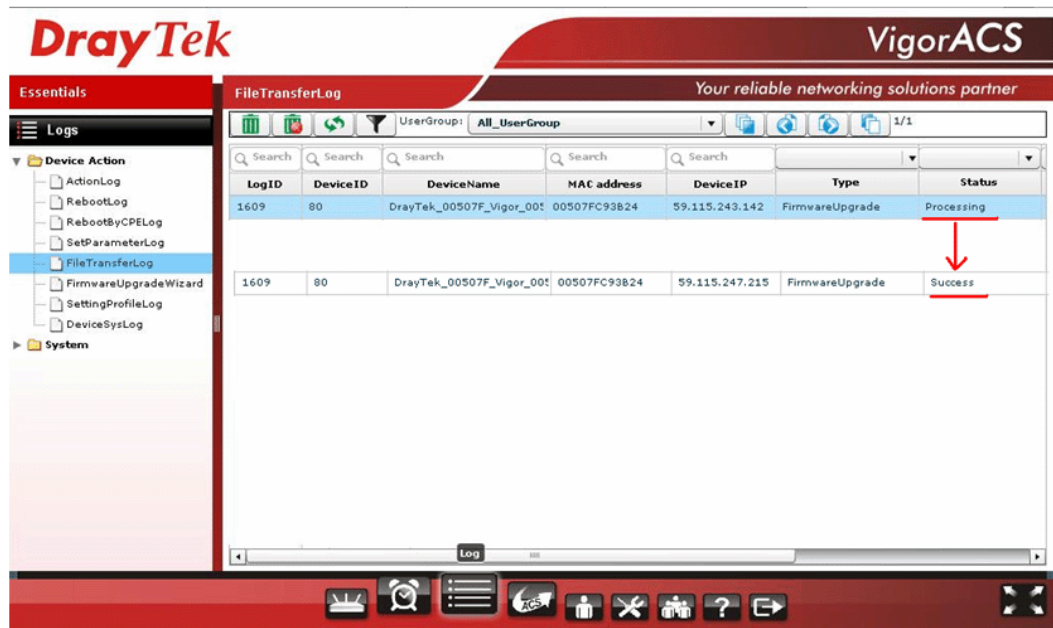
V. Choose the CPE for implementing the firmware upgrade

1. Click the **Provision** tab. Open **FirmwareUpgrade** >> **IncludeList**.
2. In the field of **ProvisionName**, choose the profile (e.g., 2920_336_to337) created in **Firmware Upgrade Global Setting** profile.
3. Choose **YES** in the field of **Select Device** for the selected CPE and click the **Save** button.



VI. Log of the File Transfer

To check if the firmware upgrade is successful or not, just click the **Log** tab. Open **Device Action** >> **FileTransferLog**. A log list will be displayed with the firmware upgrade status.



12.3 How to upgrade CPE firmware by using VigorACS SI Firmware Upgrade Wizard

I. Import firmware file to VigorACS SI server

There are two ways to import firmware file to VigorACS server:

Upload to VigorACS server from your PC

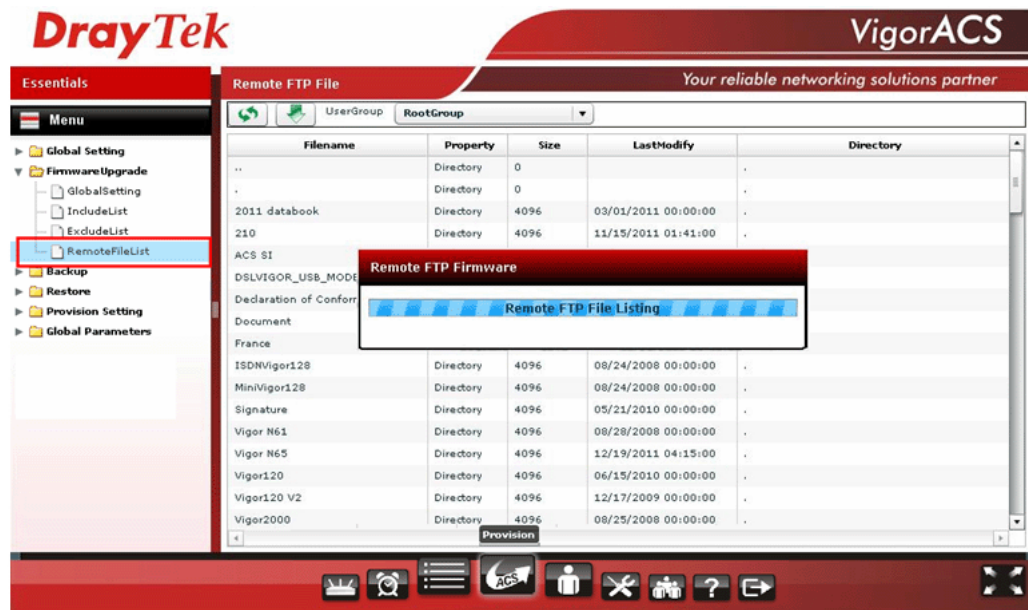
1. The newest firmware file (e.g., V3.3.7 in this case) is located on your PC. You can upload it from your PC to VigorACS SI. Just click the **Provision** tab. From the menu tree view on the right side, click the grey triangle near to **Global Setting** to unfold it.



2. Then click **Upload File** to choose the file to be uploaded to VigorACS SI server.

Download from our FTP site

1. The newest firmware file (e.g., V3.3.7 in this case) is located on FTP site. You can download it from the FTP to VigorACS SI. Just click the **Provision** tab. From the menu tree view on the right side, click the grey triangle near to **FirmwareUpgrade** to unfold it.



2. Then click **FirmwareUpgrade** to choose the file to be downloaded and uploaded to VigorACS SI server.

12.4 How to use Copy Parameter

VigorACS SI 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.

For example, there are three Vigor2920 devices (named 2920_A, 2920_B and 2920_C) under the network view, and we want to copy the **port redirection setting** from 2920_A to 2920_B and 2920_C.



Take a look at the port redirection setting of 2920_A.

NAT >> Port Redirection

Port Redirection					Set to Factory Default
Index	Service Name	Public Port	Private IP	Status	
1.	http server	80	192.168.1.100	v	

Index No. 1

☒ Enable	
Mode	Single
Service Name	http server
Protocol	TCP
WAN IP	2.WAN1 IP Alias[1]114.44.50.213
Public Port	80
Private IP	192.168.1.100
Private Port	8080

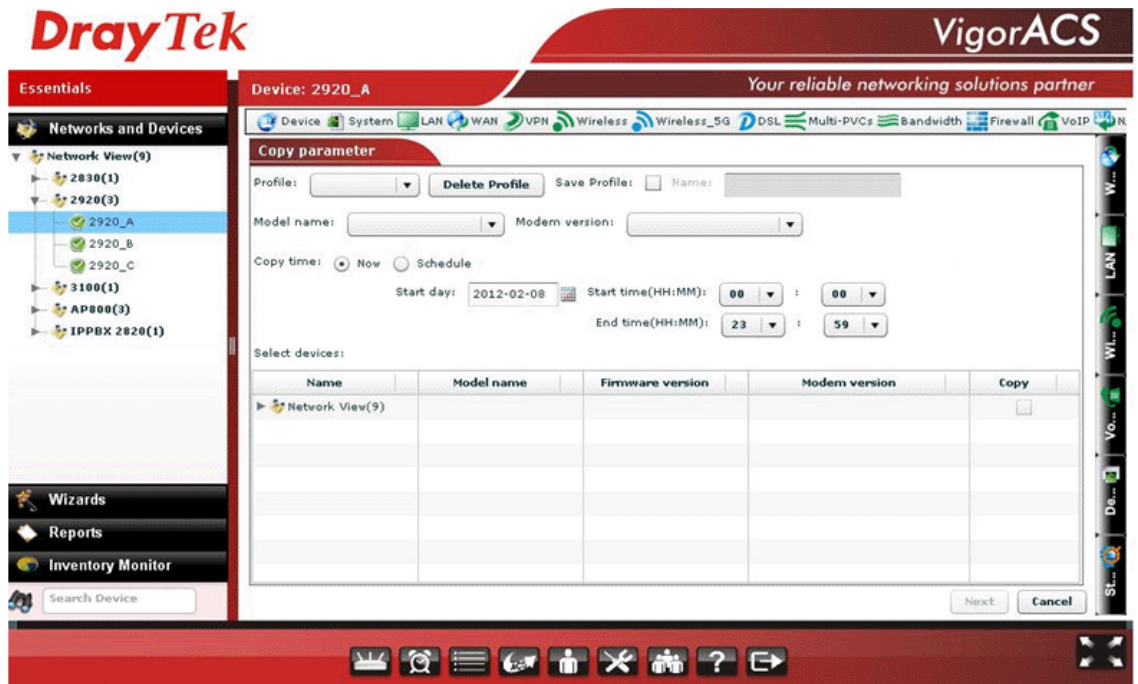
Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

Follow the steps listed below:

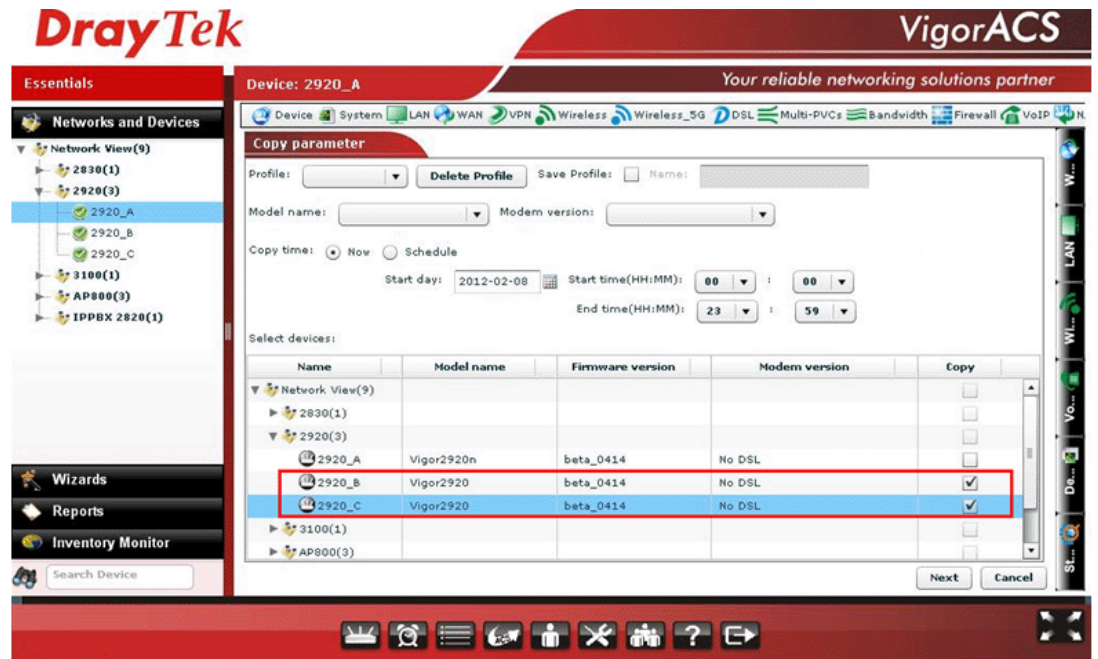
1. Access into the VigorACS SI web user interface. From the network view area located on the left side of VigorACS SI, choose and click the device (e.g., 2920_A) to select it.



2. From the top menu bar, choose the **System >> Copy Parameters** item to open the following page.



- On the **Select devices** list, select devices (e.g., 2920_B and 2920_C) that you want to copy the parameters settings from other device. Check the box of **Copy**.



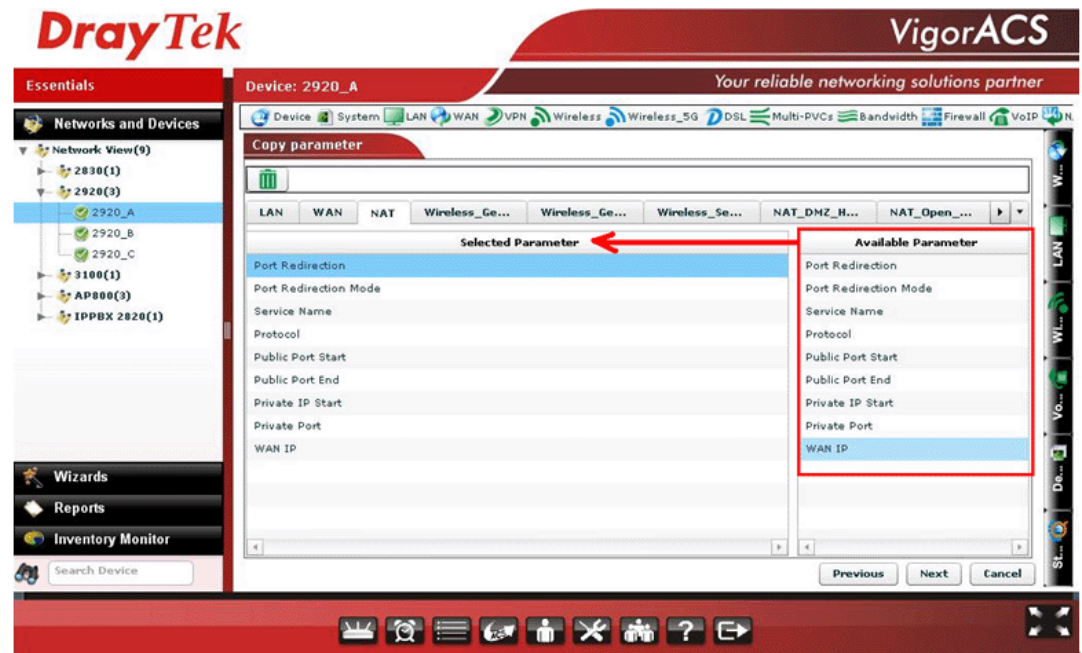
- Click the **Next** button to open the following page.



- From the drop down list, find the NAT menu to locate port redirection parameter (from 2920_A) that you want to copy from.



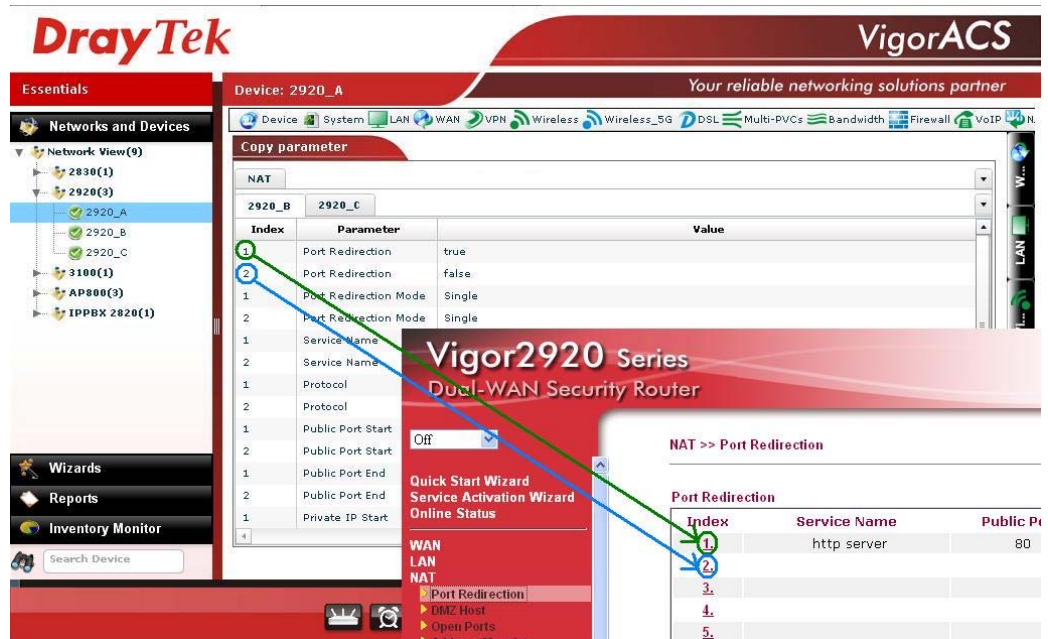
- Double click the parameters which you want to copy from 2920_A at **Available Parameter** list, then the chosen parameter will be shown under **Selected Parameter**. Press the **Next** button:



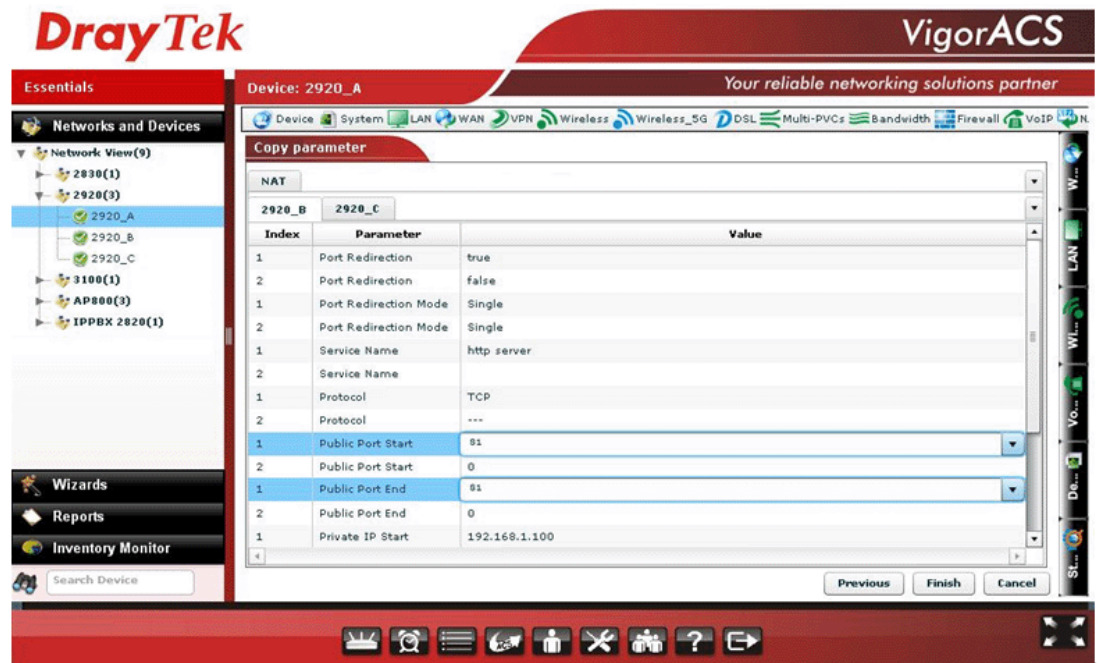
7. In the following page, all of the selected parameters with values will be shown as follows for devices respectively.



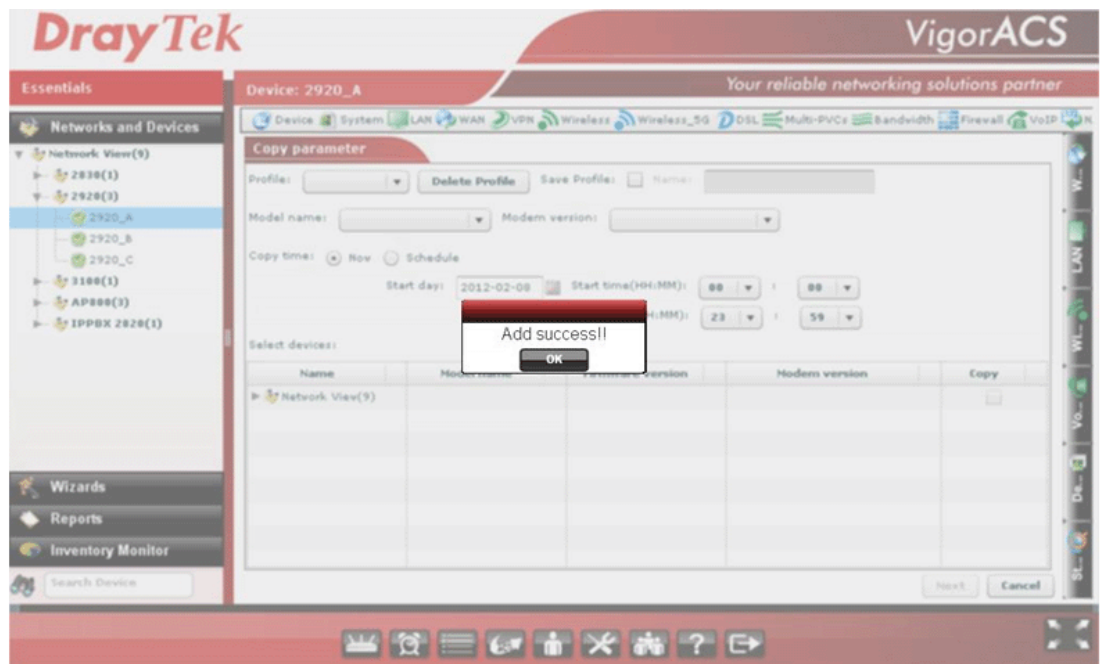
8. Parameter of index 1 is the one we want to copy to 2920_B and 2920_C. Choose index 1.



