VigorACS3

Unified Management System

User's Guide

V1.1

VigorACS 3

Unified Management System User's Guide

Manual Version: V1.1 Date: March 29, 2022 Software Version: V3.2.0 © All rights reserved.

This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders. The scope of delivery and other details are subject to change without prior notice.

Microsoft is a registered trademark of Microsoft Corp.Windows 8, 10 and Explorer are trademarks of Microsoft Corp.Apple and Mac OS are registered trademarks of Apple Inc.DrayTek is a registered trademark of DrayTek Corp.Other products may be trademarks or registered trademarks of their respective manufacturers.

VigorACS 3 License

© All rights reserved.

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

Limited Warranty

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

Customer Remedies

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

No Other Warranties

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

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

Table of Contents

Part I		1
	Chapter 1 Introduction	2
	1.1 Main Features and Benefit	2
	1.2 System Architecture	
	1.3 Web Service	
	Chapter 2 Install & Startup	
	2.1 Platform for Windows 10	
	2.1.1 Installation for Java 2.1.2 Installation for MariaDB	
	2.1.2 Installation for VigorACS 3	
	2.1.4 StartMySQL/MariaDB Database	
	2.1.5 Start VigorACS	
	2.2 Platform for Linux	
	2.2.1 Installation for MariaDB, Java and VigorACS	
	2.2.2 StartMySQL/MariaDB Databse	
	2.2.3 Start InfluxDB	
	2.2.4 Start VigorACS	
	2.2.5 Edit VigorACS IP	
	2.3 Registering VigorACS	
	2.3.1 Registration for VigorACS via Windows Platform	
	2.3.2 Troubleshooting for Unstable CPE Status	
	Chapter 3 Getting Started	
	3.1 Accessing Web Page of VigorACS	41
	3.2 Dashboard	
	3.2.1 Dashboard for Root Network	
	3.2.2 Dashboard for a Network Group	
	3.2.3 Dashboard for a Device	
	3.2.4 Menu Bar	
	3.2.5 Root Network, Group Network, and Selected CPE	
	3.2.6 Capture Packets	
	3.2.7 Set Password, Two-factor Authentication, Change and Log Out	
	3.2.8 Auto Refresh, Manual Refresh, and Widget	
	3.2.9 Overviews	
	3.2.10 Icons Used in VigorACS 3	
	3.3 Operation Procedure	
	Applications A.1 How to Register a CPE onto VigorACS 3?	
	A.1 How to Register a Cre onto vigorACs S?	
	A.2 How to Assign a New Added CPE to a Network?	
	A.4 How to Create a New User Group?	
Part II		
	Chapter 4 SD-WAN Solution	
	4.1 Topology of SD-WAN, Edge Router and ACS Server	
	4.1.1 Enabling SD-WAN on VigorACS	
	4.1.2 Auto VPN	
	4.1.3 VoIP WAN	
	4.1.4 Full Traffic Control with the Route Policy	
	4.2 Dashboard for SD-WAN Network Group	
	4.3 Statistics for SD-WAN Network Group	
	4.4 Monitoring for SD-WAN Network Group	
	4.4.1 WAN (SD-WAN)	
	4.4.2 VPN (SD-WAN)	
	4.4.3 VoIP (SD-WAN)	
	4.4.4 Data Usage (SD-WAN)	
	Chapter 5 SD-WAN CPE	
	5.1 Dashboard for SD-WAN CPE	

	5.2 Statistics for SD-WAN CPE	92
	5.3 Monitoring for SD-WAN CPE	
	5.3.1 Alarm	
	5.3.2 Logs	
	5.3.3 Flow	
	5.3.4 Diagnostics	
	5.3.5 GPS	
	5.3.6 WAN (SD-WAN)	
	5.3.7 VPN (SD-WAN)	
	5.3.8 VoIP (SD-WAN)	
	5.3.9 Data Usage (SD-WAN)	
	5.4 Configuration Menu for SD-WAN CPE	
Part III		
	Chapter 6 System Menu	110
	Chapter 6 System Menu	
	6.1 Maintenance	
	6.1.1 Scheduled Backup	
	6.1.2 Configuration Restore	
	6.1.3 Firmware Upgrade	
	6.1.4 Device Reboot	
	6.1.5 System Password Reset	
	6.1.6 Schedule Profile	
	6.1.7 File Manager	
	6.1.8 Batch Activation	
	6.2 Reports	
	6.2.1 Report Tasks	
	6.2.2 Reports 6.3 Provisioning	
	6.3.1 Global Parameters	
	6.3.2 CPE Set Parameters	
	6.3.3 CPE Keep Parameters	
	6.3.4 Firmware Upgrade	
	6.4 Network Management	
	6.4.1 Setting	
	6.4.2 Map	
	6.5 System	
	6.5.1 System Parameter	
	6.5.2 Language	
	6.5.3 External Monitoring Server	
	6.5.4 Access Control	
	6.5.5 Clear Logs	
	6.5.6 Upload Serial Number	
	6.5.7 Google API Key	
	6.5.8 Certificate	
	6.5.9 Backup Database	
	6.5.10 Login Bulletin	
	6.5.11 Adverts Carousel	
	6.5.12 Logs 6.5.13 XMPP Profile	
	6.5.14 Delete Logs Actions	
	6.5.15 Server Support Settings	
	6.6 User	
	6.6.1 User Management	
	6.6.2 Group Management	
	6.6.3 Network Group	
	6.6.4 External Authentication Server	
	6.6.5 Mail Server	
	6.6.6 Function Management	
	6.6.7 Wholesale Wizard	
	6.6.8 SMS Server	
	6.6.9 SNMP Server	
	6.7 About VigorACS	
	6.7.1 License Information	
	6.7.2 License Mail Notify	

6.7.3 License Agreements	
Applications	
A.1 How to Create a Provision Profile with Global Parameters?	
A.2 How to Modify Provision Profile with Global Parameters?	
A.3 How to Create a Network for Managing Devices?	
A.4 How to Change the Network of a Device?	
A.5 How to Add a User?	
A.6 How to Add a Group?	
Part IV	
Chapter 7 Root Network Menu	
7.1 Dashboard for the Root Network	234
7.2 Monitoring	
7.2.1 Alarm	
7.2.2 Logs	
7.2.3 Devices	
7.2.4 Cellular Data Usage	
7.2.5 Floor Plan	
7.2.6 Rogue AP Detection	
7.3 Configuration	
7.3.1 VPN	
7.3.2 AP Profile	
Chapter 8 Network Group Menu	253
8.1 Dashboard for the Network Group	
8.2 Statistics for Network Group	
8.3 Monitoring for Network Group	
8.3.1 Alarm	
8.3.2 Logs	
8.3.3 Devices	
8.3.4 Clients	
8.3.5 Cellular Data Usage	
8.3.6 Floor Plan	
8.3.7 Rouge AP Detection	
8.3.8 WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN)	
8.4 Configuration Menu for Network Group, 8.4.1 VPN	
8.4.2 AP Profile	
8.4.3 Load Balance	
8.4.4 Route Policy (SD-WAN)	
8.4.5 VoIP WAN (SD-WAN)	
8.5 Hotspot Web Portal for SD-WAN Network Group	
8.5.1 Profile	
8.5.2 Quota Management	
8.5.3 Network & Devices	
8.5.4 Analytics	
Applications	
A.1 How to apply an AP profile to AP device(s)?	
Part V	
Chapter 9 Device Menu	
9.1 Dashboard for CPE	
9.1 Dashboard for CPE 9.2 Statistics for CPE	
9.2 Statistics for CPE	
9.3.1 Alarm	
9.3.2 Logs	
9.3.3 Diagnostics	
9.4 Configuration	
9.4.1 WAN	
9.4.2 LAN	
9.4.3 Hotspot Web Portal	
9.4.4 Routing	

9.4.5 NAT	355
9.4.6 Hardware Acceleration	
9.4.7 Firewall	
9.4.8 User Management	
9.4.9 Object Setting	
9.4.10 QoS	
9.4.11 Applications	400
9.4.12 VPN	418
9.4.13 Mesh	430
9.4.14 Wireless LAN	433
9.4.14 Bandwidth Management	446
9.4.15 USB Applications	451
9.4.16 System	455
9.4.17 Switch	469
9.4.18 Advanced	481

Part I

Introduction



Chapter 1 Introduction

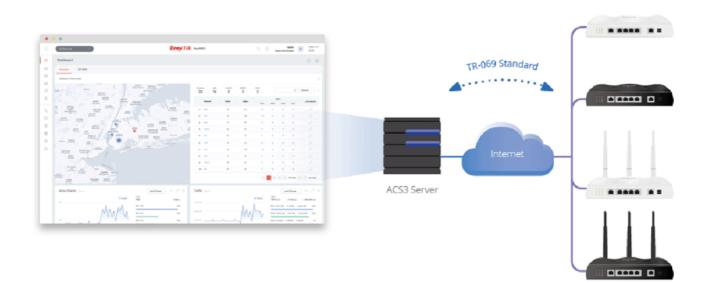
VigorACS 3 is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway, wireless AP **and switch**. VigorACS 3 has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore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

1.1 Main Features and Benefit

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

1.2 System Architecture

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



1.3 Web Service

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

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

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

Corresponding files are placed in -WebServices_TR069API.zip

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

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

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

This page is left blank.

Chapter 2 Install & Startup

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

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

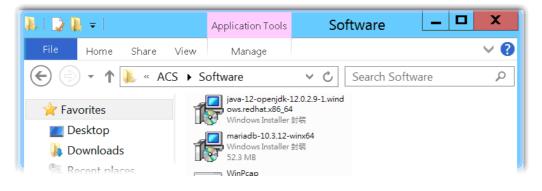
2.1 Platform for Windows 10

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

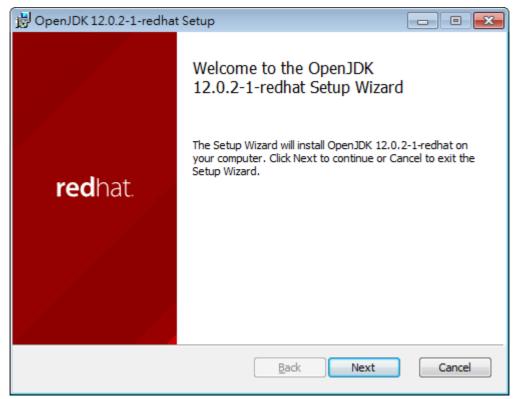
- (I) Installation for Java,
- (II) Installation for MariaDB
- (III) Installation for VigorACS 3
- (IV) Start MySQL/MariaDB Database.
- (V) Edit VigorACS ip.
- (VI) Start VigorACS.

2.1.1 Installation for Java

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



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



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

B OpenJDK 12.0.2-1-redhat Setup	
End-User License Agreement	
Please read the following license agreement carefully	
The GNU General Public License (GPL)	<u>_</u>
Version 2, June 1991	
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA	
Everyone is permitted to copy and distribute verbatim copies of license document, but changing it is not allowed.	this
Preamble	
The licenses for most software are designed to take a way your	freedom 👻
✓ I accept the terms in the License Agreement	
Print Back Next	Cancel

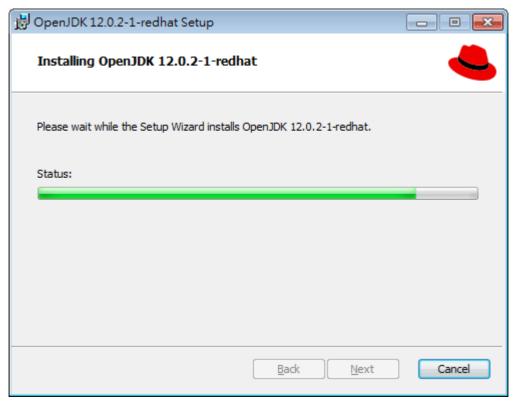
4. In this page, optional features will be listed for you to specify the destination folder for JAVA driver installation. Choose the one you need and click **Next**.

😼 OpenJDK 12.0.2-1-redhat Setup				
Custom Setup Select the way you want features to be installed.				
Click the icons in the tree below to change the way features will be installed.				
OpenJDK Runtime Mission Control	OpenJDK 12 runtime files.			
	This feature requires 314MB on your hard drive. It has 2 of 5 subfeatures selected. The subfeatures require 3KB on your hard drive.			
Location: C:\Program Files\RedHat\java-12-openjdk-12.0.2-1\ Browse				
Re <u>s</u> et Disk <u>U</u> sage	Back Next Cancel			

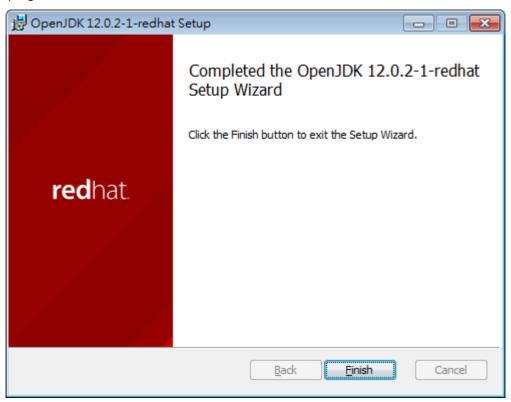
5. In the following page, just click **Install.**

B OpenJDK 12.0.2-1-redhat Setup	
Ready to install OpenJDK 12.0.2-1-redhat	
Click Install to begin the installation. Click Back to review or change any of installation settings. Click Cancel to exit the wizard.	' your
	Cancel

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

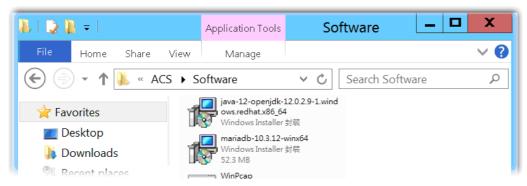


7. When the following page appears, the installation is completed. Click **Finish** to exit the installing program.



2.1.2 Installation for MariaDB

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



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

🛃 MariaDB 10.3 (x64) Setup	
MariaDB'	Welcome to the MariaDB 10.3 (x64) Setup Wizard The Setup Wizard will install MariaDB 10.3 (x64) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel

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

岃 MariaDB 10.3 (x64) Setup	
End-User License Agreement Please read the following license agreement carefully	MariaDB Server
GNU GENERAL PUBLIC LICENSE	<u>^</u>
Version 2, June 1991	
Copyright (C) 1989, 1991 Free Software Foundation Street, Fifth Floor, Boston, MA 02111-1301, USA to copy and distribute verbatim copies of this licer changing it is not allowed.	Everyone is permitted
Preamble	
The licenses for most software are designed to tal	ke away your freedom
☑ accept the terms in the License Agreement	
Print Back	Next Cancel

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

🗒 MariaDB 10.3 (x64) Setup				
Custom Setup Select the way you want features to be installed.	MariaDB Server			
Click the icons in the tree below to change the way features will be installed.				
Image: Server Image: Server Image: Server	Install server This feature requires 161MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 49MB on your hard drive.			
Location: C:\Program Files\MariaDB 10.3\	Browse			
Re <u>s</u> et Disk <u>U</u> sage	Back Next Cancel			

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

🗒 User settings	- 0 🐱			
Default instance properties MariaDB 10.3 (x64) database configuration	MariaDB Server			
Modify password for database user 'root' New root password:	Enter new root password			
Confirm: Enable access from remote machines 'root' user	Retype the password			
Use UTF8 as default server's character set				
	Back Next Cancel			

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

🛃 Database settings				• *	
Default instance properties MariaDB 10.3 (x64) database configuration		on	MariaDB Server 2	A	
✓ Install as service Service Name:	MySQL				
CP port:	3306				
Innodb engine settings					
Buffer pool size:	983 MB				
Page size:	16 🔻 KB				
		<u>B</u> ack	Next Ca	ancel	

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

ট MariaDB 10.3 (x64) Setup	×
MariaDB 10.3 (x64) setup Submit usage information	MariaDB Server
Enable the Feedback plugin and submit anonym Monty Program has created a Feedback plugin for Maric collects basic anonymous statistical information. This in developers to improve MariaDB. Enabling this plugin is a MariaDB development. Collected statistics, and more in can be viewed at http://mariadb.org/feedback_plugin More Info	formation is used by the an easy way to help with
Back	Next Cancel

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

😸 MariaDB 10.3 (x64) Setup	- • •
Ready to install MariaDB 10.3 (x64)	MariaDB Server
Click Install to begin the installation. Click Back to review or installation settings. Click Cancel to exit the wizard.	r change any of your
Back	🚱 Install Cancel

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

😸 MariaDB 10.3 (x64) Setup	
Installing MariaDB 10.3 (x64)	MariaDB Server
Please wait while the Setup Wizard installs MariaDB 10.3 (x6	;4).
Status:	
Back	<u>N</u> ext Cancel

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

🛃 MariaDB 10.3 (x64) Setup	
	Completed the MariaDB 10.3 (x64) Setup Wizard
S	Click the Finish button to exit the Setup Wizard.
MariaDB'	
	Back Einish Cancel

2.1.3 Installation for VigorACS 3

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

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

🔍 🔀 🕄 =	ACS			- 0 X
File Home Share	View			v 😮
🗲 🕘 🗸 🚹 👢 « ACS	S > ACS	× ¢	Search ACS	Q
☆ Favorites	Name	•		Date modi
🗾 Desktop 🚯 Downloads	iller setup			6/17/2016
laces 😓 Recent places				

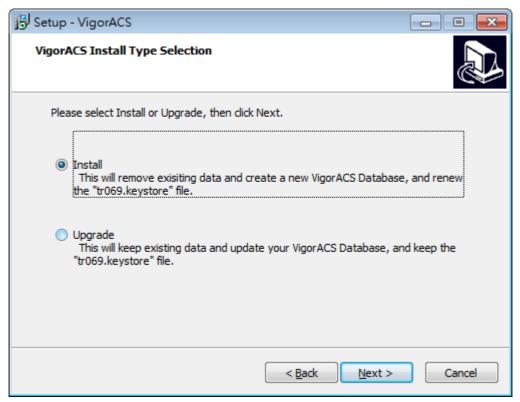
2. When the following dialog appears, choose **Local Database / Remote Database** and click **Next**.

🔂 Setup - VigorACS	x
Database Access Type Selection	
Please select Local Database if you want to update or install the TR069 database on the local MySQL, or select Remote Database if the MySQL database is on a remote host. You will be asked for the connection details later.	
Choose the one you need, and dick Next.	
 Local Database * Create or update a local database on this host. 	
 Remote Database * Connect to an existed database after finishing the installation procedure. 	
Next > Canc	el

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

15 Setup - VigorACS	- • •
Select MySQL/MariaDB Install Path	
Please specify the installation folder of MySQL/MariaDB and then click	Next button.
C:\Program Files\MariaDB 10.3	Browse
< <u>B</u> ack <u>N</u> ext	> Cancel

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



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

🕞 Setup - VigorACS	
MySQL/MariaDB Account Setting	
Please specify password of root of MySQL/ MySQL/MariaDB database has not been cor root password	MariaDB, this step can be ignored if nfigured.
confirm root password	
	_Check password
	< Back Next > Cancel
谒 Setup - VigorACS	
B Setup - VigorACS	
The InfluxDB Install Path as below	Browse
The InfluxDB Install Path as below	
The InfluxDB Install Path as below	
The InfluxDB Install Path as below	
The InfluxDB Install Path as below	
The InfluxDB Install Path as below	

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

🕞 Setup - VigorACS	- • •
Maximum And Minimum Memory What is your maximum and minimum memory?	
Please specify your maximum and minimum memory, then click Next.	
Maximum Memory: (Default maximum memory is 1024MB)	
1024	
Minimum Memory: (Default minimum memory is 900MB, can not be less than 900MB)	
900	
< Back Next >	Cancel

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

🕞 Setup - VigorACS	
System Settings	
By default, the port number is same for the VigorACS portal and CPE con	nmunication.
Use same port number for the VigorACS portal and CPE communication	on.
\bigcirc Use different port for the VigorACS portal and CPE communication.	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

🚰 Setup - VigorACS		
HTTP And HTTPS Port What is your HTTP and HTTPS port?		
Please specify your HTTP and HTTPS port,	then dick Next.	
HTTP Port:		
HTTPS Port: 443		
	< <u>B</u> ack Nex	kt > Cancel
🔁 Setup - VigorACS		- • •
Setup - VigorACS STUN And Syslog Port What is your STUN and Syslog port?		
STUN And Syslog Port	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port:	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port: 3478	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port:	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port: 3478 Syslog Port:	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port: 3478 Syslog Port:	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port: 3478 Syslog Port:	then click Next.	
STUN And Syslog Port What is your STUN and Syslog port? Please specify your STUN and Syslog port, STUN Port: 3478 Syslog Port:		cancel

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

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

🔂 Setup - VigorACS
JBoss Configuration Selection The JBoss configuration which VigorACS used for Web and CPE communication.
For enhanced security select TLS 1.3 (standalone-secure.xml) For security and compatibility with existing CPEs we recommend TLS 1.2 (standalone.xml) For compatibility with older legacy CPEs use TLS 1.0 (standalone-compatible.xml)
Choose the one you need, then dick Next.
 standalone-secure.xml * Supported Protocols: TLS 1.3 only standalone.xml (Recommended) * Supported Protocols: TLS 1.2 only
 standalone-compatible.xml * Supported Protocols: TLS 1.0 or above
< <u>B</u> ack <u>N</u> ext > Cancel

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

🔂 Setup - VigorACS	- • •
Select Vigoracs user home path	
Please specify the installation folder of Vigoracs user home and then on This folder is for storing the statistics and configurations	lick Next button.
C:\Users\Carrie\AppData\Roaming	Browse
< <u>B</u> ack Next	> Cancel

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

🔂 Setup - VigorACS	- • •
Select Destination Location Where should VigorACS be installed?	
Setup will install VigorACS into the following folder.	
To continue, click Next. If you would like to select a different folder, cli	ck Browse.
C:\Program Files\VigorACS	Browse
At least 585.3 MB of free disk space is required.	
< <u>B</u> ack Next >	Cancel

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

🔂 Setup - VigorACS	- • •
Select Start Menu Folder Where should Setup place the program's shortcuts?	
Setup will create the program's shortcuts in the following Start I	Menu folder.
To continue, click Next. If you would like to select a different folder, click	Browse.
VigorACS	Browse
< <u>B</u> ack Next >	Cancel

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

🔂 Setup - VigorACS	- • •
Select Additional Tasks Which additional tasks should be performed?	
Select the additional tasks you would like Setup to perform while installing then click Next.	VigorACS,
Additional shortcuts:	
Create a desktop shortcut	
Other tasks:	
Allow VigorACS access through Windows Firewall (Recommended)	
< <u>B</u> ack <u>N</u> ext >	Cancel

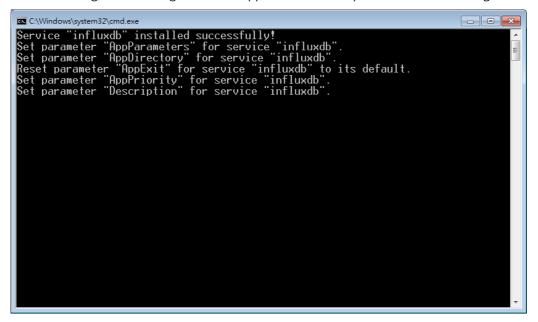
14. Now, the program is ready to install necessary features and files to your computer. Please click **Install** to start.

Setup - VigorACS	• 💌
Ready to Install Setup is now ready to begin installing VigorACS on your computer.	
Click Install to continue with the installation, or click Back if you want to review or change any settings.	
Destination location: C:\Program Files\VigorACS	*
Start Menu folder: VigorACS	
Additional tasks: Additional shortcuts: Create a desktop shortcut Other tasks: Allow VigorACS access through Windows Firewall (Recommended)	
٠	-
< <u>B</u> ack Install	Cancel

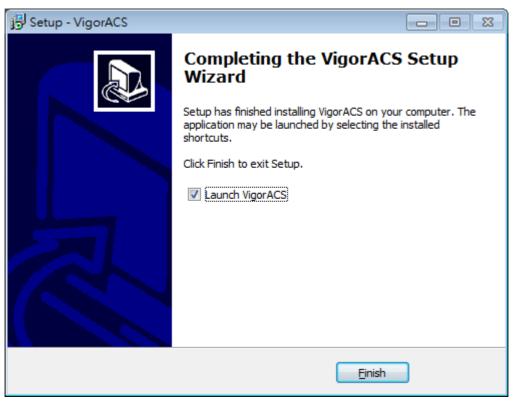
15. Please wait for a while to complete the installation.

🔂 Setup - VigorACS	- • •
Installing Please wait while Setup installs VigorACS on your computer.	
Extracting files C: \Users\Carrie\AppData\Local\Temp\is-OEDPE.tmp\bin\influx_stress.exe	
	Cancel

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



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



2.1.4 StartMySQL/MariaDB Database

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

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

2.1.5 Start VigorACS

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

	⊕ EN ~
	VigorACS
	User Name root
	Password •••••••
Dray Tek	Validation Code 5817
	Remember me 5 8 1 7
	Login

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



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

	Root Network	Dro	y <i>Tek</i> VigorAC	S 3			🖬 Ca	pture Pac	kets 🗸	Syst	car em Administra	
3	Dashboard								Aut	o Refresh	1 : 1 Minute	• C
~	Map Overview		×	Network Overvie	ew							- 2
		elwerdendiesje Zuldwo ddepoel	olde []	Network 53	Online						Q Network *	
		Beiju	um Ga	Network	Online	Offline	01		larm			Go To Dashboard
3	南霍倫 Zuidhorn Slaperstil		NOORDDIJK	Network	Unline	Offline	Total	WAN	VPN	LAN	Go To Dashi	board
	Zuiderburen Hoogemeeden	DE HOOSTE KORREWESWLJK Paddepoel	Lewenborg	Root Network	68	172	172	0	0	0		
2	Den Horn	VINGHUZEN 格羅寧根		RD8	27	22	22	0	0	0	8	
<u>ല</u>	Enumatil Lagemeeden Hoockarik	Groningen	11	RD7	0	15	15	0	0	0	8	
Ð	De Poffert		Oude Roodehaan	Shanghai	0	15	15	0	0	0	8	
<pre>S</pre>	Gem Leek Matsloot	Helpman		dvcom_kuwait	2	10	10	0	0	0	0	
5	ettelbert	Helpman	Essen, A	RD3	4	9	9	0	0	0	0	
	ettelbert	T.S. M.S.		AnPhat_VN	2	7	7	0	0	0	8	
i)	Sandebuur Roderwolde	Eelderwolde Nijveensterkolk	十 哈倫 Haren Oos 一,	VISUS	1	4	4	0	0	0	P	
		Hoornsedi 020 GeoBasis-DE/BKG (©2009) 使用	ik 用條款 回報地圖錯誤									
	Active Clients Top 20	() Last 24 hou	urs~ — 🖉 X	Traffic - Top 20						۹L	ast 24 hours 🗸	- 2
	Total 25 100 %	RD3 / 0	0%	Total 258.79 GB	î 31.23 (GB ↓ 227 GB GB	.56	RD	3 / 177.58	GB↑ 30.4	40 GB↓ 147.17	GB 69%
	125 • Total	RD2 / 14	56%	9.31 GB		• Tot	al	20	2 / 70 05 /	TD + 494	40 MB↓ 79.38 0	50
	75 MMM MMMMMM	attel / 9	36%	7.45 GB				ND.	2779.00	20 1 404.	-o mo - 75.30 (31%
	50	RD1/2	8%	5.59 GB 3.73 GB		1		RD	1 / 820.90	MB † 47.	21 MB↓ 773.69	9 MB 096

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

2.2 Platform for Linux

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

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

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

2.2.1 Installation for MariaDB, Java and VigorACS

Follow the steps listed below to install VigorACS under Linux:

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

```
#bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2 | tar xvf -
```

or

```
#tar -jxv -f VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2
```

3. Decompress the setup packages

bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2 |tar xvf -



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

chmod 755 ./install.sh

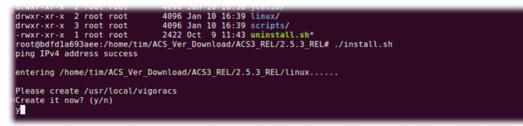
chmod 755 ./uninstall.sh

- 1	- rw- r r	. root root 1807 Oct 9 11:39 Install VigorACS Guide.txt
	-rw-rr	. root root 2972 Oct 9 11:39 Quick Start Guide.txt
	- rw- rw- r	. 1000 1000 1337654060 Jan 10 16:18 VigorACS_Unix_Like_Draytek_Pro64_2.5.3_r13188.tar.bz2
	drwxr-xr-x	root root 4096 Jan 10 16:38 acs/
	-rw-rr	. root root 10968 Oct 17 01:00 acs_lib.sh
	drwxr-xr-x	root root 4096 Jan 10 16:38 font/
	-rw-rr	root root 631 Oct 9 11:39 install.conf
	-rw-rr	root root 64660 Oct 31 11:10 install.sh
	drwxr-xr-x	root root 4096 Jan 10 16:38 jcelib/
	drwxr-xr-x	root root 4096 Jan 10 16:39 linux/
	drwxr-xr-x	root root 4096 Jan 10 16:39 scripts/
	-rw-rr	root root 2422 Oct 9 11:43 uninstall.sh
	root@bdfdla	<pre>i3aee:/home/tim/ACS_Ver_Download/ACS3_REL/2.5.3_REL# chmod 755 install.sh</pre>
	root@bdfdla	Baee:/home/tim/ACS_Ver_Download/ACS3_REL/2.5.3_REL# chmod 755 uninstall.sh
	root@bdfd1a	<pre>3aee:/home/tim/ACS_Ver_Download/ACS3_REL/2.5.3_REL#</pre>
	1001@001019	Saee:/nome/lim/ACS_ver_Download/ACS3_KEL/2.5.3_KEL#

5. Execute ./install.sh installation file.

- rw- r r	1	root	root	631	0ct	9	11:39	install.conf
-rwxr-xr-x	1	root	root	64660	0ct	31	11:10	install.sh*
drwxr-xr-x	2	root	root	4096	Jan	10	16:38	jcelib/
drwxr-xr-x	2	root	root	4096	Jan	10	16:39	linux/
drwxr-xr-x	3	root	root	4096	Jan	10	16:39	scripts/
-rwxr-xr-x	1	root	root	2422	0ct	9	11:43	uninstall.sh*
root@bdfd1a	693	aee:/	/home/t	im/ACS_Ve	r_Do	vnlo	bad/AC	53_REL/2.5.3_REL# ./install.sh
ping IPv4 a	ddr	ess s	success					
entering /h	ome	/tim/	ACS_Ve	r_Download	I/AC	53_F	REL/2.	5.3_REL/linux

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



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



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



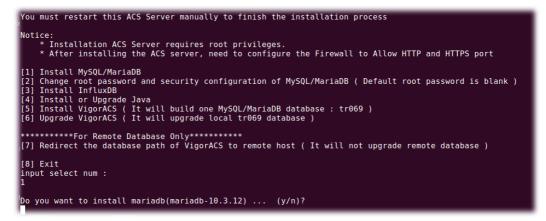
- (1) Install MySQLI/MariaDB
- (2) Change root password and security configuration of MySQLI/MariaDB
- (3) Install InfluxDB
- (4) Install or Upgrade java
- (5) Install VigorACS
- (6) Upgrade VigorACS
- (7) Redirect the database path of VigorACS to remote host
- (8) Exit

input select num :

- (i) If your computer has installed MariaDB and java previously, ignore the installation of them. Otherwise, install all the required items (MariaDB, Java and VigorACS) for your system. Item number 6 is used to upgrade VigorACS, so it is not necessary for you to execute for the first time of installation.
- 9. Input 1 to install MariaDB first. Notice that it will setup blank as default password. You can change the password by using the following command.

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

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



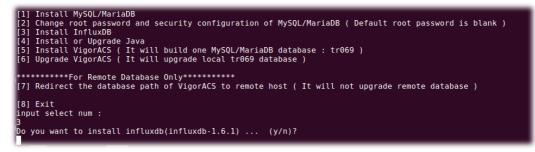
Follow the instructions on the screen to finish the MariaDB installation.

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



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

11. Input 3 to install InfluxDB.



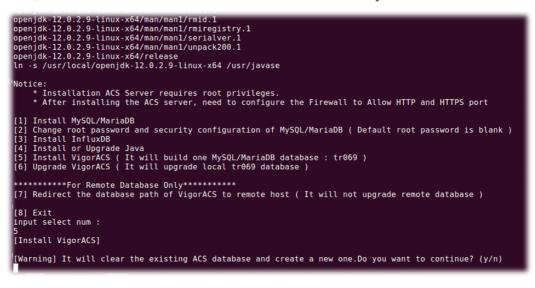
Follow the instructions on the screen to finish the InfluxDB installation.

12. Input 4 to install Java.

ln -s /usr/local/InfluxDB/bin influxdb
If you upgrade the ACS (from the version before 2.4.0) for the first time, please remember to run the rrd2influxdb tool to convert the existed/old data after ACS upgrade. It will on the /usr/local/vigoracs/VigorACS/convert_rrd2_Influxdb/ path.For more explanation, you may refer the /usr/local/vigoracs/VigorACS/convert_rrd2_Influxdb/readme.txt document.
Notice: * Installation ACS Server requires root privileges. * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port
* Alter Installing the ACS server, need to configure the Firewall to Altow HTTP and HTTPS port [1] Install MySOL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB (Default root password is blank) [3] Install InfluxDB
[4] Install or Upgrade Java [5] Install VigorACS (It will build one MySQL/MariaDB database : tr069) [6] Upgrade VigorACS (It will upgrade local tr069 database)
*********For Remote Database Only********* [7] Redirect the database path of VigorACS to remote host (It will not upgrade remote database)
[8] Exit input select num :
Do you want to install jdk(openjdk-12.0.2.9) (y/n)?

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

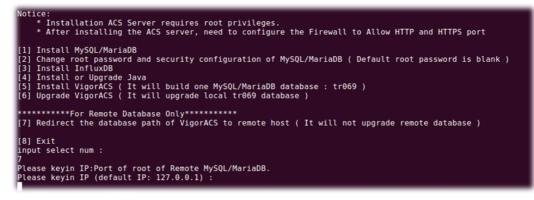
13. Input 5 to install VigorACS. It is suggested to use ACS customized MariaDB database. When asked to enter MariaDB password, press "Enter" if you haven't changed the password via the command. Then, confirm that TR-069 database has been installed successfully.



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



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



15. Input 7 to finish and exit the installation.

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

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

2.2.2 StartMySQL/MariaDB Databse

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



2.2.3 Start InfluxDB

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



Select item 3 to start InfluxDB.

2.2.4 Start VigorACS

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



Select item 5 to start VigorACS.

Mysql process id : 1286 1388 InfluxDB process id : 1430 VigorACS process id :
1. Start Mysql/MariaDB 2. Shutdown Mysql/MariaDB 3. Start InfluxDB 5. Start VigorACS 5. Start VigorACS 7. Edit bind IP of VigorACS Server (please keyin IP or servername) 8. Memory Configuration 9. Port Configuration 10. exit Input select num :
Which HTTP port do you want to bind for VigorACS service (port number or Enter for 80 port)?
Which HTTPS port do you want to bind for VigorACS service (port number or Enter for 443 port)?
Which ip address do you want to bind for VigorACS service (x.x.x.x or Enter for bind 0.0.0.0 address)?
Which STUN port do you want to bind for VigorACS service (port number or Enter for 3478 port)?
Which syslog port do you want to bind for VigorACS service (port number or Enter for 514 port)?
How many memory do you want to set for VigorACS service? (Enter for default MAX Memory is 1024, MIN Memory is 900 MB) MAX Memory What you want? (Unit: MB)
MIN Memory What you want? (Unit: MB)
* Starting WildFly Application Server vigoracs

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

2.2.5 Edit VigorACS IP

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

2.3 Registering VigorACS

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

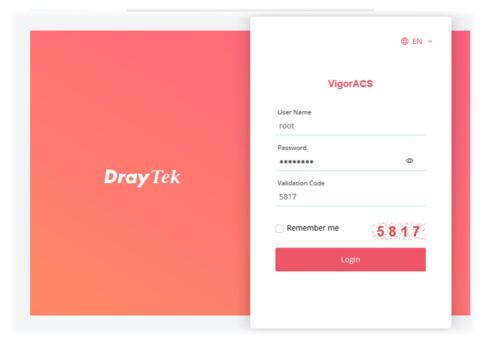
(i) While installing VigorACS, install program will register MySQL/MariaDB to Windows Service. MySQL/MariaDB will startup automatically after installing VigorACS or rebooting system. Normally, you don't need to worry about this step on Windows. But if you find any problems on VigorACS, you should check mysql/mariadb first. Please go to Windows Service check the MySQL/MariaDB Service starts or not.

After installing VigorACS, the software will startup automatically. Normally, you don't need to worry about this step on Windows. But, if you find any problem on VigorACS, you could shut down VigorACS and start VigorACS again.

2.3.1 Registration for VigorACS via Windows Platform

Below shows the steps to register VigorACS:

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



- (i) "root" and "admin123" are default settings.
- 3. A License Error dialog appears as follows. Simply click **Active**.

		⊕ EN ∽ VigorACS	
Licer Please go to	nse Warning : Your license is invalid or ex license server to activate your license.	pired.	e
	Dray Tek	Validation Code 7354 Remember me Login ()	

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

	Dray Tek _{MyVigor}	ENCLISH Learnin Passood Cogn Create Account / Get Help Return to old MyVggr	
Cospita	t & DrayTen Corp.	Terms of Service / Privacy Palicy	

(i) If you do not have any account, simply click <u>Create Account</u> to create a new one for using the service provided by MyVigor web site.

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

		roduct register (Add I	Device)
	Device Name	VigorACS3_carrie	
el	Model	VigorACS3	Ser
	MAC	ACS3200100013	
	Serial Number	ACS3200100013	
			_
		Cancel Subr	mit

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

License Status	
	License History
	Coday 2005-01-31

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

		License Agreement for ACS 3	
rrie	> Service Status	States Government shall be governed by the terms of this License Miscellaneous. This License will be governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles. If a court of competent jurisdiction finds any provision of this License invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this License will remain in full force. Failure of a party to enforce any provision of this License shall not waive such provision or of the right to enforce such provision. This License sets forth the entire agreement between the parties with respect to your use of the Supplier Software and supersedes all prior or contemporaneous representations or understandings regarding such subject matter. No modification or amendment of this License will be binding unless in writing and signed by an authorized representative of Supplier Products or any technical information and materials supplied under this Agreement without complying strictly with the export control laws and all legal requirements in the relevant jurisdiction, including without limitation, obtaining the prior approval of the U.S. Department of Commerce.	× III
		Cancel Accept	

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

License Trial Activate Date 2020-01-31 January 2020 > Su<			A	Activ	/ate	Lice	ense	of A	CS :	3		
January 2020 > Su Mo Tu We Th Fr Sa 1 2 3 4 5 6 7 8 9 10 11	> Service Status	License				Trial						
Su Mo Tu We Th Pr Sa 1 2 3 4 5 6 7 8 9 10 11		Activate Date			202	0-0	1-31					
1 2 3 4 5 6 7 8 9 10 11					Janu	ary	2020		»			
5 6 7 8 9 10 11			Su	Мо	Tu	We	Th	Fr	Sa			
									4			
				6								
12 13 14 15 16 17 18					14							
19 20 21 22 23 24 25												
26 27 28 29 30 31								31				
Reset						Rese	t					
Cancel Next		Car	ncel							Next		

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

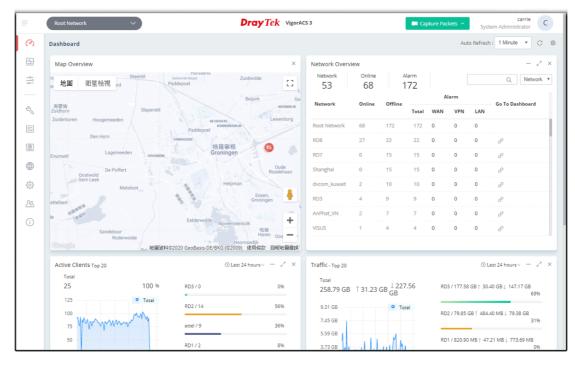
	Activate Lice	nse of ACS 3	
Service Status	Please confirm the below inform	nation then activate the license.	
	Service	ACS	
	Service Provider	DT-ACS-3	
	License	Trial	
	Activate Date	2020-01-30	
	Expire Date	2020-02-29	
	Cancel	Activate	

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

Dray Tek	
VigorACS License Information	
OPERATION 1000 : License Key OK	
LICENSE ID 0002b097	
START DATE 2020-01-30	
EXPIRE DATE 2021-02-29	
MAX NODE 0000020 TRIAL LICENSE No	
Login to ACS	

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

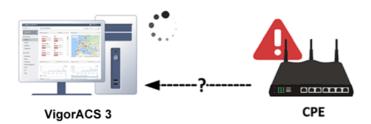
	⊕ EN ∨
	VigorACS
	User Name root
	Password 💿
Dray Tek	Validation Code 5817
	Remember me 5 8 1 7
	Login



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

2.3.2 Troubleshooting for Unstable CPE Status

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



Allow TR-069 server access from the Internet

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

System Maintenance >> Managen	nent			
IPv4 Management Setup	IPv6 Ma	anagement Setup	LAN Acc	ess Setup
Router Name DrayTek				
Default:Disable Auto-Logout		Management Port S	etup	
Enable Validation Code in Inter	net/LAN Access	User Define Port	s 🔿 Default Ports	
Note: IE8 and below version does	NOT support DrayOS	Telnet Port	23	(Default: 23)
CAPTCHA auth code.		HTTP Port	80	(Default: 80)
Internet Access Control		HTTPS Port	443	(Default: 443)
Allow management from the Int	ernet	FTP Port	21	(Default: 21)
Domain name allowed		TR069 Port	8069	(Default: 8069)
FTP Server		SSH Port	22	(Default: 22)
HTTP Server Enforce HT	TPS Access	Note:		
HTTPS Server		Ports 8001 and 8043	are used for Hotspot	Web Portal.
Telnet Server		Brute Force Protect	ion	
TR069 Server				
SSH Server		Enable brute force	e login protection	

Enable Periodic Inform

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

Protocol	HTTP	OHTTPS									
JRL											
Port	8069										
Jsername	vigor										
assword	•••••										
page.	e enable TR-06) server to allo	ow access from	Internet o	on <u>Syste</u>	n Mair	tenan	:e >>	Manag	<u>jement</u>	
page. Periodic Infor Enable	m Settings	erver to all				n Mair	tenan	:e >>	Manag	<u>jement</u>	
page. Periodic Infor Enable	m Settings) server to allo	ow access from		on <u>Syster</u>	n Mair	tenan	ce >>	Manag	<u>jement</u>	
page. Periodic Infor © Enable Time I	m Settings					n Mair	tenan	:e >>	Manag	<u>gement</u>	
page. Periodic Infor © Enable Time I Time I	m Settings e O Disable nterval					n Mair	tenan	ce >>	Manag	gement	
page. eriodic Infor Enable Time I pply Setting Enable	m Settings Disable nterval s to APs/Switc	hes				n Mair	tenan	ce >>	Manag	<u>gement</u>	

Check TR-069 authentication

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

- Register to the network of VigorACS 3

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



1 115

- Get CPE information

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

			t CPE Information			
	VigorA	CS3		CP	E	
network Management				System Maintenance >> TR-069 S	Setting	0
Search by Drives Klynami, Model, MAC, IP Address 🗠 😋	Satting Map					
 A Root Network(1) 3220n_0010AA554758 	EDelete This Device du Change Network			ACS and GPE Settings TR.069	Reporting Configuration Export Parameters	
	General Settings					
				Primary ACS Server		_
	Diable Diable	Known Device Known Thildham		ACS Server On	Internet V	
		and a second second			on System Maintenance >> Management >> Internet Access Control	
	Savera to	Referrit D		URL	Wizard	
	- Model Nume	Device Name				
	Vigor3220m	32201_90LDW6554758				
	Note 1	mite 2		CPE Client		
				Protocol OHTTP	LITTRE	
	Ber lai number	MAC Address		URL		
	20190903094(260)	0010AA354758		Port 8069		
	Location	CPE Client IP				
		132 168 105 22		Password		
	Phone Ne.	CPE Client Port	1	Note: Please enable TR-069 s page.	server to allow access from internet on System Maintenance >> Management	
		8069				
	. Bomain Name	GPE Client With		Periodic Inform Settings		
		/CWIN/CARL/REPE		🔾 Enable 🔮 Disable		
	Management Protocol	CHL Clent User Name		Time Interval	900 second(s)	
	CPE default (https) http: https	vigor				_
	Management Port	DEdia CPE Client Password				
	443	CPE Client Password				
EDelete Devloes		Press				

Check STUN setting

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

ACS and CPE Settings	Reporting Configuration	Export Parameters	
TR-069	🔿 Disable 💿 Enable		
Primary ACS Server			
ACS Server On	Internet 🗸		
Enable TR069 Server	on <u>System Maintenance >> Mar</u>	agement >> Internet Access	S Control
URL			Wizard
	Acquire URL from DHC	P option 43	
Username	acs		
Password	•••••		
STUN Settings	● Enable 〇 Disable		
Server Address	acsfaq.draytek.com		
Server STUN Port	3478		_
Minimum Keep Alive Perio	d 60 second	(s)	
Maximum Keep Alive Perio	od -1 second	(s)	

Check the ACL setting

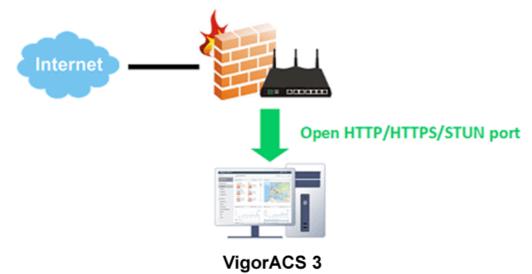
Make sure the IP of ACS server is also added into your access list once you enable it.