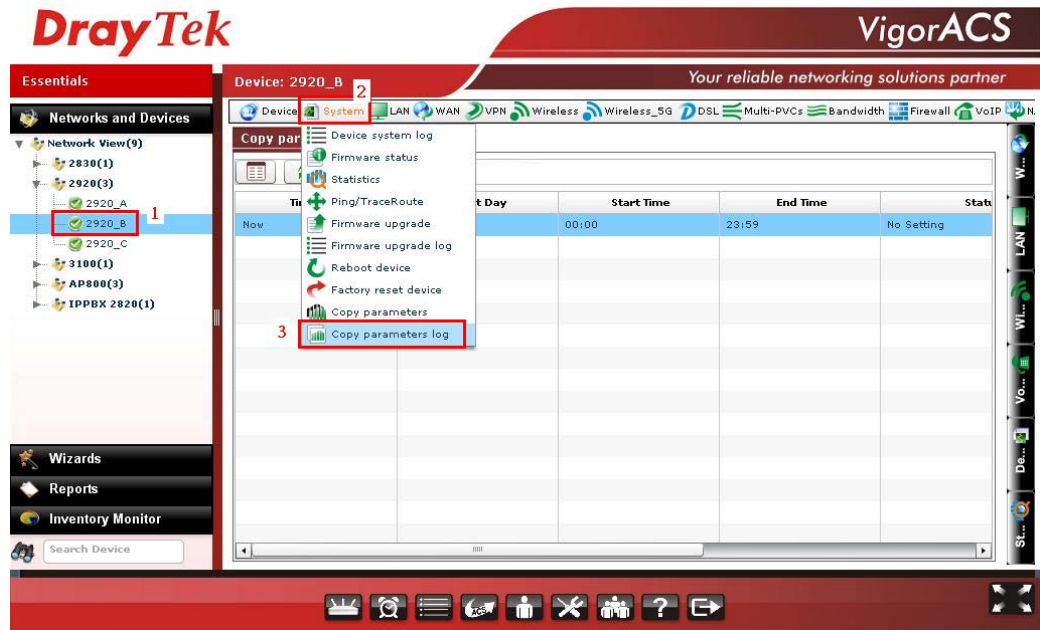
9. If you want to change the value of parameter, you should redefine it now. If not, simply click **Finish**.



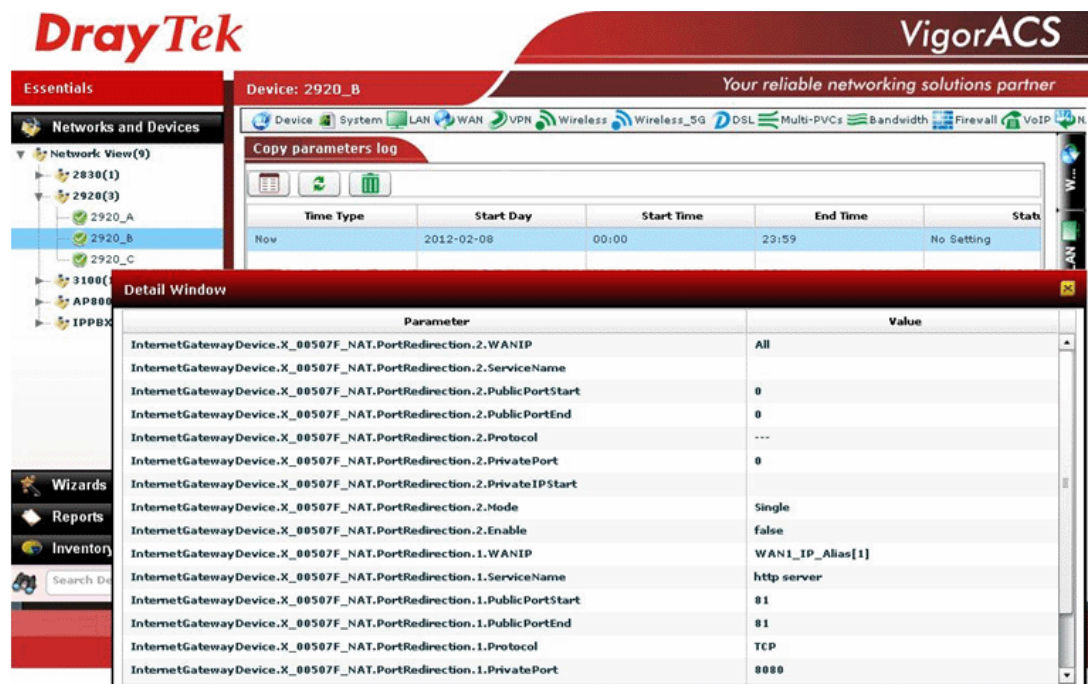
10. A window will be popped up to tell you the process of copy parameter is successful.



11. Next, check the status for the routers. Click the 2920_B or 2920_C on the network view area then open **System >> Copy parameter log** item. You will see there is a log in the list and waiting to be implemented when VigorACS SI server gets the inform packets from the CPE.



12. Double click the log to open the Detail Window for checking the details about the parameters. The log will disappear after it has been done. Therefore, if you want to cancel the copy parameter action, simply delete the log from the log list (clicking the **Delete** button on the top).



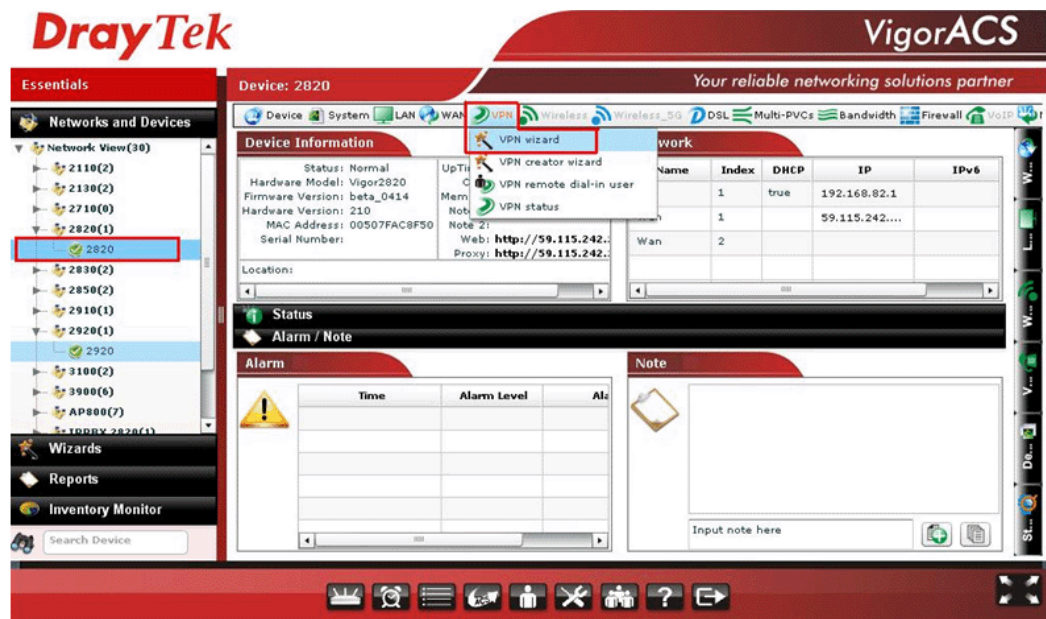
12.5 How to create a VPN by using VPN Wizard

Vigor ACS SI 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 Vigor2820 and Vigor2920.

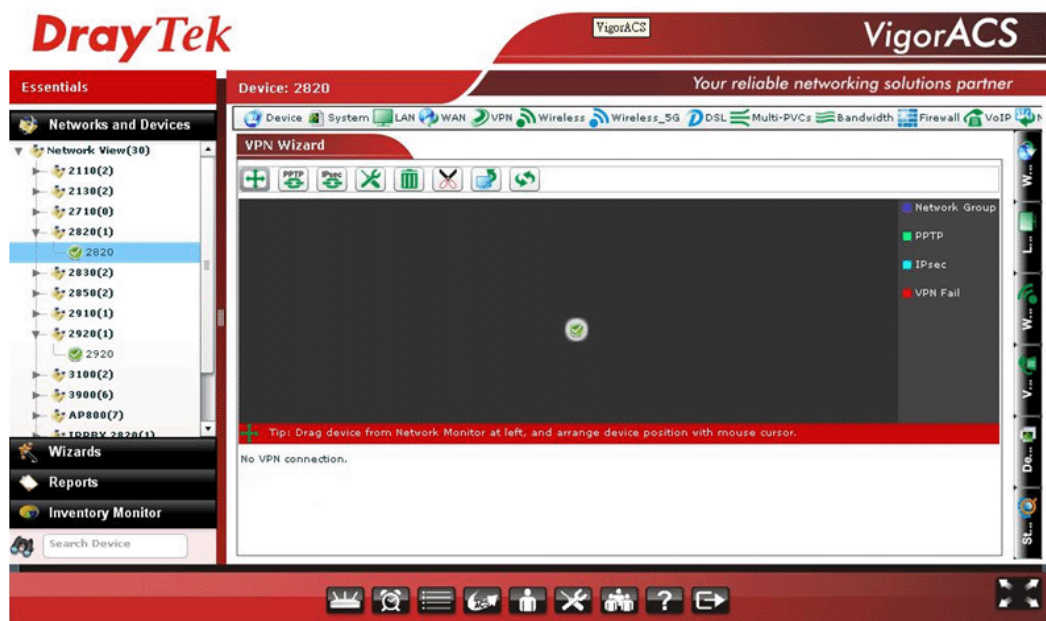
VPN server => Vigor2820, LAN network: 192.168.82.0/24

VPN client => Vigor2920, LAN network: 192.168.92.0/24

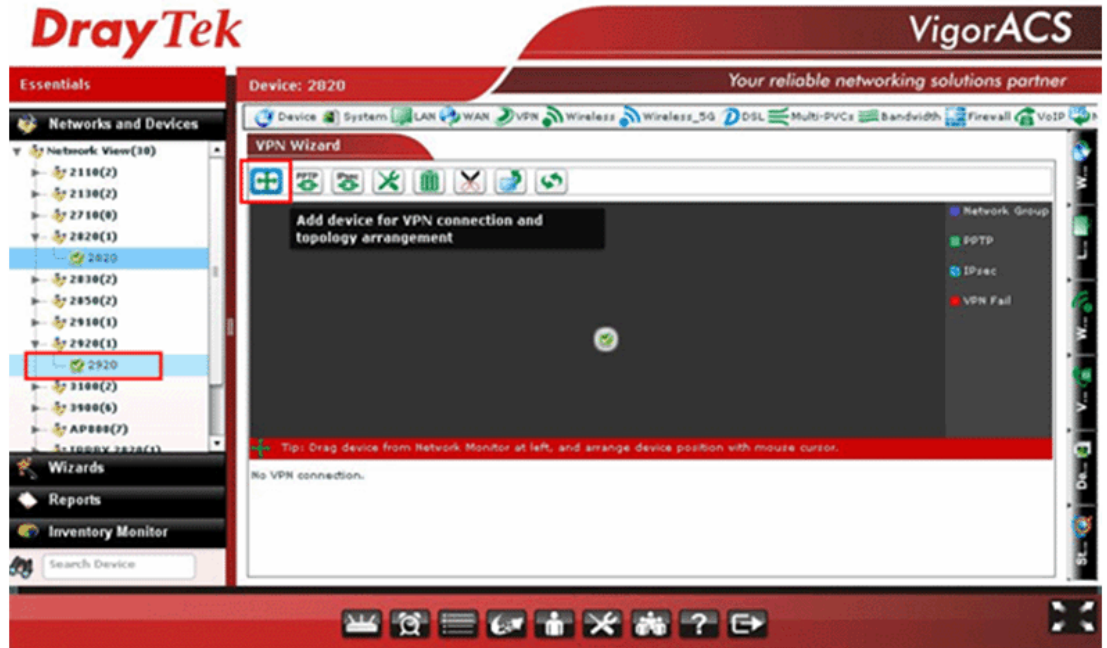
1. Click the **Device** tab and choose Vigor2820 as the VPN server from the Network View on the left side of ACS SI web.
2. Open **VPN>> VPN wizard** function on the top menu of VigorACS SI.



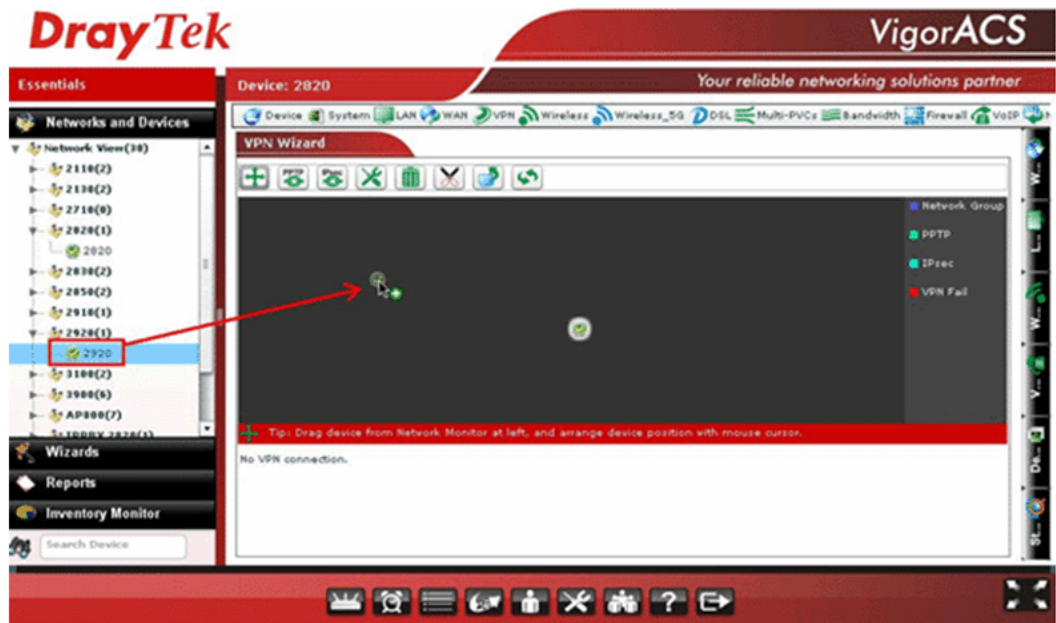
3. Then the VPN wizard web page will appear as the follows:



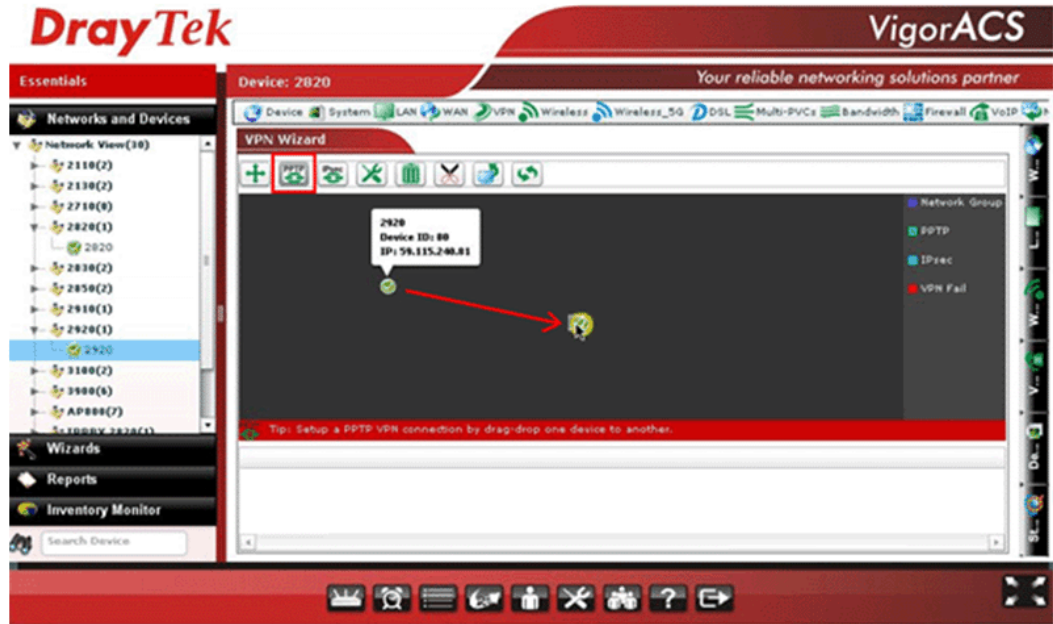
4. Press the **Add device** button, then choose the VPN client (Vigor2920) at the Network View on the left side of the ACS SI web.



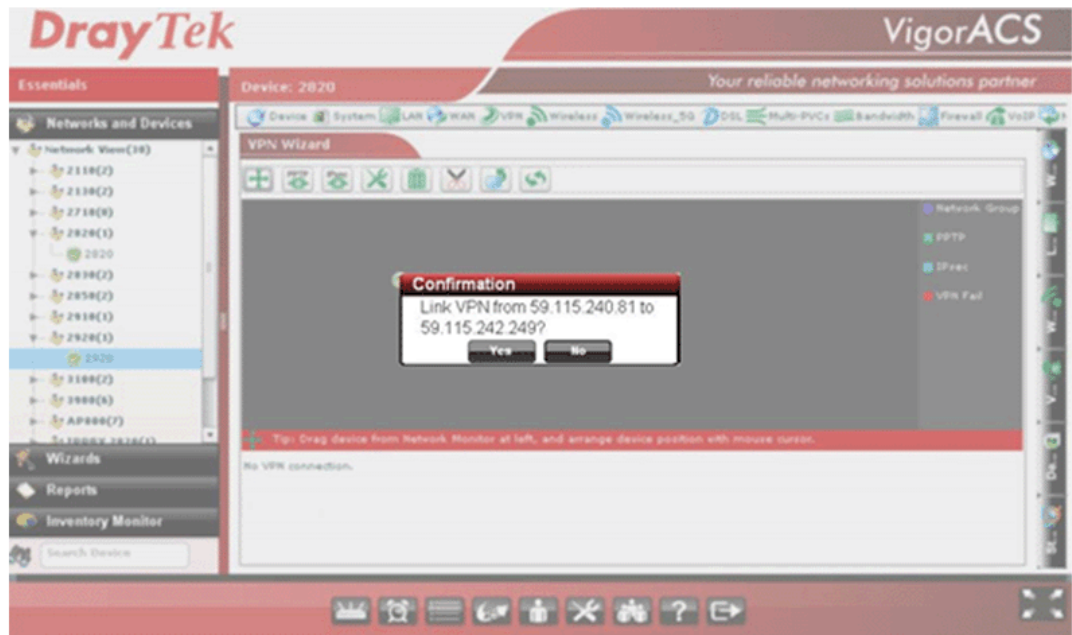
5. Click the VPN client (Vigor2920) and drag it to the black area on the right side. Then release it.



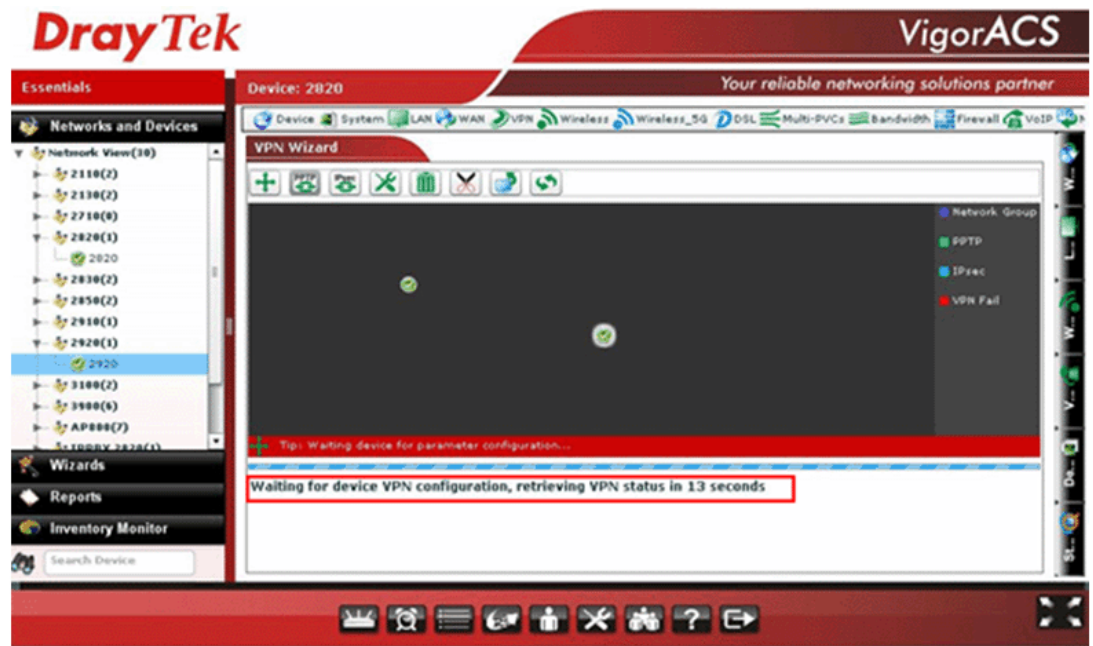
6. Press PPTP button, then Press the VPN client icon (Vigor2920) and drag it to the VPN server icon (Vigor2820), release it when you see a yellow ring surrounding the VPN server icon.



7. VigorACS SI will pop-up a confirmation window, please click the **Yes** button.



8. Wait for device VPN configuration.



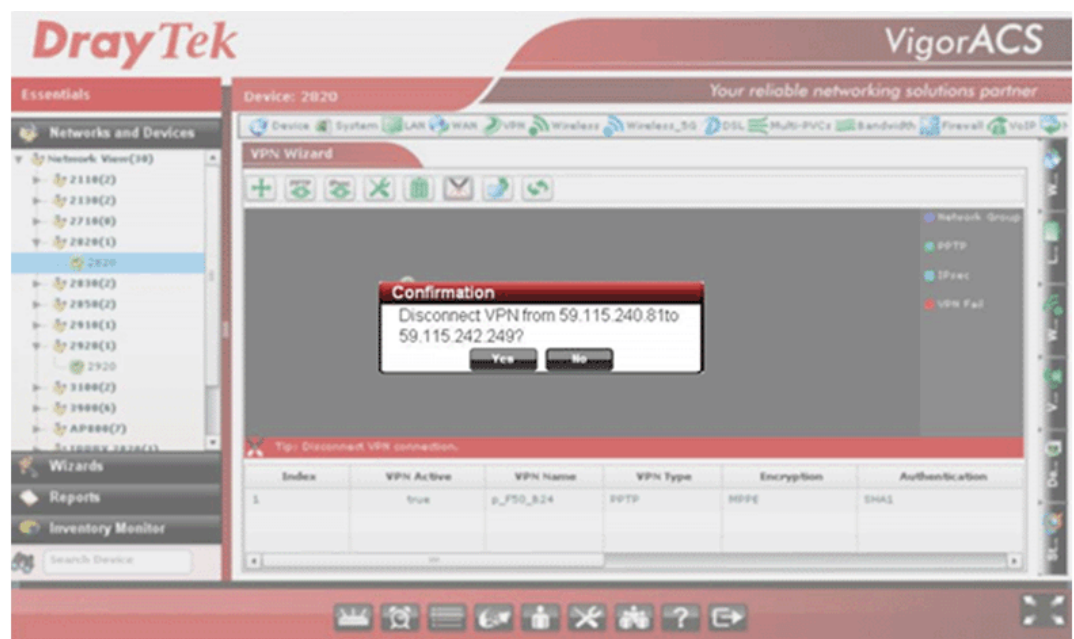
9. After PPTP connection working, there will be a green arrow from VPN client to VPN server, you could check the VPN tunnel status on the bottom of the VigorACS SI web as well.



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.



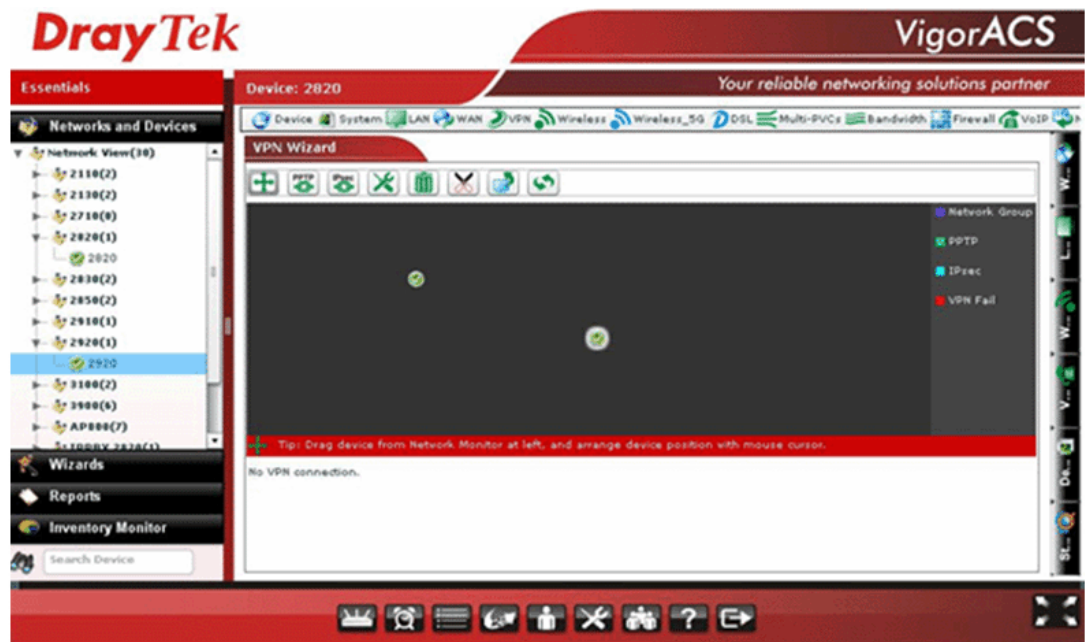
11. VigorACS SI will pop-up a confirmation window, please click the **Yes** button.



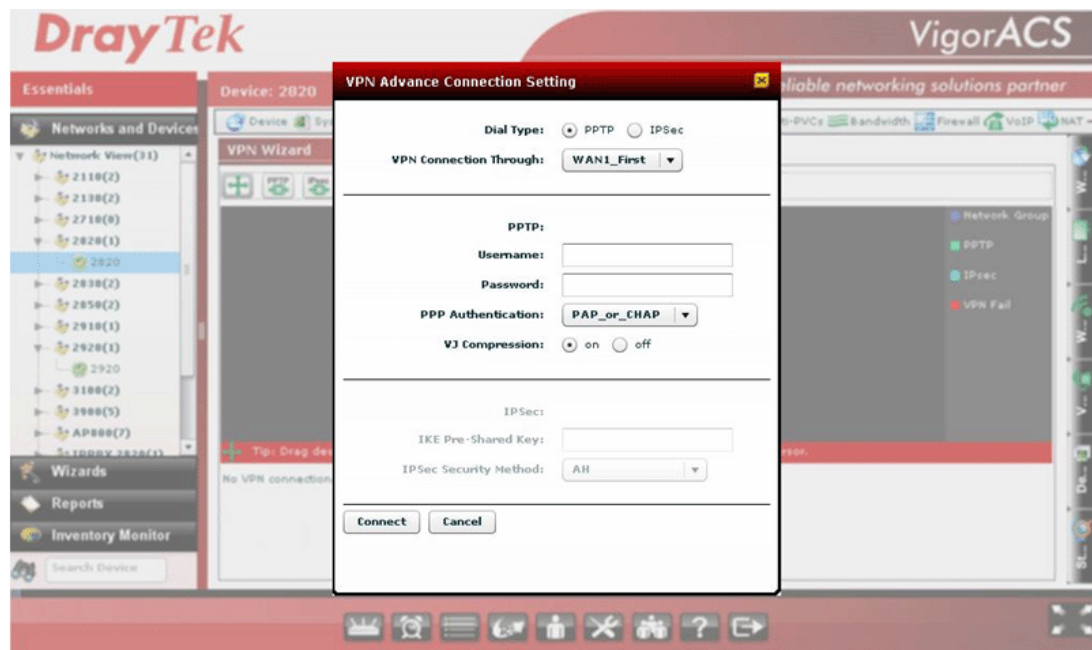
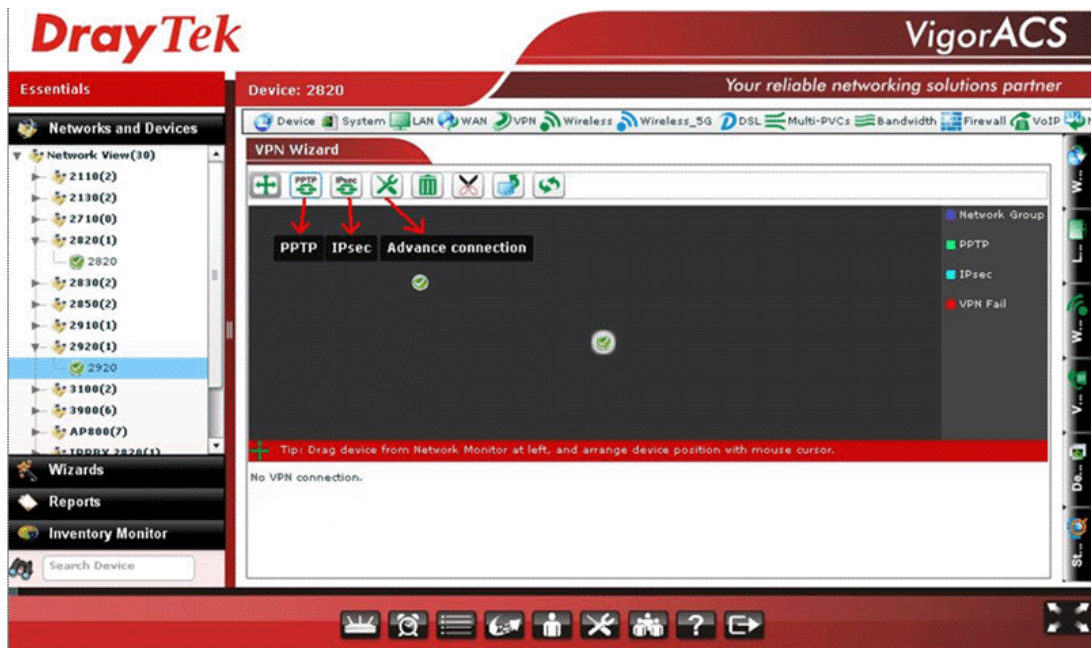
12. Wait for device VPN configuration.



13. After VPN tunnel disconnection, the message will show “No VPN connection”.



Note: VigorACS SI 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 instead at step 5.



12.6 Creating an Account for MyVigor

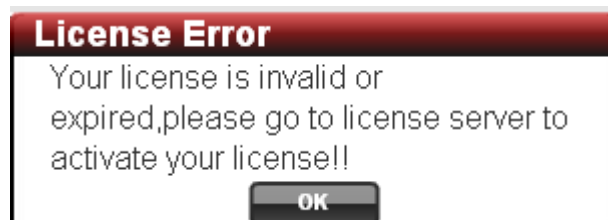
12.6.1 Creating an Account via VigorACS SI

1. Click **Programs> VigorACS SI> VigorACS Web Page** to access into VigorACS. The login page of VigorACS will be shown as the following:



The image shows the VigorACS login interface. At the top, there is a red header with the "DrayTek" logo on the left and "VigorACS" on the right. Below the header is a white login box with a black "Login" tab on the left. Inside the box, there are three input fields: "User Name" with the text "root", "Password" with masked characters "*****", and "Validated Code" with the text "7xxS". To the right of the "Validated Code" field is a small red box containing the text "7 x x S". Below the input fields are two buttons: "EN" with a dropdown arrow and a "Login" button.

2. Please type **“root”** as user name and **“admin123”** as password. Then click **Login**. A License Error dialog appears as follows:



3. Click **OK**. A login page for MyVigor web site will pop up automatically.

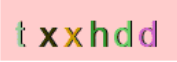


Please take a moment to register.
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

LOGIN

UserName :

Password :

Auth Code : 

If you cannot read the word, [click here](#)

[Forgotten password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or

4. Click the link of **Create an account now**.
5. Check to confirm that you accept the Agreement and click **Accept**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

===== MyVigor Agreement =====

1. Agreement
Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the modifications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration
To use this service, you have to agree the following conditions:
(a) Provide your complete and correct information according to the registration steps of this service.
(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate

☒ I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

6. Type your personal information in this page and then click **Continue**.

Register
Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement
2 Personal Information
3 Preferences
4 Completion

Account Information
UserName: *
(3 ~ 20 characters)
Password: *
(4 ~ 20 characters : Do not set the same as the username.)
Confirm Password: *

Personal Information
First Name: *
Last Name: *
Company Name:
Email Address: *
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
Tel: -
Country: *
Career: *

7. Choose proper selection for your computer and click **Continue**.

Register
Create an account - Please enter personal profile.

1 Agreement
2 Personal Information
3 Preferences
4 Completion

How did you find out about this website?
What kind of anti-virus do you use?
I would like to subscribe to the MyVigor e-letter. ☒
I would like to receive DrayTek product news. ☒
Please select the mail server for receiving the verification mail.

8. Now you have created an account successfully. Click **START**.

Register
Create an account - Please enter personal profile.

1 Agreement
2 Personal Information
3 Preferences
4 Completion

Completion
A confirmation email has been sent to **mary_ted@tech.com**
Please click on the activation link in the email to activate your account

START

9. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com portal.**

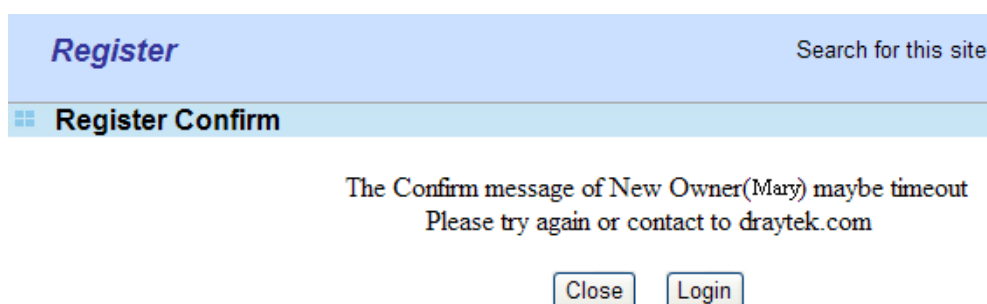
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

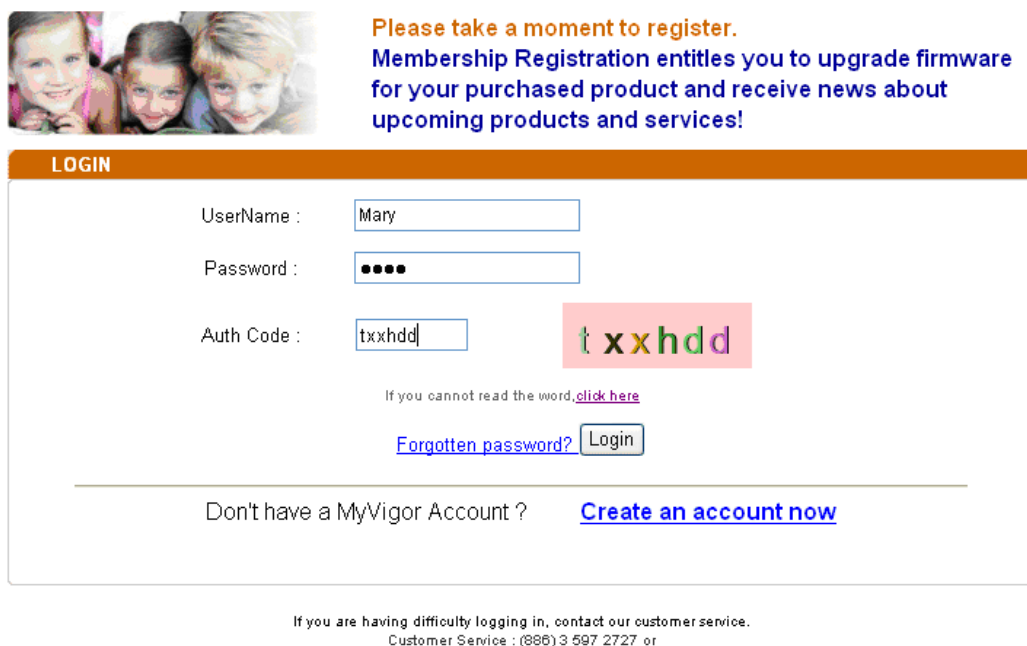


Register Search for this site

Register Confirm

The Confirm message of New Owner(Mary) maybe timeout
Please try again or contact to draytek.com

11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type th

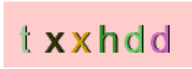


Please take a moment to register.
Membership Registration entitles you to upgrade firmware
for your purchased product and receive news about
upcoming products and services!

LOGIN

UserName :

Password :

Auth Code : 

If you cannot read the word, [click here](#)

[Forgotten password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or

12. Now, click **Login**. Your account has been activated.

12.6.2 Creating an Account via MyVigor Web Site

1. Access into <http://myvigor.draytek.com>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.

The screenshot shows the MyVigor website homepage. The header includes the DrayTek logo, the MyVigor logo, and a Customer Survey button. A navigation menu on the left lists Home, About Us, Product, My Information, and VigorPro. The main content area is titled 'MyVigor for you' and contains information about the website's purpose, supported products (VigorPro Unified Security Firewall series), and services (Vigor routers). A login section on the right includes fields for Username, Password, and AuthCode, along with a Login button and a link for 'Not registered yet? Click here!'. A search bar is located in the top right corner.

2. Check to confirm that you accept the Agreement and click **Accept**.

The screenshot shows the MyVigor registration page. The page is titled 'Register' and contains a section for 'Create an account - Please enter personal profile.' The registration process is divided into four steps: 1. Agreement, 2. Personal Information, 3. Preferences, and 4. Completion. The '1. Agreement' step is currently active. It displays the 'MyVigor Agreement' text, which outlines the terms of service and registration conditions. A checkbox is present at the bottom of the agreement text, indicating that the user has read and understood the agreement. Below the agreement text are two buttons: '<< Back' and 'Accept >>'. The 'Accept >>' button is highlighted.

3. Type your personal information in this page and then click **Continue**.

Register

Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName: * Mary

(3 ~ 20 characters)

Password: * *****

(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password: * *****

Personal Information

First Name: * Mary

Last Name: * Ted

Company Name: Tech Ltd.

Email Address: * mary_ted@tech.com

Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country: * SWITZERLAND

Career: * Supervisor

<< Back Continue >>

4. Choose proper selection for your computer and click **Continue**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter. ☒

I would like to receive DrayTek product news. ☒

Please select the mail server for receiving the verification mail. Global Server

<< Back Continue >>

5. Now you have created an account successfully. Click **START**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Completion

A confirmation email has been sent to mary_ted@tech.com
Please click on the activation link in the email
to activate your account

START

6. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

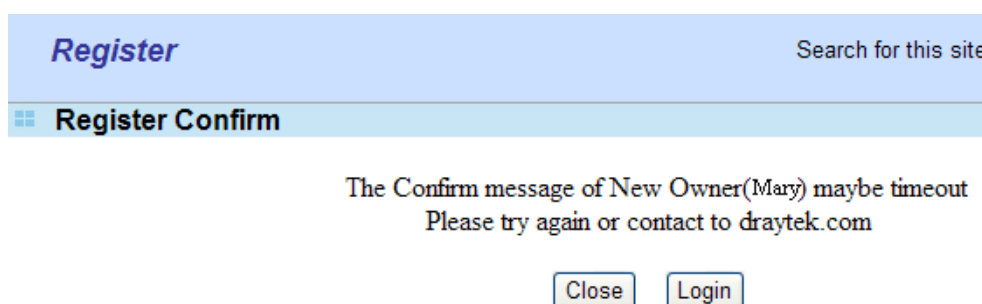
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

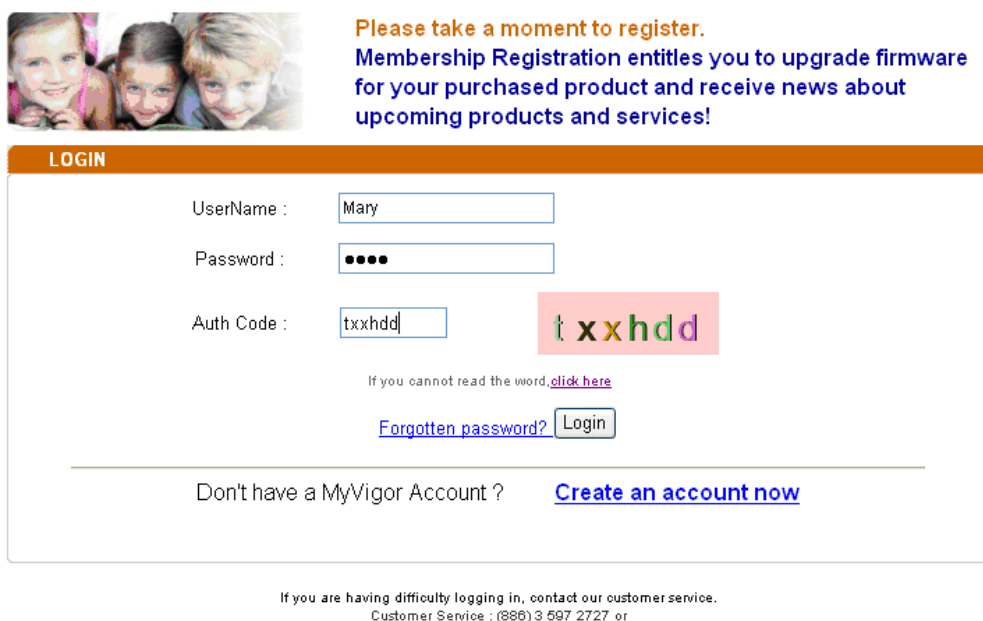
Link : [Activate my Account](#)

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



The screenshot shows a web interface with a blue header bar. On the left, the word "Register" is in a larger font, and on the right, there is a search bar with the placeholder text "Search for this site". Below the header, a blue bar contains the text "Register Confirm" next to a small icon. The main content area is white and displays a message: "The Confirm message of New Owner(Mary) maybe timeout Please try again or contact to draytek.com". At the bottom of the message area, there are two buttons: "Close" and "Login".

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.



The screenshot shows a login page with a header image of three children and a promotional message: "Please take a moment to register. Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!". Below this is a "LOGIN" section with a white background and an orange header. It contains three input fields: "UserName" with the value "Mary", "Password" with four dots, and "Auth Code" with the value "txxhdd". To the right of the "Auth Code" field is a pink box displaying the code "t x x h d d". Below the input fields, there is a link "If you cannot read the word, click here" and a "Forgotten password?" link next to a "Login" button. At the bottom, there is a link "Don't have a MyVigor Account ?" next to a "Create an account now" link. At the very bottom of the page, there is a small text: "If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or".