Acc	ess List from	the Internet		CVM Access Control		
	Eess List from Apply Access Type IP Object V IP Object V IP Object V	List to PING Index 1-acs None N	Description	CVM Access Control CVM Port CVM SSL Port AP Management C Enable AP Management Device Management Respond to external devi	8000 8443] (Default: 8000)] (Default: 8443)
6 7 8 9 10	IP Object ♥ IP Object ♥ IP Object ♥ IP Object ♥ IP Object ♥	None V None V None V				

• Check the firewall on ACS server

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

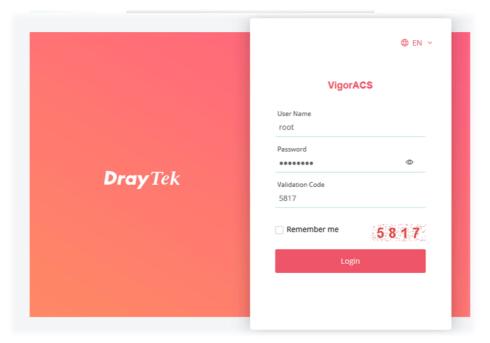
- HTTP port (Default tcp port 80)
- HTTPS port (Default tcp port 443)
- STUN port (Default udp port 3478)



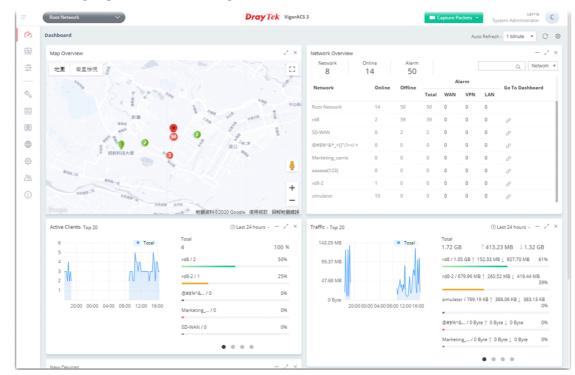
Chapter 3 Getting Started

3.1 Accessing Web Page of VigorACS

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



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



3.2 Dashboard

3.2.1 Dashboard for Root Network

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

	Root Networ	k			Dray	Tek VigorAC	5 3			(🖬 Capt	ure Packets	• Sys	carr em Administrati	
3	Dashboard											(Auto Refresi	1 Minute -	e o
43	Map Overv					2 × 1	Network Overvi	ew							- 7
1	Werumen 地面	anduw CuseAe 衛星恢復 _{Salena}	Groningen	Thesing	e 1/2	Watersum 23	Network 52	onlin 13		Alarm 233				<u>a</u> [)	letwork
-	Sherr and	Se veceslepi Paddepoel	Zuidwolde			Elokum				200		Alarm			
6			Bejum	Lagawag Carmarwold	44. / °	Luddew Hobessime	Network	Online	Offine	Total	WAN	VPN	LAN	Go To Dashb	oard
5	39.0201301	TT HOOTT		NUMBER OF	Heidenschap Li	Wigger 6	Root Network	13	233	234	0	0	0		
1		Pathepotel	ante la		at /	anosh	RD8	4	42	43	U	0	0	8	
-		Network	IR (B		P //	5 80 a m 2 	RD2	2	16	17	0	0	0	0	
Ð	HOODEER				Harksted	woudbio c	RD7	0	15	15	0	0	0	8	
2		S'M ROALS		oude oodeheen	Schar	mer 📕 🕅	Shanghal	0	14	14	0	0	0	6	
8	pot an all and		Easen			< 🛃	RD3	1	12	12	0	0	0	8	
Ð		**	Ease \ Groningen	Niteriul	201	+	dvnom kuwalt	0	12	12	0	0	0	P	
		Endorwalde Sayver	neterkolk	180	Westerbrook	- 1	AnPhat_VN	0	9	9	0	0	0	δ^i	
			Hanan.	ETRA ADDING AND AND A	алаулаарсаама нени	/ FOREAD									
	Active Clier		9 7-1	total	⊚ Last 24 hours∨		Traffic, 1ap 20			9.741	k	cal.	0	Last 24 hours >>	- /
	Active Clier 40 40		o Toul	tatal 43 1021710			Traffic. 1 pp 20 128 cm 2.78 cm 238 GB 1.86 GB				2	ы 8.07 GB 2072742.001	î 3.17	GB ↓24.9	90 GB
	40			43		- / ×	12860			o Touri Milli	2	8.07 GB	1 3.17 259 GB (24	GB ↓24.9 2308	90 GB
	40 40			43 8997798		- / ×	12830 2.4930 2.33 GB 1.85 GB 1.40 GB 476,84 MB				2 8 8	8.07 GB	1 3.17 254 онц 24 1 445.52 мв.	GB ↓ 24.9 2300 , 65.50 МВ	90 GB
	40		mil	43 10217-0 and 79		- / × 100 % 2% 2%	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2 8 8 8	8.07 GB 217 27 42 545 22 7 51 5, 52 MB 54 7 125, 91 MI	Ť 3.17 1254 (анд. 24 17 445 52 МВ. 17 403 5 МПЦ	GB ↓ 24.9 2510 68.30 MB 24.45 MB	90 GB 414 2%
	40		mil	43 899779 809779 809772		- / × 100 * //4 21% % 23%	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/22/64 MB	1 3.17 254 (41) 24 1 445.52 MB 1 404 5 MB 1 404 MB 1 20	GB ↓ 24.9 230 m GB.30 MB 24.95 MB 20 MB	90 GB 90 H 2% 104 0%
	40		mil	43 8917.0 9007.9 8097.2		- / × 100 % 2% 2%	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 16:00 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 217 27 42 545 22 7 51 5, 52 MB 54 7 125, 91 MI	1 3.17 254 (41) 24 1 445.52 MB 1 404 5 MB 1 404 MB 1 20	GB ↓ 24.9 230 m GB.30 MB 24.95 MB 20 MB	90 GB 414 2%
	40		mil	43 00070 00070 00072 RD171		- / × 100 * //4 21% % 23%	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 16:00 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/22/64 MB	1 3.17 254 (41) 24 1 445.52 MB 1 404 5 MB 1 404 MB 1 20	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	40	100 1600 2800 C000 C4	mil	43 00070 00070 00072 RD171	() Los Mihours -	- / × 100 * //4 21% % 23%	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/22/64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	40 40 20 10 12	100 1600 2800 C000 C4	mil	43 10917-10 10977-10 10977-2 RD4 / 1 10117-10	() Los Mihours -	- / × 100 % 234 244 144 - / ×	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 16:00 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/22/64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	40 40 10 10 10 12 12 New Device	.00 1600 2000 0000 04	00 08 00 Device Nam	43 10917-10 10977-10 10977-2 RD4 / 1 10117-10	 Las 24 hours - 	- / × 100 * //4 2/3 Na 2/3 IIIA - / ×	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/22/64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	 40 40 70 20 10 12 12 New Device Action 	100 16:00 20:00 00:00 04 100 16:00 20:00 00:00 04 172,172,172,172,174,433 141,181,21,185,2483	00 (200) Device Net 3910_001 20150-01	43 800770 800772 80170 80171 8017 8017	O Los 34 hours	- / × 100 m //4 21/4 14 24 10	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/25.64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	40 40 20 10 12 New Device Action	100 1600 2000 000 00 100 1600 2000 000 00 100 1600 2000 000 00 1721752174433 14176152185343 12232012322443	000 C8.00 Device Net 3910_001 291576.01 2912.001	43 1091719 109779 RD171 119779 RD171 11978 119779 RD171 11978 RD171 11978 RD171 11978 RD171 11977 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD1717 RD1717 RD171	 Los 24 hours - Device Type Vigor 3910 Vigor 29127 	- / × 100 m //4 21/4 104 104 104 104 104 104 104 104 104 10	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1600 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/25.64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3	90 GB 90 H 2% 114 0%
	*0	100 1600 2000 000 04 100 1600 2000 000 04 172.172.172.172.172.174233 144.161.21.152.14433 144.161.21.123.2443 144.161.704.2113443	000 C8 00 Device Net 3910,001 29176, 0 2912,001	43 001710 001710 001710 001710 001710 001710 001710 0017 0017 0	© Los 24 hours •	- / × 100 m //4 21/4 104 104 104 104 104 104 104 104 104 10	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	200 1000 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/25.64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3 (63.30 MB (74.45 MB) (74.45 MB) (74.45 MB) (74.45 MB)	90 GB 90 H 2% 114 0%
	40 40 20 10 12 New Device Action	100 1600 2000 000 00 100 1600 2000 000 00 100 1600 2000 000 00 1721752174433 14176152185343 12232012322443	000 C8 00 Device Net 3910,001 29176, 0 2912,001	43 1091719 109779 RD171 119779 RD171 11978 119779 RD171 11978 RD171 11978 RD171 11978 RD171 11977 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD171 RD1717 RD1717 RD171	 Los 24 hours - Device Type Vigor 3910 Vigor 29127 	- / × 100 m //4 21/4 104 104 104 104 104 104 104 104 104 10	128.58 2.78.58 2.83.08 1.80.08 1.40.58 470.84 MB 0.85%	LOC 1602 2		-yył	2: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8: 8:	8.07 GB 21/2/42 041 22/518.82 MB 24/12/34 MB 21/25.64 MB	1 3.17 224001 (24 1) 445.52 МВ. 1) 4045 МПЦ 4 404 МВЦ 20 425 МПЦ 4.1	GB ↓ 24.3 (63.30 MB (74.45 MB) (74.45 MB) (74.45 MB) (74.45 MB)	90 GB 90 H 2% 114 0%

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

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

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

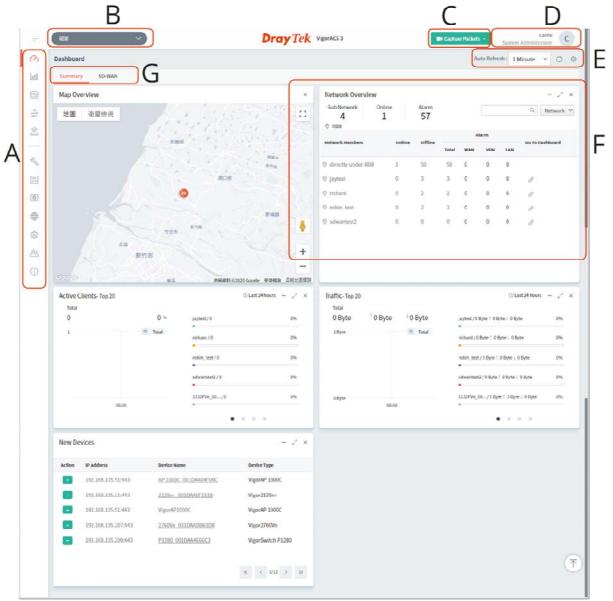
D: Selections - Display current used account and offer selections for setting password, two-factor authentication, theme change and logout.

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

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

3.2.2 Dashboard for a Network Group

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



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

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

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

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

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

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

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

3.2.3 Dashboard for a Device

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

2762Val. 001DAA653308	~		Dray Tek VigorAC	S 3		Capture Packets 👻	carrie Bystem Administrator
2762Vac_001DAA653308					Device Status: online Al	larms: U Active Clients: 0	U Auto Ketresh: Disable
Port Status				WAN Overview			() Last 24 hou
				488.28 KB			• Total
	Strenge Viele			390.63 KB		1	- 10.21
0 1			<u> </u>	292.97 KB 195.31 KB			mark
	イ 23 3 (J 28 Viger2762Vec			97.56 KB			V VV
				U Byce 12:00 14:00 15:00 18:0	0 20:00 22:00 00:0	0 02:00 04:00 06	5:00 DB:00 10:00
				Total 5.39 MB (↑3.67 MB ↓1.71	MB)		100 9
Device Information		DSL Information		WAN1 0 Byte (10 Byte + 0 Byte)			0.9
Device Name	2762Vac_001DA4653308	DSL Status	TRAINING	WAN2 5.39 MB (13.67 MB + 1.7	1 MB)		100 %
IP Address	https://192.168.105.77:443	DSL Type		WAN3 0 Eyte (10 Eyte 40 Byte)	energia energi da su de la constante de la constante anos	entenange in may a single analy entering spectrum starting	0 9
Network Name	KD8	Modulation Type	Multimode	•			
Model	Vigor 2762VaL 😋	Download Speed(kbps)	0	WAN It Line/Mode	J1 IP	41 Uptime	가 Active Mode 가
Firmware Version	r81002_bcta 😡	Upload Speed(kbps)	0	WAN1 VDSL2 / Static IP	192.168.3.73	0d 00b 00m	Always On
MAC Address	001DAA553308	SNR Margin	0	WAN2 Ethernet / Static IP	192,168,105,77	394 021 400	Failover (WAN1)
Up Time	39 days 02:43:13	Loop Attenuation(0.1dB)	0	WANZ CONTINUES STATE	192.100.100.77	390 02114011	
P	Lang	CDC F	^	WAND USE /		0d 00h 00m	Failover (WAN2)
	~ show more		~ show more				
System Resource			© Last 24 hours▼				
CDU	6.0	6 Memory	91 %	LAN Overview			() Lest 24 hou
CPU	• *		21.20	1			Active Clients
20% 15% 10%	IIII ALK	50%					
596	MANWA	016					
Connectivity and Alerts	5 21+88 01400 04:12 07:24 10:36	1212 1524 1836 2148	01:00 01:12 07:24 10:26 0/0 (3 Last 7 days *	C 12:00 14:00 16:00 18:00 1.00	26:00 22:00 00:00 https://doi.org/10.107Masth	02:00 04:00 06:0	
	5 211-25 01.00 01.12 07.27 10.96	1212 1524 1836 2148		 Italink Wan 3 Up Len 1 	0 Drue		18 10 (Bente 10 6 7
Connectivity and Alerts	5 211-25 01-20 04-12 07-24 10-26	Drable	0/0 (j) Last 7 deys+	€ Nolink Wan 3	0	15 DM	10 M Claste M
Connectivity and Alerts স্যন-ব		Droble Drable	0/0 (j) Last 7 deys+	 Italink Wan 3 Up Len 1 	0 Drue		18 10 (Bente 10 L ^a R ^a
Connectivity and Alerts স্যন-ব		Droble Drable	0/0 (j) Last 7 deys+	 Notinit: Wan 3 Up Len 1 Down Lan 2 Map 	0 Drue		G In Chanter In G G G
Connectivity and Alerts SG-3 3G-1 Workers Socion List 2.4G		Droble Drable	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	о о юлино али мил мил мил мил		18 10 (Bente 10 L ^a R ^a
Connectivity and Alerts %G-3 3G-1 Wirkless Socian List 2.4G		Droble Disable	0/0 (j) Last 7 deys+	●Nolink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 端屋細語	ona Di 1976a di Une mue enceten filiei	192.168.77.1 192.168.7.1 193.164.3.1	G Chanter G G G
Connectivity and Alerts	Wratess LAN (24	Droble Disable	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	о о юлино али мил мил мил мил	192.168.77.1 192.168.7.1 193.164.3.1	G Chanter G G G
Connectivity and Alerts 9G-3 9G-4 Wireless Station List 2,45 Wireless Station List 5G	Wintess LAN (24 Wintess LAN (3	Droble Disable	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	ona D 1978-06	192.168.77.1 192.168.7.1 193.164.3.1	10 Citation of Citatio of Citation of Citation of Citation of Citation of Cita
Connectivity and Alens 3G-3 3G-4 Windess Sustan List 2,45 Windess Station List 3G	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	ona D 1978-06	192.168.77.1 192.168.7.1 193.164.3.1	
Connectivity and Alerts SG-3 20-1 Windess Station List 2.45 Windess Station List 2.45 Mindets Station List 3G 250 Modern Information Status	Wintess LAN (24 Wintess LAN (3	Droble Disable	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	ona D 1978-06	192.168.77.1 192.168.7.1 193.164.3.1	10 Citation of Citatio of Citation of Citation of Citation of Citation of Cita
Connectivity and Alerts SG-3 3G-1 Wireless Station List 2.45 Wireless Station List 2.45 USD Modern Information Status Signal Quality (CINR)	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	●Notink: Wan 3 ●Up Len 1 ●Down Lan 2 Map 轮圈 解靈細語	ona D 1978-06	- 192.168.77.1 192.168.77.1 192.168.7.1 192.168.7.1	Community Statements
Connectivity and Alerts 50-3 30-1 Wireless Station List 2-45 Wireless Station List 2-5 Wireless Station List 5G UED Modem Information Status Signal Quality (CINR) RSSI Signal	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	● Nolink Wan 3 ● Up Len 1 ● Down Len 2 Mop 地理 WElseten Bvd W Clasteten Bvd	ona D 1978-06	- 192.168.77.1 192.168.77.1 192.168.7.1 192.168.7.1	Community Sectors
Connectivity and Alerts SG-3 SG-3 SG-1 Wireless Station List 2.45 Wireless Station List 2.55 USD Modew Information Status Signal Quality (CINR) RSSI Signal Link Speed	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	1.00 1.00	ona D 1978-06	- 192.168.77.1 192.168.77.1 192.168.7.1 192.168.7.1	
Connectivity and Alerts %G-3 3G-3 3G-4 Wireless Station List 2.43 Wireless Station List 2.43 Wireless Station List 3G USD Modern Information Status Signal Quality (CINR) RSSI Signal Link Speed Manufacturer	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	● Nolink Wan 3 ● Up Len 1 ● Down Len 2 Mop 地理 WElseten Bvd W Clasteten Bvd	ona D 1978-06	- 192.168.77.1 192.168.3.1	
Connectivity and Alerts %5-3 36-1 Wireless Station Nr 2,45 Wireless Station List	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	1.00 1.00	ona D 1978-06	- 192.168.77.1 192.168.3.1	
Connectivity and Alerts SG-3 3G-3 3G-4 Wireless Station List 2.40 Wireless Station List 2.40 Wireless Station List 3G USD Modern Information Status Status Status Status Link Speed Link Speed Revision	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	tran tran	ona D 1978-06	- 192.168.77.1 192.168.3.1	с отракт. Веренали и советства и советств с советства и с с советства и со
Connectivity and Alerts 3G-3 3G-3 3G-4 Wireless Station List 2,45 Wireless Statio	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0/0 (j) Last 7 deys+	1.00 1.00	ona D 1978-06	- 192.168.77.1 192.168.3.1	с отракт. Веренали и советства и советств с советства и с с советства и со
Connectivity and Alerts SG-3 3G-3 3G-4 Wireless Station List 2.40 Wireless Station List 2.40 Wireless Station List 3G USD Modern Information Status Status Status Status Status Status Status Status Marulacturer Model Revision	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0:0 () Last 7 days-	tran tran	€ EVE EVE EVE EVE EVE EVE EVE EV		с отракт. Веренали и советства и советств с советства и с с советства и со
Connectivity and Alerts SGR 2014 SGR 2014 Wireless Station List 2.4G Wireless Station List 2.4G Wireless Station List 2.4G Wireless Station List 3G USD Modem Information Status Signal Quality (CINR) Status Signal Quality (CINR) Manufacturer Model Revision Vireless	Wintess LAN (24 Wintess LAN (3	Disable Disable 4GHg is disabled GHg is disabled	0:0 () Last 7 days-	tran tran	€ EVE EVE EVE EVE EVE EVE EVE EV		
Connectivity and Alerts SGR SGR SGR Wireless Station List 2.45 Wireless Station List 2.45 Wireless Station List 36 USD Modern Information Status Signal Quality (CINR) RSS Signal Link Speed Manufacturer Model Revision VolP Status	Winters LAN (24 Winders LAN (3	Disable Disable	0:0 () Last 7 days-	tran tran	€ EVE EVE EVE EVE EVE EVE EVE EV		с отракт. Веренали и советства и советств с советства и с с советства и со
Connectivity and Alerts SGR 3GR 3GR Writees Station List 2,40 Wratess	Winters LAN (24 Winders LAN (3	Disable Disable	0.0 (c) Last 7 days-	tran tran	€ EVE EVE EVE EVE EVE EVE EVE EV		с отракт. Веренали и советства и советств с советства и с с советства и со

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

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

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

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

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

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

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

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

3.2.4 Menu Bar

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

		nu Bar for Root work.			nu Bar for Network pup.		Mei CPE	nu Bar for Selected
(7)	•	Dashboard	Ō	•	Dashboard	(3)	•	Dashboard
<u></u>	•	Monitoring	000	•	Statistics	000	•	Statistics
	•	Configuration		•	Monitoring Configuration	<u></u>	•	Monitoring Configuration
Z			((([]	•	Hotspot Web Portal			
	•	Maintenance	S	•	Maintenance	S/	•	Maintenance
-		Reports Provisioning	E		Reports Provisioning		•	Reports Provisioning
€ };	•	Network Management	8	•	Network Management	Image: A transmission of the second secon	•	Network Management
23	•	System		•	System	<u></u>	•	System
(i)	•	User	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	•	User	삼	•	User
	•	About	<u>i</u>	•	About	(i)	•	About
=	RD8	~			e cursor to each			
(7)	Configu	ration	list.	en the	drop down menu			
	VPN		Select the	e menu	item and access			
₽°₽	AP Profile		into the c	onfigur	ation web page.			
(رد <u>ا</u> :		licy (SD-WAN)						
		I (SD-WAN)						

3.2.5 Root Network, Group Network, and Selected CPE

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

3.2.5.1 The Display Tab, Root Network

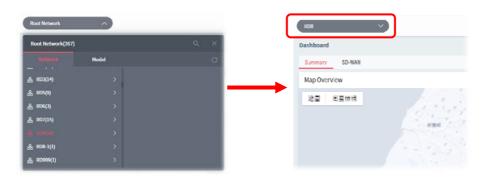
Click the **Display Tab** to display a drop-down list. This tab will display the name of the network group or the name of the selected CPE based on your selection. In default, Root Network will be shown on the Display Tab.

Root Network(267)		
	Model	
器 RD3(14)	<i>,</i>	
28 RD5(9)		
& RD6(3)		
品 RD7(15)		
옰 RDB(SB)		
읊 RD8-1(1)		
ළු RD999(1)		

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

3.2.5.2 The Display Tab, Network Group

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



3.2.5.3 The Display Tab, CPE Device

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



3.2.6 Capture Packets

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

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

	Capture Packets 👻
	Select a network interface to capture:
1	문 Oracle
	MAC: 0a:00:27:00:00:10
	IPv4: 192.168.56.1
	IPv6: fe80:0:0:0:5c57:b309:2494:bbd6
1	공 Intel(R) Ethernet Connection (2) I219-V
	MAC: 34:97:f6:81:c1:41
	IPv4: 172.16.2.222
	IPv6: fc00:0:0:0:2189:63d1:c0e0:14f6
1	윤 Realtek PCIe GbE Family Controller
	MAC: ec:08:6b:06:5f:4b
	IPv4: 192.168.105.2
	IPv6: fe80:0:0:0:830:9fe0:7168:6b42

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

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

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

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

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

🔉 Capture Settings		
Filter Settings		
Filter Examples	TCP only ~	
Custom Filter	tcp	
	ly, for more expression syntax, please visit: PCAP-FI	ILTER
	ly, for more expression syntax, please visit: PCAP-Fi	ILTER
You can type filter norma Time Settings Enable Time Limit		ILTER
You can type filter norma	ly, for more expression syntax, please visit: PCAP-FI	ILTER
You can type filter norma Time Settings Enable Time Limit		ILTER

These parameters are explained as follows:

ltem	Description
Filter Settings	Filter Examples – Choose a filter for filtering the packet corresponding to the type selected.
	For example, when TCP Only is selected, only TCP packets will be captured and recorded. When IPv4 address 127.0.0.1 is selected, then only the packets coming from/sending to that IP address will be captured and recorded.
	Custom Filter – Variation of Filter Examples will change the setting in Custom Filter. However, the system administrator can define the filter by entering correct syntax (e.g., host 172.16.2.222) if required. Packet capturing will be executed according to Custom Filter setting.
Time Settings	 Enable Time Limit – If enabled, VigorACS server will capture the packets within the time limit defined below. Time Limit (Minute) – Enter a value as a time limit.
Start Capturing	 Click to start packets capturing. After clicking it, VigorACS server will continuously capture the packets until time up or manual stop. While capturing, the system administrator can perform any job on VigorACS still. The status will be shown as the following figure. If Time Limit is disabled, the status bar will not show the timer information.
	Stop Capturing (Stop Timer: 04:25)
	• When the time is up or stop the job manually, the status of Pcap will display the icons of Download and Delete and create a new capture. Click Download to store the file on the hard disk. Later, use the tool of Wireshark to check the content of the file.

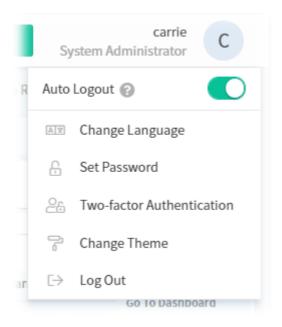
 After clicking Delete and create a new capture, VigorACS server will delete the packets just captured and restore the Capture Packets icon for next time using.
 In considering the network security, when someone performs the packet capturing on VigorACS server, other users are not permitted to use Capture Packets until the one finishes or stops the job. Only the one who performs the packets capturing can download the packet capture file.
lacksquare Pcap is now in use by "root", please wait for current capturing finished. 2
Click the Refresh button on the right side of Pcap status bar to check if someone else uses Pcap or not.

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

)18-10-23.175419.pcap				- 0	>
le			Telephony Wireless To	ols <u>H</u> elp			
		🖸 ९ 🗢 🗢 🕾 🚹 👲	୍ 📃 🔍 ପ୍ ସ୍ 🖽				
Ap	oly a display filter … «Ctrl-/	l>				🗾 👻 Expression	····
	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	192.168.50.10	192.168.105.59	TCP	66 64750 → 8069	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S	S
	2 0.001467	192.168.105.59	192.168.50.10	TCP	60 8069 → 64750	[SYN, ACK] Seq=0 Ack=1 Win=25600 Len=0 MSS=14	4
	3 0.001608	192.168.50.10	192.168.105.59	TCP	54 64750 → 8069	[ACK] Seq=1 Ack=1 Win=64240 Len=0	
	4 0.001821	192.168.50.10	192.168.105.59	HTTP	155 GET /cwm/CRN.	html HTTP/1.1	
	5 0.004302	192.168.105.59	192.168.50.10	HTTP	262 HTTP/1.1 401	Authentication Failed	
	6 0.004673	192.168.50.10	192.168.105.59	TCP		[FIN, ACK] Seq=102 Ack=209 Win=64032 Len=0	F
	7 0.005244	192.168.50.10	192.168.105.59	TCP		[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256	S
	8 0.005541	192.168.105.59	192.168.50.10	TCP	60 8069 → 64750	[ACK] Seq=209 Ack=103 Win=25600 Len=0	
	9 0.005630	192.168.105.59	192.168.50.10	TCP		[FIN, ACK] Seq=209 Ack=103 Win=25600 Len=0	
	10 0 005600	107 168 50 10	100 169 105 50	TCD	51 61750 - ROGO	[ACV] Sog-103 Ack-210 Win-64032 Lon-0	
Tr	ansmission Contro pertext Transfer		t: 64750, Dst Port: 8	68.105.59 069, Seq: 1	, Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		., Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		, Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		, Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		., Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		., Ack: 1, Len: 101		
Tr			t: 64750, Dst Port: 8		, Ack: 1, Len: 101		
Tr	pertext Transfer	Protocol		069, Seq: 1			
Tr Hy 00	pertext Transfer 00 1d aa 69 4a	Protocol e8 88 d7 f6 56 f7	99 08 00 45 00 ···1	069, Seq: 1	E.		
Tr Hy 00	00 1d aa 69 4a 00 8d 10 fa 40	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0	99 08 00 45 00 ···1 88 32 0a c0 a8 ····	069, Seq: 1	E		
Tr Hy 00 10 20	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5	99 08 00 45 00 ···i a8 32 0a c0 a8 ···· 83 a5 64 56 18 i;··	069, Seq: 1	E. 		
Tr Hy 000 100 200	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5 00 47 45 54 20 2f	99 08 00 45 00 ··· 1 a8 32 0a c0 a8 ···· 83 a5 64 50 18 i; 5 77 6d 2f 43 ····	069, Seq: 1	E. ./C		
Tr Hy 100 120 130	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74	Protocol e8 88 d7 f6 56 f7 08 80 06 00 00 c0 85 3c 14 c0 8e e5 00 47 45 54 20 2f 6d 6c 20 48 54 54 54	99 08 00 45 00 ··· 1 a8 32 0a c0 a8 ···· a8 a5 64 50 18 i; 63 77 6d 2f 43 ···· 63 77 6d 2f 12e 31 RN.h	.]	E- IP- /C		
Tr Hy 000 10 120 130 130	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 0d 0a 55 73 65	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5 00 47 45 54 20 2f	39 08 00 45 00 1 a8 32 0a c0 a8 83 a5 64 50 18 1; 63 77 6d 2f 31 50 2 f 31 2e 31 74 3a 20 4a 61	069, Seq: 1	Е. IP. ./С Ja		
Tr Hy 000 010 020 030 030 030 030 030 030 030 030 03	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 0d 0a 55 73 65 6b 61 72 74 61	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 05 3c 14 c0 8e e5 00 47 45 54 20 2f 6d 6c 20 48 54 54 6d 6c 20 48 54 54 72 2d 41 67 65 64	99 08 00 45 001 88 32 0a c0 a8 83 a5 64 50 18 1; 50 2f 31 2e 31 RN.h 74 3a 20 4a 61Us 6e 73 2d 48 74 kart	069, Seq: 1	E. IP. ./C 1 Ja Ht		
Tr Hy 100 10 10 10 10 10 10 10 10 10 10 10 10	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 60 52 4e 2e 68 74 0d 0a 55 73 65 6b 61 72 74 63 74 70 43 6c 69	Protocol e8 88 d7 f6 56 f7 09 80 66 00 02 68 53 c14 c0 8e 69 04 74 54 20 27 6d 6c 20 48 54 54 72 2d 41 67 65 62 20 43 6f 6d 6d <t< td=""><td>99 08 00 45 001 a8 32 0a c0 a8 33 a5 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RNLh 74 3a 20 4a 61Us 6e 73 2d 48 6f tpCl 10 d0 a 48 6f tpCl</td><td>069, Seq: 1</td><td>E. ./C 1 Ja Ht Ho</td><td></td><td></td></t<>	99 08 00 45 001 a8 32 0a c0 a8 33 a5 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RNLh 74 3a 20 4a 61Us 6e 73 2d 48 6f tpCl 10 d0 a 48 6f tpCl	069, Seq: 1	E. ./C 1 Ja Ht Ho		
Tr Hy 100 120 130 140 150 150 150 150 150 150 150 150	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 0d 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 93 11	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 12 c0 8e e5 00 47 54 20 26 06 42 02 45 42 27 6 66 c0 48 54 54 47 22 41 67 65 62 43 64 66 66 67 67 43 32 24 54	99 08 00 45 00 a8 32 0a 0a 83 63 77 60 2f 43 63 77 6d 2f 43 59 2f 31 2e 31 RN.h 74 3a 20 46 1 Us 56 73 2d 48 74 kart 56 73 2d 48 74 kart 31 0d 0a 48 6f tpC1 2e 31 30 35 2e st	JV @2. 	E. ./C 1 Ja Ht Ho		
Tr Hy 100 120 130 140 150 150 150 150 150 150 150 150	00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 0d 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 93 11	Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3: 1: 4: 08 e5 00 47 45 4: 20 2f 6d 6: 20 48 54 54 54 22 24 14 67 65 62 43 6f 6d 6f 65 674 2f 32 2a 31 36 38 39 32 2a 31 36 38 2e 39 32 2a 31 36 36 66 66 67 2f 33 2a 39 32 2a 31 36 38 36 36 36 66 66 67 67 31 66 36 66 67 32 2a 31 63 36 36 36 36 36 3	99 08 00 45 00 a8 32 0a 0a 83 63 77 60 2f 43 63 77 6d 2f 43 59 2f 31 2e 31 RN.h 74 3a 20 46 1 Us 56 73 2d 48 74 kart 56 73 2d 48 74 kart 31 0d 0a 48 6f tpC1 2e 31 30 35 2e st	.]	E. ./C 1 Ja Ht Ho		

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

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



3.2.7.1 Change Language

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

⊠≢ Cha	nge La	nguag	e			×
Please s	elect a la	inguage	below:			
				automatica	lly reload.	
⊖ CN	o de	● EN	O NL	O TW		
					Cancel	ОК

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

3.2.7.2 Set Password

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

Set Password	
Account :	
New Password	٢
Confirm Password	۵
	Save

3.2.7.3 Two-factor Authentication

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

For using two-factor authentication for accessing VigorACS;

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

	⊕ EN ∨
	VigorACS
	User Name root
	Password
Dray Tek	Validation Code 5817
	Remember me 5 8 1 7
	Login

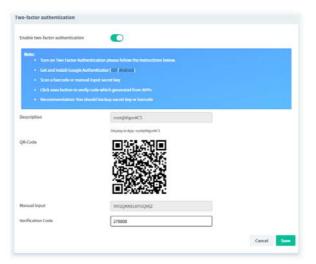
3. Open Root>>Two-factor Authentication and enable the button of Enable two-factor authentication.



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

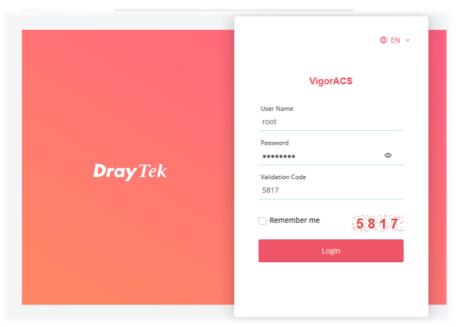


5. A key will be created randomly on the cell phone. Enter that key on the box of **Verification Code** and click the **Save** button.

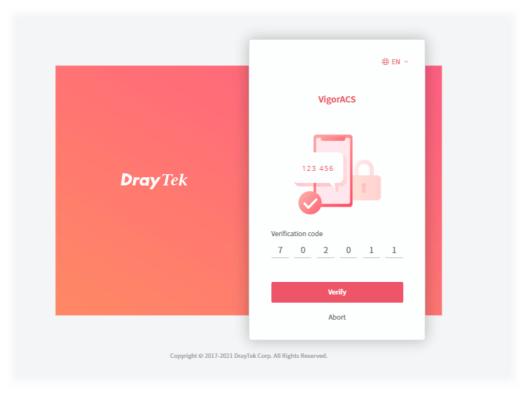


6. Logout VigorACS 3.

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



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



3.2.7.4 Change Theme

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

Automatically detect system	or browser theme (Detected: Light The	me)			
, miterini dan ja sereta ja se	i i i i i i i i i i i i i i i i i i i	,			
Light Theme			Dark Theme		
Rectificant -	Dray Tek Variatis		E Reflected 1	DrayTek versas	
(2) Boot Network(74)	9, X	Annen Immi - C.O.	(0) Root Saturdak(24)		Adv Roberts 1 Monte - C
(3)	Gill beark Overview			C work Overview	
2 A Martine Control of	Maharak Colore 12 2 Int Natasak	72 (Intention)		12 2 7	Q Reference
▲ #05 > ▲ #09 >		Online URINE BAR UNI LAN	A 400 5		
2 4 4 10	and a sector bar Martin	A. A. A. A. A. A.		-stily-under Rest National 1	
(I) A 144 (A) (A)	\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$			steer-stars	
0 Amm >					
A analysis	a series and a series of the s		A senderetta	uturing surver 1	
	9 KL MAR			///n.m. 🤞	
8	P second III			Ref. / The Presentation	
0	+ 14	1.2.2.1.1.1	O	X /	
	_ 100	TO DA 0403 DA 04 14		A dama and the set	

3.2.7.5 Logout VigorACS

Click **Logout** icon to logout VigorACS immediately. Or, switch the toggle of Auto Logout to enable the function of exiting VigorACS after five minutes without any operation.

	Sy	carrie stem Administrator
R	Auto	Logout 😨
	AÌÌ	Change Language
	ß	Set Password
	26	Two-factor Authentication
		Change Theme
an	$[\rightarrow$	Log Out
		Go to Dashboard

3.2.8 Auto Refresh, Manual Refresh, and Widget

Auto Refresh : 1 Minu	ute Y C 🕸					
ltem	Description					
Auto Refresh	Select the time interval for refresh the web page automatically.					
Manual Refresh	Click to refresh the web page immediately.					
Widget	There are six display views to select, including Network Overview, Map Overview, Clients, Traffic, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard. Auto Refresh : 1 Minute Network Overview Map Overview Clients Traffic New Devices Reset to default					

3.2.9 Overviews

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

ctive Clie	nts Top 20			🕲 Last 24 hours 🗸 🚽 🧭 🗙	Traffic - Top 20	③ Last 24 hours →
Total 27 125 100 75 50 25 21		100 % Total	RD3 / 0 RD2 / 13 attel / 11 RD1 / 3 RD8 / 0	0% 48% 41% 11% 0%	Total 251.28 GB 1 30.38 GB GB 9.31 GB 7.45 GB 5.59 GB 3.73 GB 1.86 GB 0 Byre 20.0000.0004.0008.00 12:00 16:00	RD3 / 172.67 GB 29.52 GB 143.15 GB (RD2 / 77.24 GB 518.84 MB 76.74 GB RD1 / 818.54 MB 47.23 MB 771.31 ME attel / 453.14 MB 245.69 MB 207.46 M
New Devic	les			- 2 ×		RD8 / 129.48 MB † 73.38 MB ↓ 56.10 MB
Action	IP Address	Device	Name	Device Type		
+	172.17.5.151:4433	3910_0	001DAA18E740	Vigor3910		
+	14.161.2.165:443	2912Fr	n_001DAA8C0F0C	Vigor2912Fn		
+	123.20.123.2:443	2912_0	001DAA87FAE4	Vigor2912		
+	14.167.99.211:443	2912_0	001DAA88040C	Vigor2912		
+	192.168.11.5:443	AP 810	_001DAA0F3320	VigorAP 810		
				ki < 1/45 > bi		

3.2.9.1 Network Overview / Device Overview

This area displays the Network Overview or the Device Overview.

ltem	Description
Category	Switch between Network or Device.
- / ~	-(Collapse) - Hide the page. (Fullscreen) - Display the page in fullscreen.
×	x (Delete) - Delete this widget.

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

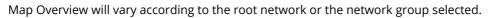
Network O	3	Alarm 56					Q Network
Network	Online	Offline	Alarm				Go To Dashboard
Network	Online	Omine	Total	WAN	VPN	LAN	Go To Dashboard
Root Network	3	56	56	0	0	0	
rd8	1	39	39	0	0	0	S
simulator	0	10	10	0	0	0	P
SD-WAN	0	2	2	0	0	0	P
tttt1	0	1	1	0	0	0	8
2020-01-14_addNetwork_A	0	0	0	0	0	0	P
@#\$%^&*_+{}":?> -+</td <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>8</td>	0	0	0	0	0	0	8
Marketing_carrie	0	0	0	0	0	0	B

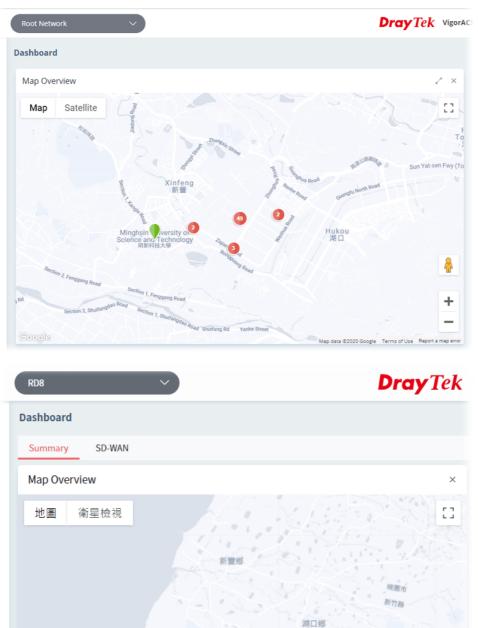
Under **Device Overview**, move the scroll bar left and right to check basic information for each device. Click >> (Next) or << (Previous) arrow to display next page for checking information for other devices.

Routers 44	APs 12	Switch 3			Q D	evice
Device Name	Model	MAC	UP Time	Firmware Version	LAN Clients	VPN
2926LVac_1449BCFFF9A8	Vigor2926LVac	1449BCFFF9A8	0d:0h:0m:0s	r86993_beta	0	0
2926Vac_001DAA5DCAF0	Vigor2926Vac	001DAA5DCAF0	0d:0h:0m:0s	r86955_beta	0	0
810_001DAA7D6514	VigorAP 810	001DAA7D6514	0d:0h:0m:0s	1.2.5	0	0
902_001DAA3D4F16	VigorAP 902	001DAA3D4F16	0d:0h:0m:0s	1.2.3.1	0	0
130_001DAA83A094	Vigor130	001DAA83A094	0d:0h:0m:0s	a	0	0
130_001DAA8411C8	Vigor130	001DAA8411C8	0d:0h:0m:0s	r70663_beta	0	0
130_001DAA854204	Vigor130	001DAA854204	0d:0h:0m:0s	r72469_beta	0	0
130_001DAA8D3FA0	Vigor130	001DAA8D3FA0	0d:0h:0m:0s	a	0	0

3.2.9.2 Map Overview

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





新竹製

竹北市

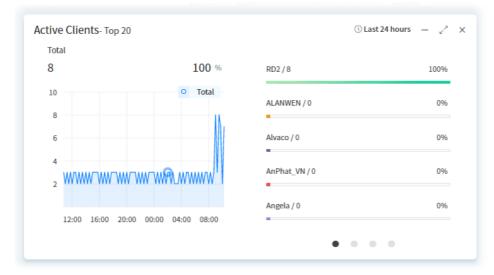
北區

新竹市

新埔額

3.2.9.3 Active Clients

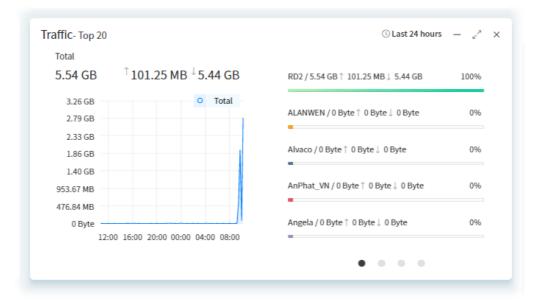
This area displays the top 10 clients or top 20 clients accessing into VigorACS during the last 24 hours, 7 days or 30 days.



Item	Description
Last 24 hours	Use the drop down list to specify the time period, last 24 hours, 7 days or 30 days.
- / 2	- (Collapse) - Hide the page.
×	x (Delete) - Delete this widget.

3.2.9.4 Traffic

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



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

3.2.9.5 New Devices

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

ction	IP Address	Device Name	Device Type	
+	192.168.105.143:443	2862Vac_001DAAEA38C0	Vigor2862Vac	
+	192.168.11.12:443	2920LVac_1449BCFFF9A8	Vigor2926LVac	
+	192.168.15.10:443	2926Vac_001DAA5DCAF0	Vigor2926Vac	
+	192.168.105.81:443	810_001DAA7D6514	2862Vac_001. 438C0	
+	192.168.105.89:8442	902_001DAA3D4F16		
			Port Status	
			ACT WAR2 Line Distance USB DIL Parent 240 50 Phone2 In.	
			Device Information	
			Device Name	2862Vac_001DAAEA38C0
			IP Address	https://192.168.105.143:443
			Network Name	AutoTestNetwork
			Model	Vigor2862Vac

ltem	Description
- / 2	- (Collapse) - Hide the page.
	(Fullscreen) - Display the page in fullscreen.
×	x (Delete) - Delete this widget.
F	Click the button to add a new device onto the network.
	Refer to "Applications, A.3 How to Assign a New Added CPE to a Network?" for detailed information.

3.2.9.6 Reset to Default

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

Auto Refresh :	1 Minute 🔻 🔿 🐵
	Network Overview
	☑ Map Overview
	Clients
	Traffic
	New Devices
	Reset to default

3.2.10 Icons Used in VigorACS 3

ltem	Description
+	Add a new device.
- / <	Hide the page / Display the page in fullscreen.
×	Delete the selected widget.
	Switch these two icons by click the mouse cursor on it. - means "Enable". - means "Disable".