Now, click **Login**. Your account has been activated.

Note: To register VigorACS SI, please return to Chapter 3 and follow the corresponding steps for registration.

12.7 Upgrade VigorACS with New License Key

To control and manage the CPEs effectively, the administrator must acquire a new license from DrayTek regularly. Usually, the valid time of the license is one year. You have to renew your license when it is going to be expired.

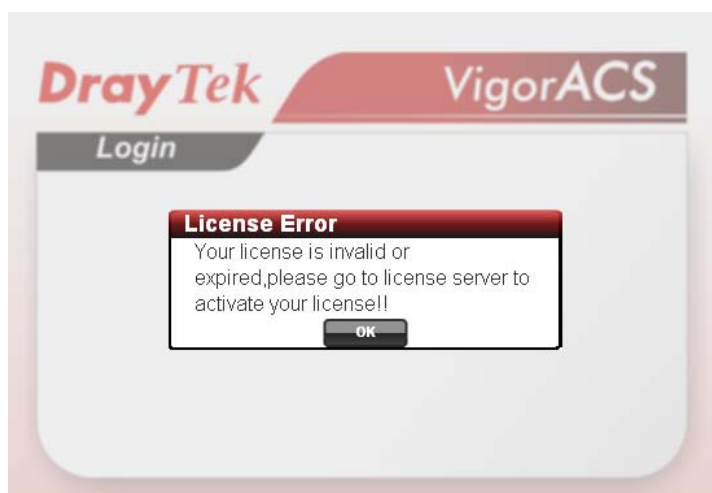
Please follow the steps listed below to get a new license for your VigorACS SI.

12.7.1 License Is Invalid or Expired

1. Click **Programs> VigorACS SI> VigorACS Web Page** to access into VigorACS. The login page of VigorACS will be shown as the following:



2. Please type user name and password. Then click **Login**. A License Error dialog appears as follows. It indicates that you cannot access into VigorACS SI due to the invalid license. Please purchase a new one and return here to upgrade the license for using VigorACS SI. When you have prepared a new license, click the **OK** button.



3. A login page for MyVigor web site will pop up automatically. Type your account (user name) and password in this page. Enter the authentication code with the characters displayed on the screen. Then, click **Login**.



Please take a moment to register.

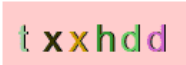
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

LOGIN

UserName :

Password :

Auth Code :



If you cannot read the word, [click here](#)

[Forgotten password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or

4. MyVigor will verify and authenticate if the user account you typed is allowed to access into the web site. If yes, Device Information will appear as follows. Find and click **Renew** for the service item of ACS.

My Product

Device Information

Nickname : carrie_yfn

Host ID :

Model : VigorACS

Device's Service
Expired License

Service	Provider	Action	Status	Start Date	Expired Date	Nodes
ACS	DT-ACS	Renew	On	-	-	

● Means such service is in use.

● Means such service is not in use.

● Means such service has not been activated yet.

● Means such service is in use and will be invalid soon(less than one month).

Trial

Allows you to have the free trial for service.

Renew

Allows you to renew service license.

Activate

Allows you to activate service.

From the page, you can see the basic information for the trial version of VigorACS.

5. You will be guided to the following page. Type the new license number you purchase from the service provider in the corresponding field. And click **Add License**.

Apply For A License Number

Cancel

Service Name: ACS
Service Provider: DT-ACS

STEP 1

License Number : FD234-B61E3-3676F-B37B7

Add License

Tip : Please ensure that the licence key you enter is for the correct (your preferred) service provider.

Next

6. The new added license number will be displayed on the screen as shown below. Click **Next** for next page.

Apply For A License Number

Cancel

Service Name: ACS
Service Provider: DT-ACS

STEP 1

License Number :

Add License

Tip : Please ensure that the licence key you enter is for the correct (your preferred) service provider.

Flag	License	Provider	Nodes	Status
del	FD234-B61E3-3676F-B37B7	DT-ACS	1000	valid

Next

7. Check the box of “**I have read and accepted the above...**” and click **Next**.

Confirm Message

Cancel

User Name : yfn
Serial : 20100128013339
Model : VigorACS

License Number	Service Provider	Status	Nodes
FD234-B61E3-3676F-B37B7	DT-ACS	valid	1000

DrayTek VigorACS SI Series End-User License Agreement

IMPORTANT:

DrayTek IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN DrayTek IS UNWILLING TO LICENSE THE

☒ I have read and accept the above Agreement. (Please check this box).

Next

8. The activation date will be displayed automatically. Simply click **Next**.

Apply For A License Number

Cancel

Service Name: ACS

STEP 2

Activation Date (MM-DD-YYYY): 03-10-2020 Next

9. A confirm message page will be shown as follows. If there is no problem, please click **Confirm**.

Confirm Message

User Name : carrie_yfn
Host ID :
Activate Date : 2010-03-10
Expired Date : 2011-03-09

License Number / Host ID	Service Provider	Status	Nodes
FD234-B61E3-3676F-B37B7	DT-ACS	valid	1000
Total: 1000 nodes			

Cancel Confirm

10. When the following screen appears, it means the new license for VigorACS SI has been activated. Click **Login to VigorACS**.

VigorACS License Information

Operation	1000 : Service activation
License id	00001b7a
Start date	2010-03-10
Expire date	2011-03-09
Max node	00000020
Is trial license	No

Login to ACS

11. Click **Login to ACS**. You will see the following screen with the new license information.

License Key Information



License Id:	00001b7a
Start Date:	2010-03-10
Expire Date:	2011-03-09
Max Node:	1000
Is trial license:	No

12.7.2 License Is Valid Still

1. Click **Programs> VigorACS SI> VigorACS Web Page** to access into VigorACS. The login page of VigorACS will be shown as the following:

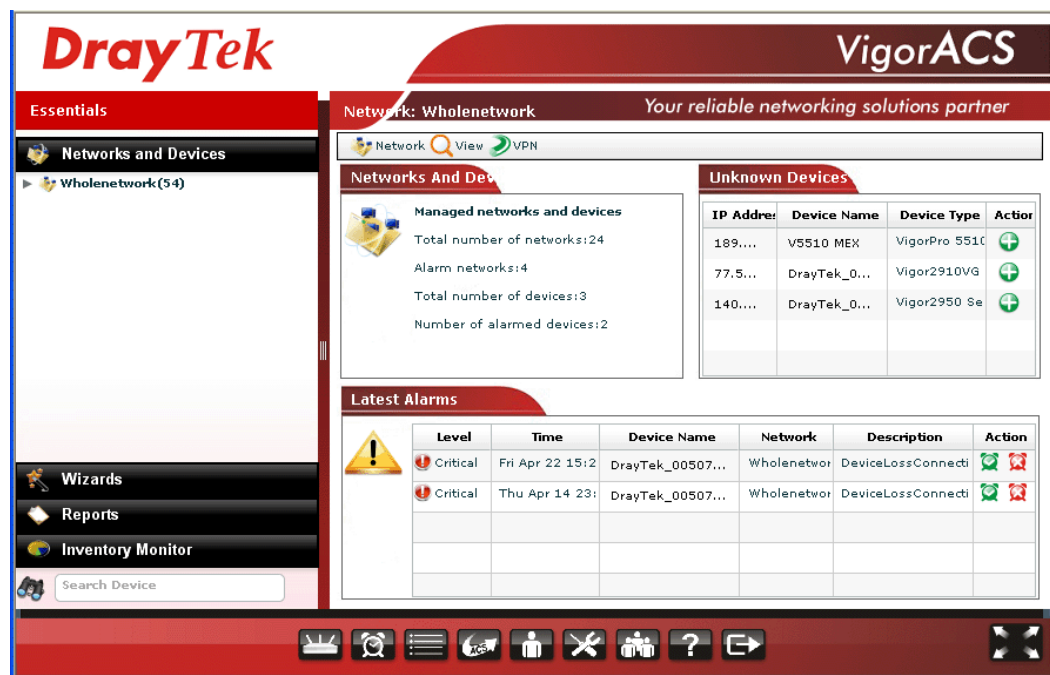


The login page features the DrayTek logo on the left and the VigorACS logo on the right. Below the logos is a 'Login' section with the following fields:

- User Name:** A text box containing 'root'.
- Password:** A text box containing '*****'.
- Validated Code:** A text box containing '7xXS' and a button with '7 x x S'.

At the bottom of the login section are two buttons: 'EN' and 'Login'.

2. Please type “root” as user name and “admin123” as password. Then click **Login**.



The main dashboard displays the DrayTek logo and the VigorACS logo. The left sidebar contains the following menu items:

- Essentials
- Networks and Devices
- Wholenetwork (54)
- Wizards
- Reports
- Inventory Monitor
- Search Device

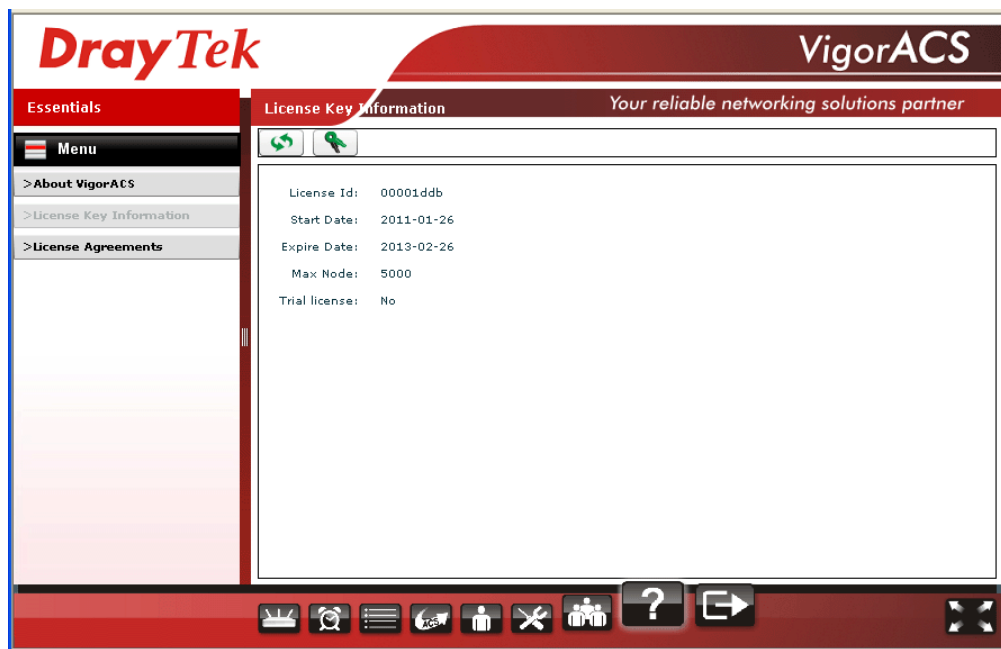
The main content area is divided into several sections:

- Network: Wholenetwork** (Your reliable networking solutions partner)
- Networks And Dev** (Managed networks and devices)
- Unknown Devices** (Table of unknown devices)
- Latest Alarms** (Table of latest alarms)

IP Address	Device Name	Device Type	Action
189...	V5510 MEX	VigorPro 5510	+
77.5...	DrayTek_0...	Vigor2910VG	+
140...	DrayTek_0...	Vigor2950 Se	+

Level	Time	Device Name	Network	Description	Action
Critical	Fri Apr 22 15:2	DrayTek_00507...	Wholenetwork	DeviceLossConnecti	+
Critical	Thu Apr 14 23:	DrayTek_00507...	Wholenetwork	DeviceLossConnecti	+

3. Open **Help**.



4. Click  from License Key Information page.
5. The welcome screen will be shown as follows. Type the username and password, and click **Login**.



Please take a moment to register.

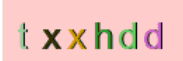
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

LOGIN

UserName :

Password :

Auth Code :



If you cannot read the word, [click here](#)

[Forgotten password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or

6. The following screen will appear. Find and click **Renew** for the service item of ACS.

My Product

Device Information

Nickname: **carrie_yfn**
Host ID:
Model: **VigorACS**

[Rename](#) [Delete](#) [Transfer](#) [Back](#)

[Device's Service](#) [Expired License](#)

Service	Provider	Action	Status	Start Date	Expired Date	Nodes
ACS	DT-ACS	Renew	 On	2010-03-03	2010-04-02	20

 Means such service is in use.
 Means such service is not in use.
 Means such service has not been activated yet.
 Means such service is in use and will be invalid soon(less than one month).

[Trial](#) Allows you to have the free trial for service.
[Renew](#) Allows you to renew service license.
[Activate](#) Allows you to activate service.

7. You will be guided to the following page. Type the new license number you purchase from the service provider in the corresponding field. And click **Add License**.

Apply For A License Number

[Cancel](#)

Service Name: **ACS**
Service Provider: **DT-ACS**

STEP 1

 License Number: [Add License](#)

Tip : Please ensure that the licence key you enter is for the correct (your preferred) service provider.

[Next](#)

8. The new added license number will be displayed on the screen as shown below. Click **Next** for next page.

Apply For A License Number

[Cancel](#)

Service Name: **ACS**
Service Provider: **DT-ACS**

STEP 1

 License Number: [Add License](#)

Tip : Please ensure that the licence key you enter is for the correct (your preferred) service provider.

Flag	License	Provider	Nodes	Status
del	FD234-B61E3-3676F-B37B7	DT-ACS	1000	valid

[Next](#)

9. Check the box of “**I have read and accepted the above...**” and click **Next**.

Confirm Message

Cancel

User Name : yfn
Serial : 20100128013339
Model : VigorACS

License Number	Service Provider	Status	Nodes
FD234-B61E3-3676F-B37B7	DT-ACS	valid	1000

DrayTek VigorACS SI Series End-User License Agreement

IMPORTANT:

DrayTek IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN DrayTek IS UNWILLING TO LICENSE THE

☒ I have read and accept the above Agreement. (Please check this box).

Next

10. The activation date will be displayed automatically. Simply click **Next**.

Apply For A License Number

Cancel

Service Name: ACS

STEP 2

Activation Date (MM-DD-YYYY): 04-03-2010 Next

11. A confirm message page will be shown as follows. If there is no problem, please click **Confirm**.

Confirm Message

User Name : carrie_yfn
Host ID :
Activate Date : 2010-04-03
Expired Date : 2011-04-02

License Number / Host ID	Service Provider	Status	Nodes
FD234-B61E3-3676F-B37B7	DT-ACS	valid	1000
Total: 1000 nodes			

Cancel Confirm

12. When the following screen appears, it means the new license for VigorACS SI has been added. You can access into VigorACS.

VigorACS License Information

Operation	1000 : Service activation
License id	00001b7a
Start date	2010-03-03
Expire date	2010-04-02
Max node	00000020
Is trial license	Yes

[Login to ACS](#)

Note: For the trial version is still in valid period, you will see VigorACS SI with two licenses controlled under My Vigor website.

When the trial version is expired, please click the **On** (with red light) button to activate the new added license for VigorACS SI.

Host ID :
Model : VigorACS

[Rename](#) [Delete](#) [Transfer](#) [Back](#)

Device's Service		Expired License				
Service	Provider	Action	Status	Start Date	Expired Date	Nodes
ACS	DT-ACS	Renew	 On	2010-03-03	2010-04-02	20
ACS	DT-ACS	Renew	 On	2010-04-03	2011-04-02	1000

Trial Version

 Means such service is in use.
 Means such service is not in use.
 Means such service has not been activated yet.
 Means such service is in use and will be invalid soon(less than one month).

[Trial](#) Allows you to have the free trial for service.
[Renew](#) Allows you to renew service license.
[Activate](#) Allows you to activate service.

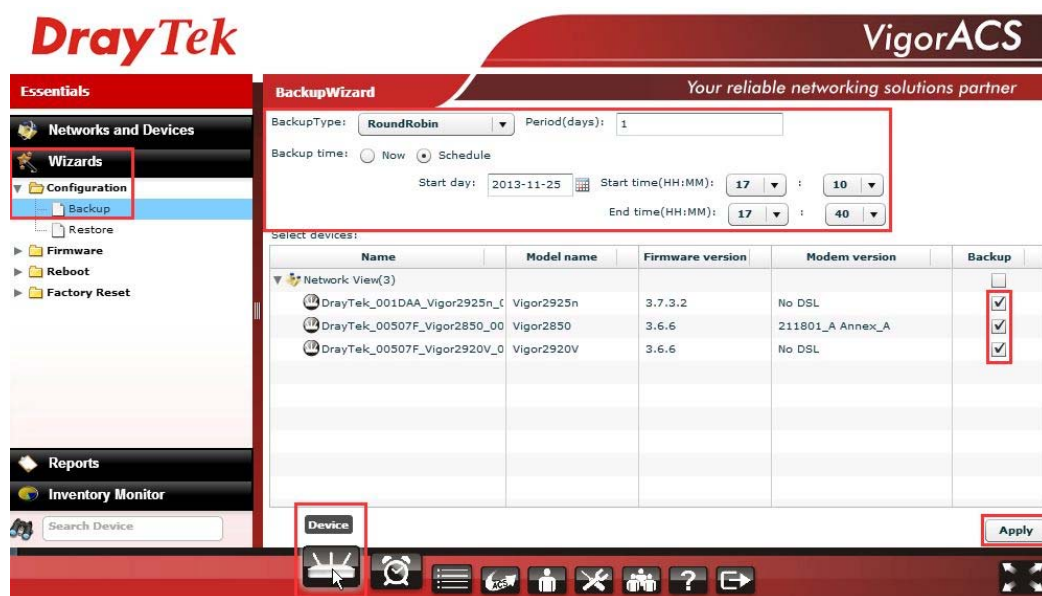
12.8 How to Backup CPE's Configuration via Wizards

Settings for several CPEs can be back up by VigorACS SI wizards. It can save time for it is very convenient to execute setting backup for the administrator.

1. Click the icon of **Device**.



2. Open **Wizards >> Configuration >> Backup**.



Determine the **Backup Type**. Here we use **RoundRobin** as an example. (RoundRobin: The file name will be tagged as 1~20. The system can save at most 20 files. The 21st file will cover the 1st file.)

Type the number you want as **Period (days)**. Here we use “1” as an example. It means backup configuration will be executed once a day. Then, choose the type of Backup time. Here we use **Schedule** as an example and set time with 17:10~17:40).

Choose the CPE(s) to apply the configuration backup by checking the Backup box(s).

3. After finished the above settings, click **Apply** to save the settings.
4. Click the icon of **Log**.



- Open **Device Action >> FileTransferLog**. We can see all of the specified CPEs have already finished backup configuration.

FileTransferLog									
UserGroup: RootGroup									
LogID	DeviceID	DeviceName	MAC address	DeviceIP	Type	Status	Event	FirmwareUp	
29	12	DrayTek_00507F_Vigor2850	00507FE83088	118.160.95.20	Backup	Success	Nothing	0	
28	11	DrayTek_00507F_Vigor2920	00507FC9962C	118.160.86.54	Backup	Success	Nothing	0	
27	10	DrayTek_001DAA_Vigor2925	001DAAAC96F8	192.168.106.1	Backup	Success	Nothing	0	

- Check where the configurations are saved. Click the icon of **Provision**.



- Open **General >> Upload File**. Three entries named by MAC addresses are displayed under **Filename**. Each CPE's configuration is saved in its folder.

Essentials
 Menu
 General
 Upload File
 Trigger
 FirmwareUpgrade
 Backup
 Restore
 Provision Setting
 Global Parameters

Provision UploadFile
 UserGroup: RootGroup

Filename	Property	Size	LastModify	Di
..	Directory	4096	2013/11/22 17:08:01	.
.	Directory	4096	2013/11/25 16:28:00	./RootGroup
SharedFirmware	Directory	4096	2013/11/25 16:29:07	./RootGroup
00507FC9962C	Directory	4096	2013/11/25 17:19:48	./RootGroup
00507FE83088	Directory	4096	2013/11/25 17:20:37	./RootGroup
001DAAAC96F8	Directory	4096	2013/11/25 17:19:48	./RootGroup

Double-click on one of the entries named by MAC address, the configuration file (named with 1.cfg) for the selected entry will be displayed on the screen.

VigorACS					
Provision UploadFile					
UserGroup: RootGroup					
Filename	Property	Size	LastModify	Directory	
..	Directory	4096	2013/11/25 16:28:00	./RootGroup	
.	Directory	4096	2013/11/25 17:19:48	./RootGroup/00507FC9962C	
1.cfg	cfg file	6376	2013/11/25 17:19:48	./RootGroup/00507FC9962C	

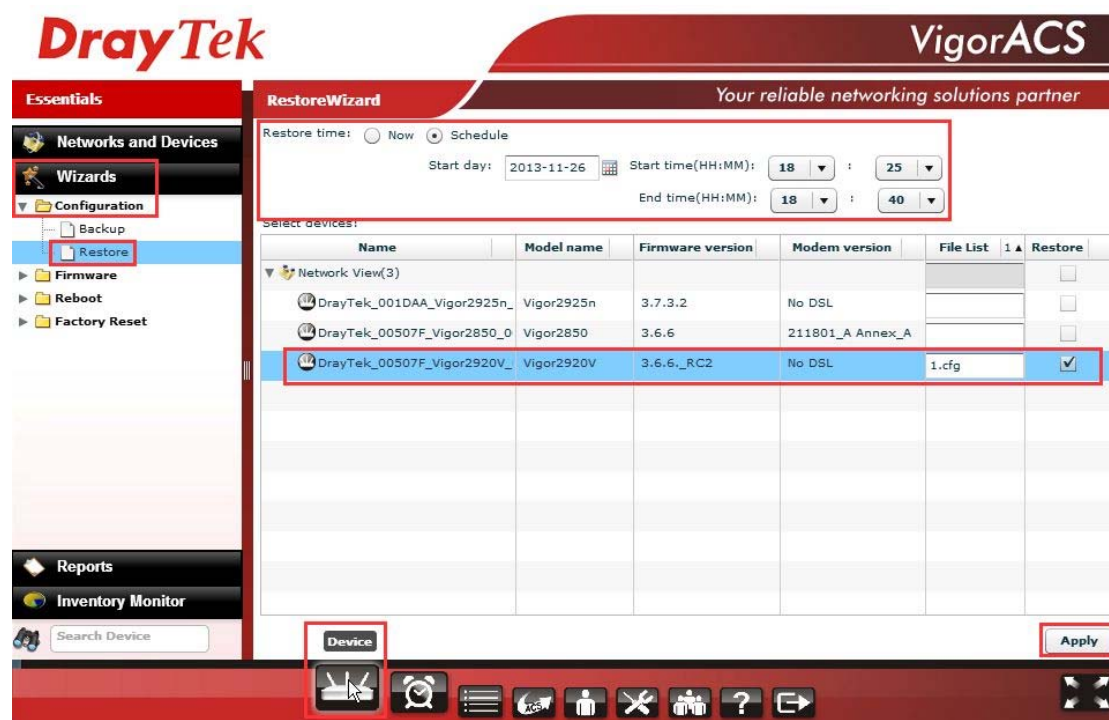
12.9 How to Restore CPE's Configuration via Wizards

Settings for several CPEs can be restored by VigorACS SI wizards. It can save time for it is very convenient to execute setting restoration for the administrator.

1. Click the icon of **Device**.



2. Open **Wizards >> Configuration >> Restore**.



Choose the type of **Restore time**. Here we use **Schedule** as an example and set time with 18:25~18:40).

Choose the model (e.g., Vigor2920 in this example) you want to restore the configuration file for it. Use the File List drop down list to select the configuration file you want (here we choose "1.cfg" file). Then, check the **Restore** box.

3. After finished the above settings, click **Apply** to save the settings.
4. Click the icon of **Log**.



5. Open **Device Action >> FileTransferLog**. We can see LogID: 32 indicating that Vigor2920 has successfully restored the configuration.

FileTransferLog								
				UserGroup: RootGroup				
Q Sea	Q Search	Q Search	Q Search	Q Search	Q Search			Q S
LogID	DeviceID	DeviceName	MAC address	DeviceIP	Type	Status	Event	Firm
32	11	DrayTek_00507F_Vigor2920V_	00507FC9962C	118.160.93.20	Restore	Success	Nothing	0
31	10	DrayTek_001DAA_Vigor2925n_	001DAAAC96F8	192.168.106.1	Backup	Success	Nothing	0
30	12	DrayTek_00507F_Vigor2850_00	00507FE83088	118.160.89.151	Backup	Success	Nothing	0
29	12	DrayTek_00507F_Vigor2850_00	00507FE83088	118.160.89.151	Backup	Success	Nothing	0
28	11	DrayTek_00507F_Vigor2920V_	00507FC9962C	118.160.93.20	Backup	Success	Nothing	0
27	10	DrayTek_001DAA_Vigor2925n_	001DAAAC96F8	192.168.106.1	Backup	Success	Nothing	0

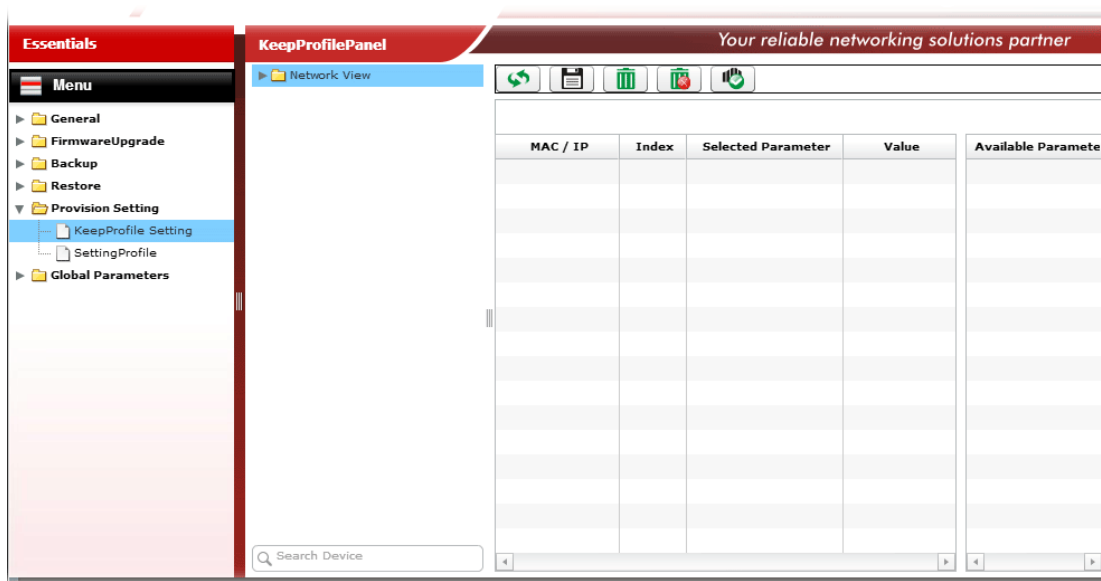
12.10 How to apply KeepProfile Setting in Provision for a New CPE

Suppose VigorACS SI has made KeepProfile configuration for a CPE. Later, due to some reason, the CPE is replaced by another CPE with the same model. The administrator can use KeepProfile setting to maintain some parameters of the new CPE the same as the old one.

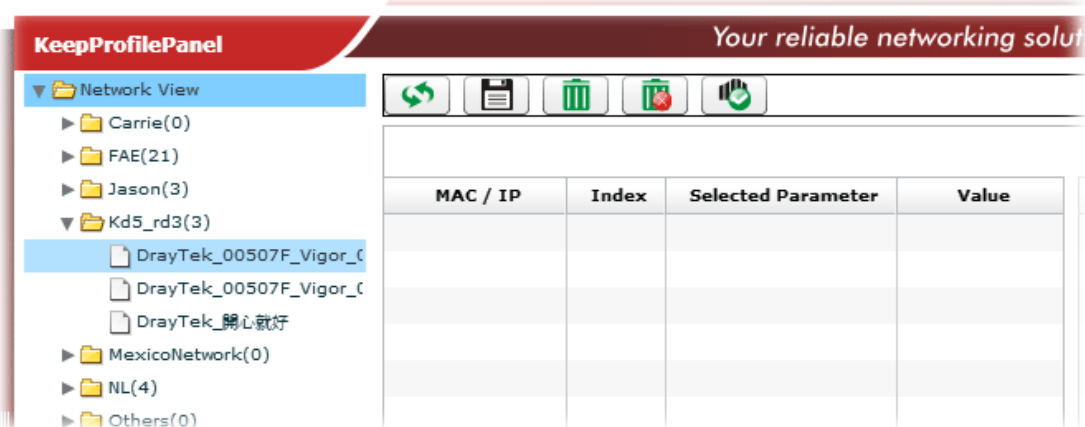
1. Click the icon of **Provision**.



2. Open **Provision Setting**>>**KeepProfile Setting**.



3. Expand **Network View** by clicking the triangle and locate the new CPE.



- Double click the CPE you want. Wait for a moment until the menu tabs displayed.

MAC / IP	Index	Selected Parameter	Value	Available Paramete
001DAAA8A880	1	Reboot device	false	

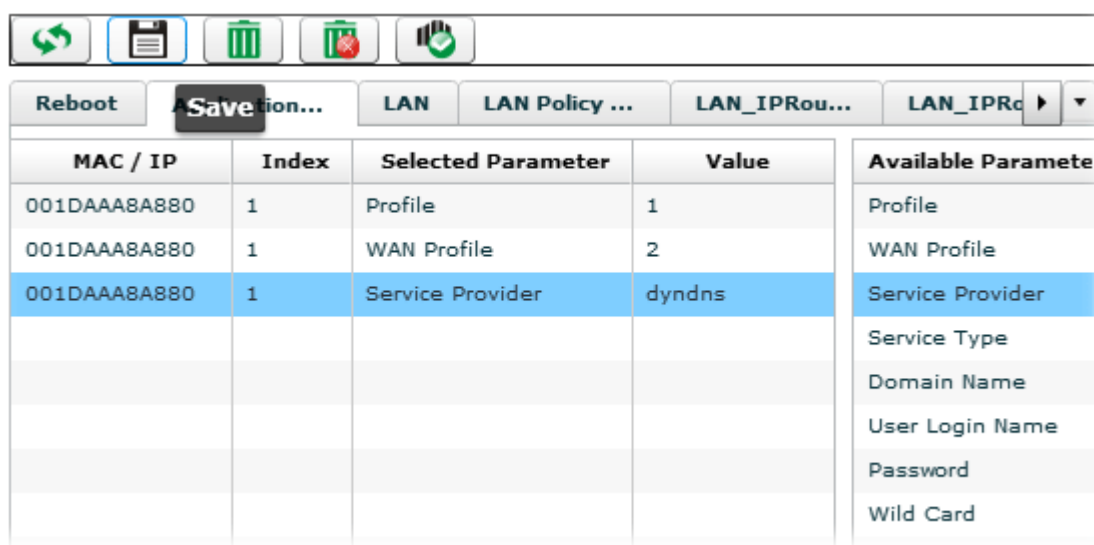
- Click the menu tab needed to be modified, e.g., Application in this case.

MAC / IP	Index	Selected Parameter	Value	Available Parameter
				Profile
				WAN Profile
				Service Provider
				Service Type
				Domain Name
				User Login Name
				Password
				Wild Card
				Backup MX
				Mail Extender

- On the **Available Parameter** field, double click the one you want to modify (e.g., Service Provider in this case). Related settings will be displayed on the screen. All you have to do is changing the value.

MAC / IP	Index	Selected Parameter	Value	Available Parameter
001DAAA8A880	1	Profile	1	Profile
001DAAA8A880	1	WAN Profile	2	WAN Profile
001DAAA8A880	1	Service Provider		Service Provider
				Service Type
				Domain Name
				User Login Name
				Password
				Wild Card
				Backup MX

7. After you finished the parameter modification, click **Save** to save the modification.



The screenshot shows the VigorACS SI configuration interface. At the top, there is a toolbar with icons for Refresh, Save, Delete, Add, and Check. Below the toolbar, there are tabs for 'Reboot', 'Save', 'LAN', 'LAN Policy ...', 'LAN_IPRou...', and 'LAN_IPRc'. The 'Save' tab is currently selected and highlighted. Below the tabs, there is a table with the following columns: 'MAC / IP', 'Index', 'Selected Parameter', 'Value', and 'Available Paramete'. The table contains three rows of data, with the third row highlighted in blue. The third row shows '001DAAA8A880' for MAC / IP, '1' for Index, 'Service Provider' for Selected Parameter, and 'dyndns' for Value. The 'Available Paramete' column lists 'Profile', 'WAN Profile', 'Service Provider', 'Service Type', 'Domain Name', 'User Login Name', 'Password', and 'Wild Card'.

MAC / IP	Index	Selected Parameter	Value	Available Paramete
001DAAA8A880	1	Profile	1	Profile
001DAAA8A880	1	WAN Profile	2	WAN Profile
001DAAA8A880	1	Service Provider	dyndns	Service Provider
				Service Type
				Domain Name
				User Login Name
				Password
				Wild Card

8. Now, even anyone changed the service provider of the CPE remotely, VigorACS will restore the settings configured here for that CPE automatically.

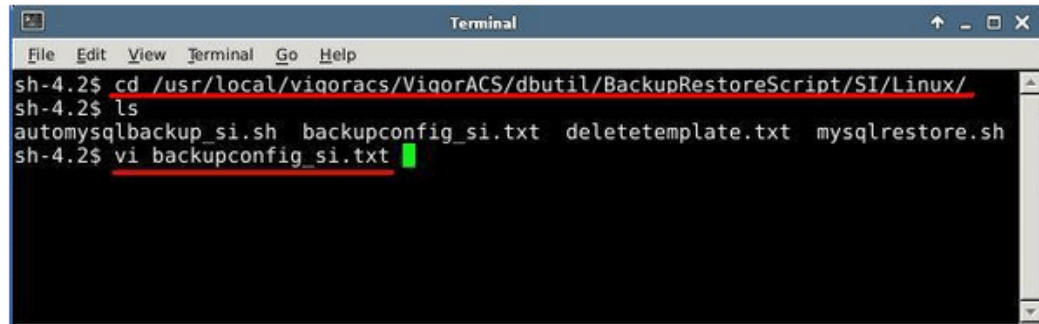
12.11 How to Backup the Database of VigorACS SI

12.11.1 For Linux Platform – Backup Instantly

1. Enter the path and edit the file “backupconfig_si.txt”.

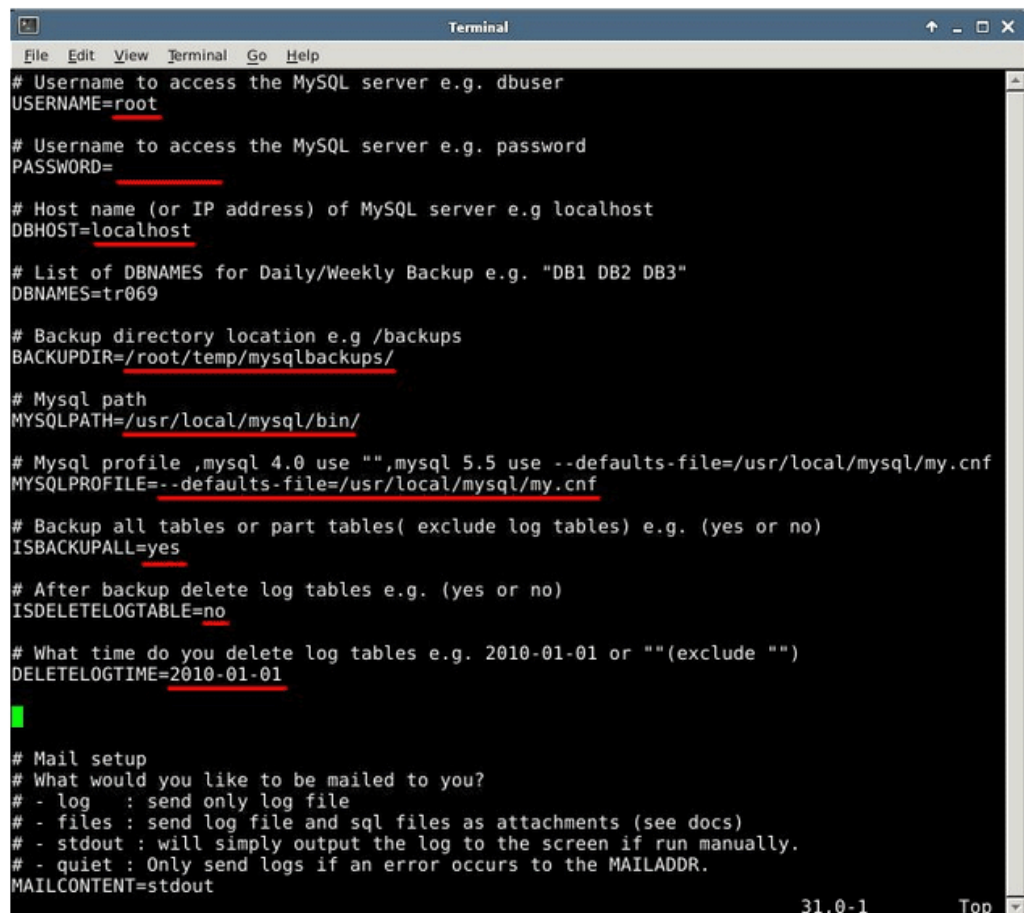
Path: /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/

Command: # vi backupconfig_si.txt



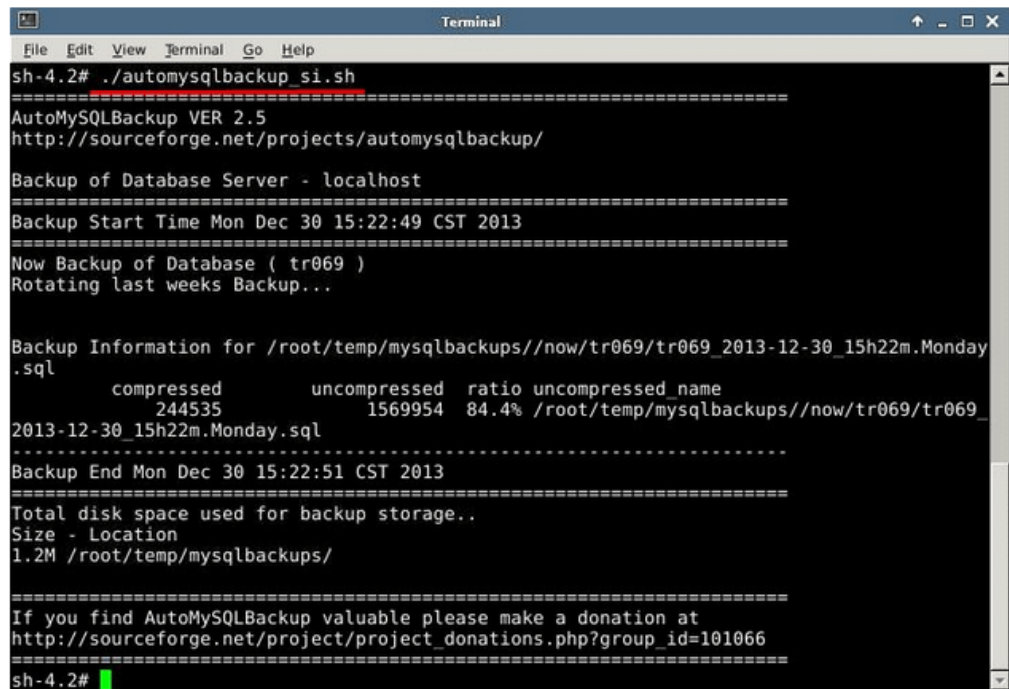
```
Terminal
File Edit View Terminal Go Help
sh-4.2$ cd /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/
sh-4.2$ ls
automysqlbackup_si.sh backupconfig_si.txt deletetemplate.txt mysqlrestore.sh
sh-4.2$ vi backupconfig_si.txt
```

2. Confirm the parameters with red underlines are correct. Please create the backup directory (/root/temp/mysqlbackups) first if you don't have.



```
Terminal
File Edit View Terminal Go Help
# Username to access the MySQL server e.g. dbuser
USERNAME=root
# Username to access the MySQL server e.g. password
PASSWORD=
# Host name (or IP address) of MySQL server e.g localhost
DBHOST=localhost
# List of DBNAMES for Daily/Weekly Backup e.g. "DB1 DB2 DB3"
DBNAMES=tr069
# Backup directory location e.g /backups
BACKUPDIR=/root/temp/mysqlbackups/
# Mysql path
MYSQLPATH=/usr/local/mysql/bin/
# Mysql profile ,mysql 4.0 use "",mysql 5.5 use --defaults-file=/usr/local/mysql/my.cnf
MYSQLPROFILE=--defaults-file=/usr/local/mysql/my.cnf
# Backup all tables or part tables( exclude log tables) e.g. (yes or no)
ISBACKUPALL=yes
# After backup delete log tables e.g. (yes or no)
ISDELETELOGTABLE=no
# What time do you delete log tables e.g. 2010-01-01 or ""(exclude "")
DELETELOGTIME=2010-01-01
# Mail setup
# What would you like to be mailed to you?
# - log : send only log file
# - files : send log file and sql files as attachments (see docs)
# - stdout : will simply output the log to the screen if run manually.
# - quiet : Only send logs if an error occurs to the MAILADDR.
MAILCONTENT=stdout
31,0-1 Top
```

3. Run `"automysqlbackup_si.sh"` to back up database.



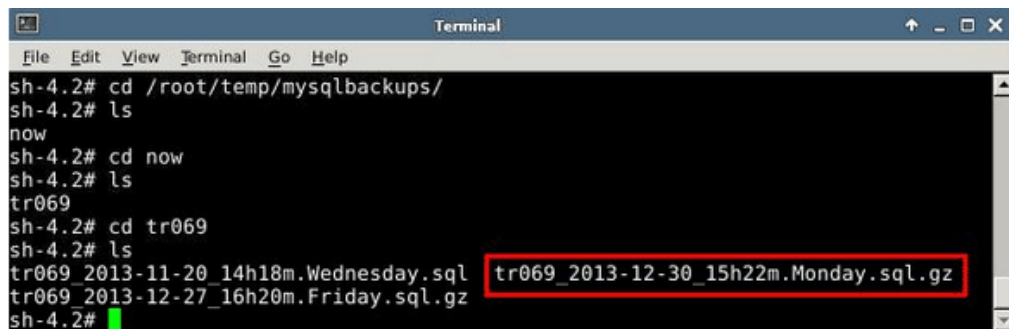
```
sh-4.2# ./automysqlbackup_si.sh
=====
AutoMySQLBackup VER 2.5
http://sourceforge.net/projects/automysqlbackup/

Backup of Database Server - localhost
=====
Backup Start Time Mon Dec 30 15:22:49 CST 2013
=====
Now Backup of Database ( tr069 )
Rotating last weeks Backup...

Backup Information for /root/temp/mysqlbackups//now/tr069/tr069_2013-12-30_15h22m.Monday
.sql
      compressed      uncompressed      ratio uncompressed_name
      244535           1569954      84.4% /root/temp/mysqlbackups//now/tr069/tr069_
2013-12-30_15h22m.Monday.sql
=====
Backup End Mon Dec 30 15:22:51 CST 2013
=====
Total disk space used for backup storage..
Size - Location
1.2M /root/temp/mysqlbackups/

=====
If you find AutoMySQLBackup valuable please make a donation at
http://sourceforge.net/project/project_donations.php?group_id=101066
=====
sh-4.2#
```