3.3 Operation Procedure

Follow the instruction listed below to operate VigorACS 3:

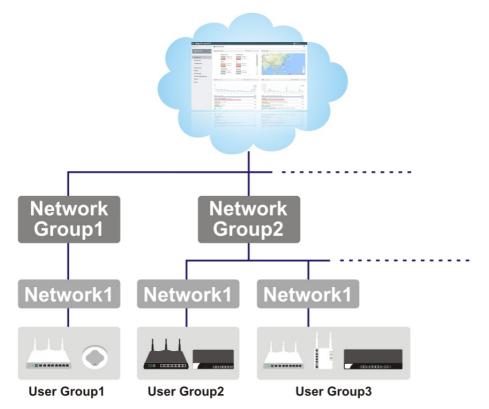
- Create networks.
- Create users and user groups.

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

User shall be assigned under different user groups. RootGroup is the default user group.

• Edit and modify the settings for the TR-069 devices.

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



Applications

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

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

The CPE to be managed by VigorACS 3 must be configured and restarted. Here we take Vigor2927Vac as an example.

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

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

System Maintenance >> Management

IPv4 Manage	ement Setup	IPv6 Management Setup
Router Name	DrayTek	
 Default:Disable Enable Validati 	e Auto-Logout on Code in Internet/L	AN Access Wanagement Port Setup User Define Ports Defa Telnet Port
Domain name a	nent from the Interne llowed Enforce HTTPS Ac er	FTP Port TR069 Port
 SSH Server SNMP Serve Disable PING fr 	r rom the Internet	Brute Force Protection Enable brute force login p FTP Server

- Allow management from the Internet – Enabled.

- TR-069 Server Enabled.
- 3. Open System Maintenance>>TR-069.

	Reporting Configuration	Export Parameters	
TR-069	🔘 Disable 💿 Enable		
ACS Server On	LAN/VPN *		
ACS Server			
URL	http://192.168.1.110:8011/ACSS	erver/services/ACSServic Wizard	
	Acquire URL from DHCP o	ption 43	
Username	acs		
Password	•••••		
	Test With Inform Event Code	PERIODIC *	
Last Inform Response	Time :Sat Jan :(NA) 🥌		
CPE Client			
	⊕ http ○ https		
CPE Client Protocol URL	⊛ нттр ○ нттрѕ http://192.168.1.1:8069/cwm/CRI	N. html	
Protocol		N.html	
Protocol URL	http://192.168.1.1:8069/cwm/CR	N. html	

- Specify the interface for ACS Server On.
- Set URL, username, password for network group.
- 4. Click **OK** and click **Test With Inform**. When the green light appears (on the Last Inform Response Time), the settings on CPE have been configured well.

Last Inform Response Time :Sat Jan 11 0:12:57 2020 🤍

- 5. Open the homepage of VigorACS 3.
- 6. Now, Vigor2927Vac has been registered onto VigorACS 3 and displayed on the homepage.

Action	IP Address	Device Name	Device Type
+	172.17.5.151:4433	3910_001DAA18E740	Vigor3910
+	14.161.2.165:443	2912Fn_001DAA8C0F0C	Vigor2912Fn
+	123.20.123.2:443	2912_001DAA87FAE4	Vigor2912
+	14.167.99.211:443	2926_001DAA88040C	Vigor2926Vac

A.2 How to Create a New Network?

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

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

2	南霍倫 Zuidhorn		Slaperstil
_	Zuiderburen	Hoogemeeden	
=>		Den Horn	
\$			
	Enumatil	Lagemeeden	HOOGKER
•		De Poffert	
Netwo	rk Management	stwold m Leek	
503	,	Matsloo	t
23	Lettelbert		
(i)	olde Harriste		

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

+Add New Network		
General Settings		
Network ID		
2		
Name		
Root Network		
Location		

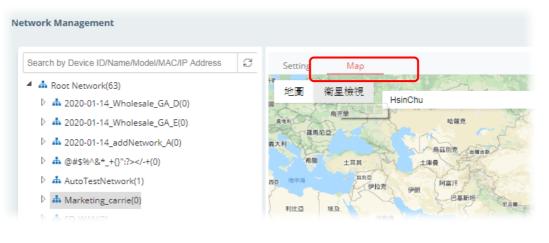
4. A pop-up window appears. Type the required information.

Parent Network		
Root Network		
Name		
Marketing_carrie		~
Location		
HsinCHu		
User Name		
carrie		~
Password		
		

- Name Enter a new name of the network.
- Location Define the location of such network.
- User Name Enter a user name for such network.
- Password Enter a password for such network.
- 5. Click **+Add** to save the settings. The new created network will be seen under the **Root Network**.

N	etwork Management
	Search by Device ID/Name/Model/MAC/IP Address
	A the Root Network(63)
	A 2020-01-14_Wholesale_GA_D(0)
	A 2020-01-14_Wholesale_GA_E(0)
	A 2020-01-14_addNetwork_A(0)
	▷ ♣ @#\$%^&*_+{}":?> -+(0)</td
	AutoTestNetwork(1)
	Marketing_carrie(0)

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



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

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

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

Total									
27		100 %	HD2/14	52%	Total 35.96 GB	† 479.24 MB	⊥ 35.49 GB	R02 / 34.04 GB 1 369.37 MB 1 33.60 GB	95%
30 25		AMALN	attel/10	37%	3.26 GB		• Total	RD1 / 1.80 GB T 46.13 MB 1 1.76 GB	516
20					2.79 GB		11.1		
15			RD1/3	11%	2.33 GB			attel / 80.99 MB 1 45.91 MB 1 35.08 MB	0%
10			1111/0	0%	1.85 GB 1.40 GB				0%
5			-	0%	953.67 MB			RD8 / 30.77 MB 1 17.82 MB 1 12.95 MB	0.0
			ALANWEN / D	0%	476.84 MB			1111/0 Byte 1 0 Byte 1 0 Byte	014
12:00	16:00 20:00 00:00 04:0	0 08:00	-		0 Byte 12:5	00 16:00 20:00 00:	00 04:00 08:00	• • • •	
12:00 New Device		0.08:00	-	• • • • - ~ ×	124	00 16:00 20:00 00:	00 04:00 08:00		
		0. 08:00 Device 1			124	00 16:00 20:00 00:	00 04:00 08:00		
New Device	25	Device 1		- 2 ×	124	10 16:00 20:00 00:	00 04:00 08:00		1.143
New Device	05 IP Address	Device 1 3910_0	* Name	- 🖍 × Device Type	124	00 16:00 20:00 00:	00 04:00 05:00		1.003
New Device	PS 172,17,5,151,4433	Device 1 3910.0 291250	Name 01DAA18E740	- ,* × Device Type Vigor3910	124	00 18:00 20:00 00:	00 04400 08500		
Action	es 19 Address 172,17,5,151,3433 14,161,2,165,443	Device 3910.0 291250 2912.0	Name 01DAA18E740 1_001DAA8C0F0C	- J* X Device Type Vigor/3910 Vigor/3912Fn	124	00 18-00 20:00 00v	0 0400 0800		

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

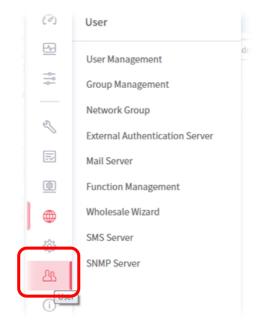
+ Add New Device			×
Add to Network	Root Network		Q
Device name:	3910_001DAA18E740		
Location:			
Emergency phone:			
Set to known device:			
		Cancel	✓ Apply

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

A.4 How to Create a New User Group?

Only the administrator can create a new user group.

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



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

er / Group	p Management										C
Catting	Management										
+Add										Search_	α,
_	Group Name	140	Max Nodes	 Used Nodes	- 18	Enable Expire Date	41 Expline Date	21 Enable Global Mail Server	11 Enable Global SNMP Sat	ver	
	RootGroup		No Limit Nodes	1		(thuilden)		(*****	(70110)		

RootGroup is a default setting.

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

User / Group Management			C
Setting Management			
Add Group			
Group name	Marketing	× .	
Nodes	10		
Enable CPE Notify Mail/SMS/SNMP			
Enable Global Mail Server	00		
Enable Global SNMP Server			
Enable Expire Date			
Expire Date	2020/09/22		
			Cancel Save

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

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

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

etting	Management												
bt												Search	
	Group Name	41	Max Nodes	17	Used Nodes	17	Enable Expire Date	47	Expire Date	Enable Global Mall Server	41	Enable Global SNMP Server	
0	RootGroup		No Limit Nodes		62		Olsabled			Enabled		Enabled	
-	Marketing		No Limit Nodes		1		Disabled)			Disabled		Obabled	

This page is left blank.

Part II

SD-WAN



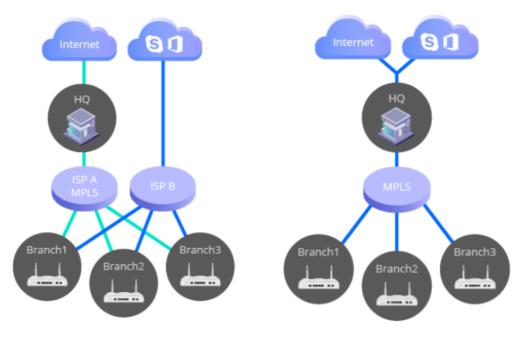
Chapter 4 SD-WAN Solution

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

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

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

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

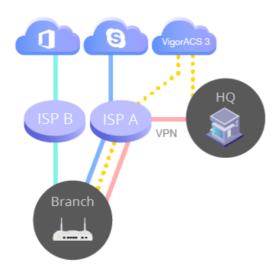


Direct Internet Access with lower cost

Tunneled via Central Site with higher cost

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

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



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

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

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

4.1.1 Enabling SD-WAN on VigorACS

To enable SD-WAN function on VigorACS, simply open Network Management under Root Network.

Specify a network group (e.g., RD8) which contains the CPEs supporting SD-WAN features. On the Setting page, turn on the toggle button of **Enable SD-WAN**. Then click **Reset Bulk Data Profiles to Default** to use the bulk data with the default values. At last, click **Save**.

	Root Network	Dray Tek VigorAC	53 mk_team_1 System Administrator
)	draytek_rd3(0)	a	
	draytek_rd5(6)	Network ID	Username
	# draytek_rd6(0)	8	draytek_rd8
	b draytek_rd7(5)	Name	Password
	draytek_rd8(14)	draytek_rd8	
	2135FVac_1449BC170DA8	Location	
		Advanced Settings	
		Enable SD-WAN	
		Enable SO-WAN	
		Bulk Data Settings	
			You can freely select the data you want to count, use drag and drop to place each category in
		corresponding profile, and specify the report interval at which	You can freely select the data you want to count, use drag and drop to place each category in the profile returns a bulk data to the ACS. If you disable bulk data categories, it will affect the
			the profile returns a bulk data to the ACS. If you disable bulk data categories, it will affect the
		corresponding profile, and specify the report interval at which WNN operation. Profile #1 Enable Profil	the profile returns a bulk data to the ACS. If you disable bulk data categories, it will affect the
		corresponding profile, and specify the report interval at which WNN operation. Profile #1 Enable Profil	the profile returns a bulk data to the ACS. If you disable bulk data categories, it will affect the e #2 Enable C Available / Disabled Bulk Data Categories
	Delete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) Report 120 200	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the e #2 Enable Control (sec) Available / Disabled Builk Data Categories
	B Delete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) 120 Bulk Data Categories Bulk Data Categories	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the e #2 Enable Available / Disabled Builk Data Categories interval (sec)
	E Delete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) Profil 120 Buik Data Categories E WAN and VPN Size #	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the e #2 Enable Control (sec) Available / Disabled Builk Data Categories
	Celete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) Eulk Data Categories WAN and VPN Size: 8 UOIP Size: 1	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the e #2 Enable Available / Disabled Builk Data Categories interval (sec)
	Boliete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) Profil 120 Buik Data Categories E WAN and VPN Size #	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the e #2 Enable Available / Disabled Builk Data Categories interval (sec)
	B Delete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profil Report interval (sec) Eulk Data Categories WAN and VPN Size: 8 UOIP Size: 1	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the end of t
	[⊕] Delete Devices	corresponding profile, and specify the report interval at which WAN operation. Profile #1 Enable Profile Report interval (sec) Buik Data Categories WAN and VPN Size # VoIP Size 1	the profile returns a builk data to the ACS. If you disable builk data categories, it will affect the end of t

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

Auto VPN

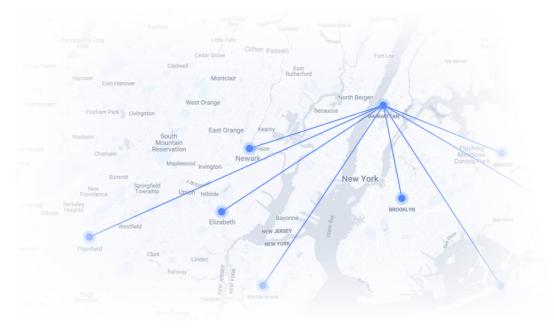
- VoIP WAN, and
- Full Traffic Control with SD-WAN Route Policy

4.1.2 Auto VPN

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

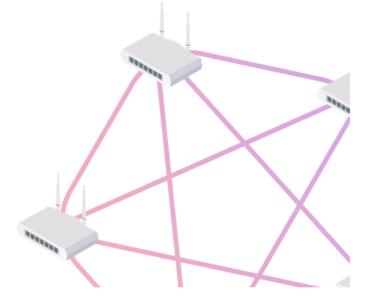
• For Hub and Spoke(s)

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



For Full Mesh

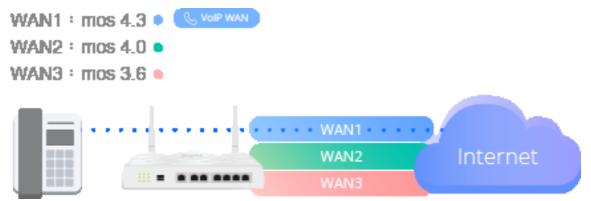
VigorACS server will create tunnels between each router automatically. If a subnet conflict occurs, VigorACS server is capable to design and suggest LAN subnets for all devices.



4.1.3 VoIP WAN

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

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



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

Real-time Call Quality Monitoring

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

Live Failover when Having Poor Call Quality

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

Live Failover Scenarios

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

4.1.4 Full Traffic Control with the Route Policy

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

(Configuration>>Route Policy>>+Add New Route Policy)

Add a New Route Policy		
Source	Апу	,
Destination	App Services	-
App Service Profile	Create a new profile From an existing profile	
Selected App Service	Amazon.com 🛞 YouTube 🛞].
Send via Interface	WAN 1	•
first. Go to SD-WAN VPN Set	Default Gateway Specific Gateway	
Packet Forwarding to WAN/LAN via	Force NAT Force Routing	
Failover		
	✓ Fallover to Default WAN ✓ when Interface offline.	
Failover to Gateway	Default Gateway Specific Gateway	
Failback	\bigcirc	
	— Basic Mode	
	Cancel Save and set to C	PE

4.2 Dashboard for SD-WAN Network Group

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

RD8	^		Dra
Root Network(251)	,	م	×
Network	Model		С
퓲 RD1(4)		品 jaytest(2)	>
옮 RD2(7)		옮 richard(2)	>
옮 RD3(14)		器 robin_test(2)	>
옲 RD5(8)		윪 sdwantest2(0)	>
옮 RD6(2)		▲ 2132FVn_001DAAE486C8	
옮 RD7(15)			ł.
음 RD8(55)		▲ 2135Vac_1449BC03B060	
유D3(55) 옮 RD8-1(1)	>		

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

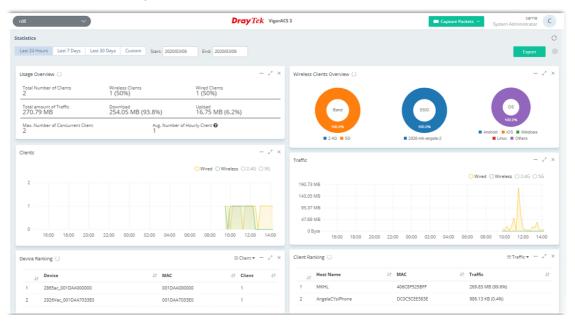
=	simulator V	Dray Tek VigorACS 3	Capture Packets > System Administrator
0	Dashboard		\bigcirc Auto Refresh: $\[5 minutes \lor\]$
<u>lat</u>	Summery <u>SD-WAN</u>		
	Wired WAN Q 74 hrs Wireless WAN Q 7 days	IPsec VPN 024 hrs Other VPN 024 hrs	VolP (07 days
Bo 111	Average MOS MOS Compliancy No Data	Average MOS MOS Compliancy No Data	Average MOS MOS Compliancy $3.9 \qquad 33 \ \% \ge 4.0$
	3.2 26 $\% \ge 4.0$	$\begin{array}{cccc} 3.4 & 31 & 5 & \geq 4.0 \\ 4.34 & 4.31 & 5 & = 1 \\ \end{array}$	✓ 3.9 ✓ 33%
Z,			
	Active Physical WAN	Active VPN	Active VoIP Call Detected 67117 — Failovered 33451
<u> </u>	• Wired 10 • Wireless 2.46 / 5G 0	• IPSec 9 • SSL 0	
@ @	U WAN Online LTE 0	9 VPN Online L2TP 0	
25	• USB 0	• PPTP 0	0
1			
	Active Physical WAN Quality	Active VPN Quality	Active Call Quality
	Great 4.3-5.0 2 Good 4.0-4.2 0	Great 4.3-5.0 3 Good 4.0-4.2 1	Great 4.3-5.0 • 360 Good 4.0-4.2 30098
	Okay 3.6-3.9 1 Poor 3.1-3.5 2	Okay 3.6-3.9 1 Poor 3.1-3.5 0	Okay 3.6-3.9 36513 Poor 3.1-3.5 146
	Bad 1.0-3.0 5	Bad 1.0-3.0 4	Bad 1.0~3.0 0
	2 Routers are Having Poor Active Physical WAN Quality. 2952Pn_001DAA00001, 2952Pn_001DA4000007 5 Routers are Having Bod Active Physical WAN Quality. 2952Pn_001DA400009, 2952Pn_001DA4000008, 2952Pn_00	4 Tunnels are Having Bad Active VPN Quality. 2952Pn_001DM400009, 2952Pn_001DM4000008, 2952Pn_00	10 Routers are Having Poor Active Call Quality. 2953Pn_001DA4600009, 2953Pn_001DA4600008, 2953Pn_00
	More	More	More

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

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

4.3 Statistics for SD-WAN Network Group

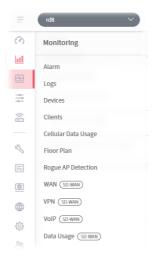
The page offers statistics for all the devices listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various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



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

4.4 Monitoring for SD-WAN Network Group

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

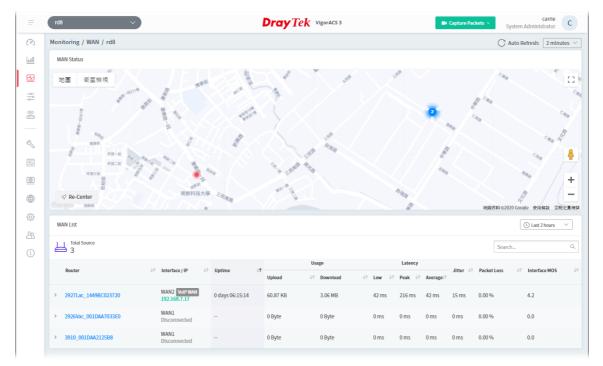


In which, the usage and settings for Alarm, Logs, Devices, Clients, Cellular Data Usage, Floor Plan and Rogue AP Detection are totally the same as the network group without SD-WAN enabled. For detailed information, refer to **Chapter 8 Network Group Menu**.

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

4.4.1 WAN (SD-WAN)

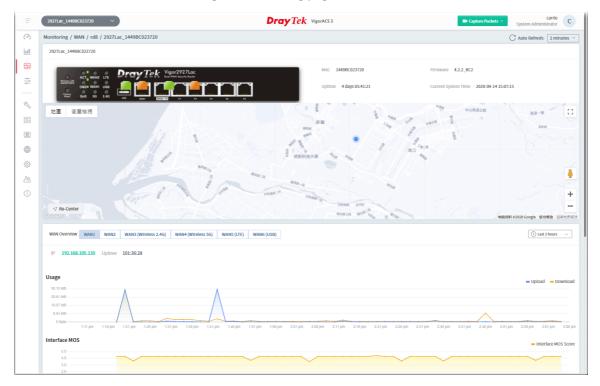
This page displays the location, name, interface/IP, uptime, usage, latency, jitter, packet loss and interface MOS of the routers within the group.



These parameters are explained as follows:

ltem	Description
WAN Status	Displays the location of the network group.
WAN List	Displays the total number of CPEs within the selected group.

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



4.4.2 VPN (SD-WAN)

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

	rd8 V	Dray Tek VigorACS 3	Capture Packets Capture Packets Carrie C
(⁷)	Monitoring / VPN / rd8		\bigcirc Auto Refresh: 2 minutes \checkmark
400	VPN Status		<u>818</u>
62	地園 衛星檢視		1
		and the second s	
2	0 Tunnel(s)	• •	
2	Great 0 Good 0	11/11/1	
	Okay 0 Poor 0		4
	Bad 0 Disconnected 0	0.00	+
() ()	+ Add VPN Tunnel(s)		地圖資料 ©2020 Google 使用條款 回轉地圖燈錄
	Tunnel List		\odot Last 2 hours \checkmark
0	Total Source		Search Q
	# 라 Source 라 Destination - 라 Type - 라 Upt	time -11 Usage Latency Jitter Upload -11 Download -11 Low -11 Peak -11 Average -11	থি Packet Loss থি Interface MOS থি
		No data available	

4.4.2.1 AutoVPN Establishment

As a Hub-and-Spoke network,

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

4.4.2.2 Creating VPN with Basic Mode

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

VPN Setup	×
Туре	Hub and Spoke Full Mesh
Hub Devices	2927Lac_1449BC023720 (Vigor2927Lac) 🛞
Support spokes count	64
	+ Advanced Mode
	× Cancel Save and set to CPEs

These parameters for Basic Mode are explained as follows:

ltem	Description
Туре	Hub and Spoke - Simply select a router as the hub router, the rests would be spokes automatically.

	VPN Setup ×	
	Type Hub and Spoke Full Mesh	
	Hub Devices 2927Lac_1449BC023720 (Vigor2927Lac) ③	
	Support spokes count 64	
	Full Mesh - It is effective only when there are more than three CPEs on the group.	
	VPN Setup ×	
	Type Hub and Spoke Full Mesh	
	Full Mesh Devices 2927Lac_1449BC023720 (Vigor2927Lac) ③ 2927Lac_1449BC0237E8 (Vigor2927Lac) ③	
	Support spokes count 64	
Hub Devices / Full Mesh Devices	Lists the name of the hub device or full mesh device. Select one device as the hub device.	
Support spokes count	Displays the total number of devices, excluding the main device.	
+Advanced Mode	Click to open the configuration page with more options.	
Save and Set to CPEs	Save the above configuration and set to CPE devices.	

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

n88 ~	Dray Tek VignerACS 3	Bi Capture Packets - System Administrator
	Creating VPN Hub and Spoke Connections,	
	Succeed: 1 Processing: 0 Waiting: 0 If alled: 0 Processing: 0 Succeed: 0	

3. The VPN tunnel has been set successfully.

4.4.2.3 Creating VPN with Advanced Mode

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

Туре	Hub and Spoke Full Mesh
Hub Devices	2927Lac_1449BC023720 (Vigor2927Lac) 🛞
Support spokes count	64
	+ Advanced Mode

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

VPN Setup	×	
Туре	Hub and Spoke Full Mesh	
Hub Devices	2927Lac_1449BC023720 (Vigor2927Lac) 🛞	
Support spokes count	64	
Spoke Devices VPN Connection Through Dial Type	2927Lac_1449BC0237E8 (vigor2927Lac) ⊗ WAN1 First ✓ IPsec Tunnel PPTP L2TP SSL	
IPsec		
Customize IKE Pre-Shared Key		
IKE Pre-Shared Key	Required, Please input IKE Pre-Shared Key	
IPSec Security Mathod	AES ~	
— Basic Mode		
	× Cancel Save and set to CPEs	

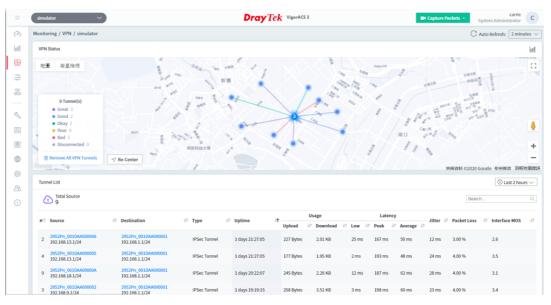
These parameters for Advanced Mode are explained as follows:

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

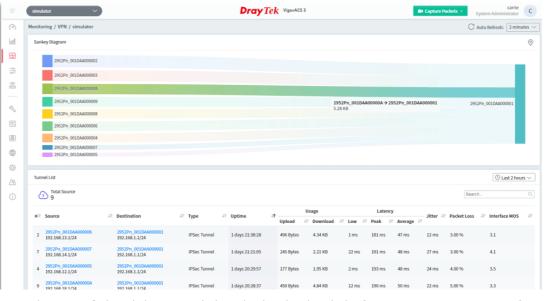
	with no authentication.						
	AES						
	AH						
	DES_NO_AUTH						
	DES						
	3DES_NO_AUTH						
	3DES						
	AES_NO_AUTH						
	AES						
PPTP - PPTP is selee	cted as Dial Type						
РРТР	Username - Enter a username for establishing VPN connection.						
	Customize Password - Click to enable the password configuration.						
	• Password - Enter a username for establishing VPN connection.						
	PPP Authentications - Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.						
	VJ Compression - Click to enable Van Jacobson (VJ) header compression						
	to improve throughput on slow connections.						
	Dial Type IPsec Tunnel PPTP L2TP SSL						
	РРТР						
	Username Generate automatically						
	Customize Password						
	PPP Authentications PAP/CHAP/MS-CHAP/MS-CHAPv2						
	VJ Compression						
L2TP - L2TP is selec	ted as Dial Type						
L2TP	L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP						
	VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:						
	• None - Do not apply the IPsec policy. Accordingly, the VPN						
	connection employed the L2TP without IPsec policy can be viewed						
	as one pure L2TP connection.						
	 Nice to Have - Apply the IPsec policy first, if it is applicable during pagatiation. Otherwise, the dial is VPN connection becomes and 						
	negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.						
	• Must - Specify the IPsec policy to be definitely applied on the L2TP connection.						
	Username - Enter a username for establishing VPN connection.						
	Customize Password - Click to enable the password configuration.						
	• Password - Enter a username for establishing VPN connection.						
	PPP Authentications - Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.						
	VJ Compression - Click to enable Van Jacobson (VJ) header compression						
	to improve throughput on slow connections.						

	Dial Type IPsec Tunnel PPTP L2TP SSL
	L2TP
	L2TP with IPsec Policy None ~
	Username Generate automatically
	Customize Password
	Password Required, Please input password IIII Required Please input password
	PPP Authentications PAP/CHAP/MS-CHAP/MS-CHAPv2 ~
	VJ Compression
SSL	Server Port (for SSL Tunnel) - Enter a port number for SSL Tunnel. The default is 443.
	Username - Enter a username for establishing VPN connection.
	Customize Password - Click to enable the password configuration.
	• Password - Enter a username for establishing VPN connection.
	PPP Authentications - Authenticate dial-in users using the PAP protocol
	only or PAP/CHAP/MS-CHAP/MS-CHAPv2.
	VJ Compression - Click to enable Van Jacobson (VJ) header compression to improve throughput on slow connections.
	SSL
	Server Port (for SSL Tunnel) 443
	Username Generate automatically
	Customize Password
	Password Required, Please input password
	PPP Authentications PAP/CHAP/MS-CHAP/MS-CHAPv2 ~
	VJ Compression
-Basic Mode	Click to return to configuration page with less options.
Save and Set to CPEs	Save the above configuration and set to CPE devices.

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



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



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

v	/PN Overview												© La	st 2 hours 🗸
S	earch VPN Tunnel List Q	To 2952Pn_001DAA0	000003 IP	192.168.105.52										
	Total													
1	To 2952Pn_001DAA000002 192.168.105.52	COD Bytes											Upload 🗕	Download
2	To 2952Pn_001DAA000003 192.168.105.52	400 Bytes 200 Bytes												
3	To 2952Pn_001DAA000004	0 Byte	1:26 pm	1:36 pm	1:40 pm	1:58 pm	2:08 pm	2:18 pm	2:26 pm	2:38 pm	2:45 pm	2:50 pm	3:06 pm	3:16 pm
4	To 2952Pn_001DAA000005	Interface MOS											 Interface I 	MOS Score
5	To 2952Pn_001DAA000006	3.0 2.0 1.0											L	
6	To 2952Pn_001DAA000007	0.0	1:28 pm	1:38 pm	1:45 pm	1:58 pm	2:08 pm	2:18 pm	2:28 pm	2:38 pm	2:48 pm	2:58 pm	3.06 pm	3:10 pm
7	To 2952Pn_001DAA000008	200 ms 150 ms										-	Low – Average	e – Peak
	To 2952Pn 001DAA000009	100 ms												

	() Last	2 hours \sim
	Last 1 hour	
S	Last 2 hours	~
	Last 3 hours	
	Last 6 hours	
Packet Loss	Last 8 hours	
	Custom	
3.00 %		ОК
2.00 %	4.0	

4.4.3 VoIP (SD-WAN)

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

nito	oring / Vo	P / simulator													(
IP (Call List													🕚 Last 2 ho	urs 🗸
	1414 Tetal	11 • Great 5.0 - 43	4.2 - 4.0		4 • Poor 3.5 - 3.1 Finished (810	0 • Bad 3.0 - 1.0					Rows	10 +	н с и	1160 >	DK
		10002							Latency					1 Packet Loss J1 MOS	
	Status 11	cus11 LAN IP 1	11 Peer IP 11 Call ID11	Via Interfa	sce 🕸 Start Time		Failovered Interface 41		Low or	Peak 47	Average		Packet Loss +1 M	MOS	
	3	192.168.120.118	40.197.130.3	4 8850	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:37 PM			00:00:53	15 ms	484 ms	220 ms	12 ms	0 %	4
	S	192.168.120.119	231.242.7.11	2 8849	WAN3	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:26 PM			00:01:04	7 ms	467 ms	240 ms	14 ms	1 %	4
	8	192.168.120.120	140.51.54.84	8848	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:57 PM			00:00:33	18 ms	478 ms	279 ms	12 ms	0 %	4
	ß	192.168.120.116	98.108.133.2	32 8846	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:46 PM			00:00:44	10 ms	493 ms	252 ms	12 ms	0 %	3.8
	\$	192.168.120.117	147.116.111.	78 8845	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:41 PM		-	00:00:49	7 ms	481 ms	237 ms	14 ms	0 %	4
						2020/03/19 03:53:30 PM									

These parameters are ex	plained as follows:
-------------------------	---------------------

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

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

4.4.4 Data Usage (SD-WAN)

	rds 🗸	Dray Tek VigerACS 3	Capitare Packets - System Administrator
Ó	Monitoring / Data Usage / rd8		C Auto Refresh: Sminutes 🗸
Int	Source Map		
-	地图 高量抽消		0
⊕ 18 18 19 4H	✓ Recenter	an a	A114
\$		BHB	©tarthous v ∃≣
26	App Source Overview		() Last 2 hours → 1:22 () Last 2 hours → 1:22
0	1 Total Source	Sort Dy Device Name Traffic &	South. 9.
	2927Lac_14498C023720 VigeC07/Lac (1498C023720)	2865ac_001DAA800000	2855ac_14498C05F1A8 VigeoRisk (1460C05F1A8)
	Upited Described 90.88 MB 211.02 MB	Upload Download 469.23 KB 115.56 KB	Uptood Download O Byte
	2926Vac_0010AV7023E0 Viger78New (0010AV7023E0	2927Lav: 1449BC022740 Vige/317Lav: (1448BC022740)	2927Lax_14496C0227E8 Wgr/107Lax_(1440621718)

4.4.4.1 Data Usage of Selected CPE

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

2977Lac_14498C023720 ~	Dray Tek VigorACS 3		Er Cuptur	Carrie System Administrator
Monitoring / Data Usage / rd8 / 2927Lac_1449BC023720				C Auto Retresh: 5 minutes
2927Lac_14498c023720				() Lost update at 2020/11/13 (1)-O pr
Usage Sorting by Application Client Device				③ Last 2 feurs
TOINI Search Category or App				
	Protocol	211,45 MB	Cithers.	\$1,64 HD
	Instant Message	24.78 105	• WHP	7,13 (0)
Total	Apple Services	2.17 Mil	Google Services	2.17 HI
301.89	Stram	1,44 MI	Turneting	928.10 10
	 Web HD 	19542 vii	 Remote Control 	3.6 0
Traffic Line Chart Upload/Downsoad By Interface				
				- Upicad - Downio
30.15.60 23.81.00	~	A		
10.27 MB 3.04 LB	\sim			
11-60 ans 11:00 ans 12:00 pm 12:00 pm 12:00 pm 12:00 pm	12-20 pm 12-30 pm 12-30 pm 12-40 pm 12-	C-89 pm 100 pm 1-00 pm 1-10	pm 1.10 pm 1.20 pm 1.28	n 132pm 132pm 142pm 145

These parameters are explained as follows:

ltem	Description
Usage Sorting by	Displays a pie chart related to various application usage.

	Application - C	-				sage.				
	Client Device - Click to display a pie chart for the selected CPE.									
Traffic Line Chart	Displays a line of interface. Upload/Download By Interface - Of interface.	oad - Click to	o display da	ata upload/do	wnload.					
Usage List by	Displays the dat	a usage for	common A	ons or for co	nected client					
	Application - C applications, inc download usage	luding name	e of applica	ation, number	of users, upl	oad and				
	(?) Manifuring / Bata Diage / HB / 2021Lac.	44980023720	Dray Tek	VigerACS 3		carrie C				
	Influence 2017.ex., 1460000107 Signature Varge strateg fy Application Class to Signature Non-theory or Application Signature Non-theory or Application Signature Non-theory or Application Signature Non-theory or Application Non-theory or Application Non-theory or Application	на 53,74 ы	Apple Service Protocol Grange Servic Web ID	5.09.1	• Ohen • Sanaling • Nati	© Last 10 Day.∨ 7 64 50 1,00 *0 12,4 *0 12,4 *0				
	and and and and and and and and and and	Contract (1944 - NEWS CORES)	Mar 1964 1964 1994	That that the tilles the	the the the the	1010 1010 1010				
	Usingle List by Application Claims Device				-					
	* 4 App Name	27 Users	<i>2</i>	Upland	ir Download					
	1 Facebook/Instagram 7 LINF			0 Byte 11 Dyne	0 Byte C Byte					
	Client Device - including host r system, upload	ame, IP add and downlo	ress, MAC							
	10-50 July	te liter the the th	n tiller (Mer 1964))	te the life life life i	to the the the late	Inter Inter Inter				
	Usage List by Application Camer Device				Upate					
	a 🏭 Host Name 🔅 19 Address	2 MAC Address	Enconction Type	# 05 # Upload	a Download					
	1 adam MBP 190,348.13 2 Unknown 192,368.13		T Wireless (5G) (5, word	100 Bytes 100 June	132 Bytes 2.14 KB					
	3 #2000675 192,348,23 4 YRCs-iPhone 152,348,134		A Wind	© 1551.H8	4.44 MB					
	4 TRCs-iPhone 152,366,134	11 BEISCEDCERC2	T WITHHAL CALL	GD 644.29 KB	36.63 MD					
	5 gboy20 192.168.13	13 EM/RESCHEDAD	TWeeless (50)	© 4.80 KB	13.03 KB	100				

Chapter 5 SD-WAN CPE

The menu items related to a CPE:



5.1 Dashboard for SD-WAN CPE

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

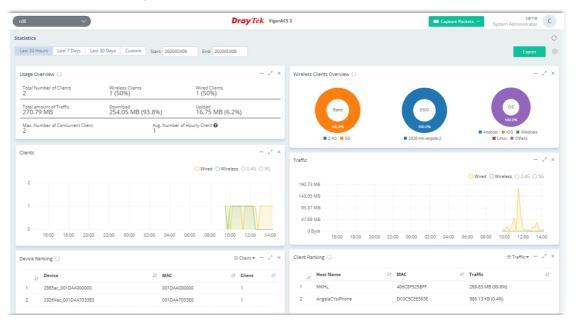


In this case, we choose Vigor2865 series (e.g., Vigor2865ac) as an example.

2865ac_001DAA000000)	-	Dray Tek	VigorACS 3	🖬 Сар	ture Packets ~ Sy	carrie stem Administrator	С
2865ac_001DAA00000	00			Device Status: onli	ne Alarms: 0 Active	Clients: 1 Auto Re	iresh: Disable 🗠	c
ell Port Status				WAN Overview			⊙ Last 24 h	
-0 -0 -0		2865oc Ing Famal	The second se	76.29 MB 57.22 MB 38.15 MB 19.07 MB 0 Byte			• Tot	V
Device Information	2865ac. 001DAA000000	DSL Information		18:00 20:00 22:00 Total (↑70.42 MB ↓ 529.86 MB)	00:00 02:00 04:00	06:00 08:00 10:00		16:00 100 %
IP Address	https://192.168.105.123:443	DSL Type	VDSL2	WAN1 (↑0 Byte ↓0 Byte) WAN2 (↑70.42 MB ↓529.86 MB)				0%
Network Name	rd8	Modulation Type	Multimode	WAN3 (↑ 0 Byte ↓ 0 Byte)				0%
Model	Vigor2865ac 🥏	Download Speed(kbps)	0	WANS (10 Byte +0 Byte)				0%
Firmware Version	4.2.0.1_STD 🥑	Upload Speed(kbps)	0	WAN4 (10 Byte +0 Byte)				0%
MAC Address	001DAA000000	SNR Margin	0					
Up Time	2 days 02:25:01	Loop Attenuation(0.1dB)	0	WAN6 (↑0 Byte ↓0 Byte)				0%
	~ show more		~ show more	WAN ↓↑ Line/Mode	.↓† IP	J↑ Uptime	J↑ Active Mode	Ψţ
System Resource			⊙ Last 24 hours ~	WAN1 VDSL2 / PPPoE WAN2 Ethernet / Static IP	192.168.105.123	0d 00h 00m 2d 02h 23m	Always On Always On	
CPU	5%	CPU Temperature	100 °C	WAN3 Wireless_2.4G /		0d 00h 00m	Always On	
30% 20% 10%	when the	150°C 100°C 50°C		WAN4 Wireless_5G /		0d 00h 00m 0d 00h 00m	Always On	
0% 21:20 Memory	02:40 08:00 13:20 82 %	0°C 21:20 02:40 08:00	13:20	WANG USB/		0d 00h 00m	Always On	
100%				I AN Overview			③Last 24 h	

5.2 Statistics for SD-WAN CPE

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

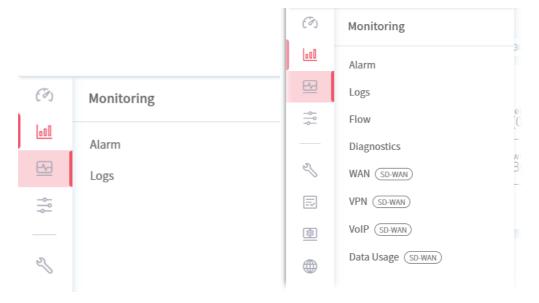


In addition, the statistics can be exported as ".XLS" file if you click the **Export** button on the top side.

5.3 Monitoring for SD-WAN CPE

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

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



5.3.1 Alarm

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

	2927Lac_14498C023720 V		Dr	ay Tek VigerACS 3		in Capture Packets	System	carrie Administrator	
(P)	Monitoring / Alarm					2020/08/15 to 2020/09/14 ~	search No. /	Device Name	/ MAC C
al.	Alarm History								
83	🖷 Download 🕈 Delete All 🕁 Download					80 K	1 /1	> H (2 0
-0-	No. Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	AL	arm Type	
S				No data available					
5									

	29271	Lac_1449B(C023720 ~		Dray 1	ek VigorACS 3		Capture Packets	carrie System Administrator
(7)	Monito	oring / A	larm					2020/08/15 to 2020/09/14 \vee	search No. / Device Name / MAC Q
000	Ala	rm	History						
6		elete 🗎 🖨	Delete All 🕁 Download					ы <	$1 / 1 \rightarrow \mathbb{N} \mathbb{C} \otimes$
		No.	Time	Device Name	MAC Address	Clear Time	Alarm Level	Alarm Message	Alarm Type
		63328	2020/09/10 01:50:36 PM	2927Lac_1449BC023720	1449BC023720	2020/09/10 02:07:47 PM	4 Warning	WAN2 Loss Connection	Interface Lost Connection
Z		63274	2020/09/10 01:19:26 PM	2927Lac_1449BC023720	1449BC023720	2020/09/10 01:45:58 PM	👃 Warning	WAN2 Loss Connection	Interface Lost Connection
Ð		63240	2020/09/10 10:12:13 AM	2927Lac_1449BC023720	1449BC023720	2020/09/10 01:18:19 PM	🗘 Warning	WAN2 Loss Connection	Interface Lost Connection
<u></u>		63056	2020/09/07 10:43:29 AM	2927Lac_1449BC023720	1449BC023720	2020/09/07 11:05:53 AM	\Lambda Critical	Device Loss Connection	Device Lost Connection
		63008	2020/09/04 03:32:37 PM	2927Lac_1449BC023720	1449BC023720	2020/09/07 10:35:33 AM	▲ Critical	Device Loss Connection	Device Lost Connection
÷\$}		62878	2020/09/02 03:51:10 PM	2927Lac_1449BC023720	1449BC023720	2020/09/02 03:51:26 PM	▲ Critical	Device Loss Connection	Device Lost Connection
28		62615	2020/08/26 01:13:59 PM	2927Lac_1449BC023720	1449BC023720	2020/08/26 01:28:00 PM	▲ Critical	Device Loss Connection	Device Lost Connection
(j)		61863	2020/08/24 11:14:42 AM	2927Lac_1449BC023720	1449BC023720	2020/08/24 11:14:42 AM	A Critical	Device Loss Connection	Device Lost Connection
		61548	2020/08/19 02:31:46 PM	2927Lac 1449BC023720	1449BC023720	2020/08/19 02:43:28 PM	▲ Critical	Device Loss Connection	Device Lost Connection

These parameters are explained as follows:

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

5.3.2 Logs

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

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

28654	IC_001DAA00	xxxxx ~			Dray Tek Vigor ACS 3		III Capture Packet	System Administrator
Monito	oring / Log	55					2020/08/26 to 2020/09/25 ~	search ID / Device Name / Devic
All CPI	E Actions	Device Reboot Reboot By CPE	Reset System Password	Set Parameter	File Transfer Setting Profile	Device SysLog CPE Notify	Device Register Device Operate	
	iete 🔀 🕻	elete All 🕹 Download					ы <	1 /2 > ▷ C 1
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
	57063	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Set Parameter Values	6778	2020/09/25 03:02:51 PM
	57060	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Set Parameter Values	6775	2020/09/25 03:02:48 PM
	57055	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Set Parameter Values	6771	2020/09/23 02:25:41 PM
	57044	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Set Parameter Values	6769	2020/09/23 02:24:59 PM
	57032	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Set Parameter Values	6768	2020/09/23 02:24:20 PM
	57031	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22613	2020/09/23 02:24:19 PM
	57030	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22612	2020/09/23 02:24:17 PM
	57029	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add ObJect	22611	2020/09/23 02:24:16 PM
	57028	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22610	2020/09/23 02:24:14 PM
	57027	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22609	2020/09/23 02:24:12 PM
	57026	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22608	2020/09/23 02:24:11 PM
	57025	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22607	2020/09/23 02:24:09 PM
	57024	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22606	2020/09/23 02:24:07 PM
	57023	2865ac_001DAA000000	166	001DAA000000	192.168.105.123	Add Object	22605	2020/09/23 02:24:06 PM

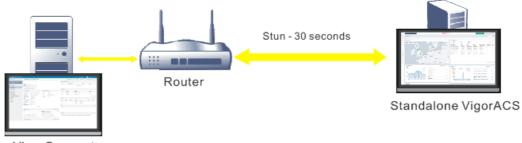
These parameters are explained as follows:

ltem	Description
Log Туре	Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page.
search ID / Device Name / Dr Q	Enter the condition for VigorACS to search and display relational information.
Delete	Clear the selected record.
Delete All	Clear all of the records.
Download	Click this button to save log as a XLS file.

5.3.3 Flow

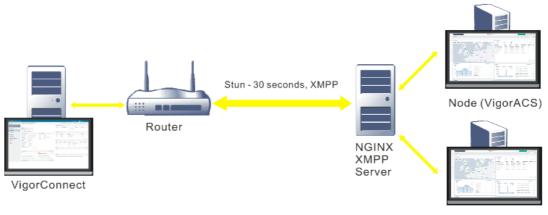
Vigor router adopts the function of NetFlow to collect the quantity and data of incoming and outgoing packets. With analysis of the collected data, the network administrator can get the source and destination IPs of the packets, type of network service, and the reason for network congestion.