4. Check the backup file just created.



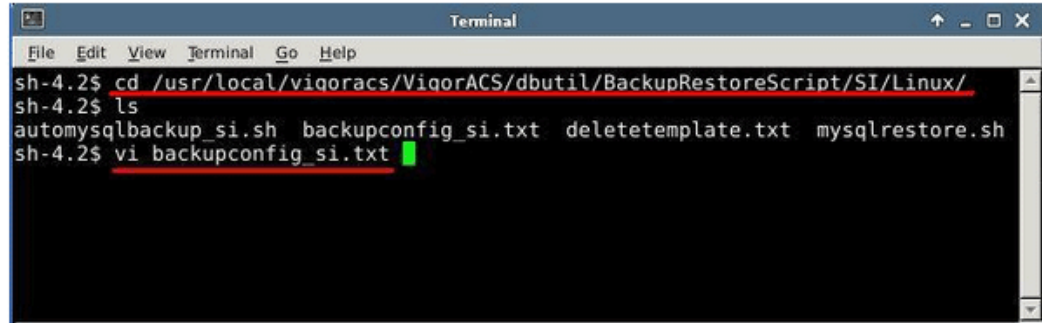
```
sh-4.2# cd /root/temp/mysqlbackups/
sh-4.2# ls
now
sh-4.2# cd now
sh-4.2# ls
tr069
sh-4.2# cd tr069
sh-4.2# ls
tr069_2013-11-20_14h18m.Wednesday.sql  tr069_2013-12-30_15h22m.Monday.sql.gz
tr069_2013-12-27_16h20m.Friday.sql.gz
sh-4.2#
```

12.11.2 For Linux Platform – Backup by Schedule

1. Enter the path and edit the file “backupconfig_si.txt”.

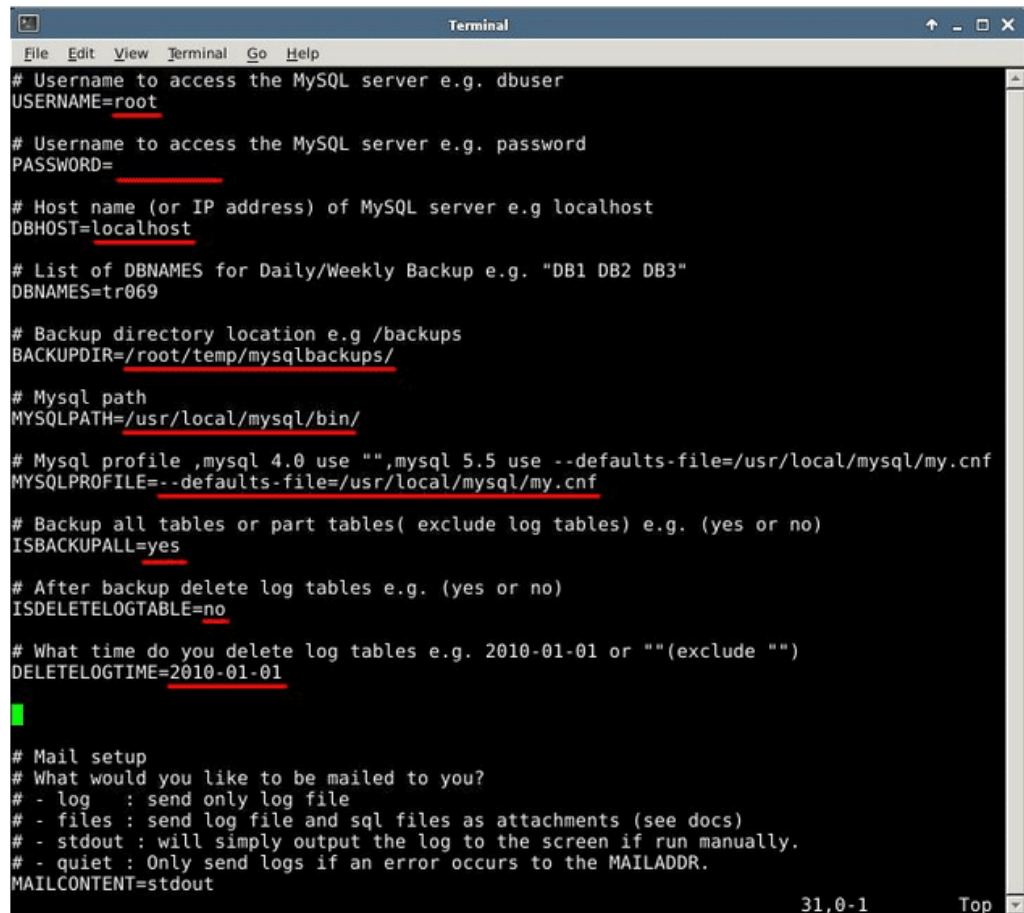
Path: /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/

Command: # vi backupconfig_si.txt



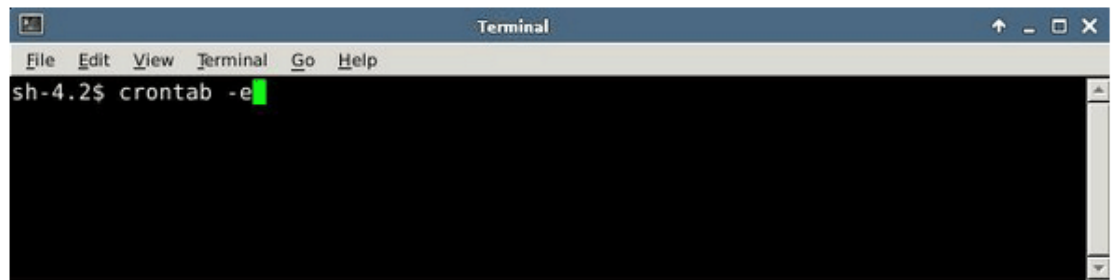
```
Terminal
File Edit View Terminal Go Help
sh-4.2$ cd /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/
sh-4.2$ ls
automysqlbackup_si.sh  backupconfig_si.txt  deletetemplate.txt  mysqlrestore.sh
sh-4.2$ vi backupconfig_si.txt
```

2. Confirm the parameters with red underlines are correct. Please create the backup directory (/root/temp/mysqlbackups) first if you don't have.



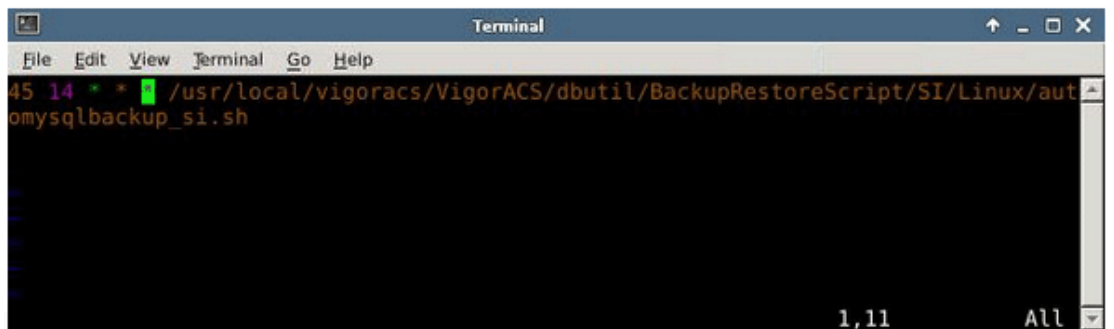
```
Terminal
File Edit View Terminal Go Help
# Username to access the MySQL server e.g. dbuser
USERNAME=root
# Username to access the MySQL server e.g. password
PASSWORD=
# Host name (or IP address) of MySQL server e.g localhost
DBHOST=localhost
# List of DBNAMES for Daily/Weekly Backup e.g. "DB1 DB2 DB3"
DBNAMES=tr069
# Backup directory location e.g /backups
BACKUPDIR=/root/temp/mysqlbackups/
# Mysql path
MYSQLPATH=/usr/local/mysql/bin/
# Mysql profile ,mysql 4.0 use "",mysql 5.5 use --defaults-file=/usr/local/mysql/my.cnf
MYSQLPROFILE=--defaults-file=/usr/local/mysql/my.cnf
# Backup all tables or part tables( exclude log tables) e.g. (yes or no)
ISBACKUPALL=yes
# After backup delete log tables e.g. (yes or no)
ISDELETELOGTABLE=no
# What time do you delete log tables e.g. 2010-01-01 or ""(exclude "")
DELETELOGTIME=2010-01-01
# Mail setup
# What would you like to be mailed to you?
# - log : send only log file
# - files : send log file and sql files as attachments (see docs)
# - stdout : will simply output the log to the screen if run manually.
# - quiet : Only send logs if an error occurs to the MAILADDR.
MAILCONTENT=stdout
31,0-1 Top
```


3. Set up the file “crontab -e”. Input the command “crontab -e”.



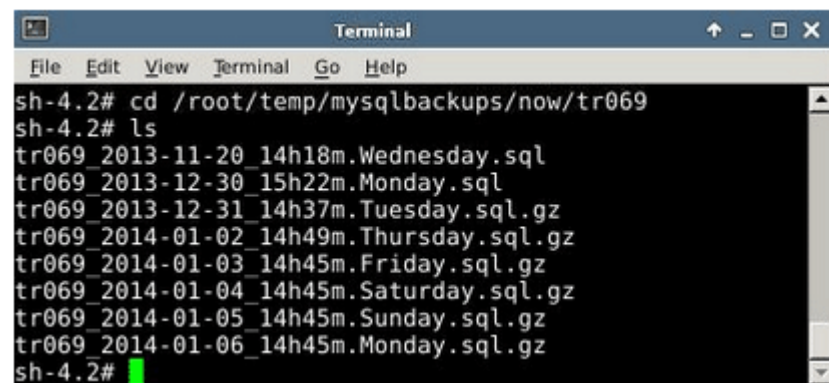
```
Terminal
File Edit View Terminal Go Help
sh-4.2$ crontab -e
```

Enter the value “45 14 * * *
/usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/automysqlbackup_si.sh”, which means we will back up ACS SI once a day at 14:45.



```
Terminal
File Edit View Terminal Go Help
45 14 * * * /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/automysqlbackup_si.sh
1,11 All
```

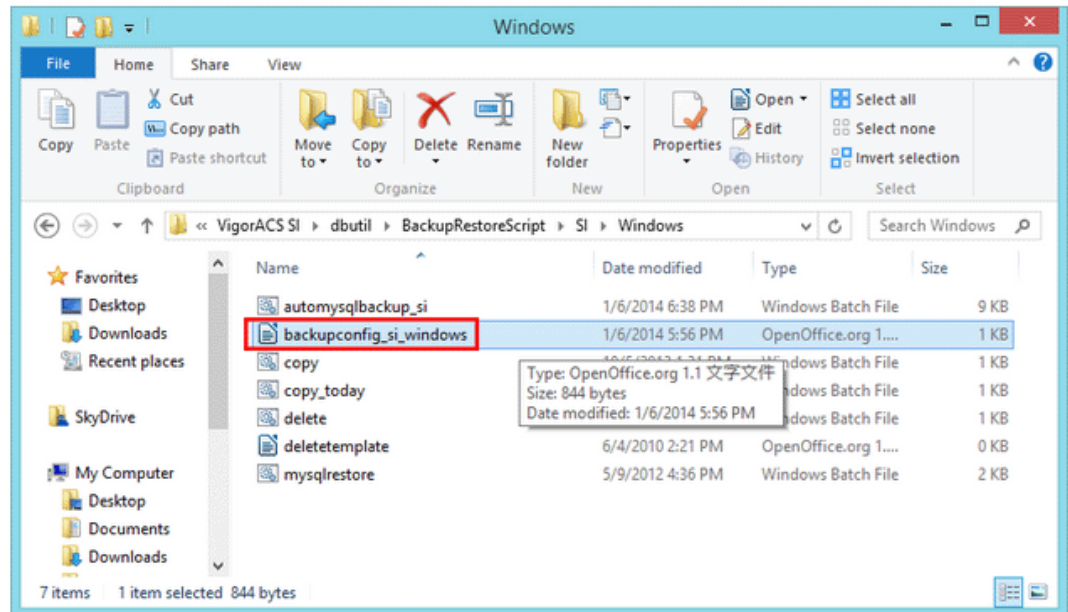
4. Check the file just created.



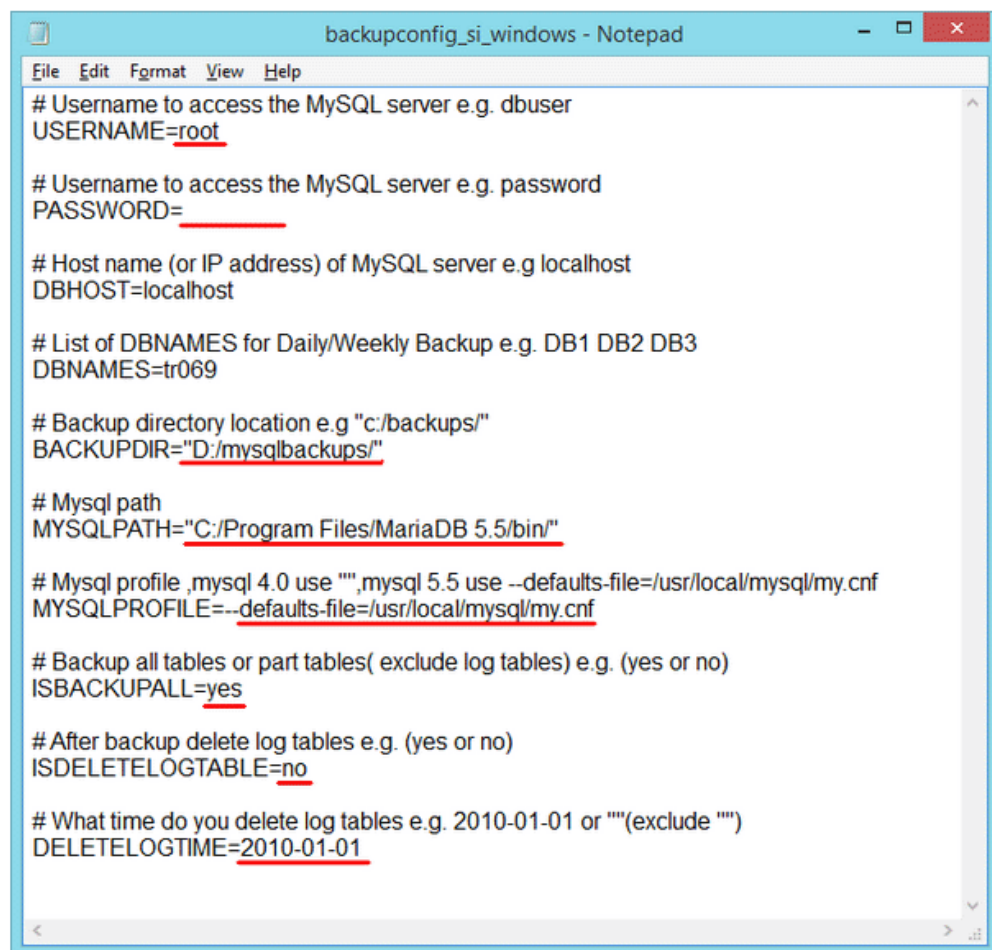
```
Terminal
File Edit View Terminal Go Help
sh-4.2# cd /root/temp/mysqlbackups/now/tr069
sh-4.2# ls
tr069_2013-11-20_14h18m.Wednesday.sql
tr069_2013-12-30_15h22m.Monday.sql
tr069_2013-12-31_14h37m.Tuesday.sql.gz
tr069_2014-01-02_14h49m.Thursday.sql.gz
tr069_2014-01-03_14h45m.Friday.sql.gz
tr069_2014-01-04_14h45m.Saturday.sql.gz
tr069_2014-01-05_14h45m.Sunday.sql.gz
tr069_2014-01-06_14h45m.Monday.sql.gz
sh-4.2#
```


12.11.3 For Windows Platform – Backup Instantly

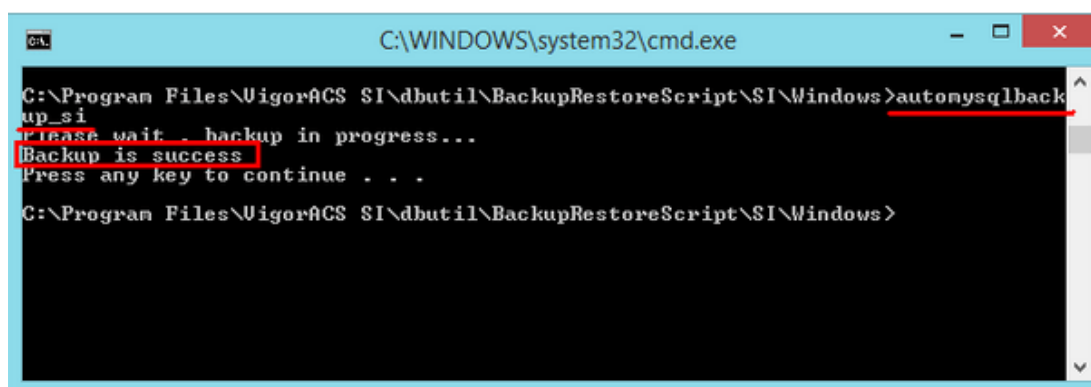
1. Edit file “backupconfig_si_windows.txt”.



2. Confirm the parameters with red underlines are correct.



3. Run "automysqlbackup_si.sh" to back up database.

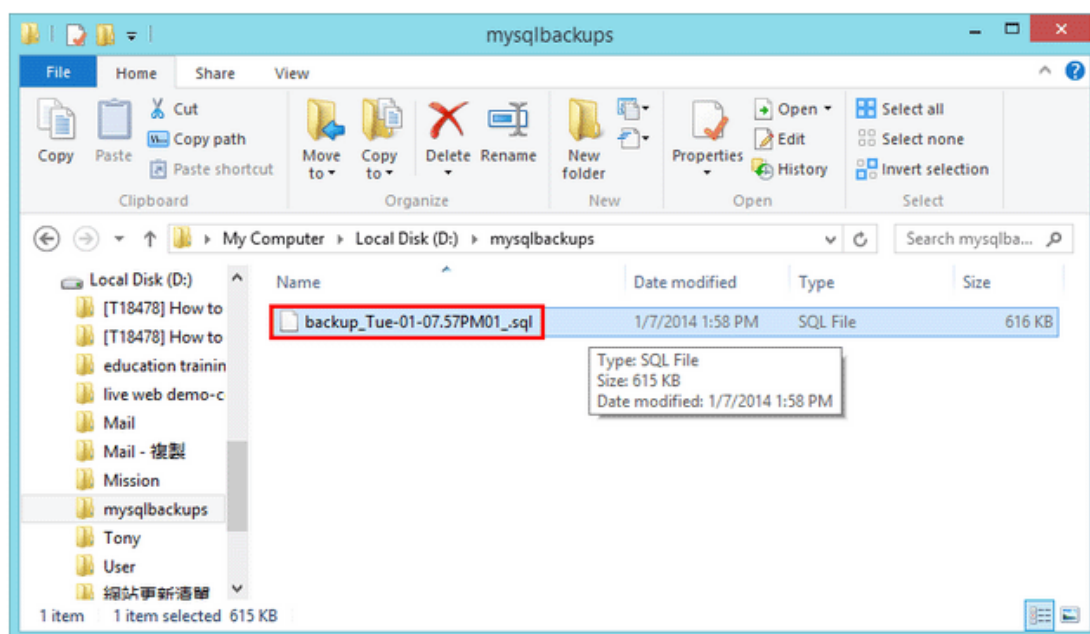


```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\UigorACS SI\dbutil\BackupRestoreScript\SI\Windows>automysqlback
up_si
Please wait... backup in progress...
Backup is success
Press any key to continue . . .

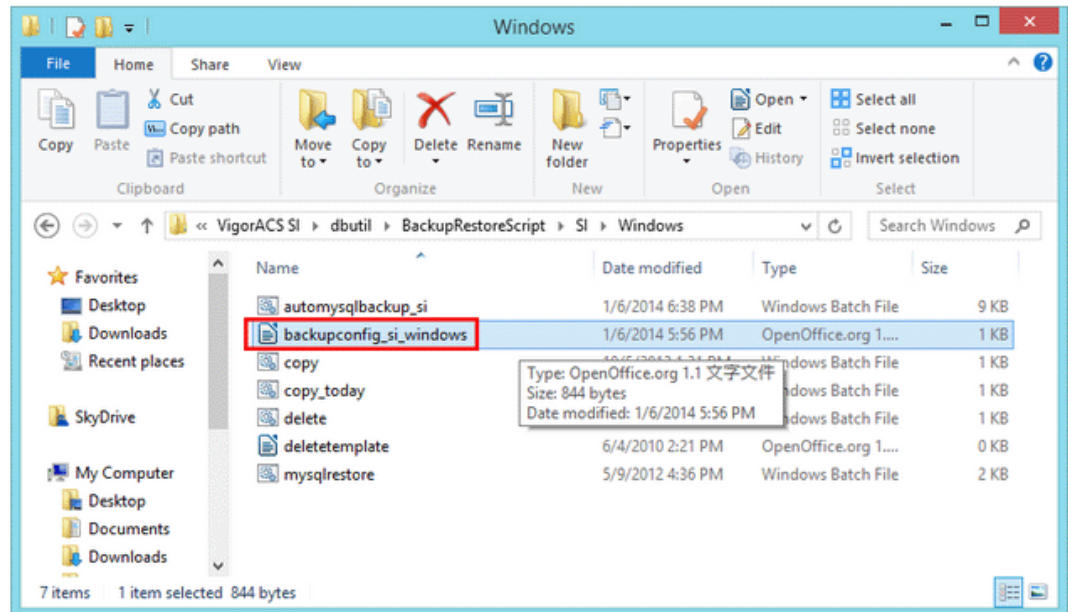
C:\Program Files\UigorACS SI\dbutil\BackupRestoreScript\SI\Windows>
```

4. Check the backup file just created.

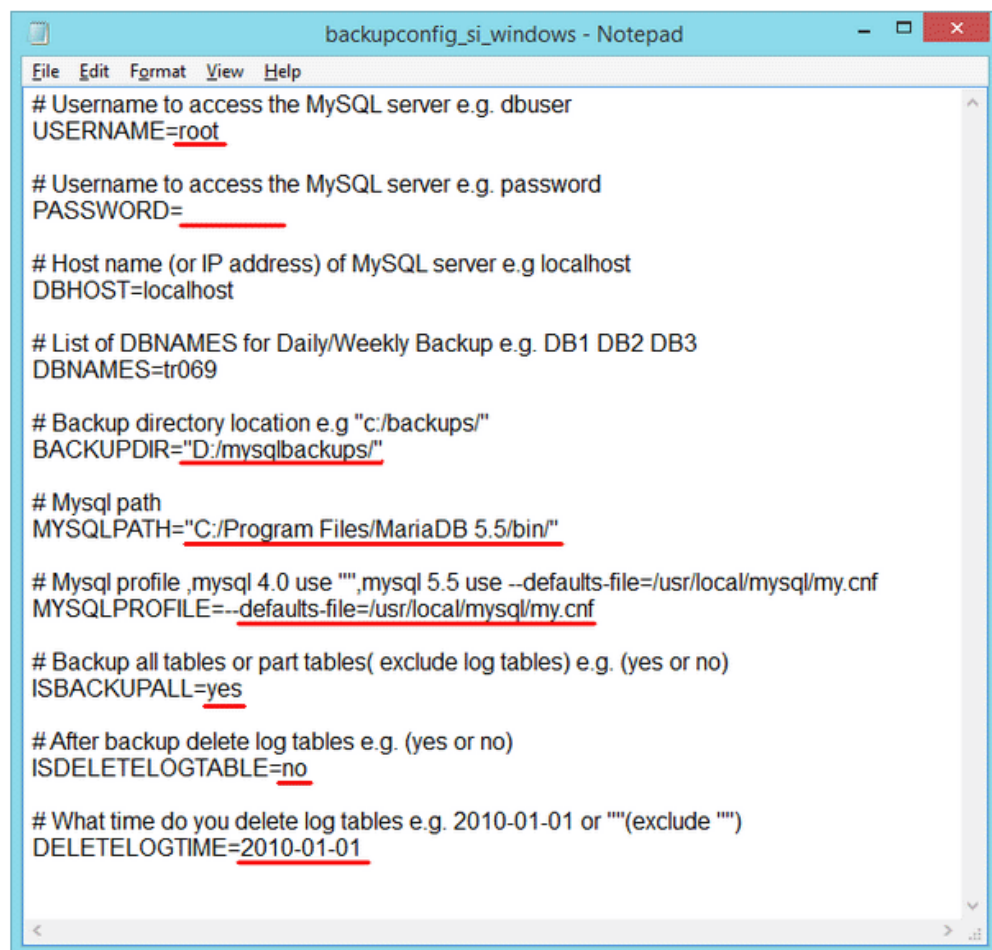


12.11.4 For Windows Platform – Backup by Schedule

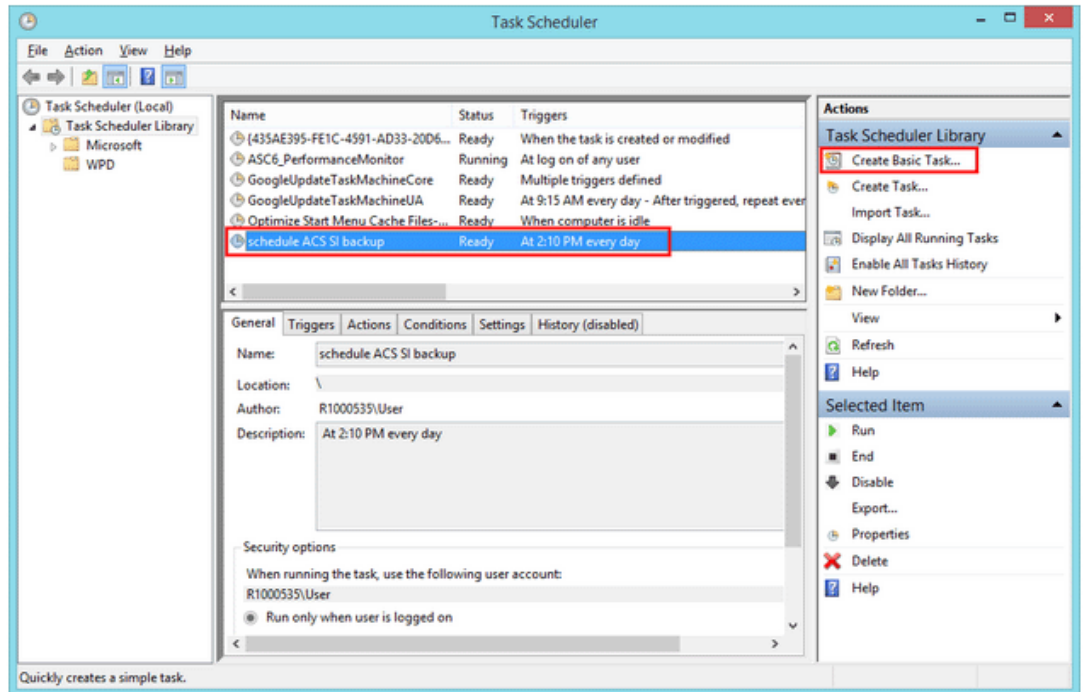
1. Edit file “backupconfig_si_windows.txt”.



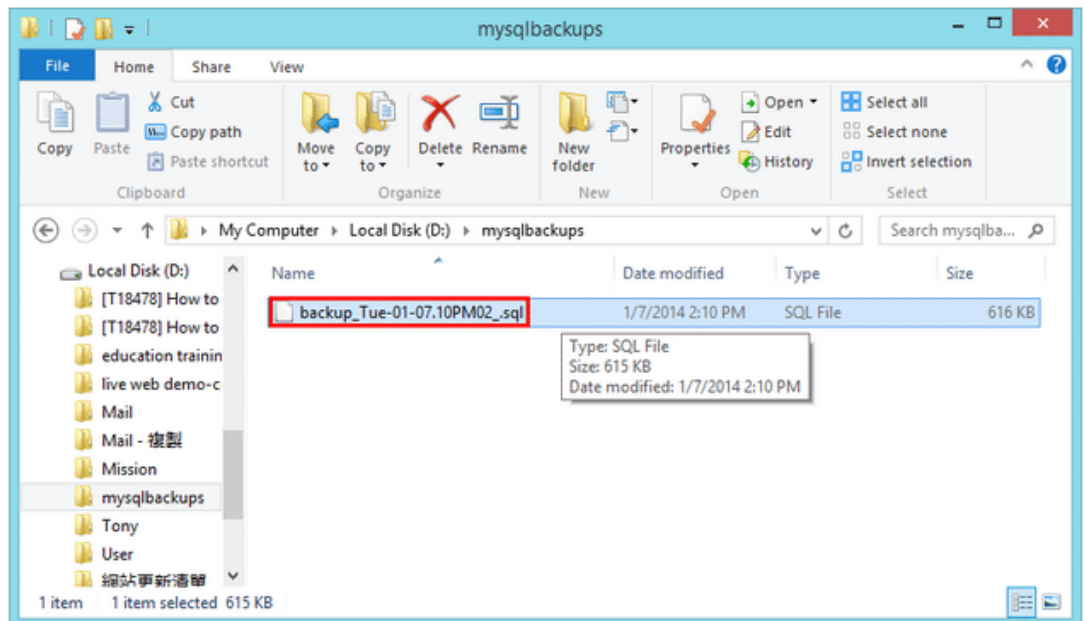
2. Confirm the parameters with red underlines are correct.



3. Create an ACS SI backup Task. In the following example we create a task to back up ACS SI once a day at 14:10.



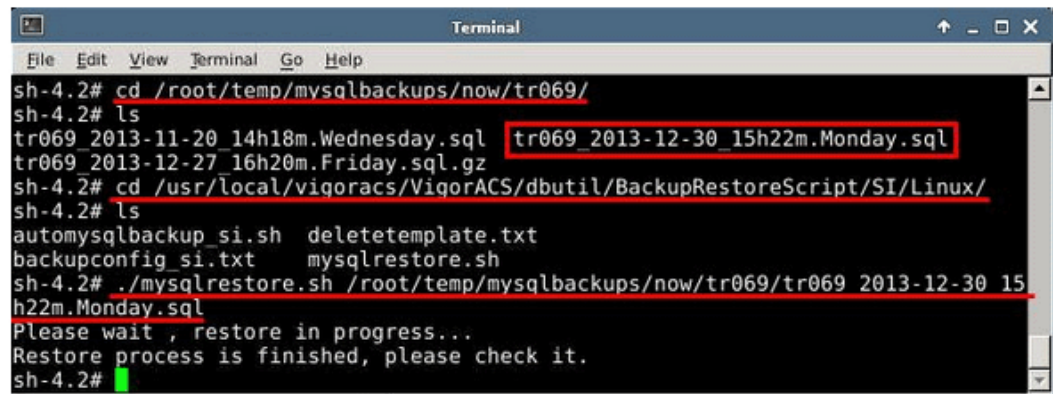
4. Check the file just created.



12.12 How to Restore the Database of VigorACS SI

For Linux Platform

1. Check your backup file path and name that you want to restore.
Note: If your file extension is “.gz”, please decompress it first. For example:
file path: /root/temp/mysqlbackups/now/tr069/
file name: tr069_2013-12-30_15h22m.Monday.sql
2. Change the path into “/usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/”.
3. Run "mysqlrestore.sh" to restore VigorACS SI database.
command: # ./mysqlrestore.sh
/root/temp/mysqlbackups/now/tr069/tr069_2013-12-30_15h22m.Monday.sql
4. Check the restore status.
5. You will see “Restore process is finished, please check it”.



```
sh-4.2# cd /root/temp/mysqlbackups/now/tr069/
sh-4.2# ls
tr069_2013-11-20_14h18m.Wednesday.sql tr069_2013-12-30_15h22m.Monday.sql
tr069_2013-12-27_16h20m.Friday.sql.gz
sh-4.2# cd /usr/local/vigoracs/VigorACS/dbutil/BackupRestoreScript/SI/Linux/
sh-4.2# ls
automysqlbackup_si.sh deletetemplate.txt
backupconfig_si.txt mysqlrestore.sh
sh-4.2# ./mysqlrestore.sh /root/temp/mysqlbackups/now/tr069/tr069_2013-12-30_15h22m.Monday.sql
Please wait , restore in progress...
Restore process is finished, please check it.
sh-4.2#
```

For Windows Platform

1. Check your backup file path and name (of VigorACS SI) that you want to restore. For example,
file path: D:\mysqlbackups\
file name: backup_Tue-01-07.57PM01_.sql
2. Change the path into
“C:\Program Files\VigorACS SI\dbutil\BackupRestoreScript\SI\Windows\”.
3. Run "mysqlrestore.sh" to restore database.
4. Check the restore status. You will see “Restore process is finished, please check it”.

```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\VigorACS SI\dbutil\BackupRestoreScript\SI\Windows>dir
Volume in drive C has no label.
Volume Serial Number is A202-D3A6

Directory of C:\Program Files\VigorACS SI\dbutil\BackupRestoreScript\SI\Windows

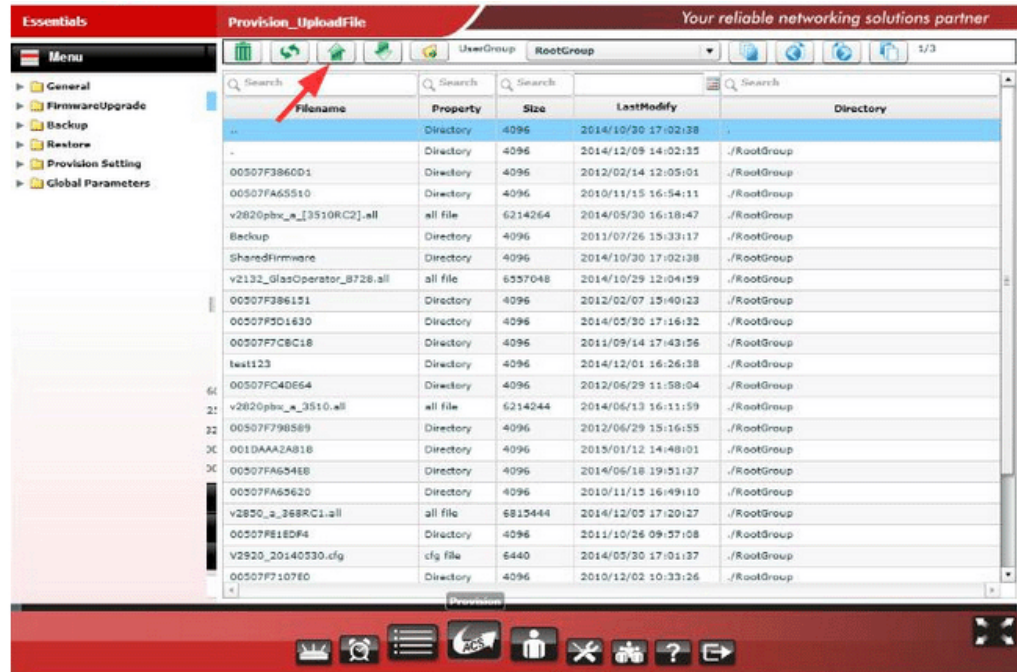
01/06/2014  06:38 PM    <DIR>          .
01/06/2014  06:38 PM    <DIR>          ..
01/07/2014  01:55 PM             8,674 automysqlbackup_si.bat
01/06/2014  05:56 PM             844 backupconfig_si_windows.txt
10/05/2012  01:31 PM             138 copy.bat
10/05/2012  03:05 PM             204 copy_today.bat
10/05/2012  01:30 PM             169 delete.bat
06/04/2010  02:21 PM              0 deletetemplate.txt
05/09/2012  04:36 PM             1,190 mysqlrestore.bat
              7 File(s)              11,219 bytes
              2 Dir(s)  61,779,529,728 bytes free

C:\Program Files\VigorACS SI\dbutil\BackupRestoreScript\SI\Windows>mysqlrestore.
bat D:\mysqlbackups\backup_Tue-01-07.57PM01_.sql
Please wait , restore in progress...
Restore process is finished, please check it.
Press any key to continue . . .
```

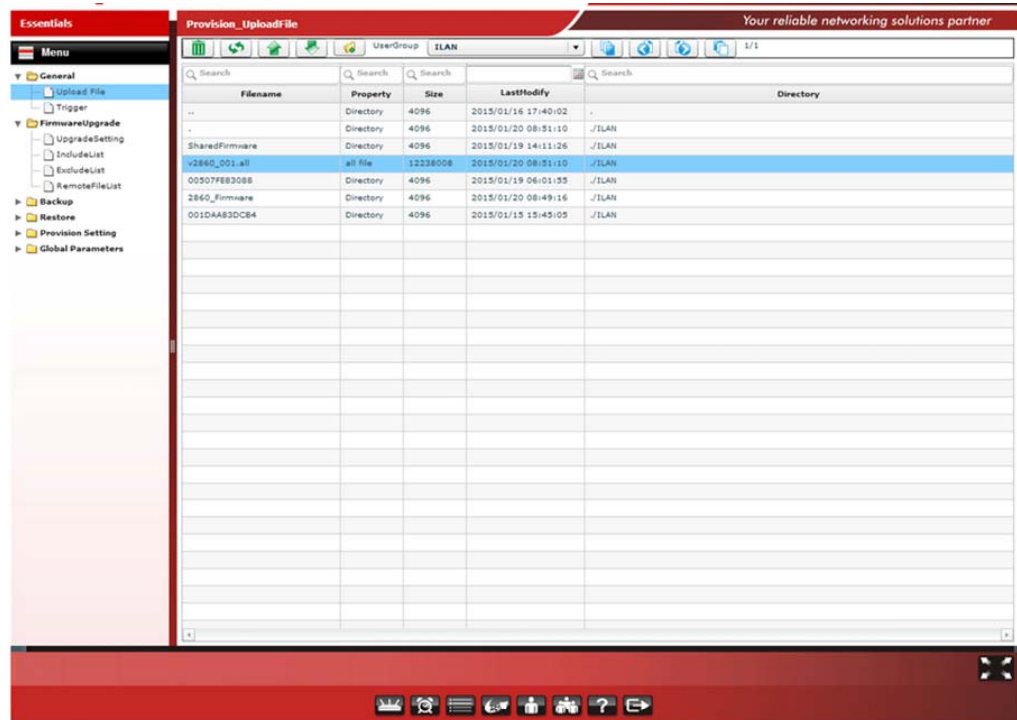

12.13 How to use VigorACS SI to do batch firmware upgrade

This document introduces how to do Batch Firmware Upgrade with VigorACS SI.

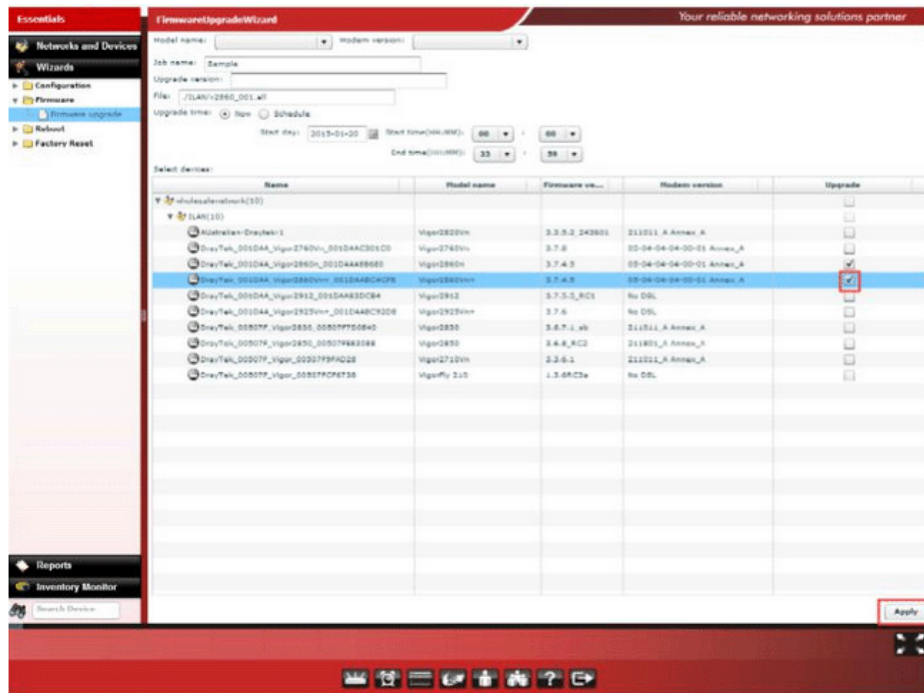
1. First, upload the firmware file to ACS server: Go to Provision, click on **Upload File** and select the firmware file for the Vigor routers.