Type 1: The working diagram among VigorConnect, Vigor router, and Standalone VigorACS.

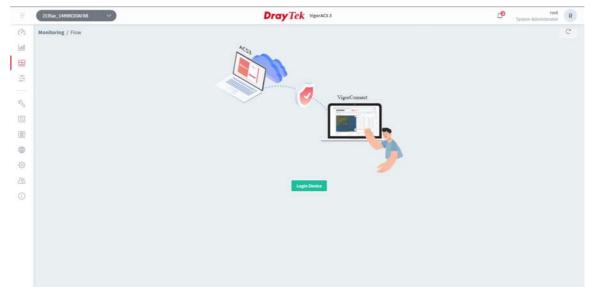


VigorConnect

Type 2: The working diagram among VigorConnect, Vigor router, XMPP Server, and Cloud/Cluster VigorACS.



Node (VigorACS)



The following page appears if visiting this page for the first time.

Click Login Device to display the advanced page.

(i) The device must support and enable the NetFlow protocol. In addition, it has to be registered to both VigorACS and VigorConnect first.

5.3.3.1 Device Overview

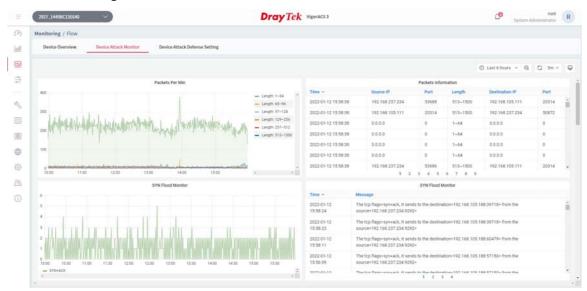
NetFlow uses several types of data to identify the data flow, for example, source IP address, destination IP address, source port number, destination port number, IP protocol, interface, and so on.

This page displays the pie charts and tables related to the IP address(es) and the transmission data usage of the selected device.

Devic	Device Att	ack Monitor	Device Attack Defe	nse Setting		
						🔿 Last é hours - Q 🖏 Sm -
inspect.)	SourceIP 192.168.237.234 +	Impect, DestiP	192.168.237.234 +			
		Top 10 De	tinations From 192.168	237.234		Top 10 Sources To 192.168.237.234
Destin	wtion IP			Usage -	Source IP	Usage -
192.16	58.105.111			947.7 kB	192.168.105.180	1.7 MB
192.16	58.105.180			842.0 kB	192.168.105.111	1.4 M8
192.16	68.105.238			139.3 kB	192.168.105.188	296.6 kB
192.16	66.105.188			125.3 kB	192.168.105.238	73.0 kB
192.16	68.105.235			8.3 10	192.168.105.235	0.8
8.8.8.8	8			6.6 kB	192.168.105.234	08
192.16	58.105.234			4.1 kB	8.8.8.8	08
224.0	0.251			0.8	224.0.0.251	0.8
		1	Flow Usage	- Countream 3.5 s/8 - Optimer 3.1 MB		L3 Protocol Visit Rate - 10P 72.0 - 17P 222 - 0Pers 0.0

5.3.3.2 Device Attack Monitor

This page displays data information related to attacks on the device. Use the scroll bar to the right side of each column to get/view the detailed information.

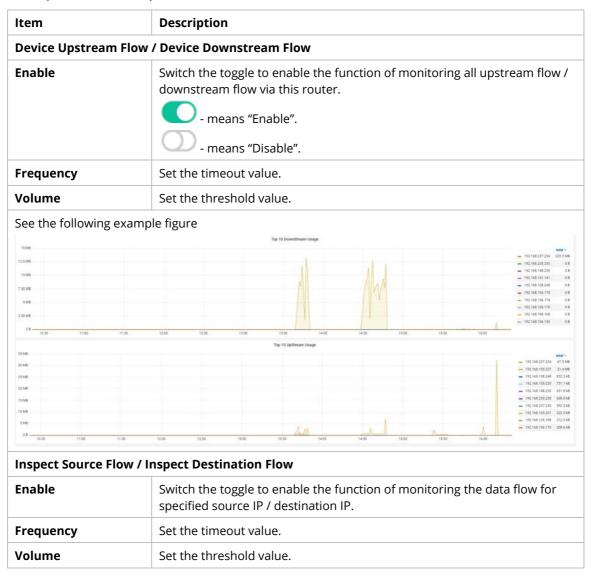


5.3.3.3 Device Attack Defense Setting

The purpose of this page is to configure the attack defense settings to detect the router from being attacked by external hackers or system attacks. When the volume of the transmitted packets arrives at a certain value and reaches the timeout, the system will notify the administrator through the mail, SMS, or SNMP service.

2927_14498C13E640 ~		Dray Tek VigorACS 3	CO root System Administrator
Monitoring / Flow			
Device Overview Device Attack Monito	or Device Attack Defense Setting		
Device Upstream Flow			
Enable	Ð		
Frequency	30 min	w.	
Volume	1	G8 ~	
Device Downstream Flow			
Enable	D		
Frequency	30 min	*	
Volume	1	GB ~	
Inspect Source Flow			
Enable	0		
Frequency	30 min	~	

These parameters are explained as follows:



Monitoring / Flow	Davies March Dalases Families						
Device Overview Device Attack Monitor	Device Attack Defense Setting						
			🔿 Last 6 hours - 🔍 💭 Sm - 😡				
Inspect,Sourcell* 192.168.237.234 - Imspect,Dest#	Top 10 Destinations From 192.168.227.234		Top 10 Sources To 192.168.237.234				
Destination IP	Usage -	Source IP	Usage -				
192.168.105.111	34.1 MB 32.1 MB	192.168.105.230 192.168.105.111	227.5 MB 3.6 MB				
192.168.105.188	935.0 kB	192.168.105.188	2.2 MB				
192.168.105.238	90 D kB	192.168.105.228	69.638				
192.168.105.225	8.7kB 6.6kB	192.168.105.235 192.168.105.234	08				
192,168,105,234	4.718	8.8.8.0	0.8				
274.0.0.251	68	274 8 0 751	0.8				
APP Flow							
Enable		to enable the function of ous APPs via the router.	f monitoring the data flow				
Frequency	Set the timeout v						
Volume	Set the threshold						
SYN Flood		vulue.					
Enable	Cultab the territ	to anable the function of	fmonitoring CVNI flood deferre				
Enable			f monitoring SYN flood defense.				
	When the arrival	rate of SYN packets excee	eds the Threshold value, the				
	router will start to	o randomly discard TCP S	YN packets for a period of time				
		•					
		as defined in Timeout. This is to prevent TCP SYN packets from exhausting					
	router resources.						
		The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively.					
Frequency	Set the timeout v	Set the timeout value.					
Volume	Set the threshold	Set the threshold value.					
ICMP Flood							
Enable	Switch the toggle to enable the function of monitoring ICMP flood defense						
	When the arrival rate of ICMP packets exceeds the Threshold value, the						
	router will start to randomly discard TCP SYN packets for a period of time						
	as defined in Timeout.						
	The default values of threshold and timeout are 250 packets per second						
	and 10 seconds,	respectively.					
Frequency	Set the timeout v						
Volume	Set the threshold						
UDP Flood	Set the threshold	value.					
Enable	Switch the toggle	to enable the function of	f monitoring UDP flood defense				
	When the arrival	rate of UDP packets exce	eds the Threshold value, the				
		•					
	router will start to randomly discard TCP SYN packets for a period of time						
	as defined in Timeout.						
	The default value	s of threshold and timeo	ut are 2000 packets per second				
	and 10 seconds,						
Frequency	Set the timeout v	· ·					
Volume	Set the threshold						
Land Flood							
Enable	Control of the second	the second leader of the second	f monitoring LAND attack events				

Frequency	Set the timeout value.				
Volume	Set the threshold value.				
Tiny Fragment					
Enable	Switch the toggle to enable the function of monitoring SYN packet fragments.				
Frequency	Set the timeout value.				
Volume	Set the threshold value.				
Push ACK Flood					
Enable	Switch the toggle to enable the function monitoring the ACK Flood attack.				
Frequency	Set the timeout value.				
Volume	Set the threshold value.				
RST Flood					
Enable	Switch the toggle to enable the function of monitoring the RST Flood attack.				
Frequency	Set the timeout value.				
Volume	Set the threshold value.				
Save	Click to save the settings.				

5.3.4 Diagnostics

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

5.3.4.1 Ping

← Configuration	2865ac_001DAA000000 / Monitoring / Diagn	nostics	
	Protocol	IPV4	~
Trace Route	Ping Through	Auto	~ ~
Routing Table ARP Table	Ping To	DNS-8.8.8.8	v
DHCP Table	Source IP	Auto	~
	IP Address	8.8.8.8	
		n't want to specify which WAN to ping through, j II fill Source IP according to the interface you pin	

These parameters are explained as follows:

ltem	Description
Protocol	Select the protocol (IPv4 or IPv6) to perform the ping operation.
Ping Though	Select a WAN interface from drop down list to through which you want to perform the ping operation, or choose Auto to be let the router select the WAN interface.
Ping To	Select the type of target (Host/IP, DNS, Gateway) to which you wish to ping. DNS-8.8.8.8 ~ Host/IP
Source IP	Select a WAN IP as the source IP. If Auto is selected, the source IP will be specified according to the interface chosen for ping through.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Run	Click to perform the job.

5.3.4.2 Trace Route

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

← Configuration	2865ac_001DAA000000 / Monitoring / Diag	nostics	С
Ping Trace Houte Routing Table ARP Table	Type Trace through Protocol	IPV4 IPV5	
DHCP Table Sessions Table	IP Address / Domain		
			tun

These parameters are explained as follows:

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

5.3.4.3 Routing Table

This page displays the IPv4/IPv6 routing information.

← Configuration	2865ac_001DAA0	00000 / Monitoring / Diag	gnostics					C
Ping	IPv4 Routing T	able						
Trace Route	Index	Destination	Subnet Mask		Gateway		Key	Iface
	1	0.0.00	0.0.0.0		192.168.105.1		•	WAN2
	2	192.168.105.0	255.255.255.0		directly connected		с	WAN2
ARP Table	3	192.168.10.0	255.255.255.255		192.168.1.2		S~	LAN1
DHCP Table	4	192.168.1.0	255.255.255.0		directly connected		C~	LAN1
	5	211.100.88.0	255.255.255.255		192.168.1.3		S~	LAN1
	IPv6 Routing T	ected S: Static R: RIP	*: default ~: private					
	Destination	Prefix Len	gth	Interface	Flags	Metric	Next Hop	p
	FE80::	64		LAN1	U	256	::	
	FE80::	64		LAN2	U	256	**	
	FE80::	64		LAN3	U	256	=	
	FE80::	64		LAN4	U	256	11	
	FE80::	64		LAN5	U	256		
	FE80::	64		LAN6	U	256		
	FE80::	64		LAN7	U	256		
	FE80::	64		LAN8	U	256		
	FE80:: FF00::	64		DMZ LAN1	U	256		
	FF00::	8		LAN1 LAN2	U	256 256		
	FFUU:	8		LANZ	U	256		

5.3.4.4 ARP Table

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

	_											
← Configuration	2865ac	_001DAA000000) / Monitoring / Diag	nostics								C
	B Clea	r										
Trace Route	LAN	WAN										
Routing Table												
	Show	AN		ALL LANS		~						
DHCP Table	Show	/LAN		ALL VLANs		~						
Sessions Table												
	Index	IP	MAC Address	HOST	D Interf	ice	VLAN	Port	Device	Description	Comment	
	15	192.168.1.10	8-D6-C7-01-A2-34	R1000	675 LAN1			P3				
← Configuration	2865ad	_001DAA00000	0 / Monitoring / Diag	nostics								(
Ping	B Cle	ar										
Trace Route	LAN	WAN										
Routing Table												
	Show	WAN		ALL WANS		~						
DHCP Table	Index	IP	MAC Address		IOST ID Inter		VLAN	Port	Device	Description	Comment	
Sessions Table	1	192.168.105.52			WAN		VLAN	Port	Device	Description	Comment	
	2	192.168.105.52			WAN							
	3											
	3	192.168.105.62	00-1D-AA-F7-C0-E2		WAN	2		-				
	4	192.168.105.62 192.168.105.71	00-1D-AA-F7-C0-E2 00-50-7F-F1-00-16		WAN	2						
	4 5	192.168.105.62 192.168.105.71 192.168.105.81	00-1D-AA-F7-C0-E2 00-50-7F-F1-00-16 00-1D-AA-7D-65-14		WAN WAN WAN	2 2 2		-				
	4	192.168.105.62 192.168.105.71 192.168.105.81 192.168.105.96	00-1D-AA-F7-C0-E2 00-50-7F-F1-00-16 00-1D-AA-7D-65-14		WAN	2 2 2 2		-				

These parameters are explained as follows:

ltem	Description
Show LAN / VLAN /	Select the LAN(s), VLAN(s) and WAN(s) to display ARP table information.
WAN	By default, information on all LANs, VLANs and WANs is displayed.

5.3.4.5 DHCP Table

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

← Configuration	2865ac_001DAA	000000 / Monitoring / Diagn	ostics			C
Ping	IPv4 Address	Assignment Table				
Trace Route	Name	IP	Mask	Start IP	End IP	DHCP Server
Routing Table	LAN1	192.168.1.1	255.255.255.0	192.168.1.10	192.168.1.209	On
ARP Table	() Note:					
DHCP Table		ick on a specific LAN to display	the detailed information of the	DHCP client.		
Sessions Table	IPv6 Address	Assignment Table				
	Interface	IPv6 Address	IAID	Link-Layer Address	Leased Time	DUID
				No data available		

5.3.4.6 Sessions Table

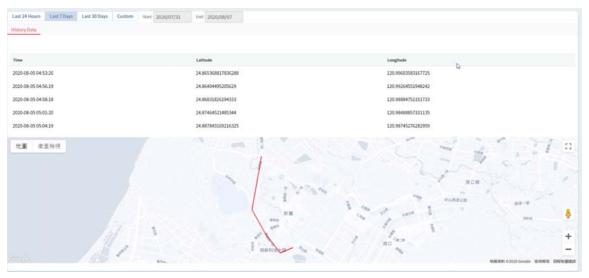
← Configuration	2865ac_001	DAA000000 / Monitoring /	Diagnostics				
	Index	Private IP	Private Port	Pseudo Port	Peer IP	Peer Port	Interface
Ping	1	192.168.1.10	64325	32837	8.8.4.4	53	WAN2
Trace Route	2	192.168.1.10	64325	32837	8.8.8.8	53	WAN2
Routing Table	3	192.168.1.10	65186	33698	216.58.200.227	443	WAN2
ARP Table	4	192.168.1.10	65196	33708	52.229.206.30	443	WAN2
	5	192.168.1.10	65289	33801	40.90.189.152	443	WAN2
DHCP Table	6	192.168.1.10	65433	33945	204.79.197.219	443	WAN2
	7	192.168.1.10	49270	50550	210.61.142.105	30513	WAN2
	8	192.168.1.10	49300	50580	192.168.121.1	8069	WAN2
	9	192.168.1.10	49304	50584	172.16.3.136	8069	WAN2
	10	192.168.1.10	49322	50602	192.168.2.1	8069	WAN2
	11	192.168.1.10	49364	50644	20.184.57.167	443	WAN2
	12	192.168.1.10	49366	50646	210.61.142.105	30513	WAN2
	13	192.168.1.10	49388	50668	192.168.124.15	8069	WAN2
	14	192.168.1.10	49399	50679	192.168.124.11	8069	WAN2
	15	192.168.1.10	49437	50717	192.168.50.17	8069	WAN2
	16	192.168.1.10	49448	50728	192.168.50.101	8069	WAN2
	17	192.168.1.10	49469	50749	192.168.20.1	8069	WAN2
	18	192.168.1.10	50192	51472	52.229.206.30	443	WAN2

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

5.3.5 GPS

It is available only when the selected CPE supports GPS feature.

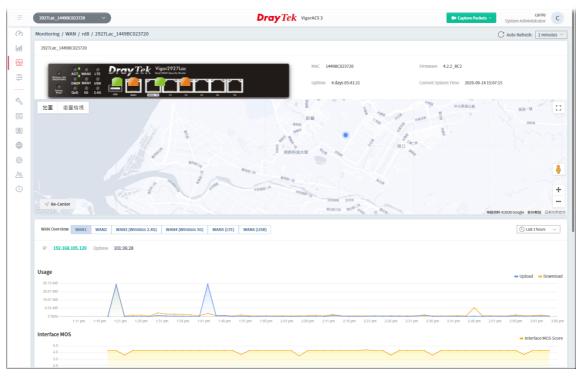
The GPS page will display the moving path (including time and coordinate position, latitude, and longitude) of the Vigor device.



5.3.6 WAN (SD-WAN)

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

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



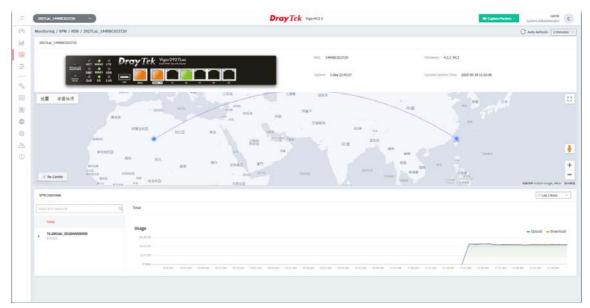
|--|

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

5.3.7 VPN (SD-WAN)

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

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



5.3.8 VoIP (SD-WAN)

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

nito	oring / Vol	P / simulator													(
/olP	Call List													C Last 2 ho	iurs 🗢	
(1414 Tetal	11 • Great 5.0 - 4.3	991 • Good 4.2 - 4.0 All (1598)	408 • Okay 3.9 - 3.6	4 • Poor 3.5 - 3.1	0 • Bad 3.0 ~ 1.0					Proof	10 •	6 с	/160 >		
		<i>u</i> ,	No (1336)	ACTIVE (100)	Pinoned (\$10)						Latency		N N	7160		
	Status 🖓	LAN IP	LAN IP	11 Peer IP	in Call ID	01 Via Interface	at Start Time	41	Failovered Interface	Up Time 11	Low ST	Peak 37	Average		Packet Loss	MOS
	8	192.168.120.118	40.197.130	.34 8850	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:37 PM			00:00:53	15 ms	484 ms	220 ms	12 ms	0 %	4	
2	S	192.168.120.119	231.242.7.1	112 8849	WAN3	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:26 PM			00:01:04	7 ms	467 ms	240 ms	14 ms	1 %	4	
1	6	192.168.120.120	140.51.54.8	34 8848	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:57 PM			00:00:33	18 ms	478 ms	279 ms	12 ms	0 %	4	
	3	192.168.120.116	98.108.133	.232 8846	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:46 PM		**	00:00:44	10 ms	493 ms	252 ms	12 ms	0 %	3.8	
5	\$	192.168.120.117	147.116.11	1.78 8845	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:41 PM		**	00:00:49	7 ms	481 ms	237 ms	14 ms	0 %	4	
						2020/03/19 03:53:30 PM										

These parameters are explained as follows:

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

5.3.9 Data Usage (SD-WAN)

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

29271.ac_14498C023720 V	Dray Tek VigorACS 3		Capture Packets	System Administrator
Monitoring / Data Usage / rd8 / 2927Lac_1449BC023720				C Auto Refresh: 5 minutes
2927Lac_1449BC023720				
Usage Sorting by Application Client Device				() Last 2 hours
Search Category or App				
	Protocol	97.35 MI	Others	5.43 MB
Total	Google Services	2.74 MB	Instant Message	1.31 MB
109.63	VolP	1.20 MR	 Turnseling 	826.83 KB
MB	Apple Services	769.39 Kill	Web HD	40,76 KD
Traffic Line Chart Upinad/Download By Interface				
				- Upload - Downloa
67,22,M0				^
28.15 MB				
19.07 MB	\sim			
0 Byte 2:00 pm 2:10 pm 2:20 pm 2:00 pm	2.40 pm 2:50 pm 3:00 pm 3:10 pm	n. 3/20 pm	0.00 pm 0.40 p	vn 150 pre 400

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

							ection type, op	
SVS	tem, u	pload and	d downlo	ad usage.				
				0				
ingen er en	IC LOW COART Lightend	Gowninad By Montaia						
								- WAN1 - W
	a la sel							
	14.4							
		Mar. Mar. 1944 - 1	ter tile tile tile	n tilps inter inter it	for the 3	We life life 10	e liter liter the liter lite	- Jelge J
	Char Char		ipe tilge tilge tilge	n tilpe telpe telpe til	(m. 19m.)	Ne Me Me 1	n liter liter then then the	- 14pr 1
			ip läp läp läp	a tilga iniga iniga ti	(m. then)	We life life 10	e liter liter the the two	n leine l
Usag	office office	Client Device					e liter liter liter liter liter Vege	n 14m 1
Usag	Char Char		for the the the	n tiller tiller tiller til d Connection Type	in the l			n 14m 1
Usag	office office	Client Device					Unage	- 10pm 1
Usag	o List by Application	Climi Dentar	# MAC Address	# Connection Type	≓ os	27 Upleed	Usage 21 Deventional	- 34p- 1
Usag	e Unit by 'Application & Heat Name	Climit Davinar 27 IB Address 192 306-124-12	 MAC Address RCHVRDCHAR2 	리 Connection Type 약 Workers (KG)	# 05 ©	27 Uplead 100 Tytes	Usage # Deemland 332 Bytes	- 14pr 1
1944	e List by Application F Hest Kanne L adam MSP 2 Unknown	Clint Owner # W Address INV 106 LTA LT 190.306 LTA 20	 MAC Address BCRY002C0662 000077303EE2 	은 Connection Type 약 Workens (56) 초 Word	# 05 ©	27 Uplead Los nyos 3.52 KB	Unage (*) Deventional 132 Dytes 2.34 40	- 14e- 1
1944	I adam MSP Unknown Unknown Katook/S	Client Consus # # Address 192.106.124.12 192.306.124.29 192.306.124.30	 MAC Address BC0108220662 000077393282 B80179567799 	ි Connection Type ?? Winniers (Mi) නි Wind නි Wind	# 05 ©	27 Opticed List Tytes Jack XB List Also	Unage 21 Described 322 Parts 2.14 40 4.44 MB	- 14pr

5.4 Configuration Menu for SD-WAN CPE

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

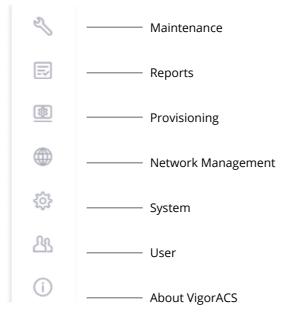
Part III

System Menu



Chapter 6 System Menu

System menu contains:



6.1 Maintenance

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

(9)	Maintenance
<u></u>	Scheduled Backup
	Configuration Restore
	Firmware Upgrade
Z	Device Reboot
	System Password Reset
\$	Schedule Profile
	File Manager
	Batch Activation
<u>4</u> 2	
(j)	

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

6.1.1 Scheduled Backup

6.1.1.1 Networks & Devices

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

Root Network 🗸 🗸		Dray Tek VigorACS 3	Bi Captore 7	System Administrator
faintenance / Scheduled Backup				
User Group : RootGroup ~				
Retworks & Devrces Backup Settings Pro	me			
Name	File Type	Backup Setting		
Root Network(90)	Configuration File	Empty		
ALANWEN(3)	Configuration File	As Parent	v	
() 🐼 AnPhat_VN(8)	Configuration File	As Parent		
p S ArlesTest(0)	Configuration File	As Parent		
b @ Cshih(2)	Configuration File	8K_711 (Not an this User Group)	. u	
▷ ③ FAE(3)	Configuration File	555	w.	
Marketing_carrie(0)	Configuration File	As Parent		
OCTOBER(1)	Configuration File	As Parent	U C	
() 🐼 RD1(3)	Configuration File	As Parent	*	
b SEG1(1)	Configuration File	As Parent	υ.	
5 🐼 ScanAccess(3)	Configuration File	As Parent		
() () TreeDepthTest(0)	Configuration File	As Parent	~	
p 🕜 USA(1)	Configuration File	As Parent	. U	
() 🕜 cole6666(0)	Configuration File	As Parent	*	
	Configuration File	As Parent	6	
b @ mam(e(2))	Configuration File	BK_711 (Not in this User Group)	7.0	
() 💿 robintest2(0)	Configuration File	As Parent		
p 🕜 mwerwe(0)	Configuration File	As Parent		
() (0) test(0)	Configuration File	As Parent	v	
b (c) test6666666(0)	Configuration File	As Parent		

ltem	Description						
User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.						
File Type	Display the file type used for the device.						
Backup Setting	Choose a profile defined in Backup Settings Profile for applying onto the selected CPE.						
	As Parent ~						
	As Parent						
	Empty						
	Default						
	As Parent - The backup setting for the selected network / device is the same as the top setting.						
	Empty - No backup setting for the selected network / device.						
	Default - Use the default backup setting for the selected network / device.						
	Others - In addition to As Parent, Disable and Default, profiles defined in						

	Backup Settings Profile also will be listed in this drop-down list.
Save	Save the current settings.

6.1.1.2 Backup Settings Profile

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

Networks & Devices Backup Settings Profile					
+ Add					
Name	Period(Days)	Туре	Time Interval	Action	
Default	2	The Last 20	00:00-23:59	∂ Edit	IR Delete
55	1	The Last 20	Now	@ Edit	B Delete
anı	1	The Last 20	Now	Ø.Edit	2 Delete
nce a day	1	The Last 20	Now	Ø Edit	S Delet
nce in two days	2	The Last 20	Now	Ø Edit	2 Deleb
ince in three days	3	The Last 20	Now	Ø Edit	18 Delete
d52	10	All	11:36-24:00	Ø €dit	1 Delet
tena_backup	1	The Last 20	Now	@ Edit	ft Delete
et's backup	100	All	Now	∂.Edit	2 Delet
CS test	1	The Last 20	Now	∂ Edit	2 Delet
ris_backup	1	The Last 20	Now	Ø Edit	12 Delet
atc_profile	1	The Last 20	Now	8 Edit	12 Delete
lice profile	1	The Last 20	00:00-24:00	Ø €dit	B Delet
oseph trial	1	The Last 20	14:55-15:02	∂ Edit	S Delete
ULIA	1	The Last 20	Now	ℓ Edit	8 Delet
shih test	1	The Last 20	Now	@ Edit	18 Delet

These parameters are explained as follows:

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

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

tworks & Devices Backup Setting	Profile	
lame		
Backup Period(days)	1	
Keep Files	The Last 20 All	
Backup Time	Now Scheduled Schedule Profile	
Schedule Profile	reset_password_wizard ~	

ltem	Description
User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.
Name	Enter a name of the backup profile.

		The u	nit is "	ʻday". I	f you t			r the backup executed by means the backup will be
Keep Files	Choose to files.	keep	all of	the file	es (rou	ter's c	onfigu	ration files) or the last 20
Backup Time	Set a time interval for executing the backup work for networks and devices.							
		v - The Save b		-	rk will	be exe	ecuted	l immediately after clicking
		edulec date a			-			ecuted at the specified time
	• Sch	edule	Profil	e - The	e back	up wo	rk will	be executed according to ng the Save button.
Scheduled	Start Tim and minu							display a clock. Set the hou ock.
	50 45 40 Select tir	_	0 05 0 25 1 02	1:10	Profile	le the	time s	-
	Specify St Date – Cli					to cho v	ose a	date as the starting date.
	Date – Cli	ck to p			endar	to cho ~ Fr]	date as the starting date.
	Date – Cli	ck to p Jan	oop up	~ 2	endar 022	~	>	date as the starting date.
	Date – Cli	ck to p Jan	oop up	~ 2	endar 022	~	> Sa	
	Date – Cli	ck to p Jan Mo	oop up	✓ 2 We	endar 022 Th	∽ Fr	> Sa 1	
	Date – Cli	Jan Mo	Tu	✓ 2 We 5	o22 Th	Fr 7	> Sa 1 8	
	Date – Cli K Su 2 9	Jan Mo 3 10	Tu 4	 ✓ 2 We 5 12 	endar 022 Th 6 13	 Fr 7 14 	> Sa 1 8 15	
	Date - Cli	Jan Mo 3 10 17	Tu 4 11 18	 ✓ 2 We 5 12 19 	endar 022 Th 6 13 20	 Fr 7 14 21 	> Sa 1 8 15 22	

	reset_password_wizard	~
	reset_password_wizard	
	reboot_wizard	
	restore_wizard	
	backup_wizard	
	default	
	test1	
	test2	
	test3	
	test4	
	test5	
	test6	
	test7	
	tt1	
Save	Save the changes on this page.	
Save	Save the changes on this page.	

6.1.2 Configuration Restore

6.1.2.1 Apply to Devices

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

User Group : RootGroup Apply to Devices Restore Settings Pro	file		
Quick Setting			
Name	Apply File List	Restore Profile	
4 🕢 Root Network(91)			
ALANWEN(3)			
@ 2952n_001DAAE061E8		Empty	
@ 2960_00507FFF3900	0	Empty	
3910_001DAA18E740	õ	restore_wizard Default	
▷ (AnPhat_VN(8))		^RD8TestTestTest 1111	
AriesTest(0)		2222 3.333	
		3.355	
Cshih(2)			
David_Test_n1(3)			
₽			
Marketing_carrie(0)			
OCTOBER(1)			
() (C) RD1(3)			
SEG1(1)			
b 🔿 ScanAccess(3)			

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

	Quick Setting
	Common Config File /AP903_20190715.cfg 🗸
	\triangle Notice: To apply ACL CFG file to APs, please make sure the firmware version is 1.2.5 or newer. With old
	firmware, your AP might be reset to factory settings, so the selected AP with old firmware will be ignored automatically.
	Common Restore Profile v
	Device Filter APs Switches
	Select Devices
	Name Model Name Firmware Version
	▷ ■ ◇ ALANWEN(0) ▷ ■ ◇ AnPhat, VN(6)
	AriesTest(0) Schih(0)
	David_Test_n1(0)
	Image: Second
	▷ OCTOBER(0) ▷ OCTOBER(0) ▷ OCTOBER(0)
	▷ = ⊗ SEG1(0)
	× Close Next →
	In which, click the Common Config File to select a "cfg" file. Then select a
	restore profile and specify the device filter (AP or switch). From the Select
	Devices list, select one or more APs/Switches required to apply the configuration file. Click Next to get the following page.
	configuration file. Click Next to get the following page.
	• Quick Setting ×
	Common Config File /AP903_20190715.cfg
	▲ Notice: To apply ACL CFG file to APs, please make sure the firmware version is 1.2.5 or newer. With old firmware, your AP might be reset to factory settings, so the selected AP with old firmware will be
	ignored automatically.
	Common Restore Profile Default
	Device ID Device Name Model Firmware Version User Group ☑ 136288 AP 903_00507FF19216 VigorAP 903 1.3.5RC7 RootGroup
	× Close ← Previous ✓ Apply
	Check if the selected devices are correct or not. If yes, click Apply . The
	selected configuration file will apply to all of the selected devices.
Apply	Click the icon to enable configuration restoration for the selected CPE.
File List	Open a dialog to choose one of the files for the file restoration of the selected CPE.

	Select a config file								×
	Filename	4	Property	.↓↑	Size	Last Modified	J↑	File Path	↓↑
	⊵		Directory		0 Byte	02/19/2020 13:10:11			
	AP1000C_20190604	fg	cfg file		9.41 KB	06/04/2019 14:09:13		./RootGroup	
	() AP910C_acl_2018120	06.cfg	cfg file			06/04/2019 11:22:24		./RootGroup	
	 To apply ACL Cl 	G file to APs, pl	ease make s	ure ti	he firmware	re the firmware on both de version is 1.2.5 or newer. I firmware will be ignored a	With old	d firmware, yo	ur
	ेट ३८							×	Close
Restore Profile	Choose a profile selected CPE.	defined	in Rest	or	e Setti	ngs Profile for	арр	lying on	to th
Restore Profile			in Rest	tor	e Setti	ngs Profile for	арр	lying on	to th
Restore Profile	selected CPE. Empty restore_wizard Default ^RD8TestTestTe 1111 2222	st ore settir e default tion to Er	ng for tl restor mpty ar	he e s	selecte etting f Default	d network / de or the selected , profiles defin	vice. net	work / d	evice

6.1.2.2 Restore Settings Profile

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

User Group : RootGroup ~			
Apply to Devices Restore Settings Profile			
FAdd			
Name	Trigger Profile	Time Interval	Action
estore_wizard	restore_wizard	05:12-05:17	🖉 Edit 🛛 🕄 Delete
efault	default	00:00-00:00	2 Edit 🗊 Delete
RD8TestTestTest	3	06:12 AM-06:17 AM	C Edit 🗊 Delete
111	2	Now	C Edit 🛛 🗟 Delete
222	10	Now	🖉 Edit 🗊 Delete
.333	-	Now	C Edit 🗊 Delete

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

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

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

Iaintenance / Configuration User Group: RootGroup	Restore	
pply to Devices Restore Settin		
Name		
Restore Time	Now Scheduled Schedule Profile	
Start Time	Select time	
End Time	Select time	
Specify Start Date	\odot	

Item	Description
User Group	Specify a user group for applying the restore settings profile.
	Each user group can be configured with different restore settings profiles.
Name	Enter a name of the restore setting profile.
Restore Time	Set a time interval for restoring the configuration settings for networks and devices.
	 Now - The setting restoring work will be executed immediately after clicking the Save button.
	 Scheduled - The setting restoring work will be executed at the specified time and date after clicking the Save button.
	• Schedule Profile - The setting restoring work will be executed according to the selected schedule profile after clicking the Save button.
Now	The configuration restore will be executed after clicking Save.
Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.
	45 15 40 20 Profile 35 30 25
	Select time
	Specify Start Date – Click to enable the time setting.

	Date -	- Cli	ck to p	op up	o a cale	endar	to choo	ose a
		<	Jan		~ 2	022	~	>
	4	Su	Мо	Tu	We	Th	Fr	Sa
								1
		2	3	4	5	6	7	8
		9	10	11	12	13	14	15
	1	16	17	18	19	20	21	22
		23	24	25	26	27	28	29
	:	30	31					
Schedule Profile	Trigge which,	, Vig	orACS	offer	s defa			
			passwo					
	re re b	eboo esto	_passw ot_wiza re_wiza up_wiza Ilt	ird ard	vizard			
ave	Save t	he c	urrent	t setti	ngs.			

6.1.3 Firmware Upgrade

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

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

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

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

User Group : Root	•								
Firmware Upgrad	All Complete Jobs								
Name	↓↑ File Path	41	Schedule⊧∤↑	Device Count	1	Status 🕂	Result 41	Action	
2952_3892tw	./RootGroup/v2952_3892_TW.all		Any	1		Disabled	Success:0 Fail:0	🖉 Edit	🗊 Delete
2952_390	./RootGroup/v2952001.all		Any	1		Complete	Success:1 Fail:0	🖉 Edit	Delete

These parameters are explained as follows:

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

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

aintenance / Firmware Upgra	de	
User Group : RootGroup		
Firmware Upgrade Job Sett	lings	
rinnware opgrade 500 Sec	unga	
Name		
Status	Disable Enable	
Upgrade Time	Now Scheduled	
Start Time	Select time	
End Time	Select time	
Date	Select a date	
Apply Firmware		
Device to Upgrade 🛛 🕆		
Name	MAC Address Model Name Firmware Vers	tion Modem Version
Root Network(2)	mos concess model name Pittimate veta	notelli version
þ 💿 111111(0)		
222222(0)		
D Manual_Carrie(1)	00-20-27-F1-01-0F 10+0.000 1.4-3	M- DC1

These parameters are explained as follows:

ltem	Description
Name	Enter a name of the job profile.
Status	Click Enable to activate the firmware upgrade profile.
Upgrade Time	Set a time interval for executing the firmware upgrade job for networks

	 Now - The firmware upgrade job will be executed immediately after clicking the Save button. 										
	•	Sch	edule	d - The	e firm	ware u		-	b will be exec		
		spe	cified t	ime a	nd da	te afte	r cli	cking	the Save butto	on.	
cheduled						ick Sel numb			to display a clo clock.	ock. Set the	hour
			0	1 :14	ļ	<u> </u>					
			23	00	13						
		4/	22 11 10	10	2 14						
		4	21 9 o	1	3 15						
			²⁰ 7 19	6 5	⁴ 16 17						
				18							
		01:	14	Ü	√Select tir	me 🛱					
	Dat	t e – Cli	ck to r	າດ ເມ	o a cal	endar	to c	hoose	a date as the	starting da	ite.
		_1									
		<	Jan		~	2022		~	>		
			Juli			2022					
		Su	Мо	Tu	We	Th	Fi	S			
								1	le		
		2	3	4	5	6	7	8			
		9	10	11	12	13	14	1	5		
		16	17	18	19	20	21	1 2	2		
		23	24	25	26	27	28		_		
				25	26	21	20	5 2	9		
		30	31								
		C									
pply Firmware						ect a fi ted file		vare fi	le. VigorACS v	vill upgrade	the
	-	Select a fir	mware								×
		Filename	•			Property	J† S	ize	Last Modified	↓↑ File Path	J↓
	D □ SharedFirmware					Directory Directory		Byte Byte	02/19/2020 13:10:11	./RootGroup	
		🗅 Vigor2	960_001DAA	694AE8		Directory		Byte	06/04/2019 13:55:45	./RootGroup	
	2	Public.	Area			Directory	0	Byte			

Device to Upgrade	Click the Filter icon to set the filtering conditions.							
	Device to Upgrade 🛛 🖓							
	Filter							
	Device Name							
	MAC Address							
	Model All ~							
	Firmware Version All ~							
	Modem Version All ~							
	Cancel Q Apply							
	Device Name - Enter the name of the device to be shown on the table.							
	MAC Address - Enter the MAC address of the device to be shown on the table.							
	Model – Select a model of CPE.							
	Firmware Version – Select a firmware version. CPE with the selected							
	firmware will be shown on the table. Modem Version - Select a modem version. CPE with the selected modem							
	will be shown on the table.							
	Apply - After clicking Apply , the table below will show the devices according to filter conditions.							
Table	Select one device or more devices to apply the firmware upgrade provision.							
	Device to Upgrade V							
	Name MAC Address Model Name Firmware Version Modem Version							
	 ▲ ③ Root Network(91) ▲ ③ ALANWEN(3) 							
	C @ 2952n_001DAAE061E8 001DAAE061E8 Vigor2952n 3.9.1.1_RC3 No DSL							
	2960_00507FFF3900 00507FFF3900 Vigor2960 1.3.0_Beta undefined							
	O 3910_001DAA18E740 001DAA18E740 Vigor3910 3.9.2_Beta r1064_84359 No DSL							
	b							
	Medel Name Display the model name for identification							
	Model Name – Display the model name for identification.							
	Firmware Version – Display the firmware version that the model used currently.							
Cancel	Discard current settings and return to previous page.							
Save	Save the current settings and exit the page.							

6.1.4 Device Reboot

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

6.1.4.1 Networks & Devices

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

tworks & Devices Reboot Settings Profile	
Name Model Name Firmware Version Mo	vm Version Reboot Setting
a 💿 Root Network(90)	Empty ~
D & ALANWEN(3)	As Parent 🔍
AnPhat_VN(8)	As Parent 🧹
) 🐼 AriesTest(0)	As Parent
▷ ② Cshih(2)	As Parent 👻
) 🐼 FAE(3)	As Parent. 🐱
Marketing_carrie(0)	As Parent 🗸
D CCTOBER(1)	As Parent. 👻
p @ RD1(3)	As Parent 🗸
⊳ 📀 SEG1(1)	As Parent 🔍
b ScanAccess(3)	As Parent 🗢
p 🐼 TreeDepthTest(0)	As Parent 🔍
p 🐼 USA(1)	As Parent \sim
p 📀 cole6666(0)	As Parent 🛁
b S cole777777777777777777777777777777777777	As Parent 👻
p 🐼 mamie(2)	As Parent 👻
p 💿 robintest2(0)	As Parent 😔
p 📀 mwerwe(0)	As Parent 🗢
p 💿 test(0)	As Parent ~
p 🕜 test666666(0)	As Parent 👻

ltem	Description
Reboot Setting	 Choose a profile defined in Reboot Settings Profile for applying onto the selected CPE. Reboot Setting Empty As Parent As Parent Empty reboot_wizard Default tti As Parent - The reboot setting for the selected network / device is the same as the top setting. Empty - No reboot setting for the selected network / device. Default - Use the default reboot setting for the selected network / device. Others - In addition to As Parent, Empty and Default, profiles defined in Reboot Settings Profile also will be listed in this drop-down list.
Save	Save the current settings.

6.1.4.2 Reboot Settings Profile

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

aintenance / Device Reboot				
User Group : RootGroup				
Networks & Devices Reboot Settings	rofile			
FAdd				
Name	Period(Days)	Time Interval	Action	
eboot_wizard	365	00:00-23:59	🖉 Edit 🌐 Delete	
Default	1	00:00-00:00	2 Edit 🕆 Delete	
ti -	1	Now	🖉 Edit. 🗇 Delete	
	365	01:05-03:15	🖉 Edit. 🕆 Delete	
shih_test		13:15-17:05	d Edit 🗇 Delete	

These parameters are explained as	d as follows:
-----------------------------------	---------------

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

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

User Group Robott Group Reboot Settings Profile Name Period (days) Reboot Time Specify Start Date Specify Start Date Sett a date	taintenance / Device Reboot	
Name Period (days) 1 Reboot Time Now Schedule Profile Start Time End Time Select time Select time	Jser Group : RootGroup ~	
Period (days) 1 Reboot Time Now Schedule Profile Start Time Sectify Start Date	tworks & Devices Reboot Settings Profile	
Reboot Time Schedule Profile Sart Time End Time Select time Select time	Name	
Start Time End Time Select time Select time Select time	Period (days)	1
Select time D	Reboot Time	Now Scheduled Schedule Profile
Specify Start Date		Start Time End Time
		Select time
Date Select a date	Specify Start Date	0
	Date	Select a date
		Cancel

Item	Description
Name	Enter the name of the profile.
Period(days)	Determine the frequency for the CPE reboot by VigorACS. The default value is 1 day.
Reboot Time	 Set a time interval for executing the device reboot. Now Scheduled
	 Schedule Profile Now - The device reboot will be executed immediately after clicking the Save button.
	• Scheduled - The device reboot will be executed at the specified time and date after clicking the Save button.
	• Schedule Profile - The device reboot will be executed according to the selected schedule profile after clicking the Save button.

Scheduled								ie to display a clock. Set the ho he clock.	
	Speci	20 3:10 fy St	23 11 10 9 8 7 19	6 5 18 1 ¹ Sector	2 14 3 15 4 16 7 elect tim	o enab	ole the	time setting. ose a date as the starting date.	
		<	Jan		•	2022	~	>	
		Su	Мо	Tu	We	Th	Fr	Sa	
								1	
		2	3	4	5	6	7	8	
		9	10	11	12	13	14	15	
		16	17	18	19	20	21 28	22	
		23	24	25	26	27		29	
		30	31						
Schedule Profile								ile from the drop down list. In profile.	
	reset_password_wizard ~								
	reset_password_wizard reboot_wizard restore_wizard backup_wizard default test1 test2 test3								
		est4							
Cancel	Discar	rd cu	Irrent	settin	σς αρι	d retur	n to pr	evious page.	

6.1.5 System Password Reset

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

aintenance / System Password Res	set			
Reset Time	Now Scheduled			
Start time	00:00			
End time	23:59			
Start Date	01/07/2022			
Select devices				
Name	Model Name	Firmware Version	Modern Version	
A OR Root Network(2)		11111111111111111	HOUSEN PERIOD	
þ 🐼 111111(0)				
b @ 22222(0)				
þ 🐼 Manual_Carrie(1)				
■	VigorAP 903	1.4.2	No DSL	

Description
Now - Reset the password for the selected device(s) immediately. Scheduled - To specify a certain time to perform the job, choose this one and specify start day, start time and end time respectively. VigorACS will perform the job for the selected CPE (s) according to the schedule set here. • Start Time / End Time - Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock. • 03 : 10 • 03 : 10 • 23 00 13 • 13 12 • 20 7 6 5 • 16 • 16 • 17 • 18 • 17 • 17 • 18 • 17 • 17 • 18 • 17 • 19 • 18 • 17 • 17 • 18 • 17 • 19 • 18 • 17 • 17 • 18 • 17 • 19 • 18 • 17 • 17 • 18 • 17 • 19 • 18 • 17 • 17 • 18 • 17 • 19 • 18 • 17 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 10 • 10 • 10 • 11 • 12 • 13 • 14 • 17 • 18 • 17 • 18 • 17 • 18 • 17 • 18 • 18 • 17 • 10 • 18 • 17 • 18 • 18 • 17 • 18 • 17 • 18 • 19 • 18 • 17 • 18 • 17 • 18 • 19 • 19 • 10 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 17 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 17 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19 • 19

		:	Jan		× 2	022	~	>
			Juli			022		
	s	Su	Мо	Tu	We	Th	Fr	Sa
								1
		2	3	4	5	6	7	8
	9	9	10	11	12	13	14	15
	1	.6	17	18	19	20	21	22
	2	23	24	25	26	27	28	29
	3	30	31					
Select devices	Choose t	he c	device	that y	/ou wa	nt to	do dev	vice pa
Save	Save the	curi	rent se	etting	S.			

6.1.6 Schedule Profile

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

Add					
Add .					
Name	Start Day	End Day	Start Time	End Time	Action
eset_password_wizard	2017-04-27		07:08	07:13	P Edit 17 Delet
boot_wtzard	2017-06-20		08:21	20:11	P Edit 🕅 Delet
istore_wtzard	2016-12-14		05:12	05:17	d' Edit 🖷 Delet
ackup_wtzard	2016-12-07		03.05	03:25	🥒 Edit 🛛 🖹 Delet
etauit	2016-10-08	2016-10-09	00:00	00:00	a? Edit 🛛 🗐 Delet
est1	2017-04-19	2017-04-11	00:00	00:00	de Edit 🗊 Delet
st2					Selet 19 Delet
513					Sedit 🗐 Deler
864					P Edit 🛱 Delet
525					d Edit 🗇 Dele
st6					d ² Edit
st7					🖉 Edit 🔞 Dele
1			00:00	23:59	Sedit II Delet

These parameters are explained as follows:

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

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

Maintenance / Schedule Profile				
User Group : RootGroup ~				
Profile Name				
Date Type	Scheduled	~		
Start Date	Select a date			
Check End Date				
End Date	Select a date			
Time Type	Scheduled	~		
Start Time	Select time			
End Time	Select time			
				Cancel Add

These parameters are explained as follows:

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

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

6.1.7 File Manager

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

🕹 Upload 💩 Download 🖹 Delete 🕒 New Folder 🔿 DrayTek FTP								0
	Filename	UT Device Name	Property	Ψî	Size J	↑ Last Modified	$\downarrow\uparrow$ File Path	
	SharedFirmware		Directory			07/30/2020 09:16:40	./RootGroup	
	🗅 test555		Directory			06/06/2019 14:22:59	./RootGroup	
	🗅 ttl		Directory			03/04/2019 14:39:56	./RootGroup	
	D Vigor2925Vac_001DAAF06DF0		Directory			10/08/2019 11:23:27	./RootGroup	
1	D VigorAP 902_001DAA3D9808		Directory			10/08/2019 13:25:36	./RootGroup	
	D VigorAP 960C_1449BC775566		Directory			07/09/2020 10:24:02	./RootGroup	
	🗅 11@22.txt		txt file			03/04/2019 15:46:09	./RootGroup	
	🗅 test2.txt		txt file			05/22/2019 14:03:32	./RootGroup	
	🗅 docker.txt		txt file		1.98 KB	06/19/2019 09:22:04	./RootGroup	
1	C certificate.cfg		cfg file		5.92 KB	03/04/2019 14:40:01	./RootGroup	
1	AP903_20190715.cfg		cfg file		7.58 KB	09/21/2020 14:57:52	./RootGroup	
]	acs2_url.txt		txt file		19.38 KB	03/04/2019 14:39:51	./RootGroup	
	ap810_r9031_125.all		all file		5.17 MB	06/19/2019 09:22:35	./RootGroup	
	ap910c_r10090_128.all		all file		6.76 MB	06/19/2019 09:20:01	./RootGroup	
]	ap920_r9469_125.all		all file		15.88 MB	06/19/2019 09:16:57	./RootGroup	

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

Upload	Click to upload a file to VigorACS 3 server.						
	L Upload File ×						
	Target: ./RootGroup Browse						
	▲ The file must be less than 50MB.						
	× Cancel ✓ Apply						
Download	Download a driver (*.all, *.rst and etc.) related to CPE device from VigorACS 3 server.						
Delete	Click to delete the selected profile.						
New Folder	Create folders for files classification/management.						
DrayTek FTP	After clicking the link, the following page will appear for you to download file from DrayTek FTP directly.						

6.1.8 Batch Activation

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

-	Root Network	~	DrayTek VigorACS 3	Capture Packets - root System Administrator
3	Maintenance / WCF Batch Ad	tlvation (For Cyren)		
9	LAM			
	create rime	4T create user	3⊤ Devices count	41 Action
			\wedge	
			Nu clata available	
2				
<u>8</u>]				
Ð				
ĝ.				
8				
i)				

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

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

Maintenance / WCF Batch Activation (For Cyren)
Login MyVigor First
 Note: Batch Activation is the feature which provided to the distributor only, please login MyVigor with the distributor privilege account. If you have the requirement of batch activation, please contact your local distributor for further assistance.
Vsername Assword
↑ Back to profile list

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

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

	-	
Import WCF batch activation	data	
Upload file	Browse	
	\Lambda Download entry sample file	
↑ Back to profile list		
		A Upload
ltem	Description	
Upload file	Click Browse to locate the import-batch-activation-file	
	Maintenance / WCF Batch Activation (Fo	r Cyren)
	Import WCF batch activation data	
	Upload file	import-batch-activation-file.csv Browse
		🚣 Download entry sample file
	↑ Back to profile list	
	If there is no file existed, cli download one file.	ick "Download entry sample file" link to
Download entry	Click to download an entry	sample file (import-batch-activation-file.csv).
sample file	Open the CSB file and ente device.	r the "MAC address" and "WCF KEY" for each
Back to profile list	Return to the previous pro	file list page.
Login	Access into next page.	

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

Upload Result		WCF Batch Activation (For Cyren)					
Image: Constraint of the state of the st	Upload Resu	lt					
2865Lac_14498C0D8F00 14498C0D8F00 MKT_manual 6F6CD-CF2A6-EE7CE-6C5D2 © Check OK * Back to profile list ************************************	🖧 Export						
* Back to profile list							ĻΎ
	v 20	0522C_1443BC0D8F00	1445BC0D6F00	MRI_IIIaliual	0F0CD-CF2A0-EE7CE-0C5D2	Check OK	
	Back to profile lis	t				Deview	

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



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

Maintenance / WCF Batch Activation (For Cyren)		
Binding device with MyVigor account		
MyVigor account	MyVigor account e-	
name	mail	
↑ Back to profile list		
		Previous Next

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

Maintena	nce / WCF Batch Activation	(For	Cyren)							
MyVigo	r Devices & License Che	ck								
ය Expor	t									
ΨŤ	Device Name	.↓↑	Device MAC	$\downarrow\uparrow$	Network	ψt	License Key	$\downarrow\uparrow$	MyVigor Check St	atus
~	2865Lac_1449BC0D8F00		1449BC0D8F00		MKT_manual		6F6CD-CF2A6-EE7CE-6C5D2		Check OK	
↑ Back to p	profile list									
									Previous	Activate

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

Root Net… V	Dray Tek VigorACS 3		
Maintenance Save OK Result	(For Cyren)	×	
Result —			

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

Root Net… 🗸		Ľ	ray Tek Vigor	CS 3	
Maintenance / WCF Bate	ch Activation (F	For Cyren)			
+Add					
Create Time	.↓↑ . d	Create User	↓↑ Devices Count	↓↑ Action	
2021-02-26 06:27:12	r	root	1	Q View Log 💼 Delete	
ltem	Desci	ription			
		-		·	
+Add	Click	to create a	a new batch act	ivation profile.	

Click to view the records of the WCF batch activation.

Click to remove the selected record.

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

example 1

Root Network					D	orayTek vigo	rACS 3			Capture Packe	sts 👻 System Administr	root R	R
Maintenance / WCF Ba	tch Acti	vation (For	r Cyren)									
All Processing Co	mplete	Fail	search [Device Name / MAC / Key									
🛆 Export													
A Export	41 -	IAC	ψţ	License Key Number	łt	License Date	† Network	ψţ.	Last Update Time 47	Status 41	Result		-
		MC 449BC0D8F0		License Key Number B3072-A595A-FE7C3-F7CEF		License Date 4 2021-02-26-2021-03-28	Network	ψ†	Last Update Time 41 2021-02-26 06:27:14	Status ↓↑ Processing	Result MyVigor added license suc	cessfully	

example 2

Device Name	41	MAC	 License Key Number	1.127	License Date	-47.	Network	Last Update Time	Status 👫	RESUL
860n+_001DAAD1E290		001DAAD1E290	03F10-D646B-2B0A1-40DA6		2019-02-13-2019-03-15		RDS	2019-04-02 11:30:41	Complete	CPE sync license successfully
925Ln_001DAADD75B0		001DAADD75B0	671C8-8222F-55F4E-907CB		2019-02-13~2019-03-15		RD8	2019-04-02 11:32:40	Fail	Cannot connect to CPE (timeout)

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

6.2 Reports

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

(7)	Reports
<u></u>	Report Tasks
	Reports
Z	
Ð	
Report	s

6.2.1 Report Tasks

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

User Group :	RootGroup ~								
+ Add							Search Title/Type		Q
Title	Network/Device	Report Content	Report Delivery	Schedule/Period	Last Implemented	Action			
test	Root Network	Traffic	Email	Weekly on Sunday	12 1	0 Edit	3 Delete		
CPE_Marketing		Traffic	Email	Later 09/13/2017 00:00	70	0 Edit	11 Delete		
lest	2860ac_00507F0000af,2860ac_00507F0000ae,	Information	Email	Now	-	Ø Edit	1 Delete		
eportTest		Device Configuration	Download	æ		d Edit	🖹 Delete	i Download	
oie_test7	AnPhat_VN,yyyyy	Firmware	Download	-	-	0 Edit	E Delete	& Download	
374802test	Root Network,Cshih	Network	Download	<u></u>		0 Edit	🖹 Delete	de Download	
572884	Root Network	Network	Download			/ Edit	fî Delete	J. Download	
lest2	Root Network	Traffic	Email	Later 03/01/2020 00:00		d Edit	🗊 Delete		
est	Root Network	Traffic	Email	Now		/ Edit	II Delete		

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

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

Create new report	Task	
Enable This Task		
Task Title		
Report Content	Traffic ~	
	LAN Statistic ~	
Report delivery	Send By Email Download File	
File Type	PDF CSV Excel Word	
Created By		
Run Report	Once Repeat	
	Later ~ 02/25/2021 00:00	
Email Subject	LAN Statistic Report	
Fmail From		
	Cancel) Sa

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

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

Select de	evices		
Name		Model Name	Firmware Version
4 4 4	 Root Network(11) @ @#\$96^&*_+{}'`:?><!---+(0)</li--> @ Marketing_carrie(0) @ asasse(123)(0) @ rd8(0) 		
Þ	 ♂ rd8-2(1) ✓ ● 2862Vac_001DAAEA38C0 	Vigor2862Vac	3.8.8.1_STD
	2927Lac_1449BC023768	Vigor2927Lac	4.1.0_RC2_SDWAN
e Save t	he settings and ı	return to previous	s page.

6.2.2 Reports

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

Root Network	\checkmark
Report / Report	
Create a Report	

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

Create new report			
Select report type			
Traffic	~)	~	
Select devices			
Model Name	Modem Version	Severity	~
Name	Model Name	ALL Critical Major Firmware Version Minor	
Root Network		Warning Normal	
			× Cancel + Quer

ltem	Description
Select report type	At present, VigorACS offers five types of report, including traffic, firmware, network, status, information and device configuration.
	Traffic Traffic Firmware Network Status Information Device Configuration
	Next, select the way (statistic or graph) to show the report.

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

6.3 Provisioning

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

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

6.3.1 Global Parameters

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

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

6.3.1.1 Global Profile

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

Jser Group : RootGroup									
Global Profile Network & Devices									
rofile Edit Mode : All Web UI View	XML File Parameter List								
+ Add 🕁 XML Template									
Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action			
Empty	Web UI View	General	No	0					
oot_group_always_keep	Web UI View	General	Yes	559	2017/11/20 05:49:56 PM	@ Edit	Delete	С Сору То	E View Log
globalparameter_test	Web UI View	General	No	322	2018/10/03 02:18:02 PM	@ Edit	Delete	С Сору То	₩ View Log
Manoj	Web UI View	General	No	18	2018/02/02 11:59:50 AM	@ Edit	Delete	С Сору То	E View Log
Stefan	Web UI View	General	No	2	2018/03/09 12:06:19 PM	@ Edit	B Delete	С Сору То	Se View Log
namie	Web UI View	General	No	42	2018/11/29 09:43:12 AM	🖉 Edit	🗊 Delete	С Сору То	E View Log
Carrie_MKT	Web UI View	General	Yes	2	2020/03/06 03:23:39 PM	@ Edit	Delete	С Сору То	₽ View Log
AnPhat	Web UI View	General	No	0	2017/05/18 11:17:30 PM	🖉 Edit	1 Delete	С Сору То	Wew Log
Elena	Web UI View	General	No	5	2017/07/14 04:04:17 PM	Ø Edit	Delete	С Сору То	₩ View Log
Amy	Web UI View	General	No	ō	2017/07/14 03:54:23 PM	Ø Edit	Delete	С Сору То	I View Log
ris	Web UI View	General	Yes	17	2018/10/05 11:20:43 AM	@ Edit	Delete	С Сору То	€ View Log
lulla	Web UI View	General	No	1	2017/07/14 03:54:52 PM	@ Edit	🖹 Delete	С Сору То	E View Log
Joseph_Wireless Parameter	Web UI View	General	No	2	2017/07/14 04:00:59 PM	@ Edit	Delete	C Copy To	₽ View Log

ltem	Description			
Profile Edit Mode	 All - Displays all of the profiles. Web UI View - Displays the profiles related to web UI view. XML File - Displays the profiles with the file format of "XML". Parameter List - Displays the profiles related to parameter settings for different CPEs. 			
+Add	Click to create a new provision profile.			
XML Template	Click to store current global parameter configuration as a file (*.xml).			
	XML Template			
	The XML is separated into two parts, you may edit it based on your requirement: • Item: Specify the unique "Item Id" for each TR-069 parameter that you want to configure • Profile: Specify the parameter value for each "parameter id", ACS will check the parameter id(mapping to item id) with the parameter name. • Profile Name: The profile name will display in the global parameter page. • Steep: We could decide whether to keep the value of this parameter. Setup true then ACS will detect and change it back if someone edits the value: • ord: ACS will apply the setting based on the order of parameters.			
Profile Name	Displays the name of the profile.			
Profile Edit Mode	Displays the edit mode.			
Model	Display the model name of the device.			
Always Keep	Yes – Such profile is kept always.			
	No – Such profile is not kept always.			
Revision	Displays the time for last modification.			
Last Modification At	Displays the time and date of the last modification of the provision.			

	Delete – Click to delete the profile. Copy To – If the administrator wants to apply the provision to certain user group, such action shall be used.
	2 Copy the profile to ×
	Copy To: Pick some user group RootGroup SDWAN rd8
	2.
	View Log – Click to review detailed information for the selected profile.
	View Log – Click to review detailed information for the selected profile.
	View Log – Click to review detailed information for the selected profile. Provisioning / Global Parameters
	View Log – Click to review detailed information for the selected profile.
	View Log - Click to review detailed information for the selected profile. Vovisioning / Global Parameters View Group: RootGroup Vorfile Information Profile Information Profile Information Profile Eddt Mode Web Ul View Mode View Seep View Seep Last Modelfied 2017/11/20 05:49:59 FM

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

Group: RootGroup		
al Profile Network & Devices		
Add a Profile		
Create Profile by	choose an action V	
	choose an action	
Always Keep	Sampling from an Online Device	
Reboot after Provisioning	Sampling from an XML flie Creating a New Parameter List	
2		
 Rote: After applying the par Provisioning Time 	meters, ACS will check the CPE responses and ask the CPE to reboot if needed. Now Scheduled Schedule Profile	

These parameters are explained as follows:

tem	Description	
-----	-------------	--

There are three methods (Sampling from an Online Device, Sampling from an XML file, Creating a New Parameter List) to create a profile.
Profile Name - It is available when Sampling from an Online Device / Creating a New Parameter List is specified on "Create Profile by".
Enter a name for the parameter profile.
Select Device - Click Edit to choose the device.
by Network by Model
Name Model Name Firmware Version
A 🏚 Root Network
ALANWEN
D 📥 AnPhat_VN
D 📥 Cshih
D 📥 FAE
Select XML file - Click Browse to choose a file.
Profile Name - Enter a name to create a new profile.
Some ISPs do not wish CPE client changing the parameters of CPE device, therefore make the profile being kept is required.
Enable it to reboot the CPE after the provisioning is applied by certain CPE.
Set a time interval for executing the backup work for networks and devices.
• Now
• Scheduled
• Schedule Profile
Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.
03:10 22 11 22 11 21 9 20 7 6 19 13 19 17 9 8 03:10 Select time Specify Start Date - Click to enable the time setting. Start date - Click to pop up a calendar to choose a date as the starting

		-						
		<	Jan		•	2022	~	>
		Su	Мо	Tu	We	Th	Fr	Sa
								1
		2	3	4	5	6	7	8
		9	10	11	12	13	14	15
		16	17	18	19	20	21	22
		23	24	25	26	27	28	29
		30	31					
Schedule Profile		zer Pr	rofile -	- Choo	ose a f	trigger	profile	e fron
			offers		ılt sch	trigger edule p edule Profi	orofile.	
	Vigo	Now reset_j reboot	offers Schee passwor t_wizard p_wizard	defau duled rd_wiza i	llt sch Sche	edule p	orofile.	
ancel	Vigo	reset_ reboot restore backup default test1 test2 test3	offers Schee passwor t_wizard e_wizard t	defau duled rd_wiza I d	Sche	edule p	lle	~

6.3.1.2 Network & Devices

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

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

er Group : RootGroup ~		
obal Profile Network & Devices		
	Profile Id	
Root Network(90)	Empty	
ALANWEND	root_group_always_keep	
AnPhat_VN(8)	(As Parent)	v
ArtesTest(0)	(As Parent)	
D 🐼 Cshib(2)	Manoj	<u>ل</u>
((FAL(3)	(As Parent)	
> () Marketing_carrie(0)	(As Parent)	×
CTOBER(1)	(As Parent)	
b @ R01(3)	(As Parent)	u .
6 SEC1(1)	(As Parent)	
b 🐼 ScanAccess(3)	(As Parent)	
- TreeDepthTest(0)	(As Parent)	
D 💿 USA(1)	(As Parent)	~
cole5656(0)	(As Parent)	u .
b	(As Parent)	
b @ mamie(2)	Empty	u
p (p robintest2(0)	(As Parent)	
p S mwerwe(0)	(As Parent)	-
0 (a) test(0)	(As Parent)	*
b (2) test666666(0)	(As Parent)	
() 🐼 wholesaletest(0)	(As Parent)	
(a) (0000000(0))	(As Parent)	0
10 (D) (V) (D) (D) (D) (D) (D) (D) (D) (D) (D) (D	(As Parent)	*
2762Vac_001DAA653308	(As Parent)	*
2860/m+_0010AAD83080	(As Parent)	

These parameters are explained as follows:

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

6.3.2 CPE Set Parameters

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

① CPE Set Parameters is suitable and convenient when there are several CPE (with the same model) devices required to be configured with **different** settings and values.

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

Jser Gro	RootGroup	Ŷ					
†Add	ிimport XML க்ல	AL Template					search Profile Name / Device O
	File Id / Profile Id	Profile Name / Device Name			Complete	Action	
Y	26	CPE Set Parameter Test.xml				Delete	
305		13.13.13.13	Model: Renew Count: 2	Reboot: 1 Retry: 0	No Set.	🐵 View Parameters 🛛 🗟 Vie	rwLog
467		001DAA5D585A	Model: Renew Count: 0	Reboot: 0 Retry: 0	No Set.	∞ View Parameters 📾 Vie	ewlog
5	28	CPE_Set_Parameter_Examplxxxxxxe.xml				1 Delete	
3	1	Henry Test.xml				🛱 Delete	
>	4	test.xml				1 Delete	

Item Description **User Group** Specify a user group. The devices under that group will be displayed on this page. +Add Click to create a file saved with the file format of XML. Import XML Click to upload a file to VigorACS 3 server. Upload File Bro Cancel Apply **XML** Template Click to store current global parameter configuration as a file (*.xml). XML Template The XML is separated into two parts, you may edit it based on your requirement: Item: Specify the unique "item id" for each TR-069 parameter that you want to configure Profile: Specify the parameter value for each "parameter id", ACS will check the parameter id(mapping to item id) with the parameter name. Profile Name: The profile name will display in the global parameter page. Iskeep: We could decide whether to keep the value of this parameter. Setup true then ACS will detect and change it back if someone edits the value: ord: ACS will apply the setting based on the order of parameters. Close Download X

Displays the profile name or the device name.

Delete – Click to delete the profile.

profile.

Displays the number of parameter file or the ID number of the profile.

View Parameters - Click to display parameter settings for the selected

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

Name Action

File Id / Profile Id

Profile Name / Device

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

Create a XML File			
Constant and Constant and Constant			
 Note: After applying the para 	imeters, ACS will check the CPE responses a		
File Name			
Device MAC or IP	Q		
Reboot after Provisioning	0		
Name(optional)			
Network(optional)			

These parameters are explained as follows:

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

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

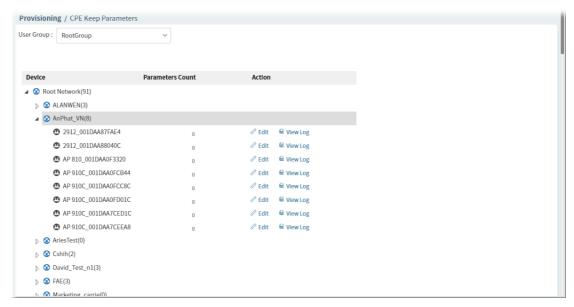
ice: 172.16.2.222		Web UI View Parameter Li
VAN	Select the parameters to be set	
AN IAT		
Object Settings		
205		
irewall		
olP		

ltem	Description
Device	Display the name of the device which will be applied with the parameters configured in this page.
Web UI View	Parameters (including WAN, LAN, NAT, Object Settings, QoS, Firewall,

	System, Routing, Wireless, Applications and etc.) ready for each CPE provision profile can be seen and configured in this page.
	The setting page for each parameter listed in left side will be displayed on the right side. Simply click the parameter to expand the sub-menu items. Then, choose a sub-menu item and click +Add to open setting page. After entering the required information for that menu item, click Save .
Parameter List	Display an overview of settings configured in Primary View.
Back to Profile List	Return to Profile List page.

6.3.3 CPE Keep Parameters

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



ltem	Description
Edit	Click to open the configuration page.
	Device : 3910_001DAA18E740 Web LII Mew Parameter List
	Reboot After Provisioning Note: After applying the parameters, ACS will check the CPE responses and ask the CPE to reboot if needed. Enable Concell See
	The menu list to the left will show available parameters regarded to the device.

6.3.4 Firmware Upgrade

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

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

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

6.3.4.1 Firmware Upgrade Job List

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

irmware Upgı +Add									
Name ↓↑	Status 4	Model 11	FW Version ↓↑	FW File	$\downarrow\uparrow$	Schedule 4	Start Date $\downarrow\uparrow$	Action	
0131-1	Disabled	Vigor	1.1.0_RC1	./RootGroup/ap810_r6227_1171.all		Now	N/A	🖉 Edit	🗇 Delete
123	Disabled	Vigor2910V	3.2.6			Now	N/A	🖉 Edit	🗇 Delete
5555	Disabled	44	44	./RootGroup/ap900_r4669_1153RC3.all		Now	N/A	🖉 Edit	🗓 Delete
AP902	Enabled	VigorAP 902	1.2.0RC6a	./RootGroup/ap902_r6078_1171.all		15:05-18:43	N/A	🖉 Edit	🖞 Delete
ap920r	Disabled	Vigor2910V	3.2.6	./RootGroup/ap920r_r7233.all		Now	N/A	🖉 Edit	🗓 Delete
CSHIH_TEST	Enabled	Vigor2762	3.8.4.6_RC2a_VT2	./RootGroup/ap810_r6227_1171.all		Now	N/A	🖉 Edit	🗓 Delete
Period_2860	Disabled	Vigor2860ac	3.8.5_RC5a	./RootGroup/v2860std_r51496_001.all		Now	N/A	🖉 Edit	🖞 Delete
sample	Disabled	Vigor2760n	3.1.1.1_RC6	v2k7v_a_3.1.1.1_RC6.all		Now	N/A	🖉 Edit	🗓 Delete
/2860_fang	Disabled	Vigor2860Vac	3.8.5_RC2	./RootGroup/v2860_385_00_en.all		Now	N/A	🖉 Edit	🗓 Delete
v2922_Fang	Disabled	Vigor2922n	3.8.5	./RootGroup/v2922001.all		Now	N/A	🖉 Edit	🗇 Delete
xclude Device	S Delete								

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

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

The following setting page appears if **+Add** for **Firmware Upgrade Job List** is clicked.

Provisioning / Firmware Upgrade		
User Group : RootGroup ~		
Firmware Upgrade Job Settings		
10		
Name		
Status	Disable Enable	
Upgrade Time	Now Scheduled Schedule	Profile
opprare time		
Job Type	Normal Auth Key Check	
Device Criteria		
Model 🚱	Vigor2927*	4
Upgrade Type 😡	Target Current	
Upgrade Type 🖌	tanget Current	
Device does not match firmware version	1.4.2	~
Modem Version	No DSL	*
		_
Firmware Upgrade & Network sele	ction	
Apply Firmware		
Name Model Name	Firmware Version Modern Version	Apply
 Root Network(2) 		NO
A 11111100		An Deserve

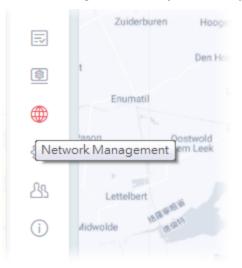
ltem	Description	
Firmware Upgrade Job Settings		
Name	Enter a name of the job profile.	
Status	Disable – Firmware upgrade is not allowed for such job profile. Enable – Firmware upgrade is allowed for such job profile.	
Upgrade Time	Set a time interval for executing the backup work for networks and devices.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

20 7 6 5 16 ule Profile 03:10 Select time Specify Start Date – Click to enable the time setting. Date – Click to pop up a calendar to choose a date as the starting date.
Schedule Profile Trigger Profile – Choosing a trigger profile from the drop down list. In which, VigorACS 3 offers default schedule profile.
reset_password_wizard ~
reset_password_wizard
reboot_wizard
restore_wizard
backup_wizard
default test1
test2
test3
Job Type Normal – VigorACS 3 performs firmware upgrade without using any authentication key.
Auth Key Check – To avoid hacker's attack via Vigor device (router or AP special authentication key is used for communication between Vigor device and VigorACS 3. That is, VigorACS 3 will verify all of the Vigor devic via authentication key issued by DrayTek to ensure the network security.
Device Criteria
Model Choose a model for firmware upgrade.
Upgrade Type Select Target or Current.
Target - If the firmware version of the CPE is different from the one liste in "Device matches firmware version", the firmware upgrade job will be performed immediately.
 Device does not match firmware version - Displays current firmware version recorded on VigorACS server.
Current - If the firmware version of the CPE is the same as the one listed "Device matches firmware version", the firmware upgrade job will be performed immediately.
 Device matches firmware version - Displays current firmware version recorded on VigorACS server.
Modem Version Available versions from VigorACS 3 database will be displayed in this field
Choose the correct modem version of the device, e.g., Annex A, Annex B and etc.
Before performing firmware upgrade for the CPE, VigorACS 3 will check i
the received model name, modem firmware version, and software version
match with the information recorded in VigorACS 3 server or not. If you type "*" in this filed, the modem version will not be regarded as a

	comparison condition in the process of firmware upgrade. It will be ignored.				
Firmware Upgrade 8	& Network selection				
Apply Firmware	Click to open a dialog.				
	Select a firmware ×				
	Filename Property ↓↑ Size Last Modified ↓↑ File Path ↓↑				
	▷ Directory 0 Byte 11/19/2019 17:07:11 .				
	SharedFirmware Directory 0 Byte 05/08/2019 08:36:52 /RootGroup				
	□ test555 Directory 0 Byte 06/06/2019 14:22:59 /RootGroup				
	다 tt1 Directory 0 Byte 03/04/2019 14:39:56 /RootGroup				
	□ Vigor2925Vac_001DAAF06DF0 Directory 0 Byte 10/08/2019 11:23:27 /RootGroup				
	□ VigerAP 902_001DAA3D9808 Directory 0 Byte 10/08/2019 13:25:36 /RootGroup				
	C PublicArea Directory 0 Byte .				
	X Close				
	Available versions from VigorACS 3 database will be displayed in this f Select the firmware version of the device and click Close .				
Apply	As Parent - The setting for the selected network / device is the same as the top setting.				
	NO - No setting for the selected network / device.				
	YES - Use the firmware selected above for the network / device.				
	Discard current settings and return to previous page.				
Cancel	Discard current settings and return to previous page.				

6.4 Network Management

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



lt 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.

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

6.4.1 Setting

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

6.4.1.1 Settings for Root Network

Network Management		
Search by Device ID/Name/Model/MAC/IP	Setting Map	
A the Root Network(253)	+Add New Network	
▷ 📥 1111(0)	General Settings	
ALANWEN(3)	General Settings	
D 📥 Alvaco(0)	Network ID	User Name
AnPhat_VN(9)	2	acs
🗅 🎄 Angela(6)	Name	Password
Cshih(2)	Root Network	
DraytekChina(0)	Location	
▷ ♣ FAE(3)	Koldingweg 19-1, Groningen, Nederland	
GetterNetwork(1)		
▷ ♣ IK1(1)		Save
Marketing_carrie(0)		
Novanet(0)		
OCTOBER(1)		
▷ ♣ RD1(4)		
Delete Devices		
El Déleté Dévices		

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

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

- Add Network	
Parent Network	
Root Network	
Name	
Marketing_carrie	 Image: A set of the set of the
Location	
HsinChu	
Username	
carrie	×
Password	
•••••	 •

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

6.4.1.2 Settings for Network Group

To add, change or delete a network group, please specify a network group (under **Network Management).**

sarch by Device EpName/Medel/MAC/IP Address	C Setting Map			
Root Network(70) A ((#5%^*.*()^.?**(+(0)))	+ Add New Network 🕆 Delete This Network 🚓 Change Not	work		
b all Layer2(0)	General Settings			
b All Marketing_carrie(0)	Network (D	Username		
D 21 SD-WAN(2)	3	rt8		
b aasaaa(123)(0)	Name	Password		
b #1 rd7(0)	ed8	*asses		
1 108(S2)				
b #1 rd8-1(0)	Location			
b #1 rd8-2(0)				
1				
5 🚠 simulator(12)	Advanced Settings			
C 2960 001DAA694AE8				
3008 001DAAA66350	Enable 5D-WAN	Enable SD-WAN		
3900 001DAAF99078				
P1290_001DAA06F2A3	Bulk Data Settings			
		n freety select the data you want to count, use drag and drop to place each ila categories, it will affect the SD-WAN operation.	category in the corresponding profile, and specify the report interv	
	Set the category of data to be collected for statistical analysis. You ca	ata categories, it will affect the SD-WAN operation.	category in the corresponding profile, and specify the report interv Available / Disabled Bulk Data Categories	
	Set the category of data to be collected for statistical analysis. You ca which the profile returns a bulk data to the ACS. If you disable bulk d	ata categories, it will affect the SD-WAN operation.		
	Set the category of data to be collected for statistical analysis. You can which the profile returns a bulk data to the ACS. If you dhade bulk d Profile s1 Endois	ata categories, it will affect the SD-WAN operation.) Profile #2 Enuise		
	Set the category of data to be collected for statistical analysis. You ca which the profile returns a build data to the ACS. If you disable build Profile s1 Enable Separt Interval (ac)	Inla categories, II will affect the SD-WAN operation.) Profile #2 Enuble Profile #2 Enu		
	Set the category of data to be obtected for statistical analysis. You ca which the profile returns a build data to the ACS. If you disable build Profile P1 Endow (pp) horevel (pc) 120	tal categories, it will affect the SD-WAN operation.		

ltem	Description		
Search device ID/name/model/MAC	Enter the ID, name, model or MAC address of the device you want to locate.		
+Add New Network	Click to add a new network. New created network will be the sub-network of current selected network.		
Delete This Network	Remove current network group.		
Change Network	Click to change the network / group for the selected CPE.		
General Settings	Move the mouse cursor on the network you want and click Apply .		
Network ID	Display a number which is given by VigorACS randomly for the selected network.		
Name	Display the name of the parent network. You can modify it if required.		
Location	Type the location (e.g., HsinChu, New York) for this network.		
Username	Display the name of the selected network (e.g., rd8, in this case). Change it		

Advanced Settings Enable SD-WAN Enable SD-WAN Bulk Data Settings Profile # Profile # Ena If y Report Interval (sec) Bulk Data Categories Bulk Data Categories Available / Disabled Bulk Data Categories Cig Available / Disable / Disable Bulk Data Categories Cig Available / Disable / Disable Bulk Data Categories Cig Available / Disable / Disable / Disabl	able or disable able - Click to ou disable bul ecify the repor- ver. the category ely select the c edrag and dro ecify the repor- orACS server. present, availa	e the SD- ¹ enable o lk data ca rt interva of data t data you op to plac t interva able cates n be join by using	WAN function or disable thategories, it al for the pro- to be collect want to co ce each cate al at which the gories inclu- ned to the se drag-and-d	on for curren le profile. will affect the ofile returning ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop.	ange it if require t network group e SD-WAN opera g a bulk data to v cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed ata Settings.	o. ation. VigorACS I can to cofile, and to <i>and Apps</i> . from the
Enable SD-WAN Ena Bulk Data Settings Frofile # Profile # Ena If y Report Interval (sec) Specentiation of the second	able - Click to rou disable bul ecify the repor- ver. the category of ely select the c edrag and dro ecify the repor- torACS server. present, availa ch category cat ected profile, b ck to reset to fa-	enable o lk data ca rt interva of data t data you op to plac t interva able catea n be join by using factory de	or disable th ategories, it al for the pro- to be collect want to co ce each cate I at which the gories inclu- ied to the se drag-and-d efault settin	e profile. will affect the ofile returning ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop.	e SD-WAN opera g a bulk data to V cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed	ation. VigorACS I can rofile, and to and Apps. from the
Bulk Data Settings Profile # Profiles to default Disable All Bulk Data Data Profiles 4 All Bulk Data Profile # Profi	able - Click to rou disable bul ecify the repor- ver. the category of ely select the c edrag and dro ecify the repor- torACS server. present, availa ch category cat ected profile, b ck to reset to fa-	enable o lk data ca rt interva of data t data you op to plac t interva able catea n be join by using factory de	or disable th ategories, it al for the pro- to be collect want to co ce each cate I at which the gories inclu- ied to the se drag-and-d efault settin	e profile. will affect the ofile returning ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop.	e SD-WAN opera g a bulk data to V cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed	ation. VigorACS I can rofile, and to and Apps. from the
Profile # Enaility Report Interval (sec) Spection Bulk Data Categories Set freeder Bulk Data Categories Set freeder Available / Disabled At gradements Bulk Data Categories Clice Reset Bulk Data Clice Profiles to default Image: Set freeder Disable All Bulk Data After	eou disable bul ecify the repor- ver. the category of ely select the of e drag and dro ecify the repor- orACS server. present, availa ch category cat ected profile, b ck to reset to fa	lk data ca rt interva of data t data you op to plac t interva able cate n be join by using factory de	ategories, it of for the pro- to be collect want to co ce each cate il at which t gories inclu- ned to the so drag-and-d efault settir	ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop.	g a bulk data to v cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed	VigorACS I can rofile, and to and Apps. from the
If yReport Interval (sec)Specent second sec	eou disable bul ecify the repor- ver. the category of ely select the of e drag and dro ecify the repor- orACS server. present, availa ch category cat ected profile, b ck to reset to fa	lk data ca rt interva of data t data you op to plac t interva able cate n be join by using factory de	ategories, it of for the pro- to be collect want to co ce each cate il at which t gories inclu- ned to the so drag-and-d efault settir	ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop.	g a bulk data to v cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed	VigorACS I can rofile, and to and Apps. from the
Report Interval (sec) Spearer Bulk Data Categories Set free Bulk Data Categories Set free Vig Available / Disabled Bulk Data Categories At generation to the set of t	ecify the report ver. the category of ely select the c e drag and dro ecify the report orACS server. present, availa ch category cate ected profile, b ck to reset to for ext	rt interva of data tu data you op to plac t interva able cate n be join by using factory de	al for the pro- co be collect want to co ce each cate I at which t gories inclu- ied to the se drag-and-d efault settir	ofile returning ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop. ngs of Bulk Da	g a bulk data to v cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed	VigorACS I can rofile, and to and Apps. from the
Bulk Data Categories Set free Bulk Data Categories Set free Use Spec Vig Vig Available / Disabled At grade Bulk Data Categories At grade Reset Bulk Data Clice Profiles to default Image: set grade Disable All Bulk Data After set grade	ver. the category of ely select the of e drag and dro ecify the report orACS server. present, availa ch category cat ected profile, k ck to reset to find the set to find the	of data t data you op to plac t interva able cate n be join by using factory de	o be collect want to co ce each cate I at which t gories inclu ied to the se drag-and-d efault settir	ed for statisti unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop. ngs of Bulk Da	cal analysis. You orresponding pr urns a bulk data <i>and VPN, Users c</i> e or be removed ata Settings.	rofile, and to and Apps. from the
free Use Spec Vig Available / Disabled Bulk Data Categories Reset Bulk Data Profiles to default Image: Clice Im	ely select the of e drag and dro ecify the report orACS server. present, availand ch category can ected profile, h ck to reset to france the set to france the set to france the set to reset to france the set to	data you op to plac t interva able cate n be join by using factory de	want to co ce each cate I at which t gories inclu ied to the se drag-and-d efault settir	unt. egory in the co he profile retu de <i>VoIP, WAN</i> elected profile rop. ngs of Bulk Da	orresponding pr urns a bulk data <i>and VPN, Users d</i> e or be removed ata Settings.	rofile, and to and Apps. from the
Bulk Data Categories Each selection of the se	ch category can ected profile, t ck to reset to f least	n be join by using actory de	ed to the so drag-and-d efault settir	elected profile rop. ngs of Bulk Da	e or be removed ata Settings.	from the
Profiles to default	t Interval (Sec)	-		-	_	5
Disable All Bulk Data Aft	t Interval (Sec)	Enable 💽	Profile #2	-	Available / Disabled Bulk Data Categories	5
	WAN and VPN VoIP	Size 8 Size 1	Ripport Interval (sec) 300 Ruth Data Categories E Users and Apps	See 4	£	
dis me Ho	ta report for al lected for Vigo played on the enu. wever, the SD-	ll CPEs un prACS. Th sub item -WAN fur	nder the se nus, no data ns based or nctions suc	lected networ a, message ca a SD-WAN feat h as Hub and	e # will be remov rk group will not n be collected by ture under Moni Spoke, Full Mes	: be y and itoring h VPN,
					ork group are st	
Bigor	lle #1 1 Interval (sec)	Enable	Profile #2 Report Interval (sec)	Enable 🕖	Available / Disabled Bulk Data Categories	s Size: 8
0		<i></i>	0	. v.	Users and Apps	Size: 4
Bue C	Suta Categories)	Bulk Data Categories)	= VolP	Size 1
Save Clic	ck to save the					

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

Add Network	
Parent Network	
rd8	
Name	
МКТ	~
Location	
HsInChu	
Username	
YFN	~
Password	

These parameters are explained as follows:

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

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

Network Management

Search by Device ID/Name/Model/MAC/IP Address].
A 👬 Root Network(70)	
▷ 👬 @#\$%^&*_+{?":?> -+(0)</td <td></td>	
▷ 👬 Layer2(0)	
Marketing_carrie(0)	
▷ 👬 SD-WAN(2)	
b 👬 aaaaaa(123)(0)	
⊳ 🚓 rd7(0)	
⊿ 🚑 rd8(52)	
▷ # MKT(0)	
902_001DAA3D4F16	
130_001DAA8411C8	
130_001DAA854204	

6.4.1.3 Settings for Device

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

Open Network Management. This web page allows to:

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

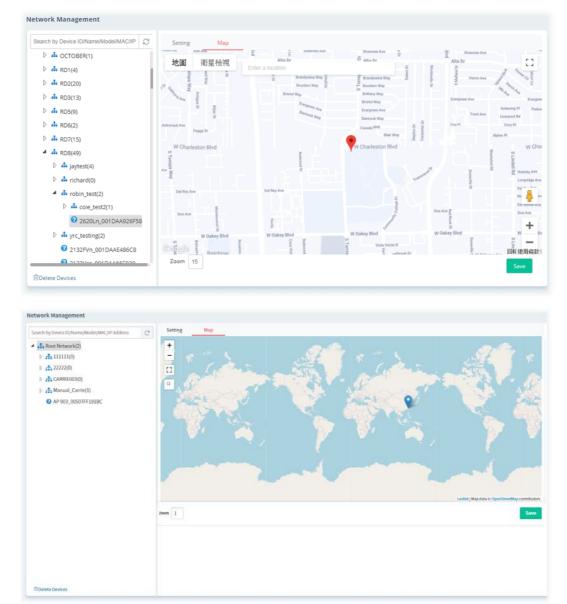
Choose and click any one of the CPE displayed on **Root Network** tree view to get the following web page.

Network Management				
Search by Device ID/Name/Model/MAC/IP Address	Setting Map			
▷ ♣ RD6(3)	Delete This Device 🖧 Change Network			
RD7(15)				
🖌 🚠 RD8(58)	General Settings			
jaytest(3)				
richard(2)	Status Disable Enable	Known Device Known Unknown		
robin_test(2)	Device ID	Network ID		
sdwantest2(0)	141307	53		
2132FVn_001DAAE486C8	Model Name	Device Name		
2133Vac_001DAA66E020	Vigor2927Lac	2927Lac_1449BC023720		
2135Vac_1449BC03B060	Note 1	Note 2		
2762Vac_001DAA653308				
2830n+ v2_001DAA000000	Serial number	MAC Address		
2860n+_001DAAD1E290		1449BC023720		
2862Vac_001DAAED3840				
2862Vac_001DAAF7C0E0(2)				
2865ac_001DAA41DF18	Location	CPE Client IP 192.168.105.120		
2865ac_001DAA41DF78				
	Phone No.	CPE Client Port 8069		
2 2912n 001DAA8E14B0				
2 2922n_001DAA8CAC84	Domain Name	CPE Client URI /cwm/CRN.html		
2925Ln_001DAADD75B0				
2925ac_001DAA512820	Management Protocol CPE default (https) http https	CPE Client User Name vigor		
		/Edit		
2926Vac_001DAA5DCAD0	Management Port 4433	CPE Client Password		
2927Lac_1449BC023720	1.00	······ •		
@ 2927Lac_1449BC023740		₽Edit		
Delete Devices				
		Save		

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

	+ Change Network ×
	Name 2020/ur_001DA4926758
	Add to network
	A floot Network A strategy A st
General Settings	
Status	Disable – The selected device will be hidden on the tree view.
	Enable – The selected device can be displayed on the tree view.
Known Device	Known – The selected CPE is known(⁽²⁾) to VigorACS 3.
	Unknown – If the selected CPE is new added device, it will be identified as Unknown (②).
Device ID / Network	Device ID – Display the number of that device which is given by VigorACS 3
ID	randomly.
	Network ID - Display the ID number of the network that selected device is grouped under.
Model Name / Device Name	Model Name – Display the model name of the selected device. Model name cannot be changed.
	name cannot be changed. Device Name – Display the name of the device for identification. It can be
Name	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device.
Name Note 1 / Note 2	name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network.
Name Note 1 / Note 2 Serial number / MAC	 name cannot be changed. Device Name - Display the name of the device for identification. It can be changed if required. Note 1 - Display brief description for the selected device. Note 2 - Display brief description for the network. Serial number - Enter a number for identification of the device.
Name Note 1 / Note 2 Serial number / MAC Address	name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device.
Name Note 1 / Note 2 Serial number / MAC Address Location	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device. Display the position of the device. It is optional and is used to offer additional information for reference. If
Name Note 1 / Note 2 Serial number / MAC Address Location Phone No.	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device. Display the position of the device. It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device. Enter a domain name for a CPE. Later, simply click the domain name to
Name Note 1 / Note 2 Serial number / MAC Address Location Phone No. Domain Name	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device. Display the position of the device. It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device. Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE. Enter a port number which will be used for accessing into web user
Name Note 1 / Note 2 Serial number / MAC Address Location Phone No. Domain Name Management Port Management	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device. Display the position of the device. It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device. Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE. Enter a port number which will be used for accessing into web user interface of the CPE.
Name Note 1 / Note 2 Serial number / MAC Address Location Phone No. Domain Name Management Port Management Protocol CPE Client IP / Port /	 name cannot be changed. Device Name – Display the name of the device for identification. It can be changed if required. Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network. Serial number – Enter a number for identification of the device. MAC Address – Display the MAC address of the device. Display the position of the device. It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device. Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE. Enter a port number which will be used for accessing into web user interface of the CPE. Choose HTTPS or HTTP.