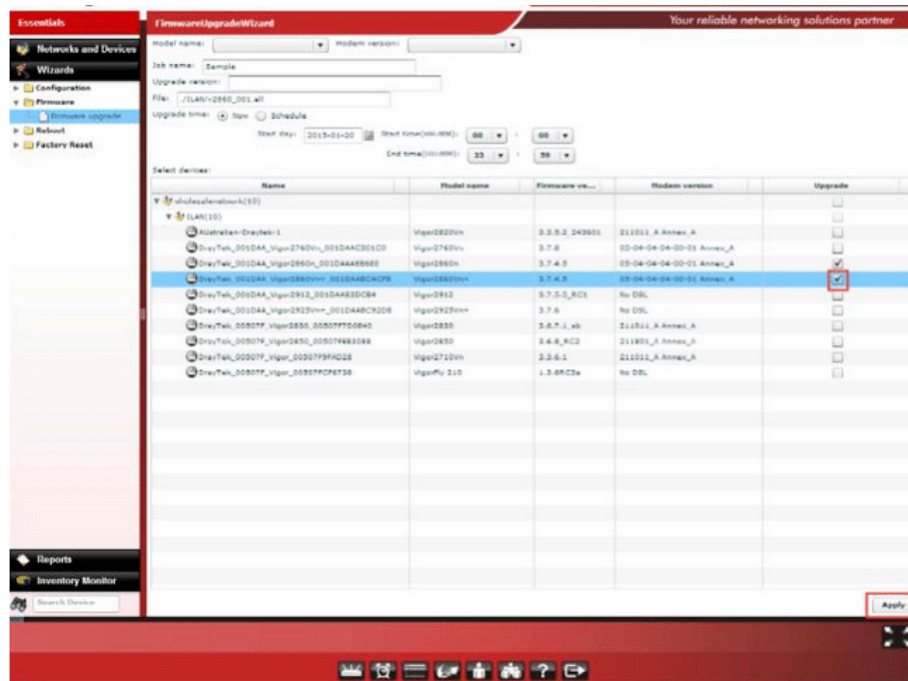
2. Users will see the file in the list once it is uploaded and ready for use.



3. Go to **Device >> Wizards >> Firmware >> Firmware upgrade.**



- Enter **Job name**.
 - Click on **File** and select the firmware file.
 - Set the **Upgrade Time**.
 - In **Select Devices**, find the devices which you want firmware upgrade to be done and check the Upgrade box.
 - Click **Apply** button to upgrade.
4. Go to **Log** to find out about the upgrade process. It will generate the step by step logs of firmware upgrade process from initial phase up to completion process.



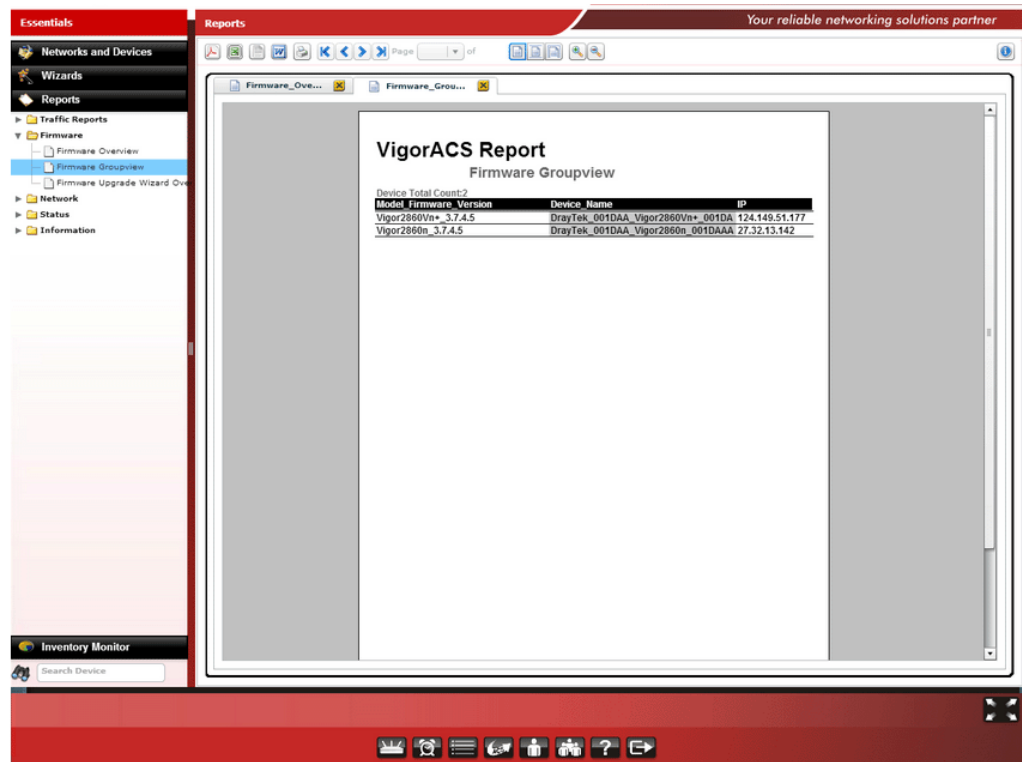
5. At the end of the upgrade process, users can generate the report by from **Device >> Reports >> Firmware >> Firmware Groupview**.

Log ID	Action	Device ID	Device Name	MAC Address	Device IP	Action ID	Time
421504	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177517	2015/01/20 12:16:57
421503	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177516	2015/01/20 12:06:19
421502	TransferComplete	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	113736	2015/01/20 12:05:08
421501	Reboot	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	1144	2015/01/20 12:05:08
421500	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177515	2015/01/20 12:05:07
421499	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177514	2015/01/20 12:03:25
421498	TransferComplete	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	113735	2015/01/20 12:02:39
421497	Reboot	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	1143	2015/01/20 12:02:38
421496	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177513	2015/01/20 12:02:37
421495	Download	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	137148	2015/01/20 12:00:39
421494	Download	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	137147	2015/01/20 12:00:32
421492	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177511	2015/01/20 11:31:16
421491	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177510	2015/01/20 11:27:42
421486	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177505	2015/01/20 09:46:35
421485	SetParameterValues	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	944	2015/01/20 09:46:33
421484	Inform	372	DrayTek_001DAA_Vigor2925Vn+_001D	001DAAAB8660	124.168.184.13	177504	2015/01/20 09:46:31
421459	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177488	2015/01/19 18:55:18
421458	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177487	2015/01/19 18:55:11
421457	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177486	2015/01/19 18:52:02
421456	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177485	2015/01/19 18:48:09
421455	TransferComplete	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	113731	2015/01/19 18:47:32
421454	Reboot	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	1139	2015/01/19 18:47:31
421453	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177484	2015/01/19 18:47:30
421452	Download	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	137143	2015/01/19 18:42:31
421450	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177482	2015/01/19 18:38:33
421449	SetParameterValues	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	943	2015/01/19 18:38:30
421448	SetParameterValues	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	942	2015/01/19 18:38:27
421447	SetParameterValues	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	941	2015/01/19 18:36:54
421446	SetParameterValues	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	940	2015/01/19 18:36:53
421445	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177481	2015/01/19 18:34:09
421444	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177480	2015/01/19 18:34:07
421441	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177478	2015/01/19 18:02:41

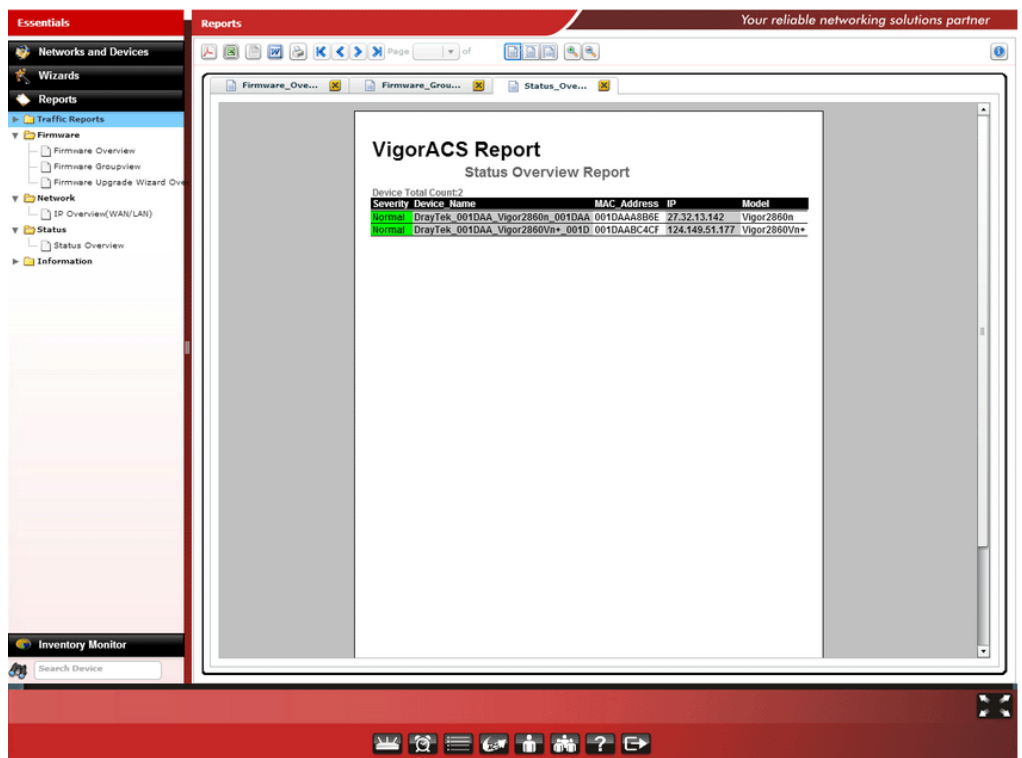
Select the device you want, check the **Report** box, and click **Apply**.

Log ID	Action	Device ID	Device Name	MAC Address	Device IP	Action ID	Time
421504	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177517	2015/01/20 12:16:57
421503	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177516	2015/01/20 12:06:19
421502	TransferComplete	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	113736	2015/01/20 12:05:08
421501	Reboot	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	1144	2015/01/20 12:05:08
421500	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177515	2015/01/20 12:05:07
421499	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177514	2015/01/20 12:03:25
421498	TransferComplete	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	113735	2015/01/20 12:02:39
421497	Reboot	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	1143	2015/01/20 12:02:38
421496	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177513	2015/01/20 12:02:37
421495	Download	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	137148	2015/01/20 12:00:39
421494	Download	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	137147	2015/01/20 12:00:32
421492	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177511	2015/01/20 11:31:16
421491	Inform	374	DrayTek_001DAA_Vigor2860Vn+_001D	001DAAAB8660	124.149.51.177	177510	2015/01/20 11:27:42
421486	Inform	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	177505	2015/01/20 09:46:35
421485	SetParameterValues	366	DrayTek_001DAA_Vigor2860n_001DAA	001DAAAB8660	27.32.13.142	944	2015/01/20 09:46:33
421484	Inform	372	DrayTek_001DAA_Vigor2925Vn+_001D	001DAAAB8660	124.168.184.13	177504	2015/01/20 09:46:31
421459	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177488	2015/01/19 18:55:18
421458	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177487	2015/01/19 18:55:11
421457	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177486	2015/01/19 18:52:02
421456	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177485	2015/01/19 18:48:09
421455	TransferComplete	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	113731	2015/01/19 18:47:32
421454	Reboot	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	1139	2015/01/19 18:47:31
421453	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177484	2015/01/19 18:47:30
421452	Download	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	137143	2015/01/19 18:42:31
421450	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177482	2015/01/19 18:38:33
421449	SetParameterValues	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	943	2015/01/19 18:38:30
421448	SetParameterValues	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	942	2015/01/19 18:38:27
421447	SetParameterValues	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	941	2015/01/19 18:36:54
421446	SetParameterValues	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	940	2015/01/19 18:36:53
421445	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177481	2015/01/19 18:34:09
421444	Inform	370	DrayTek_00507F_Vigor2830_00507FDD	00507FDD0E40	118.169.45.17	177480	2015/01/19 18:34:07
421441	Inform	367	DrayTek_00507F_Vigor2850_00507FEB	00507FEB3088	114.43.177.27	177478	2015/01/19 18:02:41

Then you will get the **Group Report**.



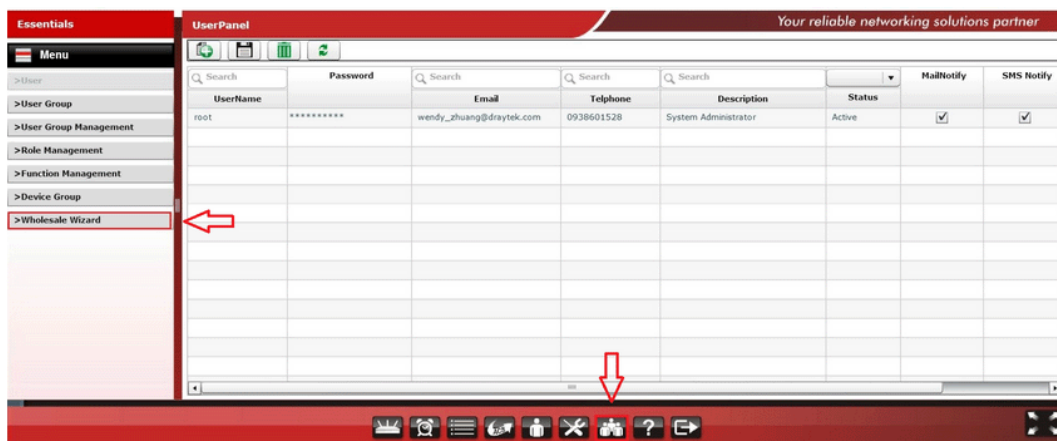
6. Similarly, you can generate **Status Report** from **Reports >> Status >> Status Overview** to check the status and severity of the connected devices.



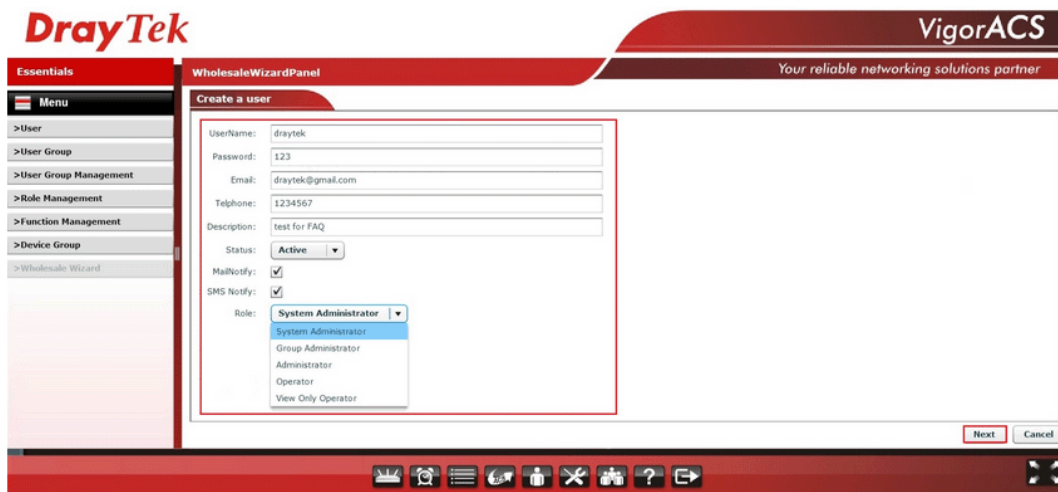
12.14 How to create user account and network group by Wholesale Wizard

This document demonstrates how to use Wholesale Wizard to create user account, user group and network.

1. Go to **User** page, click **Wholesale Wizard** to start to create user accounts.

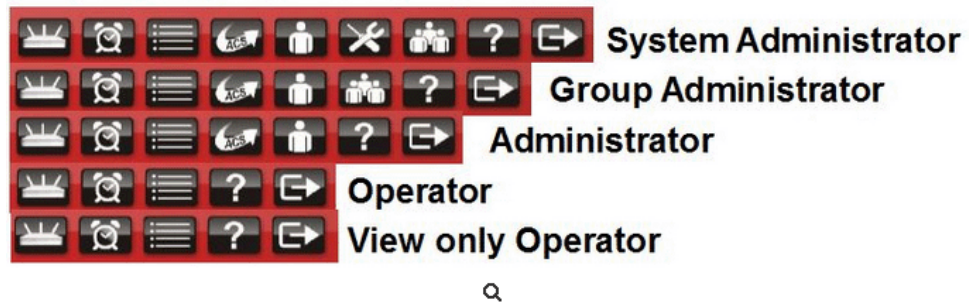


2. Setup the user account details:



- a. Type the Username and Password.
- b. Type the Email and telephone number if the user need to receive some logs by mail and message.
- c. Choose **Active** as status.
- d. Check the **Mail Notify** and **SMS Notify** if needed.
- e. Choose the role to give the account different level of authority.
- f. Click **Next**.

Note: The authority of each role is illustrated in the picture below.



3. Choose an existing group or create a new user group:

The screenshot shows the 'Create a user group' wizard in the DrayTek VigorACS SI User's Guide. The 'New group' tab is selected, and the 'test_group' name is entered. The 'EnableGlobalMailServer' checkbox is checked, and the 'Nodes' field is set to -1. The 'EnableExpireDate' checkbox is also checked, and the 'ExpireDate' is set to 2015/11/30. A calendar widget is visible for the 'ExpireDate' field.

- a. Type the group name.
- b. Check **EnableGlobalMailServer** if needed.
- c. Enter the maximum users of the group in the node field (Default is -1 which means there is no limits).
- d. If administrator wants to set the date when user access permission expires, enable **EnableExpireDate** then choose the **Expire Date**.
- e. Click **Next**.

4. Choose an existing network or create a new network:

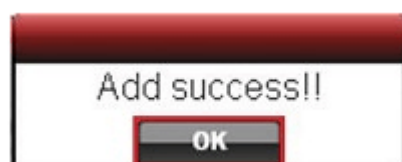
The screenshot shows the DrayTek Wholesale Wizard Panel. On the left is a sidebar with a menu. The main panel is titled 'WholesaleWizardPanel' and has a sub-tab 'Create a network'. There are two radio buttons: 'Existing network' and 'New network'. The 'New network' option is selected. Below it, there are several input fields: 'Parent Network' (a dropdown menu showing 'Network View'), 'NetworkName' (text box with 'test_network'), 'Location' (text box with 'draytek_6F'), 'User Name' (text box with 'test'), and 'Password' (text box with 'test').

- a. Choose one of the existing networks as the **Parent Network**.
- b. Type a brief description or address for the new network **Location**.
- c. Type the **User Name** and **Password** of the new network.
- d. Click **Next**.
5. Confirm the information of user, group and network in the summary page. Then click **Finish**.

The screenshot shows the DrayTek Wholesale Wizard Panel at the 'Summary' step. The sidebar menu is the same. The main panel is titled 'WholesaleWizardPanel' and has a sub-tab 'Summary'. It displays the following information:

- User:**
 - UserName: draytek
 - Password: 123
 - Email: draytek@gmail.com
 - Telephone: 1234567
 - Description: test for ACS
 - Status: Active
 - MailNotify: true
 - SMS Notify: true
 - Role: System Administrator
- Network:**
 - New network
 - Parent Network: Network View
 - NetworkName: draytek
 - Location: 6F
 - User Name: test
 - Password: test
- UserGroup:**

6. The prompt window pop up shows that update new user is successful.



7. Administrator could check the new user information in **User Panel**.

DrayTek **VigorACS**
Your reliable networking solutions partner

Essentials **UserPanel**

Menu

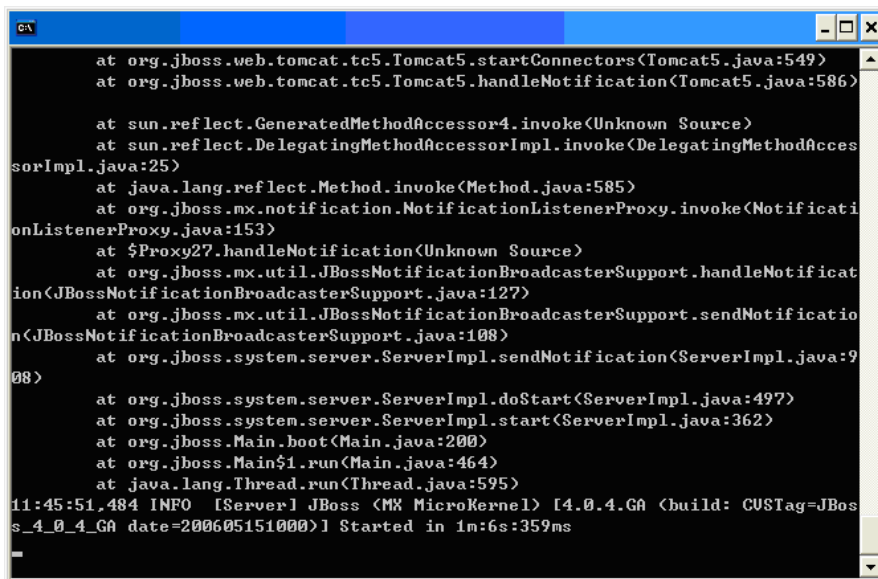
- >User
- >User Group
- >User Group Management
- >Role Management
- >Function Management
- >Device Group

Q Search	Password	Q Search	Q Search	Q Search		MailNotify	SMS Notify
UserName		Email	Telephone	Description	Status		
root	*****	wendy_zhuang@draytek.com	0938601528	System Administrator	Active	☒	☒
draytek	*****	draytek@gmail.com	1234567	test for ACS	Active	☒	☒

Chapter 13 Trouble Shooting

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 SI/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
sonListenerProxy.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: CVSTag=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.

13.1 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 14 Reference Information

14.1 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
```

14.2 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 SI

log: C:\Program Files\VigorACS SI\server\default\log\server.log
license key: C:\Program Files\VigorACS SI version\license.key
bind ip: C:\Program Files\VigorACS SI\bin\bindip.txt
mysql data: C:\mysql\data\tr069
start vigoracs : C:\Program Files\VigorACS SI\bin\StartVigorACS.bat
stop vigoracs : C:\Program Files\VigorACS SI\bin\ShutdownVigorACS.bat
```