6.4.2 Map

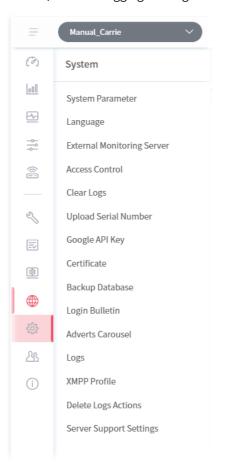


This page displays the location of the network / device on Google map / Leaflet map.

Click the **Save** button to save any changes to this map.

6.5 System

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



6.5.1 System Parameter

System / System Parameter			С
		Sea	rch Q
ID	Name	Value	
88	EnableSecureCookieSessions	false	
87	Ø JbossConfigForStandaloneMode	standalone.xml	
86	ForceWUIRedirectHttps	false	
85	NotifyServerProcessCountPerMinute	-1	
84	EnableClientRecord	true	
83	IsDeleteExpiredClientTrafficByTimestamp	false	
82	ClientRecordAliveTimeInDays	30	
81	PacketCaptureTool	true	
80	HttpProxyPort	0	
79	EnableAuditorDeletedLog	false	
78	EnableAuditorActionLog	false	
76	EnableUIGraph	true	
75	EnableGatewayGrouping	true	
74	EnableFirmwareCheck	true	
73	HealtherWebFolder	web	
72	HealtherExposelp	click me!	
S Reset to default			Cancel Save

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

ltem	Description		
5	Reset to default		
	Click the link to reset all of the system parameters with factory default values.		
1	ProvisionKeepParameter		
	It can be set with true or false.		
	True – Enable the function of Keep Profile (profile or parameters in provision).		
	False - VigorACS will disable the function of Keep Profile .		
2	ProvisionWaitCount		
	It means how many times VigorACS will compare the parameter values got from CPEs with the parameter values set within profiles. If these values are different from each other (from CPEs and from profiles), VigorACS will increase the count number by one. When the count increases to the value that users defined here, VigorACS will perform Keep Profile function.		
3	ProvisionFactoryResetEnable		
	True – The function of keep profile will perform immediately for CPE without reaching the value of 'ProvisionWaitCount'.		
4	FirmwareUpgradeCount		
	The value indicates how many CPEs can perform firmware upgrade at the same time. Set a proper value to prevent hardware from over loading and causing a crash.		
5	ProvisionDeviceAutoEnable		
	False - The CPE would not be added in Homepage when a profile defines a CPE with different names but with the same serial number.		
	True – The CPE would be added in Homepage when a profile defines a CPE with different names but with the same serial number.		
6	ProvisionChangeDeviceNameEnable		
	True - If it is set with true and a profile defines a CPE with different name but same MAC address, VigorACS would modify current CPE name with the pre-defined setting in profile.		

	That is, if the device name in profile is not the same as the log recorded in VigorACS database, the system will modify the device name automatically.
7	SettingProfileSpaceSetEnable
	True - Users can use space as character in parameter values. For example, users can use the space character as their password.
8	ParameterListLongWaitCount
	It is a positive integer (ms). After upgrading firmware, VigorACS will scan and get all parameters to restore the parameter backup. The value determines how long the waiting time out is. Multiplying the value with 50 is the maximum waiting time in millisecond.
	It will take effect after VigorACS restarts. Default is 1200.
12	GetSetParameterCount When applying the provision onto CPEs, VigorACS tries to get or set parameter from or onto CPEs. This value determines how many parameter values can be obtained or set at the same time. For example, set the value as 20. That means there are 20 parameters which can be obtained at the same time.
	Set this value properly to prevent CPEs from crashing or improve the efficiency.
13	IsDownloadUsedHttps
	When a CPE connects to VigorACS with Https, users can enable this parameter (set with true) to let CPE download file from VigorACS via Https.
14	ProvisionProfileFormat
	It can be set with 1, 2, 3 or 4.
	This value indicates the format of text configured profile.
	If the value is set with 1, the format is defined as serial number, network_device name, isreboot, and [parameter1, parameter2, and so on].
	If the value is set with 2 (as the default format), the format is defined as serial number, device name, isreboot, network, and [parameter1, parameter2, and so on].
	If the value is set with 3, the format is defined as serial number, network_device name, isreboot, address and [parameter1, parameter2, and so on].
	If the value is set with 4, the format is defined as serial number, network_device name, isreboot, network, address and [parameter1, parameter2, and so on].
15	IsRebootAfterDownload
	True- After downloading and upgrading the firmware, reboot the CPE.
	False - Users must reboot the CPE manually.
16	KeepProfileUpdateRule
	It can be set with is 1, 2 or 3.
	The value 1 means after uploading profile, keep original Keep Profile settings and add extra parameter settings (if the profile contains more parameter settings).
	The value 2 means after uploading profile, delete original Keep Profile setting if the device name changed.
	The value 3 means after uploading profile, delete original Keep Profile settings every time.
17	IsSetGlobalParameter
	False - Disable global parameter configuration function. When it is disabled, even users set global parameters, these parameters won't be applied.
19	IsTurnOffPeriodicInform
	True - If PeriodicInform interval (configured in 59. CPEPeriodicInformInterval) is too short, CPE may send too much information to VigorACS and cause the server crash. Set this value true only if the case happened (server crashed). The default interval setting shall be 900 seconds.

	False - After adjusting the PeriodicInform (configured in 59. CPEPeriodicInformInterval) of CPEs, remember to set this value false.
20	PollingDeviceCount
20	The value determines the maximum number of CPEs to poll at one time. If this value is set too small (e.g., 500), it might cause server overload. However, if it is set too big (e.g., 600000), it could make CPE status refresh very slowly.
	Note: After changing this parameter value, restart VigorACS to apply the change.
21	 DeviceAutoEnable True - If it is set true, after obtaining the information from CPE, the newly added device would be added in the tree view of Homepage. False – When VigorACS receives information from new added device, it will not display the CPE on the tree view of Homepage until make configuration in SYSTEM MENU>>Network Management.
22	PollingInterval
	Set the polling interval for VigorACS to examine CPE. The unit is milliseconds. Default is 900000.
23	CPEWebUiPort
	Set a port number for VigorACS system accesses into CPE's WUI.
26	VPNIPSecDefaultSecurity
	Set the default security method for establishing VPN based on IPsec.
27	CheckDeviceStatusCount
	Determine how many times shall VigorACS system check the device before the device becomes offline.
28	VPNChangeEnable
	True – If one of the WAN IP addresses changes on both ends of VPN, VigorACS will change the setting automatically to rebuild the VPN tunnel.
	False – Default value.
29	WANSeverity
	Set the severity (critical, major, minor, warning and normal) for WAN connection.
30	VPNSeverity
	Set the severity (critical, major, minor, warning and normal) for VPN connection.
32	EnableHttpChunkedMode True - Use chunked mode (chunked transfer encoding) for HTTP. False – Default value.
33	CPEWebUiProtocol Set HTTP (default) or HTTPs as the protocol for accessing CPE's web user interface.
34	EnableValidateCodeCheck
J-1	True – Enable the function of validating code check on the login page. False – Disable the function. It is the default value.
35	VPNIPSecDefaultMode
	Set the default mode for IPsec VPN connection.
	Main
	Aggressive
36	StatisticsStep
	Set the time interval (default is 900) for data collection for RRD traffic.

38	EnableWebServices
	True – The third party software can get/set VigorACS functions through web services.
	False – Default value.
41	HidePassword
	True – Hide the password value on provision page.
	False – Default value.
43	VPNEnablePingKeepAlive
	True – Enable the function of Enable PING to keep VPN alive for CPE while creating VPN by
	using the VPN wizard.
	False – Default value.
44	CPEDetectMode
	Set the CPE detection mode. 0 means TR069; 1 means ping.
46	EnableRRD
	True – Enable the function of data collection (StatisticsStep) for RRD traffic.
47	AutoDetectRouteName
	True – Get CPE's router name.
	False – Default value.
48	EnableBatchActivation
	True – Enable the batch activation license to MyVigor portal server function.
	False – Default value.
49	DefaultSetDeviceKnown
	True – Set the new added CPE as a known device.
	False – Default value.
50	KeepProfileRebootByBOOTSTRAP
	True – VigorACS will ask the CPE to reboot if receiving CPE request including BOOTSTRAP.
	False – Default value.
51	DisableAlarmMailByACSReboot
	True – VigorACS will not send alarm message within 15 minutes after turning on VigorACS.
	False – Default value.
52	DeleteOldDeviceBySameIP
	True – If a new CPE with an IP address which is the same as an old device recorded on
	VigorACS database, VigorACS will delete the information for the old device.
	False – Default value.
54	DisablePolling
	True – Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration.
	False – Default value.
55	DisableAlarmMailByClear
	True – Disable the function of sending alarm e-mail when alarm status is clear. It is the default setting.
	False – VigorACS will send alarm e-mail when alarm status is clear.
56	
90	UseStunAddressForVpn True – Remote IP address will use the STUN IP address for VPN connection.
	False – Default value.

57	EnableChangeNetworkByNetworkUser
	True – Default value. When VigorACS finds that the username and password sent from the CPE changed, it will move the CPE to the network group with the same username and password.
	False – Disable such function.
58	FWUpgradeFailInterval
	If the firmware upgrade failed, the next firmware upgrade will execute after the time interval configured here. Default value is 86400 seconds.
59	CPEPeriodicInformInterval
	CPE will send general information to VigorACS periodically. The default value is 900 seconds. If required, enter the time interval for the CPE to send general information to VigorACS.
60	EnableForceSetCPEPeriodicInformInterval
	True –Default value. Enable the function of CPEPeriodicInformInterval.
	False – Disable the function of CPEPeriodicInformInterval.
61	TimeFormat
	Display the time format. 0 means 24-hour clock; 1 means 12-hour clock.
62	EnableRecordActionLog
	True – Enable the function of record action log. It is the default value.
	False – Disable the function of record action log.
63	EnableBackupCheck
	True – VigorACS will check the parameter value of
	"InternetGatewayDevice.X_00507F_System.ConfigBak.ConfigChanged" and perform the configuration backup automatically if any change made for CPE's configuration.
	False – Default value.
64	CheckCPEValidByAuthKey
	True – VigorACS will check if the authentication key informed by CPE is valid or not.
	False – Default value.
65	New_DeleteOldDeviceBySameIP
	True – If a new CPE with an IP address which is the same as an old device recorded on
	VigorACS database, VigorACS will delete the information for the old device and write the
	configuration on the database related to the old CPE onto new CPE. False – Default value.
66	CheckCPEValidByNetworkUser
	True – Each network can be set with a group of username and password individually. All of the CPEs grouped under the network shall use such username and password for connecting
	to VigorACS. Such function let VigorACS check if the username and password sent from the
	CPE match with the settings on the network or not. If not, VigorACS will ignore the CPE
	request and change the group of the CPE into root network. False – Default value.
<u> </u>	
67	EnableAutoChangeWebPort
	True – Enable for changing web port automatically. It is the default setting. False – Disable the function.
<u> </u>	
68	DisableSaveInformLog
	True – Disable the function of Save Inform Log. False – Default value.
70	
70	ShowTreeCount

	Set how many devices will be shown on the home device tree. Default value is 100.
71	EnableSendCPENotify
	True - When the value of parameters for CPE is changed, a notification of 'IntenetGatewayDevice.X_00507F_Notify' will be sent to VigorACS. VigorACS will send the message to the specified user by e-mail, SMS or SNMP.
	False - When the value of parameters for CPE is changed, a notification of 'IntenetGatewayDevice.X_00507F_Notify' will be sent to VigorACS. VigorACS will not send the message to the specified user.
72	HealtherExposeIp
	It means the exposed IP in Monitoring Server message. Default is one of VigorACS host IP addresses. You can change to any IP without restarting ACS Server.
73	HealtherWebFolder
	It means the folder name of VigorACS in JBoss deployment folder. It is used to create the URL for the device in Monitoring Server message. Default folder name is set as "web".
74	EnableFirmwareCheck
/-	True - VigorACS will compare current firmware of the device with the file version detected from DrayTek website. Therefore, while viewing the Firmware Version on the dashboard of the selected device, a pop-up window with current firmware version detected will appear if both firmware versions are different.
75	EnableGatewayGrouping
	True – Enable the function of grouping VigorAP devices by using gateway addresses and displaying AP devices behind the gateway routers. False – Default value.
76	EnableUIGraph
76	EnableUIGraph True – Enable the function of displaying graph of web user interface. It is the default value.
76	-
76 78	True – Enable the function of displaying graph of web user interface. It is the default value.
	True – Enable the function of displaying graph of web user interface. It is the default value. False – Disable the function.
	True – Enable the function of displaying graph of web user interface. It is the default value.False – Disable the function.EnableAuditorActionLogTrue – The auditor action will be recorded and displayed on SYSTEM MENU >> System >>
	True – Enable the function of displaying graph of web user interface. It is the default value. False – Disable the function. EnableAuditorActionLog True – The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False – Default value. When the auditor deletes logs or protects identity information on
78	 True – Enable the function of displaying graph of web user interface. It is the default value. False – Disable the function. EnableAuditorActionLog True – The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False – Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded.
78	 True - Enable the function of displaying graph of web user interface. It is the default value. False - Disable the function. EnableAuditorActionLog True - The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False - Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded. EnableAuditorDeletedLog True - The selected logs will be moved to another table which can be read by auditors. While protecting client identity information, the protected value can be recovered for
78	 True - Enable the function of displaying graph of web user interface. It is the default value. False - Disable the function. EnableAuditorActionLog True - The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False - Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded. EnableAuditorDeletedLog True - The selected logs will be moved to another table which can be read by auditors. While protecting client identity information, the protected value can be recovered for auditors. False - Default value. The selected logs will be deleted from database permanently. While
78 79	True – Enable the function of displaying graph of web user interface. It is the default value. False – Disable the function. EnableAuditorActionLog True – The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False – Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded. EnableAuditorDeletedLog True – The selected logs will be moved to another table which can be read by auditors. While protecting client identity information, the protected value can be recovered for auditors. False – Default value. The selected logs will be deleted from database permanently. While protecting client identity information, the protected value cannot be recovered for auditors.
78 79	 True - Enable the function of displaying graph of web user interface. It is the default value. False - Disable the function. EnableAuditorActionLog True - The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions. False - Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded. EnableAuditorDeletedLog True - The selected logs will be moved to another table which can be read by auditors. While protecting client identity information, the protected value can be recovered for auditors. False - Default value. The selected logs will be deleted from database permanently. While protecting client identity information, the protected value cannot be recovered for auditors. False - Default value. The selected logs will be deleted from database permanently. While protecting client identity information, the protected value cannot be recovered for auditors. HttpProxyPort It can be set with 0 to 65535, or a port range (e.g. 10000-10005). If the value set to 0, the proxy port number will be automatically allocated. If you start the proxy server before change this value, you have to restart VigorACS Server to apply this change on the current proxy. If the proxy port is only one number large than 0, you can only create one proxy

82	ClientRecordAliveTimeInDays
	Set the number of days for reserving the record (about client traffic). When exceeding the
	day limit, VigorACS will delete the record.
	Default value is 30(days).
83	IsDeleteExpiredClientTrafficByTimestamp
	True – Enable the function of ClientRecordAliveTimeInDays.
	False – Default setting.
84	EnableClientRecord
	True – Default value. Enable the function of recording client traffic and displaying related
	information on NETWORK MENU >> Monitoring >>Clients.
85	NotifyServerProcessCountPerMinute
	It can be set with -1, 100 to 100000. This parameter determines how many Emails, SMS, and health parameters notification items the notification server can process per minute.
	-1 means unlimited.
96	
86	ForceWUIRedirectHttps True - Force ACS WUI to HTTPS only. If you encounter login failed error after changing this
	parameter, please clear the browser's cache then try again. If the
	EnableSecureCookieSessions parameter is set to "true", this parameter will be automatically
	enabled and disallow set to false.
87	JbossConfigForStandaloneMode
	The Default Configuration for standalone Mode is "standalone.xml" (default). The
	standalone-secure.xml will enhance the security protections of your ACS website with plugins that prevent hacking.
88	EnableSecureCookieSessions
00	True - Secure flag is to prevent cookies from being observed by unauthorized parties due to
	the transmission of a the cookie in clear text. If the value set to true, the
	ForceWUIRedirectHttps parameter will be automatically enabled and the cookie will only be
	sent in a secure manner (i.e. Https). False - Default setting.
89	LogRotationHandlerType - Select one of the following types for log.
	SizePeriodic
	Periodic-size
01	
91	MapServiceProvider There are two mechanisms to display maps on VigorACS, Google and Leaflet.
00	
92	EnableUsermailValidation
	True - If it is enabled, the user will receive an e-mail first and be guided to pass the authentication when he tries to log in to VigorACS.
	After switching the toggle to enable this function, the VigorACS system will open the
	User>>Mail Server page. You have to check if the mail server is enabled and other options have been configured correctly.
	False - Default setting.
Save	Save the current settings.
Juve	save the carrent settings.

6.5.2 Language

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

	Dray Tek VigorACS	⊕ EN ∨ CN DE EN NL
Dray Tek	Username	 ©
RD8	C Remember me	
0 • 0		

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

System / I	anguage									
<u></u> Upload				И	<	1	/1	>	Ы	C
	Filename	Size	Last Modified							
	lang_CN.txt	206882	07/01/2020 20:00:21							
	lang_DE.txt	357818	07/01/2020 20:00:21							
	lang_EN.txt	421645	08/26/2020 20:30:11							
	lang_NLtxt	94518	08/13/2020 20:30:04							
	lang_TW.txt	404617	08/26/2020 20:30:11							

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

6.5.3 External Monitoring Server

6.5.3.1 Health Server

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

lisanth Service	System / External Monitoring Server		
Wireless Client Information Server	Enable Server		
	URL	apt.tptechvlew.com	
	Username	acs.drayddns.com	
	Password	···· •	
	API	Health_Default_GLOBAL ~	
			Cancel Save

These parameters are explained as follows:

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

6.5.3.2 Wireless Client Information Server

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

Health Server	System / External Monitoring Server		
	User Group	RootGroup ~	
	Enable Server		
	Authentication	NAYCcCGM23N52sW2rGpVJCGapQLsE48L2kgD80Vac	
	URL	http://www.draytek.co.uk/torms/json.php	
	API	Wireless_Chent_Default_GLOBAL ~	

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

6.5.4 Access Control

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

6.5.4.1 General Setting

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

General Setting Blacklist Whitelist WUI Login None Blacklist Whitelist CPE Service None Blacklist Whitelist API WebService None Blacklist Whitelist
CPE Service None Blacklist Whitelist
API WebService None Blacklist Whitelist

These parameters are explained as follows:

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

6.5.4.2 Blacklist

This page is used for creating blacklist profiles.

System / Acce	ss Control						
General Setting	Blacklist Whitelist						
						Search IP / Description	Q
+ Add 👘 I							Limit: 2/256
	IP	↓↑ Description	J↑ WUI Login	↓↑ CPE Service	↓↑ API WebService	1¢	
	172.16.2.116					🖉 Edit	
	192.168.105.170	192.168.105.170				🖉 Edit	
							Save
							_

ltem	Description
------	-------------

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

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

Description	Marketing_CAN				
Address Type	Single IP Address	~			
Start IP Address	123.12.1.1		~		
Service Enable	🗹 WUI Login 🔽 CPE Service				
	API WebService				
				× Cancel	🕲 Save

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

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

6.5.4.3 Whitelist

This page is used for creating whitelist profiles.

System / Access	s Control							
General Setting	Blacklist Whitelis	st						
							Search IP / Description	c
+ Add 🗇 De								Limit: 1/25
	IP	41	Description	4↑ WUI Login	↓↑ CPE Service	J↑ API WebService	ψî	
	192.168.1.12		white_for_market	2	•		🖉 Edit	
								Save
								Save

These parameters are explained as follows:

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

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

+ IP Address For	m				×
Description	white_for_market				
Address Type	Single IP Address	~			
Start IP Address	123.12.1.10] ~		
Service Enable	🗹 WUI Login 🔽 CPE Service				
	API WebService				
				× Cancel	🖹 Save

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

6.5.5 Clear Logs

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

System / Clear Logs		
Delete Time Delete Type 🕢	All C Log C Alarm C Device log	
Auto Clear		
Duration	Every Day Every Week Every Month	
Periodic(weeks)	1	
Week	Tuesday 🗸	
Delete Now		Cancel

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

CancelDiscard current settings and restore the default settings.	
Save	Save and activate the current settings.

6.5.6 Upload Serial Number

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

rstem / Upload Serial Number						
 Download Template Delete					И	< 1 /2 > P C
Mac Address Ut	Serial Number 41	Device Name	↓↑ Network	↓↑ Model	↓† WAN IP ↓†	LAN IP 41 FW 41
001DAAA8BCE8	12A002099451					
001DAAA8C450	12A002099452					
001DAAA8D100	12A002099453					
001DAAA8D10a	12A002099453					
001DAAA8D10s	12A002099453					
001DAAA8D10z	12A002099453					
001DAAA8D11z	12A002099454					
001DAAA8D12z	12A002099455					
001DAAA8D13z	12A002099456					
001DAAA8Da00	12A002099453					
001DAAA8Ds10	12A002099453					

ltem	Description
Upload	Click 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.
	Select SerialNumber File × upload_serial_number (1).cs Browse × Cancel ✓ Apply
Download Template	Click to download a template from the VigorACS server to your local host.
	This template is convenient for the system administrator to enter the required information for lots of devices at one time. Later, the template can be uploaded to VigorACS server.
	Please open the template with a software which can read and write ".CSV" file. Fill the MAC address and serial number (printed on the rear side / bottom) of a device.
Delete	Click to delete the selected entry.
Check box	Check the box to specify an entry. Later, the selected one can be deleted if required.

6.5.7 Google API Key

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

Google Maps API Key 🛛		
	Please go to the function management to assign user roles to access the map.	Function Management
	Or go to system parameter page to select another map service.	System Parameter
oogle Analytics API Key 🚱		
		El Sa

These parameters are explained as follows:

ltem	Descript	Description						
Google Maps API Key	 Enter the key you obtained from Google. Function Management - Click this button to open the setting page. Determine which user role can view the map and switch the toggle to enable the map display for the user. 							
	Group Administrator							
	Administrator		•					
	Commissioning							
	Operator			C				
	View Only Operator							
	Author							
	-		meters - ogle and				to display maps need.	
	91 O Mapfento/Veeder					Leafet		
	91 O MapSe					Google		

6.5.8 Certificate

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

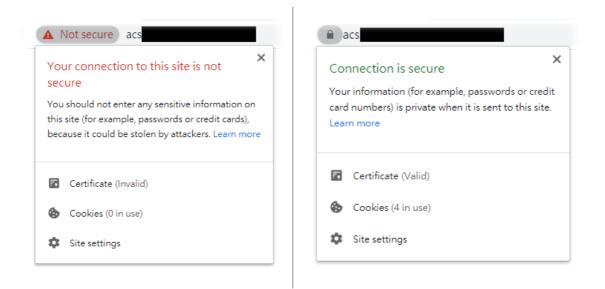
It is suggested to use HTTPS protocol for encrypting the connection between the browser and the web server for every website to prevent private information (such as account, password, personal data, credit number, and others) entered by users from leakage.

Browsed by Google Chrome

Browsed by Google Chrome

A prompt for HTTPS web site encrypted with **INVALID** certificate

A prompt for HTTPS web site encrypted with **VALID** certificate



6.5.8.1 Certificate

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

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

ficate Certificate with private key PKCS #12					
Create a local Certificate Signing Request(CSR) :					
Generate a CSR					
		d			
① Note:					
Please submit the "centred csr" file in the C	rtificate Authority then do the part step.				
Please submit the "certreq.csr" file to the C	rtificate Authority then do the next step.				
Please submit the "certreq.csr" file to the C	rtificate Authority then do the next step.				
Please submit the "certreq.csr" file to the C Import Certificate :	rtfficale Authority then do the next step.		licera		
Please submit the "centres cor" file to the C Import Certificate sot CA Certificate (cert.crt)	rifficate Authority then do the next slep.				
Please submit the "centres cor" file to the C Import Certificate sot CA Certificate (cert.crt)	rtflickle Aufhorthy (Nen du De next diep.	Roos			
Please submit the "centreq csr" file to the C Import Certificate set CA Certificate (cent, crt)	ntflaate Authority (Sen du De next diep.				
Please submit the "centragood" file to the C Import Centificate : out CA Centificate (car, cnt) termediate CA Centificate (car, cnt)		Rease	Didde		
Please submit the "centragood" file to the C Import Centificate : out CA Centificate (car, cnt) termediate CA Centificate (car, cnt)		Rease			
In provide the formation of the Constitution of the Constitution of the Constitution of the formation of the		Rease	Didde		

These parameters are explained as follows:

ltem	Description
Generate a CSR	Click to generate a CSR certificate.
Import Certificate	 Click the Browse button to specify a file to apply the HTTPS certificate. Root CA Certificate Intermediate CA Certificate Trusted Certificate
Save	Save current settings and uploading/pasting the certificate.

6.5.8.2 Certificate with Private Key

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

System / Certificate					
Certificate Certificate with private key PKCS #12					
Certificate form	With Root and Intermediate Certificate(s)	With CA Bundle	One PEM File	None of above	
Import Method	Upload Files Paste Contents Directly				
Private Key(.key)					Browsat
Root CA Certificate(.cer, .crt)					Ercowse
Intermediate CA Certificate(.cer, .crt)					Browse
	+Add				
Trusted Certificate(.cer, .crt)					Browse
					Save

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

When One PEM File is selected				
PEM File (.pem) Click the Browse button to select one PEM file.				
Save	Save current settings and uploading/pasting the certificate.			

Example

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

AddTrustExternalCARoot.crt _{類型:} 安全性憑證	
COMODORSAAddTrustCA.crt _{類型:} 安全性憑證	Intermediate CA Certificate 1
COMODORSADomainValidationSecureServerCA.crt 類型: 安全性憑證	Intermediate CA Certificate 2
 download_xpertdata_nl.crt _{類型:} 安全性憑證	Trusted Certificate
download_xpertdata_nl.key 類型: KEY 檔案	Private Key

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

ca_bundle.crt _{類型:} 安全性憑證	CA Bundle
- certificate.crt 頑型:安全性憑證	Trusted Certificate
private.key 類型: KEY 檔案	Private Key

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

BEGIN PRIVATE KEY	
MIIEkjC	
END PRIVATE KEY	
BEGIN CERTIFICATE	
MIIGDjCCBPag	
END CERTIFICATE	

6.5.8.3 PKCS #12

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

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

item / Certificate		
ertificate Certificate with private key	PKCS #12	
Import PKCS #12 file		Browse
PKCS #12 Password		۵
Note: Place use the "tr060" as the e	ntry name for your PKCS #12 certificate file.	
Flease use the 1009 as the e	ia y name for your FRC3 #12 certificate file.	
		Save

These parameters are explained as follows:

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

6.5.9 Backup Database

6.5.9.1 Backup Tasks

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

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

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

+Add a Task				Au	to Refresh: 30 Seconds ~	C Search Profile Name/Cre
Task Name	Schedule/Period	Last Implemented Status	Last Implemented Date	Created By	Authentication	Action
testBckAllNow	Now	Completed	2018-04-11 09:25	yrctw	Internal	🖉 Edit. 🙁 Delete
testBckDally	Now	Completed	2019-03-21 14:17	yrctw	Internal	🖉 Edit 🖄 Delete
testBckDallyPM	Daity	🕒 Completed	2020-11-02 20:00	yrctw	Internal	🖉 Edit 👘 Delete
taskBckNowExclude	Now	Completed	2020-10-29 15:55	yrctw	Internal	🖉 Edit 🕫 Delete
sackup	Now	Completed	2020-03-03 09:20	aries	Internal	🖉 Edit 🗌 Delete
(i) Note						

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

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

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

🛢 Backup Database Task		\times
Task Settings		-
Enable This Task		
Task Name		
Scheduling		-
Run Backup	Once Repeat	
	Later ~ 11/03/2020 00:00	
Backup Options		-
Backup Type	Backup all tables	
Ignore License Tables		
Compress Backup File		
After backup delete log tables	Yes No	
Email Notification		-
Enable Email Notification		
Email Subject	Backup Database Task	
Email From	example1@gmail.com	
Email Contont		
	Cancel 🗈 Save	2

These parameters are explained as follows:

ltem	Description	
Task SettingsEnable This Task - Click to enable the task.		
	Task Name - Enter a name for the new task.	
Scheduling	Run Backup – Choose Once to perform the backup immediately or at certain time. Choose Repeat to perform the backup periodically.	

	•	Later / Now – It is a	vailabl	e whe	n Onc	e is selected as	Run Backup.
	•	Starts on xxxxx – lt Backup. Click Edit to time setting.				•	
		Repeat					
		Repeats Weekly *				•	
		Repeat on	Sun	Mon	🗆 Tue	U Wed	1
	b	2	🗌 Thu	🗆 Fri	🗆 Sat	0	5
		Starts on	02/25/20	20			io
		Starts time 00:00					
		Summary	Weekly or	n Sunday			
	d	e					
						Car	ncel Done
Backup Options	Back	up Type – Choose ar	n optio	n to p	erforr	n the backup.	
	_						
	B	ackup all tables		~			
	В	ackup all tables					
	E	xclude syslog tables					
	E	xclude syslog and log	tables	5			
		<u> </u>				6	
		re License Tables – \ noring the tables con					
		n, dslpmid, dslpmshov		-			-
	trans	ferring VigorACS serv	/er. Th	e defa	ult va	ue is "Enabled'	'.
	Com	press Backup File - 🛛	Гhe ba	ckup f	ile wil	be compresse	d.
	After backup delete log tables – Delete the log tables immediately when VigorACS server finishes the backup job						
Email Notification						orACS server w	ill send a
		Enable Email Notification – If enabled, VigorACS server will send a notification email about database backup to the recipient.					
	•	Email Subject – Ente	er the	subjed	t for t	he email.	
	•	Email From – Enter	the en	nail ad	dress	of the sender/	agent/registrar.
	•	Email Content – Ent	ter the	conte	ent of	the email.	
	•	Email To – Enter the	e email	addre	ess of	the recipient.	
	•	+Add recipient – Ad VigorACS server.	ld mor	e recij	oients	to receive the	email from
Cancel	Disca	ard current modificati	ion.				
Save	Save	the current settings a	and ex	it the	page.		

6.5.9.2 Backup Files

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

ackup Tasks	Backup Files Error Logs		
Delete	Download		KI < 1 /44 > DI C
	Filename	$\downarrow\uparrow$ Size $\downarrow\uparrow$	Last Modified
	backup_ACS_Trunk AutoBuild 13635_ExcludeSyslogAndLogVer_2020-02-24.2000.sql	11.88 MB	02/24/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13635_ExcludeSyslogAndLogVer_2020-02-22.2000.sql	11.85 MB	02/22/2020 20:00:03
	backup_ACS_Trunk AutoBuild 13622_ExcludeSyslogAndLogVer_2020-02-21.2000.sql	11.86 MB	02/21/2020 20:00:03
	backup_ACS_Trunk AutoBuild 13584_ExcludeSyslogAndLogVer_2020-02-19.2000.sql	11.86 MB	02/19/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13569_ExcludeSyslogAndLogVer_2020-02-18.2000.sql	11.86 MB	02/18/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13548_ExcludeSyslogAndLogVer_2020-02-15.2000.sql	11.87 MB	02/15/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13546_ExcludeSyslogAndLogVer_2020-02-14.2000.sql	11.86 MB	02/14/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13532_ExcludeSyslogAndLogVer_2020-02-13.2000.sql	11.85 MB	02/13/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13508_ExcludeSyslogAndLogVer_2020-02-12.2000.sql	11.85 MB	02/12/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13451_ExcludeSyslogAndLogVer_2020-02-10.2000.sql	11.85 MB	02/10/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13427_ExcludeSyslogAndLogVer_2020-02-08.2000.sql	11.83 MB	02/08/2020 20:00:03

ltem	Description		
Delete	Click to remove the selected filename.		
Download	Click to download the file from the hard disk of Vig restoration or transferring.	orACS server	located for
	System / Backup Database		
	Backup Files Error Logs		
	Boetee 4 Download	-1 Stor -11	Last Medified
	backup ACS_Trunk AutoBuild 2016. Exclude/systop/indi.og/ver_2020-11-02.2000.sql.zpp		11/07/2020 20:00:04
	backup, ACS_Trunk AutoBuild 2016_ExcludeSystopAndLogVer, 2020-11-01.2000.sqLap	1.09 MB	11/01/2020 20:00:02
	backup, ACS_Trunk AutoBuild 2016_ExcludeSystogAndLogVer_2020-10-31.2000.sqLpp	1.09 MB	10/31/2020 20:00:07
	backup, ACS_Trurik AutoBuilti 2016_ExcludeSyslogAndLogVer_2020-10-30.2000.sqLstp	1.09 MB	10/30/2020 20:00:07
Filename	Display the name of the backup file.		
Size	Display the size of the backup file.		
Last Modified	Display the last modified time.		

6.5.9.3 Error Logs

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

ackup Tas	ks Backup Files Error Logs							
				82	14	/1 2	91	c
	Filename	47 Size 47	Last Modified					14
	backup_ACS_Trunk AutoBuild 1024_ExcludeSystogAndLogVer_2020-07-15.2000_error.log	0 Byte	07/15/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 996_ExcludeSyslogAndLogVer_2020-07-14.2000_error.log	0 Byte	07/14/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 992_ExcludeSyslogAndLogVer_2020-07-13.2000_error.log	0 Byte	07/13/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 944_ExcludeSystogAndLogVer_2020-07-09.2000_error.log	0 Byte	07/09/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 852_ExcludeSysiogAndLogVer_2020-07-04.2000_error.log	0 Byte	07/04/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 842_ExcludeSyslogAndLogVer_2020 07-03.2000_error.log	0 Byte	07/03/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 802_ExcludeSyslogAndLogVer_2020-07-01.2000_error.log	0 Byte	07/01/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 780_ExcludeSyslogAndLogVer_2020-06-29.2000_error.log	0 Byte	06/29/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 761_ExcludeSyslogAndLogVer_2020-06-24.2000_error.log	0 Byte	06/24/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 759_ExcludeSyslogAndLogVer_2020-06-23.2000_error.log	0 Byte	06/23/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 12732_ExcludeSyslogAndLogVer_2020-06-19.2000_error.log	0 Byte	06/19/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 722_ExcludeSyslogAndLogVer_2020-06-18.2000_error.log	0 Byte	06/18/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 12732_ExcludeSyslogAndLogVer_2020-06-17.2000_error.log	0 Byte	06/17/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 664_ExcludeSyslogAndLogVer_2020-06-12.2000_error.log	0 Byte	06/12/2020 20:00:00					

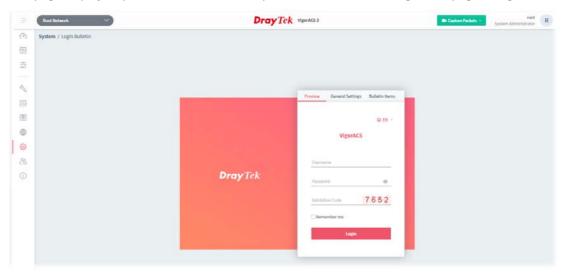
ltem	Description	
Delete	Click to remove the selected error log.	
Download	Click to download the selected error log from the hard disk of VigorACS server located.	
	The downloaded log file can be browsed by any text editor. If the content of the log contains the error message output by the program of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

6.5.10 Login Bulletin

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

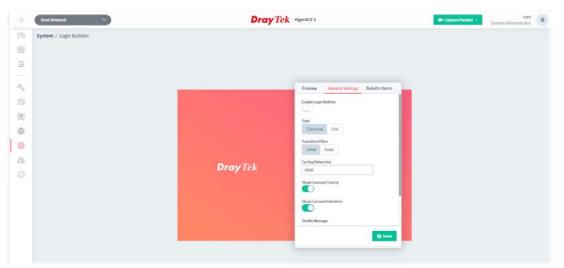
6.5.10.1 Preview

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



6.5.10.2 General Settings

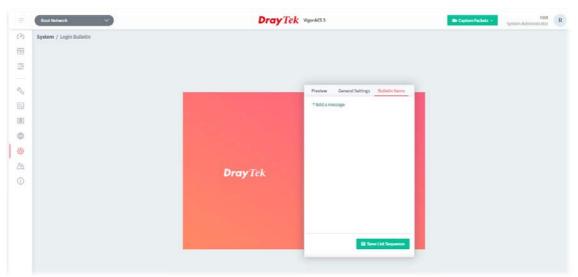
It allows the user to enable and configure settings for login bulletin.



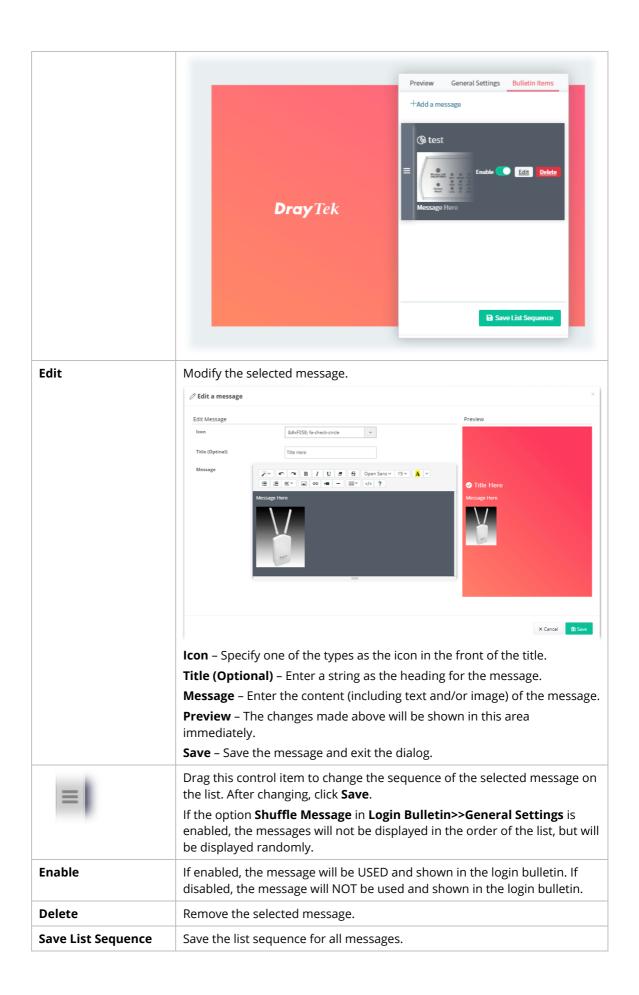
ltem	Description	
Enable Login Bulletin	If it is enabled, a bulletin with specified content will be shown on the login web page of VigorACS.	
Style	The message on the bulletin will be displayed with carousel animation or listed one by one.	
	Carousel – Messages in bulletin will be displayed with carousel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

6.5.10.3 Bulletin Items

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



ltem	Description			
+Add a message	Create a new message.			
	+ Add a message	×		
	Edit Message	Preview		
	Isen ﱐ fachedosinde ~			
	Title (Optinal) Title Here Message			
	Nessage Here	Title Here		
		Nessage Here		
	_			
		X Canrel 🚯 Save		
	Icon – Specify one of the types as the icon in th	e front of the title.		
	Title (Optional) – Enter a string as the heading	for the message.		
	Message – Enter the content of the message.			
	Preview – The changes made above will be sho immediately.	own in this area		
	Save – Save the message and exit the dialog. Reresult.	efer to the following setting		



6.5.11 Adverts Carousel

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

6.5.11.1 General Settings

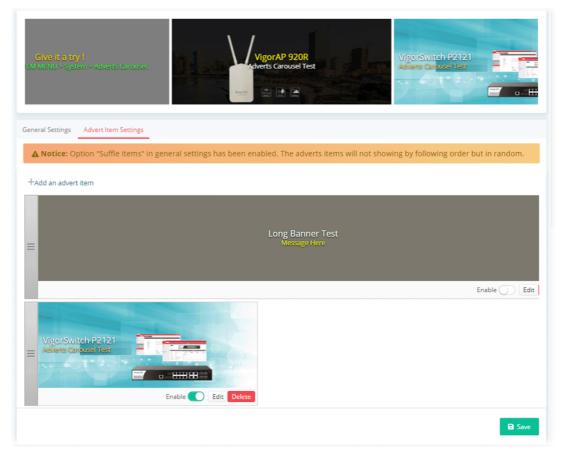
This page determines if displaying the adverts on the login page or not, enabling the auto play carousel function, selecting cycling delay time and using the shuffle items.

System / Adverts Carousel	
Adverts Carousel Preview	~
	Vigor2762 Series Adverts Carousel Test
General Settings Advert Item Settings	
Show on Login Page	
Auto Play Carousel	
Cycling Delay (ms)	5500
Shuffle Items	When enable it, the advert items will showing in random order.
	B Save

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

6.5.11.2 Advert Item Settings

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



These parameters are explained as follows:

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

To add an advert item, do the following steps.

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

+ Add an item		×
Upload Image	Please select an image. Browse	
	🏝 Upload	
(1)Note:Height will automatically a	idjust to 180px.	
 Notice: Image width needs to be § 	greater than or equal to height.	
Preview		
	Upload an Advert Image Please upload an image first.	
	Cance	el 🔯 Save

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

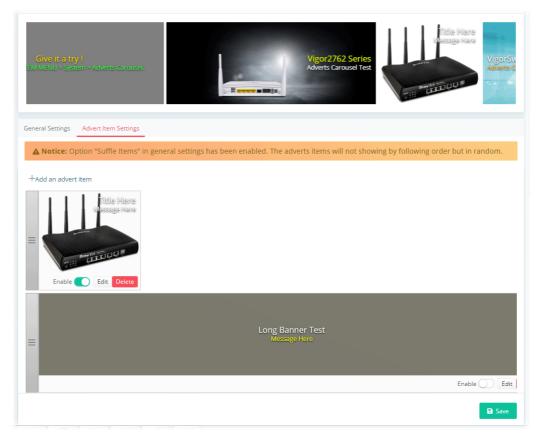
2. After specifying an image file, click the **Upload** button. Later, a page with detailed settings will appear as follows:

 Add an item 		
Upload Image	Please select an image. Browse	
	A Upload	
Title (Optinal)	Title Here	
Title Color	(Max. 60 characters)	
Message (Optinal)	Message Here	
Message Color	(Max. 250 characters)	
Enable Hyper Link		
Link Address	http://www.draytek.com/	
Text Block Position	0 1 2	
	3 4 5 6 7 8	
review		
	Tuile Hierre Wessage Hiere	
	Cancel	🕲 Save

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

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

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



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

Enable	carousel.	tem will be USED and shown in the adverts
F J14	carousel.	
Edit	Click to modify settings	for the selected image.
	🗹 Edit an item	×
	Upload Image	Please select an image. Browse
	Title (Optinal)	Give it a try ! (Max. 60 characters)
	Title Color	#ffde00
	Message (Optinal)	Change it on SYSTEM MENU > System > # (Max, 250 characters)
Delete	Delete the selected adv	/ert item.
Save	Save the current settin	gs.

6.5.12 Logs

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

VCS System	Log Syster	m Log Login											
elect butte	ons to filter Sev	verity / Category	/Result:										
Critical	Major Mir	nor Warning	Normal	Mainten	ance Reports Provisioning	Network System User Apply Succeeded Apply Failed							
									н	< 1.	16	> 0	019
ø	User	Authentication	Severity	Interface	Category	Overview	Result	Login IP		Time			
3718	pm	Internal	A Critical	WUI	User > Group Management	User root has been removed from RootGroup's group	Succeeded	172.16.3.134		2020/11/03 1	0:21:38 A	м	
8717	angela	Internal	📥 Major	WUI	Provisioning > Global Parameters	(Angela) Profile test_angela has been added.	Succeeded	172.16.3.134		2020/10/30 1	1:42:57 A	м	
3716	Kevtn	Internal	Minor	WUI	Network Management	ALANWEN (82) Network location has been changed.	Succeeded	192.168.105.99		2020/10/28 0	14:32:54 P	м	
3715	David	Internal	📥 Minor	WUI	Network Management	AP 1060C_001DAA80FED4 (141446) Device has been deleted.	Succeeded	192.168.105.135		2020/10/28 0	13:39:37 P	м	
3714	David	Internal	Minor	WUI	Network Management	Network has been moved to another parent network.	Succeeded	192.168.105.135		2020/10/28 0	13:37:47 P	м	
3713	David	Internal	A, Critical	WUI	User = User Management	User david has been created.	Succeeded	192.168.105.135		2020/10/28 0	13:04:44 P	м	
3712	aries	Internal	Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192.168.105.120		2020/10/28 0	1-16:30 F	м	
9711	link_chiang	Internal	Minor	WUI	Network Management	RD2 (136) Network Information has been updated.	Succeeded	172.16.2.145		2020/10/26 0	13:21:54 P	м	
1710	aries	Internal	Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192,168,105.2		2020/10/26 0	13:04:00 P	м	
3709	artes	Internal	Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192.168.105.2		2020/10/26 0	12-03-33 P		

ltem	Description				
ACS System Log / System Log / Login Log / Access Control Log	Click one of the types to display log of ACS System, System and Login.				
Search ID / Username / Login IP / Overview	Specify the conditions (type the ID number, username, the IP address or overview) for log searching.				
Time Setting	2021/01/26 to 2021/02/25 > search ID / Username / Login IP Q Time Last 30 Days > Cancel Q Search				
ACS System Log	Display the ID, username, login IP, category, overview, severity and time for clients accessing into VigorACS. Select buttons to filter Severity / Category / Result - Click the one of the buttons (Critical, Major, Minor, Warning, Normal, Maintenance and so on). The log related to the selected type will be displayed on the screen.				
System Log	Display the ID number, model name with MAC address for the CPE, and the action executed in CPE. Export All - Log information can be exported as a file.				
Login Log	Display the log information, including status, username, login IP, login time and logout time for clients accessing into VigorACS. Export All - Log information can be exported as a file.				
Access Control Log	Display the log information, including ID, Source IP, Service Type, Access Control Policy, Overview and Time for clients based on ACL profile applied. Export All - Log information can be exported as a file.				

6.5.13 XMPP Profile

This page is used for configure settings for XMPP (Extensible Messaging and Presence Protocol) server. It is only available for VigorACS, Cluster version.

System / XMPP Profile			С
Status	Disconnected		
Enable	\bigcirc		
Server IP Address	IPv4 format (EX : 123.12.1.1)		
Server Port	5222		
Username	admin		
Password	•••••	Φ.	
			_
		Sav	8

ltem	Description
Status	Displays current status (Disconnected/Connected) of the XMPP server.
Enable	Switch the toggle to enable/disable the XMPP server. VigorACS will try to connect to the XMPP server. If failed, a button of Connect to XMPP Server will appear. Click the button to reconnect.
Server IP Address	Enter the IP address of the XMPP server.
Server Port	Enter a port number for the XMPP server.
Username	Enter a string as username for accessing the sever.
Password	Enter a string as password for accessing the server.
Save	Save the settings.

6.5.14 Delete Logs Actions

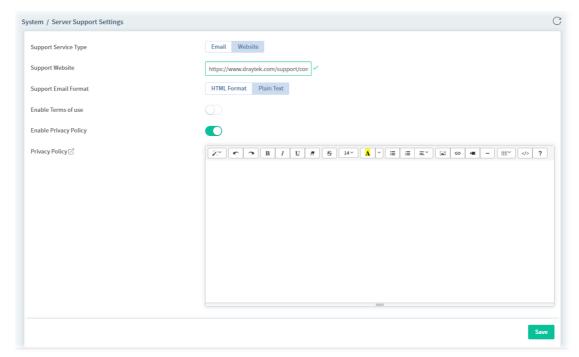
Information displayed here shall be deleted.

① Delete Logs Actions is available only for the **Root** user and the user with the role of **Auditor**.

n / Delete Logs Actions agary filters ACX Users Vilger Devices Network Clients	2021,012/610 2021,027/5 ->>> search 10 / operator / keyw	vord c
	и с 11 з и	e
: T Category : T Log Table : T Operator : F Authentication: Login IP : T Deseted Object	27 Overview 27 Time	
No e	La evolution	

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

6.5.15 Server Support Settings



This page is used for configuring the settings of Terms of use and Privacy Policy on the Login page.

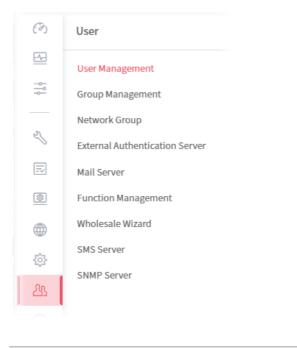
These parameters are explained as follows:

ltem	Description
Support Service Type	Specify the type of link that appears in the account activation notification letter.
	• Email - The system will direct the user to write an e-mail after the user presses the link of Contact Us.
	• Website - The system will direct the user to a website after the user presses the link of Contact Us.
Support Website	If Website is selected as the service type, enter the URL of the server website in this field.
Support Email Address	If Email is selected as the service type, enter the email address of the receiver in this field.
Support Email Format	If Email is selected as the service type, select the email format.
ronnat	HTML Format - The content of the email will be shown in HTML format.Plain Text - The content of the email will be shown in plain text.
Enable Terms of use	Switch the toggle to enable/disable the terms of use display. Terms of use - Enter the content.
Enable Privacy Policy	Switch the toggle to enable/disable the privacy policy display.
	Privacy Policy - Enter the content.
Save	Save the settings.

6.6 User

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

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



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

6.6.1 User Management

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

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

Add	R beind Ø User	Batch Settings					Search		1
owin	g 1 to 10 of 144 entries					Show 10 - entries 4	2 3 4	5 - 1	в
	Username	47 Authentication	27 Bole	47 Status	41 Mail Notify	47 SMS Notify	47	Email	
	root	Internal	System Administrator	(antivo)	0	0			
9	op	internal	Operator	CED	0	0			
9	uttester	Internal	System Administrator	Active	0	0			
ġ.	ap_sa	Internal	System Administrator	Active	0	0			
i i	ap_admin	Internal	Administrator	Active	0	6			
5	ap, gadmin	Internal	Group Administrator	(Active)	0	0			
0	ap_vop	Internal	View Only Operator	Active	0	0			
	dni	Internal	View Only Operator	Active	0	6			
	livedemo	Internal	System Administrator	Activo	0	0			
0	Alex	Internal	Group Administrator	(Aller)	0	0			

These parameters are explained as follows:

ltem	Description				
+Add	Click to add a user.				
Delete	Click to remove the selected user.				
User Batch Setting	Click to configure user batch settings (for Out-of-box experience).				
	User Batch Settings ×				
	Apply to Users operator (Internal)				
	Enable OOBE feature 🛛				
	OOBE pages to display Read the Agreements ~				
	Disable Auto Logout				
	Cancel Apply				
	Apply to Users - Select the user type (root, admin, operator) to apply the batch settings.				
	Enable OOBE feature - Switch the toggle to enable/disable the function. If enabled, the user will be guided to OOBE pages to modify settings (e.g., password, e-mail, notification, etc) for the next time to login VigorACS.				
	OOBE pages to display - Select the pages to display on the screen.				
	Disable Auto Logout - Switch the toggle to enable/disable the function. If disabled, the user has to logout the screen manually.				

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

i ser / User Management		C
Add User Profile		
Enable		
Username	carrient 🗸	
Password	e entre entr	
Role	System Administrator 🗸 🗸	
Enable WUI Login Enable API Service		
Enable API Service		
Email Notify		
Email	carrie_ntg/draytek.com	
SMS Notify		
Telephone	carrie_ni 🗸	
Description	test only	

ltem	Description			
Enable	Click to enable the user profile.			
Username	Enter a name for the new user.			
Password	Enter the password for the user.			
Role	Choose the role for the selected user . Different role represents different authority that the user group will have. The great the authority is, the more functions the user can have.			
	Operator ~			
	System Administrator			
	Group Administrator			
	Administrator			
	Commissioning			
	Operator			
	View Only Operator			
	Auditor			
	• System Administrator – Have the highest authority.			
	 Group Administrator – Have the middle authority high than "Administrator". 			
	• Administrator – Have the middle authority.			
	 Commissioning - Have the authority to add a new network and view SD-WAN settings. 			
	• Operator – Have the low authority higher than View Only Operator.			
	• View Only Operator – Have the lowest authority.			
	 Auditor - Have limited authority different from other roles. It is available for choosing only when the system administrator accesses into VigorACS with the role of Root (default account). The only action allowed is to view the deleted log information (on the page of System>>Delete Logs Action). 			

Enable Auto Logout	Switch the toggle to enable / disable the function. If disabled, the user must logout VigorACS manually.	
Enable OOBE feature Switch the toggle to enable / disable the function. When it is enabled, the user is allowed to access into the web uninterface of VigorACS and allowed to view the OOBE page(s). OOBE pages to display. If the OOBE feature is analysis of the cooperation of the cooperation of the cooperation of the cooperation.		
	OOBE pages to display - If the OOBE feature is enabled, select the page(s) to display on the screen.	
Email Notify	Click to enable/disable the function. When it is enabled, an email will be sent to the user as a notification when the connected device gets alarms. Email - Enter the email for communication between the user and VigorACS server.	
SMS Notify	Click to enable/disable the function. When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms. Telephone - Enter the telephone number for receiving the SMS notification.	
Description	Enter a brief description for the user.	
Cancel	Discard current modification.	
Create	Save the current settings and exit the page.	

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

6.6.2 Group Management

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

6.6.2.1 Setting

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

Setting	Management							
	Mining Stepart Stateless						Search	Q
	Group Name	🖓 - Max Nodes	IT Used Nodes	17 Enable Expire Date	27 Expire Date	47 Enable Global Mail Server	17 Enable Global SNMP Server	-
۵	RootGroup	No Limit Nodes	61.5	Chuhlet		(*****	Contraction	
	ap_profile_1	No Limit Nodes	1	(1111)		(Classifier)	(Citability)	
	one user account group	No Limit Nodes	0	CHANNEL		(Titalian)	(1111)	
	henry group	No Limit Nodes	5	Disabled		Enabled	(Enabled)	
	161	No Limit Nodes	1	Disabled		Disabled	(Disabled)	
	brinet	No Limit Nodes	0	(Disabled)		(Disabled)	(Disabled)	
	ScanAccess	No Limit Nodes	0	CHINNE		(Dissilied)	(Disabled)	
	attel	No Limit Nodes	3	Disabled		Disabled	Disabled	
	OptiVisus	No Limit Nodes	3.5	Disabled		Disabled	Obabled	
	network	No Limit Nodes	3	Disabled		Disabled	Disabled	
	Antipode	No Limit Nodes	0	Disabled		Ohabled	Obabled	
	Novanet	No Limit Nodes	0	Disabled		Ohabled	Dhabled	
	acsolutions	No Limit Nodes	0	Dhabled		Ohabled	Dhabled	
	easynet	No Limit Nodes	0	Dhabled		Disabled	Dhabled	
	dvcom_kuwait	No Limit Nodes	12	Disabled		Disabled	Disabled	
	insolutions	No Limit Nodes	0	Ditabled		Ditabled	Chabled	
	Shanghai	No Limit Nodes	14.5	Disabled		Dhabled	Obubled	

These parameters are explained as follows:

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

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

User / Group Management		С
Setting Management		
Add Group		
Group name	Marketing 🗸	
Nodes	-1	
Enable CPE Notify Mail/SMS/SNMP		
Enable Global Mail Server		
Enable Global SNMP Server		
Enable Expire Date		
Expire Date	2020/03/05	
	< Mar v 2020 v >	
	Su Mo Tu We Th Fr Sa	Cancel Save
	1 2 3 4 5 6 7	
	8 9 10 11 12 13 14	
	15 16 17 18 19 20 21	
	22 23 24 25 26 27 28	
	29 30 31	

These parameters are explained as follows:

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

6.6.2.2 Management

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

User / Group Ma	anagement		
Setting M	anagement		
User Group :	RootGroup ~		
Users	Available Group RootGroup rd8	nin O operator O aries O standard O henry O carrie O carrieni O	
	SDWAN Marketing		

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

6.6.3 Network Group

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

me	User Group	
Root Network(68)	RootGroup	Ŧ
▷ ③ @#\$%^&*_+{}":?> -+(0)</td <td>(As Parent)</td> <td></td>	(As Parent)	
Marketing_carrie(0)	(As Parent)	
◊ SD-WAN(2)	SDWAN	
S aaaaaa(123)(0)	(As Parent)	· · ·
◊ rd7(2)	(As Parent)	- -
◊ rd8(41)	rd8	•
◊ rd8-2(1)	(As Parent)	
 ◊ rd8-3(0) 	(As Parent) (As Parent)	*
◊ Simulator(12)	(AS Parent) SDWAN	*

These parameters are explained as follows:

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

6.6.4 External Authentication Server

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

Jser Group : All User Group ~				
Enable				
Choose User Role at Registration	View Only Operator \checkmark			
Server IP Address	172.16.1.86			
Authentication Server Type	Active Directory / LDAP ~			
Destination Port	389			
Use SSL	\bigcirc			
Note: For security consideration, it authentication server is on the Bind Type	t is strongly recommended to use LDAP or TACAC he Internet. Simple Mode Anonymous Regul			
Regular DN				
Regular Password		٢		
+ Add				Profile Number Limit: 1/5
	n Name Base Distinguished Name	Additional Filter	Group Distinguished Name	Profile Number Limit: 1/5
+ Add	1 Name Base Distinguished Name	Additional Filter	Group Distinguished Name	

ltem	Description		
User Group	Select a group to configure authentication settings.		
Enable	Click to enable this function.		
Choose User Role at Registration	The default setting for the role of the LDAP user is Operator. Usually, the role of the LDAP user can be changed by the System Administrator after it is registered to VigorACS. This option can specify/change the role of the LDAP user as Administrator, Operator or View Only Operator previously before registration to VigorACS. Administrator Operator View Only Operator		
Server IP Address	Enter the IP address of LDAP server.		
Destination Port	Enter a port number as the destination port for LDAP server.		
Authentication Server Type	 Enter a port number as the destination port for LDAP server. Active Directory / LDAP - Use SSL - Enable it to use the port number specified for SSL. Bind Type - There are three types of bind type supported: Simple Mode - Just simply do the bind authentication without any search action. Anonymous - Perform a search action first with Anonymous account then do the bind authentication. Regular Mode- Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the Regular DN and Regular Password. 		

	 Regular DN –Type this setting if Regular Mode is selected as Bind Type.
	 Regular Password - Specify a password if Regular Mode is selected as Bind Type.
	RADIUS –
	 Shared Secret – The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.
	• Confirm Shared Secret - Re-type the Shared Secret for confirmation.
	TACACS+ –
	• Authentication Protocol – Select PAP or CHAP.
	• Shared Secret - Enter the Shared Secret for confirmation.
	• Confirmed Shared Secret - Re-enter the Shared Secret for confirmation.
+Add	Click to create a profile related to LDAP.
Save	Save the current settings and exit the page.

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

User / External Authentication Server			С
User Group : All User Group v			
Profile Name	LD_1 ~		
Common Name Identifier			
Base Distinguished Name			
Additional Filter			
Note: Please type in your additional filter for 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)	BaseDN search request. For exmaple,		
Group Distinguished Name			
		Cancel	Save

These parameters are explained as follows:

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

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

Add						Profile Number Limit: 2
ld	Profile Name	Common Name	Base Distinguished Name	Additional Filter	Group Distinguished Name	Action
	Idap	uid	ou=People,dc=ms,dc=draytek,dc=com			Delete
2	LD_1	UID	MARKET		GROUP	Delete

6.6.5 Mail Server

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

r / Mail Server er Group : All_UserGroup ~		
17 Send Test Email		
Enable Server		
Security	None 🗢	
Host	172.16.2.8	
Port	25	
Authentication		
Username	carrie_ni	
Password	••••••	
From email	carrileijidrayteik.com	
Subject	Alarm Lavei 💿	
Alarm Level	Critical 🗌 Major	
	Minor Warning	
	Normal	
) Reset To Default		

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

Reset To Default

6.6.6 Function Management

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

User / Function Mana	gement						(
Role	Show Unknown Device	Wireless Is Writable	Show About Menu	Show Version Number	Show Maps	Can Delete Logs	
System Administrator							
Group Administrator							
Administrator							
Commissioning							
Operator	\bigcirc						
View Only Operator		\bigcirc					
Auditor		\bigcirc					
						s	Save

Item	Description
Show Unknown Device	Unknown device can be seen / hidden if it is enabled / disabled.
Wireless is Writable	When it is enabled, settings related to wireless connection are allowed to be configured.
Show About Menu	The About menu with information of VigorACS can be seen if it is enabled for the role.
Show Version Number	The version number can be displayed/hidden separately for various roles of users. Switch this toggle to display (enable) or hide (disable) the version number. By default, the version number of VigorACS will be shown for System
	Administrator and displayed on the page of About VigorACS.
Show Maps	Google Maps/ Leaflet Maps can be displayed/hidden for various role of user accounts.Switch this toggle to display (enable) or hide (disable) the version number.
Can Delete Logs	If enabled, logs can be deleted by the user with the role of System Administrator, Group Administrator and Administrator.

6.6.7 Wholesale Wizard

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

1. Open User >> Wholesale Wizard.

User / Wholesale Wizard				
1 Create user	2 Create user group	3 Create network	4 Summary	5 Finished
Step 1- Create user				
Username *	Carrie003			
Password *	••••	\odot		
	weak			
Telephone	5972727			
Email	carrie_ni@draytek.com			
Role	Group Administrator	~		
Enable OOBE feature 🔞				
OOBE pages to display	Read the Agreements, Set new password, Ve	rify		
Status	Active	~		
Mail Notify				
SMS Notify	\bigcirc			
				Next

These parameters are explained as follows:

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

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

r / Wholesale Wizard				
	0			
Create usar	Create user group	Courts mataeork	Summary	Finished
Step 2- Create user group				
Select group:	Existing group New group			
New group				
Group Name *	DrayTek_Marketing			
Nodes	-1			
Global Mail Server	(-1 - No Limit Nodes)			
Global Mail Server				
Enable Expire Date				
Expire Date	2021/11/03			
				Previous Hest
				Previous Next

These parameters are explained as follows:

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

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

Crasta Uner	Overall list group	3 Create network	O Sammary	O
Step 3- Create network				
Select.network:	Existing network New network			
New network				
Parent Network	Root Network	X.		
Network Name *	CARRIE003			
Username	cardtest			
Password				
Location	HsinChu			
				Previous

Item	Description	

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

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

ser / Wholesale Wizard				
Cristia user	Create sam group	Greate petwork	Summary	
Step 4-Summary				
User				
Usemame		Role		
Carrie003		Group Administrator		
Status		Mail Notity		
Active		Enable		
SMS Notify		Telephone		
Fnable		5972727		
Email		Description		
carrie_ni@draytek.com		First User		
User Group				
Group Name		Global Mail Server		
DrayTek_Marketing		Enable		
Nodes		Enable Expire Data		
-1		true		
Expire Date				
2021/11/03				
				Previous Next

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

User / Wholesale Wizard				
				5
Create user	Create user group	Create network	Summary	Finished
Step 5- Finished				
		 Completed 		
				Finish

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

6.6.8 SMS Server

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

r / SMS Server			
r Group : RootGroup ~			
Enable SMS Server			
SMS API	SMS_CHT_TW	×	
Username	Carrie003		
Password		•	
From Telephone	5972727		
Alarm Level	🗆 Critical 🖉 M	lor	
	🖸 Minor 🛃 W	rning	
	Normal		

ltem	Description
User Group	Specify a user group to apply the SMS server settings.
Enable SMS Server	Click to enable /disable the SMS server.
SMS API	Use the drop down list to choose an ISP for sending SMS.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
From Telephone	Type the phone number of the sender.
Alarm Level	There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS SMS server sends SMS to the recipient. For example, device loss connection will be treated as "Critical" event.
Save	Save the current settings.

6.6.9 SNMP Server

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

User Group: Enable SNMP server SNMP server address Port 0 Community Enable keep allve Community Enable keep allve Allve interval(sec) 0 SNMP API SNMP API Contical Minor Minor Minor Normali	Enable SMMP server SMMP server address Port 0 Community Enable Keep allve Allve Interval(see) 0 SMMP version version1 SMMP API Alarm Level	Iser / SNMP Server		
SkMP server address Image: Community Port 0 Community Image: Community Enable keep allwe Image: Community Allwe interval(sec) 0 SkMP version Version1 SkMP APF ShMP_2_CLOBAL Alarm Level Image: Community	SNMP server address Image: Community Port 0 Community Image: Community Enable keep allve Image: Community Allve interval(sec) 0 SNMP version version1 SNMP API SNMP 2_CLOBAL Allven Level Image: Community	User Group : RootGroup ~		
SkMP server address Image: Community Port 0 Community Image: Community Enable keep allwe Image: Community Allwe interval(sec) 0 SkMP version Version1 SkMP APF ShMP_2_CLOBAL Alarm Level Image: Community	SNMP server address Image: Community Port 0 Community Image: Community Enable keep allve Image: Community Allve interval(sec) 0 SNMP version version1 SNMP API SNMP 2_CLOBAL Allven Level Image: Community	Enable SNMP server		
Port 0 Community Enable keep allwe Enable keep allwe Enable keep allwe SNAP version Ve	Port 0 Community Enable keep allve Community Enable keep allve Co Allve interval(sec) 0 SNMP version Version SNMP API SNMP 2_CLOBAL C Alarm Level C Critical Minor C Marring			
Port 0 Community	Port 0 Community	SNMP server address		
Enable keep allve Enable keep allve Allve Interval(sec) G SNMP APt SNMP 2_CLOBAL C Alarm Level G Cntocal Major CManning	Enable keep altwe Enable keep altwe Altwe interviat(sec) SNMP version SNMP API SNMP_2_GLOBAL Atarm Level C Criticat Minor Marring	Port	0	
Enable keep allve Enable keep allve Allve Interval(sec) G SNMP APt SNMP 2_CLOBAL C Alarm Level G Cntocal Major CManning	Enable keep altwe Enable keep altwe Altwe interviat(sec) SNMP version SNMP API SNMP_2_GLOBAL Atarm Level C Criticat Minor Marring	Community		
Allve Interval(sec) SNMP version Version Version SNMP APt SNMP_2_CLOBAL Alarm Level Cntical Major Minor Warning	Allive Intervisi(sec) 6 SNMP version version1 SNMP API SNMP 2_CLOBAL Allivm Level Critical Minor Warning		1	
SNMP version version SNMP APF SNMP_2_GLOBAL Atarm Level Cntical Major Minor Warning	SNMP version version version version SNMP API Atarm Level Critical Minor Critical Minor	Enable keep allve		
SNMP APT SNMP_2_GLOBAL ~ Alarm Level Critical Major Minor I Warning	Atarm Level Critical Major	Allve Interval(sec)	0	
SNMP APT SNMP 2_CLOBAL ~ Atarm Level Critical Major Cliffical Warning	SINNP API SINNP 2_CLOBAL ~ Alarm Level Critical I Major I Minor U Warning	SNMP version	version1	
Z Minor	C Minor		SNMP_2_GLOBAL	~
Z Minor	C Minor	Alarm Level	Critical Maker	

ltem	Description
User Group	Specify a user group to apply the SNMP server settings.
Enable SNMP Server	Click to enable /disable the SNMP server.
SNMP server address	Enter the IP address of SNMP server.
Port	Enter the port number of SNMP server.
Community	Set the name for getting community by typing a proper character. In general, it depends on the setting that SNMP service provider offers. The default setting is public.
Enable keep alive	It is available when RootGroup is selected as User Group. Click to enable / disable keep alive function. VigorACS will notify SNMP server every period of time automatically to proof that it is still alive.
Alive interval (sec)	It is available when RootGroup is selected as User Group. Enter an interval value for keeping alive.
SNMP version	Choose the version of the SNMP server that you apply to.
SNMP API	Choose SNMP API from the drop down list.
Alarm Level	There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS mail server sends e-mail to the recipient. Specify the severity level of the mail.
Save	Save the current settings.

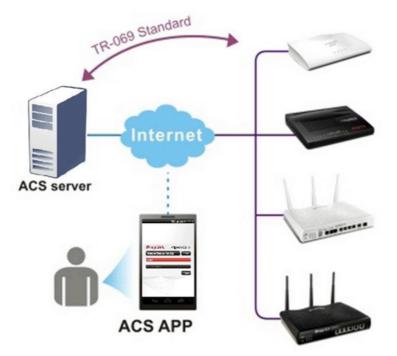
6.7 About VigorACS

(⁷)	About VigorACS Version Trunk AutoBuild 1856
	License Information
	License Mail Notify
Z	License Agreements
ζ <u>ζ</u> ζζε	
<u>4</u> 8	
()	

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

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

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



6.7.1 License Information

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

Used Nodes/Max Node	103.0 / 20000	
Expire Date	2025-03-01	
Start Date	2020-01-30	
License Type	Trial	
License ID	0002a93d	
Host ID	ACS3200100010	
License Information		Ø E

6.7.2 License Mail Notify

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

License Mail Notify		
Notify Mail Configuration		0 C
Enable		
Subject	[Get License Failed] ACS cannot get the license info from MyVigor	
Content	Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constraint of the license line Image: Constree Image: Constraint of the l	
Recipient	ttm_yang@draytek.com	lete
	mickey_chlu@draytek.com	lete
	+Add new recipient	
		Save

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

6.7.3 License Agreements

This page displays relational license information required by VigorACS 3.

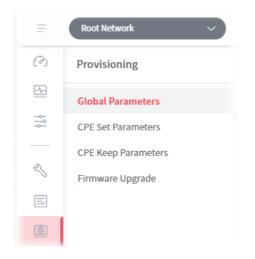
Apache License, Versio	on 2.0			MIT		
Name	Author	Web Site	Modified Source Code	Name	Author	Web Site
Ant		Ð		bootstrap		Ø
Apache POI		Ð		Chart.js		ø
Axis		Ø		CryptoJS	Jeff Mott.	Ø
Castor		Ø		DATE PICKER		Ð
Commons FileUpload		Ø		jcanvas		Ø
Dashboard	Google Inc.	Ø		JQuery		S
Eclipse Public License				LGPLv3		
Name	Autho	r	Web Site	Name	Author	Web Site
c3p0	Steve	Waldman	Ð	JasperReports		P
	Steve	Waldman	θ	JasperReports		θ
LGPLv2.1				JasperReports BSD 3-Clause		
LGPLv2.1 Name	Stere	Web Site	₽ Modified Source Code	JasperReports BSD 3-Clause Name	Author 1010 Securit	Web Site
LGPLv2.1				JasperReports BSD 3-Clause	Author Mike Bostock Mike Bostock	

Applications

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

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

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



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

Provisioning / Gl	obal Parameters		
User Group : Ro	otGroup	·	
Global Profile No	etwork & Devices		
Profile Edit Mode :	All Web UI View	XML File	Parameter List
+ Add 🕁 XM	L Template		
Profile Name			Profile Edit

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

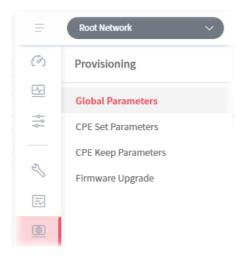
visioning / Global Parameters er Group: RootGroup ~	
Add a Profile	
Create Profile by	Creating a New Parameter List
Profile Name Always Keep	•
Reboot after Provisioning	
After applying the paramet Provisioning Time	ers, ACS will check the CPE responses and ask the CPE to reboot if needed. Now Scheduled Schedule Profile
Provisioning Lime	now schedules schedule Home Cancel Add
	Cancer Add

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

Profile Edit Mode:: All Web Ul Wew XML File Parameter List									
+ Add do XML Template									
Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action			
888888	Parameter List		No	3	2018/11/28 04:43:07 PM	🖉 Edit	Delete	С Сору То	@ View Log
angela test	Parameter List		No	1	2018/11/12 02:48:25 PM	d Edt	R Delete	С сору то	Q View Log
tt.	Parameter List		Yes	0	2018/11/08 02:38:05 PM	🖉 Edit	Il Delete	С Сору То	@ View Log
Global_parameter_Example_Parameter_List	Parameter List		No	0	2018/11/08 03:13:55 PM	d Edit	Delete	Сору То	Wew Log
66667	Parameter List		No	2	2019/05/31 08:47:36 AM	∂ Edit	🖹 Delete	Сі Сору То	@ View Log
Marketing	Parameter List		Yes	0	2020/11/03 02:18:29 PM	2 Edit	E Delete	Q Copy To	@ View Log

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

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



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

Global Profile Network & Devices								
Profile Edit Mode: All Web UI View XML File Parameter List								
+ Add 👃 XML Template								
Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action		
3888888	Parameter List		No	3	2018/11/28 04:43:07 PM	🖉 Edit 🗊 Delet	е 🗅 Сору То	🖨 View Log
angela test	Parameter List		No	1	2018/11/12 02:48:25 PM	🖉 Edit 🛛 🖄 Delet	е 🗘 Сору То	🖨 View Log
t	Parameter List		Yes	0	2018/11/08 02:38:05 PM	🖉 Edit 🗇 Delet	е 🗘 Сору То	🕯 View Log
Global_parameter_Example_Parameter_LIst	Parameter List		No	0	2018/11/08 03:13:55 PM	🖉 Edit 볩 Delet	е 🗅 Сору То	🖨 View Log
56667	Parameter List		No	2	2019/05/31 08:47:36 AM	🖉 Edit 🔞 Delet	е 🗘 Сору То	🗟 View Log
Marketing	Parameter List		Yes	0	2020/11/03 02:18:29 PM	🖉 Edit 🗎 Delet	е 🗘 Сору То	🖨 View Log

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

Provisioning	🖹 Profile Name: Marketing	
		+ Add ← Edit □ Copy □ Delete □ Parameter

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

Parameter	Value	Keep	Order	Applied Model	Source Mode
		×	0	All models	~

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

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

1. Open Network Management.



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

Network Management			
Search by Device IO/Name/Model/MAC/IP Address	C Setting Map		
 Root Network(277) ALANWEN(3) 	+Add New Network		
 Alvaco(1) AnPhat_VN(8) 	General Settings		
D at Angela(5)	Network ID	Username	
ArtesTest(0)	2	acs	
CARRIE(0)	Name	Password	
CARRIE003(0)	Root Network		0
b	Location		
b DraytekChina(0)	Koldingweg 19-1, Groningen, Nederland		
D AFFAE(3)			
b ct. GetterNetwork(1)			Save
p IKI(1)			
b A Marketing_carrie(0)			
b 🚓 Novanet(0)			
octobep(1)			

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

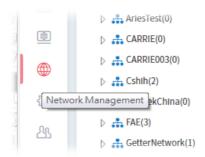
Parent Network	
Root Network	
Name	
Marketing_carrie	
Location	
HS	
User Name	
carrie	
Password	
	✓ @

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

twork Management	
Search by Device ID/Name/Model/MAC/IP Addre	Setting Map
Root Network(240)	+Add New Network
▷ 📥 1111(0)	General Settings
ALANWEN(3)	General Settings
Alvaco(0)	Network ID
Marketing_carrie(0)	2

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

1. Open Network Management.



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

Network Management	
Search by Device ID/Name/Model/MAC/IP Address	C Setting Map
 2865Lax 1449BC0C5920 2865ac_001DAA000000 	Delete This Device 🤹 Change Network
@ 2865aC_001DAA41DF18	General Settings
2865ac_001DAA41DF78	o the second sec
2866ac_001DAA41DFC0	Status Disable Enable
2912n_001DAA8E14B0	
2922n_001DAA8CAC84	Device ID 141436
2925Ln_001DAADD75B0	
2925ac_001DAA512820	Model Name Vigor2865ac
2926Vac_001DAA5DCAD0	
2927Lac_1449BC023720	Note 1
2927Lac_1449BC023740	
2927Lac_1449BC023768	Serial number
► Ø 2027 1///0PC092020/11	

3. Click Change Network.

search by Device ID/Name/Model/MAC/IP Address	C' Setting Map
2865Lax_1449BC0C5920	
2865ac_001DAA000000	a Delete His Divice and onon-be received
2865ac_001DAA41DF18	General Settings
2865ac_001DAA41DF78	General Settings
2866ac_001DAA41DFC0	Status Disable Enable
2912n_001DAA8E14B0	
2922n_001DAA8CAC84	Device ID 141436
2925Ln_001DAADD75B0	
2925ac_001DAA512820	Model Name Vigor2865ac
2926Vac_001DAA5DCAD0	
2927Lac_1449BC023720	Note 1
2927Lac_1449BC023740	
2927Lac 1449BC023768	Serial number

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

Name	
2865ac_001DAA000000	
dd to network	
	0
	Q
🔺 👬 Root Network	
ALANWEN	
Alvaco	
AnPhat_VN	
Angela	
ArlesTest	
🚓 CARRIE	
CARRIE003	
击 Cshih	
击 DraytekChina	
👬 FAE	
GetterNetwork	
IK1	
👬 Marketing_carrie	
🚓 Novanet	
A OCTOBER	
👬 RD1	
👬 RD2	
RD3	
• 005	
	× Cancel + Apply

De	100% All operations have been completed. The status of each device is as follows.									
	\bigcirc	 Suc 	ceed: 1		Proce	ssing	:0 (Walting: 0	Failed: 0	
Ge	Device Name	J↑	Model	$\downarrow \uparrow$	Retry	$\downarrow \uparrow$	Progre	ss Status		$\downarrow \uparrow$
Sta	2865ac_001DAA0	00000	Vigor286	5ac	0		8 1009		offline. Settings will I when device is online	
Den 14					— HI	de De	etails			
Mo	ALL ARD SHE				×	Clos	e			

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

earch by Device ID/Name/Model/MAC/IP Address	C Setting Map	
🚓 Root Network(277)	[⊕] Delete This Device	
ALANWEN(3)		
Alvaco(1)	General Settings	
AnPhat_VN(8)		
Angela(5)	Status DIsable Enable	
ArlesTest(0)		
CARRIE(1)	Device ID 141436	
2865ac_001DAA000000		
 	Model Name Vigor2865ac	
Cshih(2)	Note 1	
DraytekChina(0)		
FAE(3)	Serial number	

A.5 How to Add a User?

- 1. Open User>>User Management.
 - ✓
 User

 ✓
 User Management

 ✓
 Group Management

 ✓
 Ketwork Group

 ✓
 External Authentication Server

 ✓
 Function Management

 ✓
 Function Management

 ✓
 SMS Server

 ✓
 SMS Server

 ✓
 SMM Server
- 2. Click **+Add**.

Root N	letwork	~	DrayTek	VigorACS 3		🖬 Capture Packets -	System Admin	ininž
Jser /	User Management							
+Add	1 bea						Search	
Showin	g 1 to 10 of 145 entries					Show 10 ~ entries 44	2 2 4 3	\$
	Usemame	47 Authentication	21 Role	47 Status	17 Mail Notify	却 SMS Notity	47 B	mai
	root	Internal	System Administrator		0	0		
	ор	Internal	Operator	Cethe	0	0		

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

User / User Management			C
Add User Profile			
Enable			
Username	CNIIII 🗸		
Password			
Rote	Operator		
Email Notify			
Email	carrie_nigsdraytek.com 🗸		
SMS Notify			
Telephone	035972727		
Description	Router owner		
			_
		Cancel	Create

4. Click Create.

ser /	User Management	i.										0
+Add											Snarch	0,
howing	g 141 to 146 of 146 er	ntries								Show 10 - entries + 1	- н н н и	15 19
	Username	- it	Authentication	38	Role	11	Status	41 Mail Notify	41 SMS Notify	47 Email		47
٥	Sales_003		Internal		Group Administrator		(Killin)	(TITLES)	(2000)	carrie_ni@draytek.co	m	
0	adam_to		Internal		System Administrator		600	0	0			
	Link_345		Internal		System Administrator		(111)	0	0			
	david		Internal		System Administrator		Actim	0	0			
D.	Carrie003		Internal		Group Administrator		Cether	(millio)	(77177)	carrie_nt@draytek.co	m	
	CNIII		Internal		Operator		(100	(111117)	0	carrie_ni@draytek.co	m	

A.6 How to Add a Group?

1. Open User>>Group Management.

(7)	User
<u></u>	User Management
	Group Management
	Network Group
Z	External Authentication Server
	Mail Server
8	Function Management
	Wholesale Wizard
\$ <u>`</u>	SMS Server
23	SNMP Server
(1)	

2. Click +Add.

User / Group	Management				
Setting	Management				
+Add 💷	elete 🗳 Export 🗟 Delete with whole				
	Group Name	Max Nodes 41	Used Nodes $\downarrow\uparrow$	Enable Expire Date	↓↑ Expire Date
	RootGroup	No Limit Nodes	61.5	Disabled	
	ap_profile_1	No Limit Nodes	1	Disabled	
	one user account group	No Limit Nodes	0	Disabled	

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

etting Management		
dd Group		
iroup name	yfnts 🖉	
iodes	-4	
Enable CPE Notify Mail/SMS/SNMP		
nable Global Mall Server		
nable Global SNMP Server		
nable Expire Date		
Expire Date	2020/11/06	

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

4. Click Save.

ietting	Management							
dd	linites expert States a						Search	
	Group Name	17 Max Nodes	i† Used Nodes	47 Enable Expire Date	47 Expire Date	17 Enable Global Mail Server	17 Enable Global SNMP Server	
	RootGroup	No Limit Nodes	61.5	Disabled		Ensisted	Enabled	
ि	ap_profile_1	No Limit Nodes	1	(Disabled)		(Disabled)	(Disabled)	
0	one user account group	No Limit Nodes	0	(Disabled)		(Disabled)	Chabled	
	henry group	No Limit Nodes	5	Olicabled		Enabled	Enabled	
	ytnts	No Limit Nodes	0	(22)	2020/11/06	(listing)	(2000)	

This page is left blank.



Network Menu



Chapter 7 Root Network Menu

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

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

Root Network(267)		
	Model	
옮 RD3(14)	>	
ぷ, RDS(9)	>	
85 RD6(3)		
品 RD7(15)		
25 RD8(58)		
옲 R06-1(1)		

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

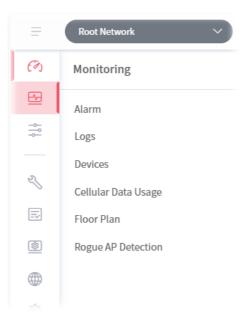


7.1 Dashboard for the Root Network

Root Network	~		Dray Tek	VigorACS 3				E4 Captu	ire Packel	ts ~	System	ca n Administra	tor C
Dashboard									A	luto Refr	esh: 1	Minute	c c
Map Overview			×	Network Overvie	2W								- 2
,地圖 衛星檢	我 Aduard Pi	etwerderslesje Zuidw ddepoel	Layerrey	Sub Network 58 © Root Network	Online 7	Alari 26						۹	Network
周間間 周間偏	Slaperstil	Bei	jum Garmerwold						A	larm			
Zuiderburen	Hoogemeeden	DE HOOSTE	Lewenborg	Network Members		Online	offline	Total	WAN	VPN	LAN	Go To Das	hboard
×	Den Horn	Paddepoel		© directly-under-Ro	ot Network	0	61	61	0	0	0		
iast	Lanemasten	格羅寧根 Groningen	0	Ø ALANWEN		0	3	3	0	0	0	8	
Enumatil	HOOGHENN	3	Oude	Ø Alvaco		0	1	1	0	0	0	8	
	De Poffert		Roodehaan	Ø AnPhat_VN		0	8	8	0	0	0	8	
	Matsloot	Helpman	Essen	Ø Angela		0	5	5	0	0	0	P	
Lettelbert			Groningen Wäterhuiz	Ø AriesTest		0	0	0	0	0	0	8	
Midwolde 84		Eelderwolde Nijveensterkolk	+	© CARRIE		0	0	0	0	0	0	B	
	Sandebuur Roderwolde		Rith Haren Oosterhaar - C	© Cshih		0	2	2	0	0	0	8	
Capelo	Deixenunte	地國資料 02020 GeoBasis-DE/BKG											
Active Clients- Top	20		🛛 Last 24 hours 🚽 🎤 🗙	Traffic- Top 20							©ц	ast 24 hours	- 2
Total				Total									
8	100 %	RD2/8	100%	7.19 GB	¹ 194.71 MB			RD2 / 7.	.19 GB † 19	94.71 MB	7.00 GB		100%
10	O Total	ALANWEN / 0	0%	2.79 GB 2.33 GB		O Tota	н	ALANW	EN / 0 Byte	e † 0 Byte	0 Byte		0%
8	1	Alvaco / 0	0%	1.86 GB					(0 B-4+ ⁺)		0.44		0%
0		Alvaco / 0	0%	1.40 GB				#eVaco /	o byse i i	0 Byte 0	byve		0%
4	L TRA AIN	AnDhut VM / A	066	953.67 MB				AnDhat	MI/ORM	to 1 A Rule	0 Ruta		006

7.2 Monitoring

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



7.2.1 Alarm

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

Netv	vork	~		Dray Tek	VigorACS 3		Captur	e Packets ~ System Administrator
oring	g / Alarm						2020/02/08 to 202	0/03/09 V search No. / Device Name / N
arm(65 Histo	ry.						
Delet	te 🗍 Del	iete All 🚽 Downl	beo					N < 1 /4 > N C €
	No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type
	27358	Not Ack	2020/03/09 09:56:05 AM	P1280_001DAA000055	001DAA000055	A Critical	Device Loss Connection	Device Lost Connection
	27357	Not Ack	2020/03/09 09:56:05 AM	G2280x_001DAA43AB4B	001DAA43AB4B	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27356	Not Ack	2020/03/09 09:55:54 AM	2927Lac_1449BC023768	1449BC023768	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27355	Not Ack	2020/03/09 09:55:50 AM	2960_001DAABABBC8	001DAABABBC8	A Critical	Device Loss Connection	Device Lost Connection
	27354	Not Ack	2020/03/09 09:55:50 AM	2912n_001DAA8E1430	001DAA8E1480	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27353	Not Ack	2020/03/09 09:55:50 AM	2925Ln_001DAADD75B0	001DAADD75B0	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27352	Not Ack	2020/03/09 09:55:42 AM	2862Vac_001DAAED3840	001DAAED3840	🛆 Critical	Device Loss Connection	Device Lost Connection
	27351	Not Ack	2020/03/09 09:55:38 AM	AP 1000C_001DAA575D38	001DAA575D38	▲ Critical	Device Loss Connection	Device Lost Connection
	27350	Not Ack	2020/03/09 09:55:36 AM	2952Pn_001DAAF8D818	001DAAF8D818	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27349	Not Ack	2020/03/09 09:55:30 AM	2925ac_001DAA512820	001DAA512820	🛆 Critical	Device Loss Connection	Device Lost Connection
	27348	Not Ack	2020/03/09 09:55:27 AM	3220n_001DAA554758	001DAA554758	🛆 Critical	Device Loss Connection	Device Lost Connection
	27347	Not Ack	2020/03/09 09:55:25 AM	AP 912C_001DAA72E14A	001DAA72E14A	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27346	Not Ack	2020/03/09 09:55:17 AM	3910_001DAA2125B8	001DAA2125B8	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27345	Not Ack	2020/03/09 09:55:17 AM	2926LVac_1449BCFFF9A8	1449BCFFF9A8	\Lambda Critical	Device Loss Connection	Device Lost Connection
	27344	Not Ack	2020/03/09 09:55:17 AM	AP 1000C_001DAA04F084	001DAA04F084	\Lambda Critical	Device Loss Connection	Device Lost Connection

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

7.2.2 Logs

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

ot Netv	vork	~		Dray Te	k VigorACS 3		🖬 Cap	ture Packets Y System Administrator
itoring	g / Logs						2020/02/08 to 2	search ID / Device Name / De
CPE Ac	tions De	vice Reboot Reboot By CPE Res	et System Password Set Pa	arameter File Transfer S	etting Profile Device SysLog	CPE Notify Device Register	Device Operate	
Delet	te 🗎 De	lete All 🚽 Download						N < 1 /12 > D C 8
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
0	4248	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2287	2020/03/09 09:53:57 AM
	4247	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2286	2020/03/09 09:53:55 AM
	4246	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2285	2020/03/09 09:53:41 AM
	4245	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2284	2020/03/09 09:53:39 AM
	4244	2865ac_001DAA000000	4339	001DAA000000	172.16.3.134	Inform		2020/03/09 09:41:04 AM
	4243	2926Vac_001DAA7033E0	129	001DAA7033E0	172.16.3.136	Inform		2020/03/09 09:39:49 AM
	4242	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Set Parameter Values	2283	2020/03/06 02:57:58 PM
	4241	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:57:43 PM
	4240	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:57:42 PM
	4239	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Set Parameter Values	2282	2020/03/06 02:47:23 PM
	4238	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:46:48 PM
	4237	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:46:48 PM
	4236	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:41:43 PM
	4235	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:41:42 PM

These	parameters	are	explained	as	follows:

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

7.2.3 Devices

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

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

onitoring / Devices											
search Device Name / II	P / MAC	Model Vig	or2865Lac, Vigı ~	Status	All	~	SSID All	~ Rows 1	0 ~ 14 <	1 /1 → ▷ 0	, ©
Download									General	Wireless	
		MAC Address	Model ↓↑	Network $\downarrow \uparrow$	Status	Up Time ↓↑	F/W Version ↓↑	Last Inform Time 🛛 🖓	Current Client 🛛 🖓	Current Traffic	
Device $\downarrow\uparrow$	IP Address ↓↑	MAC Address									
Device ↓↑ 865Lac_1449BC0D8F00	IP Address 41 192.168.105.120:443		Vigor2865Lac	MKT_manual	online	1d:23h:34m:1s	4.3.1_RC1_STD 🥝	2021/02/26 07:03:28 AM	0 (Local Wireless: 0)	536.88 KB (↑ 169.86 KB ↓	367.01
		1449BC0D8F00		MKT_manual MKT_manual			4.3.1_RC1_STD ⊘ 4.2.3 ⊘	2021/02/26 07:03:28 AM 2021/02/25 02:57:37 AM		536.88 KB (↑ 169.86 KB ↓ 0 Byte (↑ 0 Byte ↓ 0 Byte)	367.01

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

7.2.4 Cellular Data Usage

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

Monitoring / Cellular	Data Usage									Ģ
LTE Data Usage Ove	erview				Quota Settings					
Data Used O Byte	Data Cycle 11/02 - 11/08	Status: NOR	MAL	0% of 1500MB	Data Usage Alarm					
1 liyte	11/02 11/00			O Total	Data Quota	1500	M8 ~			
					Trigger Alarm When Usage Reached	51	% of Quota (765.00 MB)			
					Alarm Serverity Level	Critical		v		
		0			Data Usage Cycle	Weekly	Monthly Custom			
0 Byte		0	11-03		Weekly Reset Day	Monday		· •		
Device		Total	Download	Upload						
2866L_1449BC02F990	5	0 Byte								_
2927LVac_14498C02F	948	0 Byte							Cancel	Save
2865Lax_14498C0C59	920	0 Byte								_
2862Ln_001DAA625D	E0	0 Byte								
2925L_001DAA5B0D9	8	0 Byte								
2860Ln_001DAA5B1C	EO	0 Byte								

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

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

7.2.5 Floor Plan

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

enitoring / Floor Plan Add Profile Name k Devices bedroom 2	40 Action
ofile Name 🕴 Devices	4t Action
rofile Name 4 Devices	3t Action
droom 2	
	🖉 Edit 🛛 🛱 Delete
0	🖉 Edit 🖀 Delete
0	🖉 Edit 🛛 🛱 Delete

ltem	Description
+Add	Creates a new profile.
88	Click to change to browse view. It displays all of the floor plan profiles with the map used.
	Monitoring / Floor Plan
	bedroom 0 jog 0 tte 0
	QAdd
	и к 🖬 и х м
	You can click Add on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click Edit Map & Plan to perform the modification, or click Delete Map Profile to remove the selected floor plan profile.

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

To create a new profile:

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

Root Network 🗸 🗸		Dray Tek VigorACS 3
Monitoring / Floor Plan		
Profile Name	marketing_carrie	
Upload Map	Floor_MAP.png	Browse
		Cancel

3. Click **Edit** to display the following figure.

loot Network 🗸 🗸	Dray Tek VigorACS 3	Capture Packets 👻	carrie System Administrator
onitoring / Floor Plan			
Profile Name	marketing_carrie		
Edit Dimension + Add Device			
			•
			Cancel Save

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

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

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

itoring / Floor Plan			
ofile Name	marketing_carrie		
Edit Dimension + Add Dev	vice		
and drop a virtual AP or an ur	n-assigned AP to the floor plan.		
		Un-assigned APs	٢
		Device Name	Model
		A 810_001DAA7D6514	VigorAP
		▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084	VigorAP VigorAP
		A 810_001DAA7D6514	VigorAP VigorAP VigorAP
		▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38	VigorAP VigorAP VigorAP VigorAP
		▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7	VigorAP VigorAP VigorAP VigorAP VigorAP
		▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7 ▲ AP 800_001DAA2A5870	VigorAP VigorAP

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

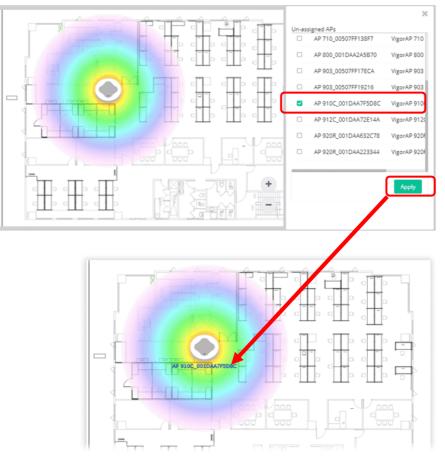
		Capture Packets System Admi	
nitoring / Floor Plan			
Profile Name	marketing_carrie		
Edit Dimension + Add D	evice		
ig and drop a virtual AP or an i	un-assigned AP to the floor plan.		
		Un-essigned APs Device Name A 810_001DAA7D6514	Model VigorAP 8
		AP 1000C_001DAA04F084	VigorAP 1 VigorAP 1
		AP 710_00507FF138F7	VigorAP 7 VigorAP 8
		AP 903_00507FF17ECA	VigorAP 8 VigorAP 9
		AP 903_00507FF19216	VigorAP 9
		AP 910C_001DAA7F5D8C	VigorAP 9

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

Root Network 🗸 🗸	Dray Tek	VigorACS 3	Carrie Capture Packets Carrie System Administrator	С
Monitoring / Floor Plan				
Profile Name	marketing_carrie			
Edit Dimension + Add Device				
			P <p< td=""><td>×</td></p<>	×

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

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



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

Add		
Profile Name	↓↑ Devices	Jî Action
edroom	2	🖉 Edit 🔯 Delete
og	0	🖉 Edit 👘 Delete
narketing_carrie	1	🖉 Edit 🛛 🖞 Delete

7.2.6 Rogue AP Detection

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

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

Itoring / Rogue AP Detection						
at 24 Hours Last 7 Days Last 30 Days Custom Se	art 2020/11/02 End 2020/11/0	3				
can Now Periodic Scan						
logue AP Known AP						Sav
itics as tracians					81 C 1 /	L > D C
BSSID It SSID It Band	f it Channel	it Security	J+ Detector	in Signal	17 Last Detected	

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

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

			5 T		
Scan Now	Periodic Scan 🌔	Daily Weekly	Start Time 10:00 🔻		Sav
-	it 💼 Delete 🐻 Delete All				K < 1 /1 > K
	BSSID		Channel	Security	Comments
	00:1d:aa:00:00:02		Any	Any	
	22:33:11:22:33:33		Any	Any	
	00:1d:aa:04:f0:81		Any	Any	

Item	Description	1					
Scan Now	Perform dev	Perform device detection immediately.					
Add	Click to crea	Click to create a new entry for entering information for access point.					
Edit	Select one o then. After clicking	·	he Edit link will	be available for clicking, will be allowed to be			
	_	Periodic Scan Known AP Edit Delete Delete All	Daily Weekly	Start Time 10:00 v			
		BSSID	Channel	Security			
	0	00:1d:aa:00:00:02	Any	Any			
	0	22:33:11:22:33:33	Any 🔻	Any 👻			
		00:1d:aa:04:f0:81	Any	Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA/802.1x WPA/802.1x Mixed(WPA+WPA2)/802.1x			
			t from the list				
Delete		selected access poir					
Delete All	Remove all o	of the access points f	rom the list.				
BSSID	Display the	MAC address of the	detected access	point.			
Channel		channel used by the ox of the selected ac	-	lick Edit .			
Security	Display the	security mode used l	ov the access po	int.			

	It can be changed.
Comments	Display a brief explanation for the access point.
	It can be changed.
Save	Save the settings.

7.3 Configuration

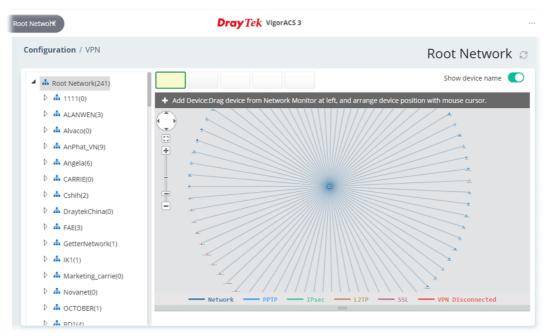
Configuration menu will vary for root network, group network and specified CPE.

=	Root Network 🗸 🗸
(7)	Configuration
<u>-</u>	VPN
۽ ڀ	AP Profile

7.3.1 VPN

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

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



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

For detailed, refer to section 8.4.1.

7.3.2 AP Profile

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

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

Add					
vofile Name	Action				
efault Profile	d' Edit 🗐 Delete 🏻 Dup	licate 🛛 Copy To			
IK	🖉 Edit 🗐 Delete 🔘 Dup	licate O Copy To			
est	State Delete Dup	licate 🛛 Copy To			
est2	Stdit 🗟 Delete 🚨 Dup	licate 🚨 Copy To			
t	a ^p Edit 🛞 Deleta 💭 Dup	licate 🖾 Copy To			
dr	P Edit 🙁 Delete 🖾 Dup	licate Copy To			
P_Carrie	d' Edit 😇 Delete 🖵 Dup	licate Copy To			
endy test	State Dup	licate O Copy To			
P_test	🖉 Edit 🗎 Delete 🔾 Dup	licate 🖸 Copy To			
vice Provisioning					
-	Model Name	Last Provisioned	Status	AP Profile	
Name	Model Name	Last Provisioned	Status	AP Profile	×
Name	Model Name VigorAP 810	Last Provisioned	Status	Emoty	
Aame A The Root Network A 2860ac_00507F00000e				Emoty (As Parent)	~
Aame A still Root Network A 2860ac_00507F00000e A 2860ac_00507F00000e	VigorAP 810 VigorAP 810		2	Empty (As Parent) (As Parent)	*
▲ 2860ac_00507F00000f	VigorAP 810 VigorAP 810 vigorAP 1 Au		-	Emoty (As Parent)	~
Ame A Boot Network A 2860ac,00507F00000e A 2860ac,00507F00000e A Pr Lto,uccutritiouse A PP 902,0010A1204F15	VigorAP 810 VigorAP 810 VigorAP 902	са. 	-	Empty (As Parent) (As Parent)	*
Kame A 3860ac,00507700000e 2860ac,00507700000e 2860ac,00507700000e A PF LIA,005077700000e A PF 902,0010A3D4F16 A PF 902,0010A3D4F16 A PF 903,00507F19236	VigorAP 810 VigorAP 810 vigorAP 1 Au		-	Emply (As Parent) (As Parent) (As Parent)	* * *
Ame A Boot Network A 2860ac,00507F00000e A 2860ac,00507F00000e A Pr Lto,uccutritiouse A PP 902,0010A1204F15	VigorAP 810 VigorAP 810 VigorAP 902			Emoty (As Parent) (As Parent) (As Parent) (As Parent)	* * * *

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

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

7.3.2.1 Add an AP Profile

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

Root Network 🗸 🗸	Dray Tek v	igorACS 3	Capture Packets 👻	carrie System Administrator
Configuration / AP Profile				
Add a Profile				
Profile Name:	AP_carrie	~		
AP Login Username:	carrieni	~		
AP Login Password:	••••••	~		
↑ Back to profile list				Save

ltem	Description				
Profile Name	Enter a name of the profile.				
AP Login Username	Enter a username for login the access point.				
AP Login Password	Enter a password for login the access point.				
Back to profile list	Return to previous page, AP profile list.				
Save	Save the settings and display the new profile on the AP profile list. Add New Profile Test Test Edit Delete Duplicate Copy To ttt Edit Delete Duplicate Copy To redf Edit Delete Duplicate Copy To AP_Carrie Edit Delete Copy To				

7.3.2.2 Edit an AP Profile

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

oot Network 🗸 🗸	Dr	ay Tek VigorACS 3	Carrie Capture Packets Y System Administrator
figuration / AP Profile			
General Setup SSID Settings	Overation Mode:	Access Point Range Extender Mesh Root Mesh Node	
Roaming	2.4G General Setup		v .
Load Balance	2.4G Wireless LAN		
LAN	802.11 Mode	Mixed(11b+11a+11n) *	
Airtime Fairness	2.4G Channel	Channel 11,2462MHz*	
Mobile Device Management	Channel Width	Auto 20/40 MHz *	
Application	Extension Channel	Channel 7.2442MHz *	
WMM Configuration	Antenna	2T2R *	
System	TX Power	100% *	
Profile Setting	MAC Clone		
	MAC Address		
\square	Band Steering		
	5G capability Check Time (sec.)	15	
Δ	Enable 5GHz Minimum RSSI		
~	Minimum RSSI (dBm)	- 78	
	Fragment Length (bytes)	2346	
	RTS Threshold (bytes)	2347)
	5 General Setup		
			ave profile

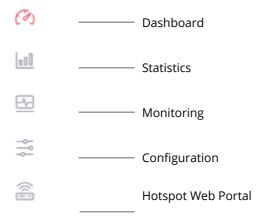
These parameters are explained as follows:

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

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

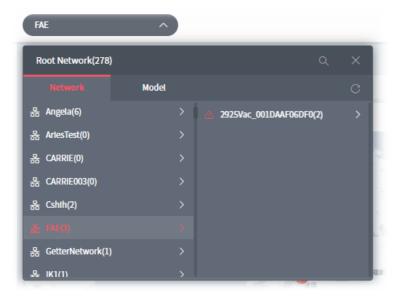
Chapter 8 Network Group Menu

The menu items related to the network group:



8.1 Dashboard for the Network Group

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



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

	FAE ~		Dray Tek	VigorACS 3			Er Cepture	Neckets - Sy	carrie dem Administrator	c
5	Dashboard							Auto Refresh :	1 Minute 👻	C
	Summary SD WAN									
2	Map Overview		ж	Device Overview					-	$\mathcal{E}^{(1)}$
	地震 東层接現		11	Routers 1	APS 1	Switch			Q, Dev	100
			2	Device Name	Model	HAC	UP Time	Firmware Version	LAN Clients	VP
	Et Martin Carl	1 4 4 C		29259ac00104AE950E9	Wgor2925Vac	001DAAF06DF0	0d:0h:0m:0s	3.8.9.5	0	0
		A (11)		AP 902 001044309808	VigorAP 902	0010AA3D9808	08.01:01:05	1.3.0RC2	0	0
	10000			P2289_001DAA0C8468	VigorSwitch P2280	001DAA0C8468	0d:0h:0m:0s	2.4.3	0	0
	1.	AN							H (1/1)	
	124	144 BAK 878	444						14 14 14 V	
	-11 C	2 and 100	\$10.0.0							
	Marth Marth		188							
			0.894							
	inter in the second sec	423								
	Active Clients- Top 20		Start24houn - / x	Traffic: Top 20					© Last 24 hours -	
	Total			Total						
	0 0		0%		¹ 0 Byte ¹ 0 I	Byte	2025Vac_00/0 Byte	0 Byte 1 0 Byte		64
	1 O Total	#2380_0010AA0C84G8/0	0%	1 Byte		o Total	P2280_0030/0 Byte	1 0 Byte L 0 Byte		0%
		•								

8.2 Statistics for Network Group

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

rd8 ~		DrayTek VigorAC	S 3	Capture	e Packets Y System Admir	carrie C
Statistics						С
Last 24 Hours Last 7 Days Last 30 Day	rys Custom Start: 2020/03/08 E	nd: 2020/03/09				Export
Usage Overview (.)		- 2 ×	Wireless Clients Overview (,)			- 2 ×
Total Number of Clients V 2 1	Nireless Clients Wire 1 (50%) 1 (5	d Clients 0%)				
Total amount of Traffic 270.79 MB 22	Download Uplo 254.05 MB (93.8%) 16.	^{ad} 75 MB (6.2%)	Band	SSID	os	
Max. Number of Concurrent Client	Avg. Number of Hourly Cli 1	ent	100.0%	100.0%	Android IOS	
Clients		- 2 ×	Traffic	-		- 2 ×
	Ow	red OWireless O 2.4G O 5G	Trank.		OWired OWireless O∶	
2			190.73 MB 143.05 MB			
1			95.37 MB 47.68 MB			
0 16:00 18:00 20:00 22:0	00 00:00 02:00 04:00 06:00 (08:00 10:00 12:00 14:00	0 Byte 16:00 18:00	20:00 22:00 00:00 02:00 04:00	06:00 08:00 10:00 12	2:00 14:00
Device Ranking (.)		≡Client• – 🖉 ×	Client Ranking (,)		≡Traff	fic• = 🗸 ×
لې↑ Device	J↑ MAC	↓↑ Client ↓↑	ليث Host Name	↓↑ MAC	↓↑ Traffic	ψţ.
1 2865ac_001DAA000000	001DAA000000	1	1 MKHL	406C8F525BFF	269.83 MB (99.6%)	
2 2926Vac_001DAA7033E0	001DAA7033E0	1	2 AngelaCYsiPhone	DC0C5CEE583E	986.13 KB (0.4%)	

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

8.3 Monitoring for Network Group

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

Ξ	rd8 V
(7)	Monitoring
080	Alarm
<u>₽</u>	Logs
	Devices
	Clients
	Cellular Data Usage
Z	Floor Plan
	Rogue AP Detection
\$	WAN (SD-WAN)
	VPN (SD-WAN)
ŝ	VOIP (SD-WAN)
29.	Data Usage (SD-WAN)

In this case, we choose RD8 as an example.

8.3.1 Alarm

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

	rd8		~		Dray	VigorACS 3		Capture Pack	carrie C System Administrator
(7)	Monit	oring / Ala	arm					2020/08/15 to 2020/09/14	search No. / Device Name / MAC Q
010	Alarr	n 43	History						
6		elete 💆 I	Delete All 🕁 🖞	Download				ld d	: 1 /3 > ▷ C' ⊗
		No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type
(((64018	Not Ack	2020/09/14 01:30:44 PM	2912n_001DAA8E14B0	001DAA8E14B0	\Lambda Critical	Device Loss Connection	Device Lost Connection
_		64017	Not Ack	2020/09/14 01:30:42 PM	AP 910C_001DAA7F5D8C	001DAA7F5D8C	\Lambda Critical	Device Loss Connection	Device Lost Connection
Z		64016	Not Ack	2020/09/14 01:30:42 PM	2133Vac_001DAA66E020	001DAA66E020	▲ Critical	Device Loss Connection	Device Lost Connection
E		64015	Not Ack	2020/09/14 01:30:40 PM	2862Vac_001DAAED3840	001DAAED3840	\Lambda Critical	Device Loss Connection	Device Lost Connection
8		64014	Not Ack	2020/09/14 01:30:32 PM	2952Pn_001DAAF8D818	001DAAF8D818	▲ Critical	Device Loss Connection	Device Lost Connection
⊕ ☆		64013	Not Ack	2020/09/14 01:30:32 PM	P2280_001DAA0C81D0	001DAA0C81D0	▲ Critical	Device Loss Connection	Device Lost Connection
292 293		64012	Not Ack	2020/09/14 01:30:27 PM	2925ac_001DAA512820	001DAA512820	▲ Critical	Device Loss Connection	Device Lost Connection
(i)		64011	Not Ack	2020/09/14 01:30:25 PM	3220n_001DAA554758	001DAA554758	\Lambda Critical	Device Loss Connection	Device Lost Connection
0		64010	Not Ack	2020/09/14 01:30:15 PM	AP 912C_001DAA72E14A	001DAA72E14A	A Critical	Device Loss Connection	Device Lost Connection
		64009	Not Ack	2020/09/14 01:30:07 PM	3910_001DAA2125B8	001DAA2125B8	A Critical	Device Loss Connection	Device Lost Connection
		64008	Not Ack	2020/09/14 01:30:07 PM	2926LVac_1449BCFFF9A8	1449BCFFF9A8	\Lambda Critical	Device Loss Connection	Device Lost Connection
		64007	Not Ack	2020/09/14 01:30:07 PM	AP 1000C_001DAA04F084	001DAA04F084	\Lambda Critical	Device Loss Connection	Device Lost Connection
		64006	Not Ack	2020/09/14 01:30:07 PM	2926Vac_001DAA5DCAF0	001DAA5DCAF0	A Critical	Device Loss Connection	Device Lost Connection
		64005	Not Ack	2020/09/14 01:30:01 PM	3900_001DAABABE50	001DAABABE50	▲ Critical	Device Loss Connection	Device Lost Connection

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

8.3.2 Logs

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

	RDB	5	~)		Dray Tek 🗤	perACS 3			pture Packets -	System Admin	carrie inistrator	С
3	Monit	coring / Logs						2021/01/31 to	2021/03/02	warch ID / Device	Name / Devi	ic Q
atl	ALCE	E Actions Device	e Reboot Reboot By CPE Reset	System Password Set Parameter	File Transfer Setting Profile	Device SysLog CPE Notify	Device Register	Device Operate				
		Delete All	-i-Download						H (71 >	н С	
11		10	Device Name	Davice ID	MAC Address	Device IP	Action	Action ID	Time			
8		3997642	2925Ln_001DAADD7580	136121	082700AAD07580	192.168.105.28	Inform	-	2021/02/17 08	-35-11 AM		
		3997641	2952Pn_001DAAF8D818	141468	001DAAF8D818	192.168.105.52	Inform	1.000	2021/02/17 08	:35:04 AM		
S		3997640	2133Vac_001DAA66E020	141455	001DAA66E020	192.168.105.59	Inform	2021,4		:35:02 AM		
B		3997630	2133Vac_001DA466E020	141455	001DAA66E020	192.168.105.59	inform	1.00	2021/02/02 09:18:1			
(0)		3997629	2133War_001DAA66E020	141455	001DAA66E020	192 168 105 59	Inform	-	2021/02/02 06-53-48 AM			
•		3997628	2133Vac_001DAA66E020	141455	001DAA66E020	192.168.105.59	Inform	1441	2021/02/02 03	1:07:36 AM		
御												
88												
0												

These parameters are explained as follows:

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

8.3.3 Devices

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

8.3.3.1 Device Overview

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

Monitoring / Devices										
search Device Name /	P/MAC	Model Vigor2133Vac,	Vig - Statu	AI	3	SSID AIL			Rows 10 ~ 10	< 1 /1 > # C
-F.Download										General Wireless
Device	17 IP Address	an MAC Address an	Model 42	Network-	Status (1	Up Time 47	F/W Version +1	Last Inform Time	Current Client	21 Current Traffic
2133Vac.001DAA66E020	192.168.105.59:443	001DAA66E020	Vigor2133Vac	RD8	online	13d:0h:47m:43s	3.9.4_RC1 ⊘	2021/03/02 09:25:13 AM	0 (Local Wireless: 0)	229.48 KB († 100.37 KB 1 129.11 K
2862Vac 001DAAF7C0E0	192.168.105.62:443	001DAAF7C0ED	Vigor2862Vac	R08	offline	0d:0h:0m:0s	3.9.4.1_BT 🕗	2021/01/08 08:16:42 AM	0 (Local Wireless: 0)	0 Byte († 0 Byte 1 0 Byte)
2865 14498C081548	192.168.105.129.8443	14498C081548	Vigor2865	RD8	offline	0d:0h:0m:0s	4.2.0.1_STD @	2021/01/08 08:22:30 AM	0 (Local Wireless: 0)	0 Byte († 0 Byte 1 0 Byte)
2925Ln 0010AA007580	192.168.105.28:443	001DAADD75B0	Vigor2925Ln	RD8	online	13d:0h:49m:36s	3.8.9.5 😡	2021/03/02 09:24:14 AM	0 (Local Wireless: 0)	209.59 KB († 94.77 KB ↓ 114.83 KB
2927Lac 14498C023740	192.168.105.27:443	1449BC023740	Vigor2927Lac	RD8	offline	0d:0h:0m:0s	4.2.2_RC5b 🔕	2021/01/04 11:37:25 AM	0 (Local Whreless: 0)	0 Byte (1 0 Byte 1 0 Byte)
2952Pn 0010AAF80618	192.168.105.52:443	001DAAFEDR18	Vigor2952Pn	RDS	online	13d:0h:47m:44s	3.9.4_RC3@	2021/03/02 09:25:48 AM	0 (Local Wireless: 0)	621.76 KB († 438.12 KB ↓ 183.64 K
AP 1000C 001DAA04F060	192.168.105.51;443	001DAAD4F06C	VigorAP 1000C	RDS	offline	0d:0h:0m:0s	1.3.3_RC2 🖸	2020/12/14 09:06:59 PM	-	
AP 810 001DAA7C2R50	192.168.105.240:443	001DAA7C2B50	VigotAP 810	RD8	omine	0d:0h:0m:0s	1.3.20	2020/12/23 03:14:30 PM	0 (Local Wireless: 0)	-
AP 920R 0010AA223344	192.168.105.92:443	001DAA223344	VigorAP 920R	RD8	offline	0d:0h:0m:05	1.3.2_RC6 😔	2020/12/23 03:14:32 PM	0 (Local Wireless: 0)	-

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

8.3.4 Clients

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

	rd8 VigorACS 3 BI Capture Packets VigorACS 3 System Administrator	С
(⁷)	Monitoring / Clients	
00	Last 24 Hours Last 7 Days Last 30 Days Custom Start: 2020/09/13 End: 2020/09/14	ort
Ð	Search Hostname / MAC / IP Type: All ✓	
	Rows V H < 1 /1 > N C o	ø
((([]	Hostname 47 MAC Address 47 IP Address 47 Connected Device Connected Device MAC 05° Type 47 SSID 47 ConnectionTime 47 Traffic	- ↓↑
Z	Mickey-Phone 748587803E45 192.168.124.12 2927Lac_14498C023720 14498C023720 WIRELESS_5g Vigor/2927-RD8-Arles-5G1 0d 04h 27m 14s 20.68MB(† 880.70KB ↓ 19.82MB)	,
	R1000675 88D7F656F799 192.168.124.10 2927Lac_1449BC023720 1449BC023720 WIRED 4d 04h 57m 59s 1.63GB(†76.47MB ±1.56GB)	
\$	YRCs-IPhone B019C6DC60E2 192.168.124.11 2927Lac_1449BC023720 1449BC023720 WIRELESS_5g Vigor/2927-RD8-Arles-5G1 0d 05h 40m 07s 130.11MB(† 3.48MB ↓ 126.63MB)	.)
-	Total Number of Clients: 3	
<u>.</u>		

Item	Description
Last 24 Hours / Last 7 Days / Last 30 Days / Custom	Display the clients detected within 24 hours, 7 days, 30 days or user defined days.
Search Hostname / MAC / IP	Enter the condition for VigorACS to search and display relational information.
Type	Check All to display information for all of the devices (including wired and wireless devices).
All R WIRED WIRELESS_2.4g	Wired – This page displays information for the device without wireless feature.
d WIRELESS 5g	Wireless_2.4g – This page displays information for the device with 2.4GHz wireless feature.
	Wireless_5g – This page displays information for the devices with 5GHz wireless feature.
SSID	This area lists information for CPE with wireless features monitored by VigorACS.
	Check All to display all of the devices; or check the name of the device to display the information related to the selected device.
	SSID - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.
Create Report	Click this button to save client's information as a "XLS" file. After clicking the button, the following page will appear.

Select the columns				
E Hostname	MAC Ad		🖬 iP Address	
Connected Device	Connec	ted Device MAC	🖬 os	
🖾 Туре	SSID		ConnectionTime	
🖬 Traffic				
Select devices				
Name	Model Name	Firmware Version		
🖌 🗮 🕜 rd8(48)				
= 🔿 810_001DAA7D6514	VigorAP 810	1.2.5		
0 902_001DAA3D4F16	VigorAP 902	1.2.3.1		
0 130_001DAAE3A094	Vigor130			
	Vigor130	r70663_beta		
130_001DAA854204	Vigor130	r72469_beta		
C 130_001DAA603FA0	Vigor130	8		
C 2120n+_001DAA0FE010	Vigor2120n+	3.8.9.2		
E 0 2130Vh_001D000000E	Vigor2130Vn	v1.5.4.2		
O 2132FVn_001DAAE486C8 O	Vigor2132FVh	1.7.9.1_CBizz_1		
O 2133Vac_0010AA66E020	Vigor2133Vac	1.9.0_RC7		
O 2620Ln_001DAA926F58	Vigor2620En	3.8.10_RC1		
🗏 🙆 2710n_00507F9A3648	Vigor2710n	3.6.8.6		
B 2830V_00507F708028	Vigor2E30V	3.8.8.2_sb_246302		
	Vigor2830I	3.6.8.7_db_RC3		
# 2850n+_001DA4D1E290	Vigor2860n+	3.8,9.3_STD		
				× Cancel
				× cancer

8.3.5 Cellular Data Usage

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

rd8	~			Dray Tek	VigorACS 3		Br Capture Packets -	carrie System Administrator	
Monitoring / Ce	llular Data Usage								
LTE Data Usag	e Overview				Quota Settings				
Data Used O Byte	Data Cycle 09/13 - 09/19	Status: WA	RNING	0% of 0MB	Data Usage Alarm	0			
1 Byte	03/13 03/13			O Total	Data Quota	0	мв ~		
					Trigger Alarm When Usage Reached	0	% of Quota (0 Byte)		
					Alarm Serverity Level	Critical		0	
					Data Usage Cycle	Weekly M	fonthly Custom		
0 Ryte			05-14		Weekly Reset Day	Sunday		0	
Device		Total	Download	Upload					
2925Ln_001DAV	ADD7580	0 Byte							
2927Lac_14498	C023720	0 Byte	0 Byte	0 Byte				Cancel	Save
2620Ln_001DA	N926F58	0 Byte							
LTE200n_00104	A93AE8C	0 Byte							
2926LVac 1449	RCFFF9AR	0 Byte							

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

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

8.3.6 Floor Plan

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

	rd8 ~		Dray Tek VigorACS 3	Capture Packets ~	carrie System Administrator	С
(7)	Monitoring / Floor Plan					
	+ Add					
<u>F</u>	Profile Name	↓↑ Devices		↓↑ Action		
49	test	0		🖉 Edit 🐵 D	elete	
(((1	test2	0		🖉 Edit 🔞 E	elete	
e.						

ltem	Description
+Add	Creates a new profile.
88	Click to change to browse view. It displays all of the floor plan profiles with the map used.

	Monitoring / Roor Plan
	Dedroom O jog O tte O
	N X 1 21
	You can click Add on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click Edit Map & Plan to perform the modification, or click Delete Map Profile to remove the selected floor plan profile.
Profile Name	Displays the name of the floor plan profile.
Device	Displays the number of AP devices placed on the plan profile.
Action	Edit - Click to modify the profile.
	Delete - Click to remove the selected profile.

To create a new profile:

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

Monitoring / Floor Plan		
Profile Name	marketing_carrie	
Upload Map	Floor_MAP.png	Browse
		Cancel

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

Profile Name	marineting_carrie	
Edit Dimension Add Device		
		Cancel Sa

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

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

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

Profile Name	marketing_carrie		
Edit Dimension + Add	Device		
ag and drop a virtual AP or ar	un-assigned AP to the floor plan.		
		Un-assigned APs	٢
		Device Name	Model
		A 810_001DAA7D6514	VigorAP 8
		AP 1000C_001DAA04F084	VigorAP 1
		AP 1000C_001DAA575D38	
		AP 1000C_001 DAA575D38	VigorAP 7
		AP 1000C_001DAA575D38 A AP 710_00507FF138F7 A AP 800_001DAA2A5B70	VigorAP VigorAP 8
		▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7 ▲ AP 800_001DAA2A5B70 ▲ AP 903_00507FF17ECA	VigorAP 1 VigorAP 7 VigorAP 8 VigorAP 9
		AP 1000C_001DAA575D38 A AP 710_00507FF138F7 A AP 800_001DAA2A5B70	VigorAP 7 VigorAP 8

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

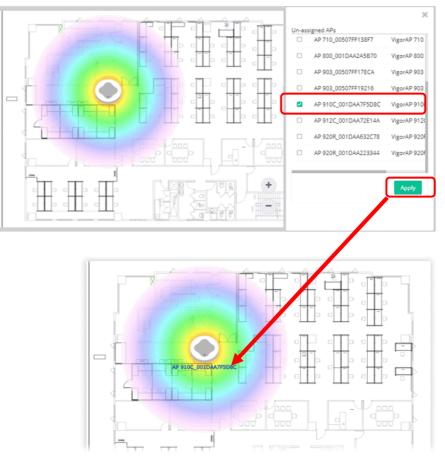
ofile Name	marketing_carrie		
Edit Dimension + Add Device			
and drop a virtual AP or an un-a	signed AP to the floor plan.		
		Un-essigned APs	٢
		Device Name	Model
4		A 810_001DAA7D6514	VigorAP 810
		AP 1000C_001DAA04F084	VigorAP 10
		AP 1000C_001DAA575D38	VigorAP 10
		AP 710_00507FF138F7	VigorAP 71
		AP 800_001DAA2A5B70	VigorAP 80
		AP 800_001DAA2A5B70 AP 903_00507FF17ECA	VigorAP 80 VigorAP 90
		AP 800_001DAA2A5B70	VigorAP 71 VigorAP 80 VigorAP 90 VigorAP 90

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

Monitoring / Floor Plan		
Profile Name	marketing_carrie	
Edit Dimension		
		×

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

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



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

						Monitoring / Floor Plan
E						
						+ Add
		↓ ↑ Action	11	Devices	↓ ↑	Profile Name
	🗊 Delete	🖉 Edit		2		bedroom
	🗊 Delete	🖉 Edit		0		ipg
	🗊 Delete	🖉 Edit		1		marketing_carrie

8.3.7 Rouge AP Detection

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

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

	rd8 ~	Dray Tek VigorACS 3	Carrie Capture Packets × Carrie C
(7)	Monitoring / Rogue AP Detection		
000	Last 24 Hours Last 7 Days Last 30 Days Custom	Start: 2020/09/13 End: 2020/09/14	
₩	Scan Now Periodic Scan	Daily Weekly Start Time 1:00 ~	
	Scan Now Periodic Scan	Daily Weekly Start Time 1:00 V	Save
	Rogue AP Known AP		
Z	+ Mark as Known 🐵 Delete 🗯 Delete All		N < 1 /1 > N C
E	BSSID ↓↑ SSID ↓↑ Band	J↑ Channel J↑ Security J↑ Detector	J↑ Signal J↑ Last Detected J↑
-		No data available	
۲		NO dada avanabile	
÷			
쓰			
(j)			

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

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

Scan Now	Periodic Scan 🔵 Daily	Weekly Start Time 10:00 -		Sav
Rogue AP Kr				
	it 💼 Delete 🐵 Delete All			
	BSSID	Channel	Security	Comments
	00:1d:aa:00:00:02	Any	Any	
	22:33:11:22:33:33	Any	Any	
	00:1d:aa:04:f0:81	Any	Any	

Item	Description				
Add	Click to create a new entry for entering information for access point.				
Edit	Change the settings for a selected access point.				
	Select one of the access points. The Edit link will be available for clicking, then. After clicking it, channel, security and comments will be allowed to be modified with different values.				
	Scan Now Periodic Scan O Dally Weekly Start Time 10:00 🔻				
	Rogue AP Known AP + Add ∠ Edit □ Delete				
	BSSID Channel Security				
	00:1d:aa:00:00:02 Any Any				
	□ 22:33:11:22:33:33 Any ▼ Any ▼ Any				
	00:1d:aa:04:f0:81 Any Disable WEP WPA/PSK WPA/2PSK WPA/2PSK WEP/302.1x WPA/802.1x WPA/802.1x WPA/802.1x				
Delete	Remove the selected access point from the list.				
Delete All	Remove all of the access points from the list.				
BSSID	Display the MAC address of the detected access point.				
Channel	Display the channel used by the access point. Check the box of the selected access point and click Edit .				
Security	Display the security mode used by the access point. It can be changed.				

Comments	Display a brief explanation for the access point.
	It can be changed.
Save	Save the settings.

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

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



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

Use default settings
Bulk Data is not configured on this network. Do you want to apply the default settings?
No Yes

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

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

Setting Map				
-Add New Network 🛛 🖄 Delete This I	Network 🛛 🚓 Change Network			
General Settings				
Network ID			Username	
254			fae	
Name			Password	
FAE		~	•••	\$
Location				
hich the profile returns a bulk data to	the ACS. If you disable bulk data	categories, it will affect the SD-WAN	operation.	category in the corresponding profile, and specify the report interval a
Profile #1	Enable 🔵	Profile #2	Enable	Avaliable / Disabled Bulk Data Categories
Report Interval (sec)		Report Interval (sec)		[
Report Interval (sec) 120	~	Report Interval (sec) 300	~	
	~		~	
120	Stre: 8	300	Size: 4	
120 Bulk Data Categories		300 Bulk Data Categories		

8.4 Configuration Menu for Network Group,

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

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

=	rd8 V
(7)	Configuration
00	VPN
<u>F-</u>	AP Profile
4°4	Load Balance
	Route Policy (SD-WAN)
_	VOIP WAN (SD-WAN)

8.4.1 VPN

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

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

RD8 V	Dray Tek VigorAC53	System Administrator
Configuration / VPN		C
A 👫 Root Network(164)	+ Add Device 37 Create VPN at Edit LAN IP 22 Unitink VPM III Remove Device	Show device name
ALANWEN(3)	+ Add Device:Drag device from Network Monitor at left, and arrange device position with mouse cursor.	
b AnPhat_VN(8)		
b Angela(7)	\odot	
D ARRIE(2)		
> 🚓 Cabib(2)		
▷ ♣ FAE(3)	e	
1- 🚠 RD1(3)		
() 👬 RD2(32)		
[- 👬 RD3(14)		
() 👬 RD5(12)		
1) 🚓 RD6(3)		
p # R07(15)		
() 🚠 RD8(9)		
b # ScanAccess(3)		
b A Shanghai(15)		
Test1 & Test2(1)	TRAPILOT STATISTICS	
5		
b attel(3)		
b dvcom_kuwait(12)	() Lindean	
p # henry(5)		
1 James_test(3)	Network	
p 🚠 nobody(0)		
h		

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

8.4.2 AP Profile

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

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

808 ~	Dray	Tek VigorACS 3		BI Capturo Packets +	carrie System Administrator	0
onfiguration / AP Profile						
+ Add						
Profile Name	Action					
Root Network-UK-Copy-edit	d Edit 🔒 Delete	Doplicate Copy To				
Marketing_carrie	S Edit 🗄 Delete	Duplicate D Copy To				
Device Provisioning						
Name	Model Name	Last Provisioned	Status	AP Profile		
Name A 🚓 RDB	Model Name	Last Provisioned	Status	AP Profile Empty	v	
	Model Name VigorAP 1000C	Last Provisioned	Status		•	
A the BDB				Empty		

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

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

8.4.2.1 Add an AP Profile

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

Root Network V	Dray Tek VigorAC	S 3 Capture Packets 🗸	carrie System Administrator
Configuration / AP Profile			
Add a Profile			
Profile Name:	AP_carrie 🗸		
AP Login Username:	carrieni 🗸		
AP Login Password:	© ~		
↑ Back to profile list			Save

ltem	Description				
Profile Name	Enter a name of	the profile.			
AP Login Username	Enter a usernam	ne for login the access point.			
AP Login Password	Enter a passwor	d for login the access point.			
Back to profile list	Return to previo	Return to previous page, AP profile list.			
Save	Save the settings	s and display the new profile on the AP profile list.			
	ttt redf	 ✓ Edit Delete Copy To ✓ Edit Delete Duplicate Copy To 			
	AP_Carrie	🖌 Edit 💼 Delete 🖸 Duplicate 🔁 Copy To			

8.4.2.2 Edit an AP Profile

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

oot Network 🗸 🗸	Dr	ay Tek VigorACS 3	Carrie Capture Packets Y System Administrator
figuration / AP Profile			
General Setup SSID Settings	Overation Mode:	Access Point Range Extender Mesh Root Mesh Node	
Roaming	2.4G General Setup		v .
Load Balance	2.4G Wireless LAN		
LAN	802.11 Mode	Mixed(11b+11a+11n) *	
Airtime Fairness	2.4G Channel	Channel 11,2462MHz*	
Mobile Device Management	Channel Width	Auto 20/40 MHz *	
Application	Extension Channel	Channel 7.2442MHz *	
WMM Configuration	Antenna	2T2R *	
System	TX Power	100% *	
Profile Setting	MAC Clone		
	MAC Address		
\square	Band Steering		
	5G capability Check Time (sec.)	15	
Δ	Enable 5GHz Minimum RSSI		
7	Minimum RSSI (dBm)	- 78	
	Fragment Length (bytes)	2346	
	RTS Threshold (bytes)	2347)
	5 General Setup		
			ave profile

These parameters are explained as follows:

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

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

8.4.3 Load Balance

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

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

rd8 V	Dray Tek VigorACS 3	Capture Packets 👻	carrie System Administrator	С
Configuration / Load Balance				С
Load Balance Mode	IP Based Session Based			
Line Speed	Auto Detect According To Line Speed			
Load Balance Weights	Custom 🔹 🗸			
Upload Bandwidth Weight	Low High			
Download Bandwidth Weight	Low High			
Low Latency Weight	Low High			
Low Jitter Weight	Low High			
Less Packet Loss Weight	Low High			
🗑 Clear			Save and Apply to CPE	

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

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

8.4.4 Route Policy (SD-WAN)

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

rdi		~				Dray Tek VigorACS 2	- Inter Carp	Carrie System Administrato	c
Cor	nfiguration / Route	Policy							С
+	Add New Route Polacy								
App	p Service Profile	In Use O	Remaining 32	Maximum 32	Note App service profiles	are currently managed by VigorACS, amound profiles will	be removed automatically.		
	art Status	4° Comme	eet.		Ir Source	10 Destination	19 Intertace	47 Action	11
						No data available			

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

SD-WAN function is not enabled in this network.	

8.4.4.1 Creating a Route Policy with Basic Mode

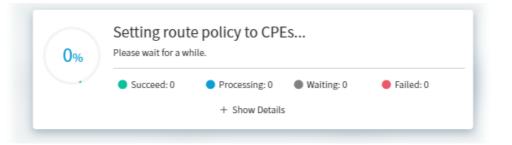
1. Click **+Add New Route Policy** to create a new profile. In default, the settings based on Basic Mode will be shown as follows.

+ Add a New Route Poli	cy ×
Enable	
Comment	Marketing_Carrie
Source	Any 🗸 🗸
Destination	App Services 🗸 🗸
App Service Profile	Create a new profile From an existing profile
Selected App Service	FTP 🛞 DNS 🛞 Wikipedia 🛞
Send via Interface	WAN 1 ~
(i) Note If you want to send via V Go to SD-WAN VPN Setti	PN (to the Hub), please dial VPN Hub and Spoke connection first. ngs
	+ Advanced Mode
	Cancel Save and set to CPEs

These parameters for Basic Mode are explained as f	ollows
These parameters for basic mode are explained as r	0110115.

ltem	Description						
Enable	Click the icon to enable / disable the policy profile.						
Comment	Enter a name of the route policy profile.						
Source	Set the source IP addresses to which this rule is to be applied.						
	Any - This rule applies to all source IP addresses.						
	IP Range - This rule applies to the specified range of source IP addresses If there is only one source IP address, enter the address in both the Start and End fields.						
Destination	Set the destination IP addresses to which this rule is to be applied.						
	Any - This rule applies to all destination IP addresses.						
	IP Range - This rule applies to the specified range of destination IP addresses. If there is only one destination IP address, enter the address in both the Start and End fields.						
	VoIP - This rule applies to VoIP packets.						
	App Services - This rule applies to App services.						
	• Create a new profile - Click this tab to create a new App Service Profile.						
	Selected App Service - Specify required App services (e.g., CNN, FTP, DNS, SMTP/SMTP STARTTLS, Wikipedia).						
	• From an existing profile - If an App service profile has been created previously, click this tab to choose an existing route policy profile.						
	Selected an AP Service Profile - From the drop-down list, choose the one you want.						
	Note that, when a route policy is set with App services, it will be applied to the router at the same time. Open Configuration>>Routing>>Load Balance / Policy Route. The routing rule with APP service will be highligher and marked as "Managed By SD-WAN". It means the policy was created by ACS SD-WAN, and can be edited or deleted by ACS SD-WAN only.						
	treat Balance/period Balance						
	Static Rocke IIV4 Index Enable Comment Protocol Interface Sociely Deat/P Static Rocke IIV4 I Enable Any WANI Range Any						
	NDP Noneed By 50 WM 2 Enable Any WANI Any APP Service						
	3 Disable Any WANI Any Any						
Send via nterface	WAN#/LAN#/DMZ/IP Routed Subnet - Select an interface from the list. The traffic will be sent to the designated interface.						
+Advanced Mode	Click to open the configuration page with more options.						
Save and Set to CPEs	Save the above configuration and set to CPE devices.						

2. Click Save and set to CPEs.



3. A route policy has been set successfully.

rdð	~			DrayTek	VigorACS 3	In Capture Packats	Carrie System Administrator	C
Configuration / Rout	e Policy							Ç
+ Add New Route Policy								
App Service Profile	in Use O	Remaining 32	Maximum 32	Rote App service profiles are currently managed	by VigorACS, unused profiles will be removed as	umatically.		
http://www.wite.com	U	~~						
* # Status	41 Comme			27 Source	J† Destination	27 Interface	at Action	- 2

8.4.4.2 Creating a Route Policy with Advanced Mode

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

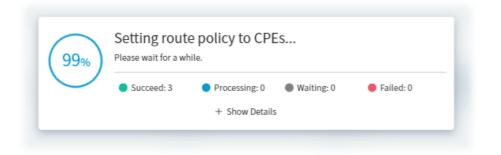
Enable		
Comment	Marketing_Carrie	
Source	Any	~
Destination	Any	~
Send via Interface	WAN 1	~
① Note If you want to send v Go to SD-WAN VPN S	a VPN (to the Hub), please dial VPN Hub and Spoke c ettings + Advanced Mode	onnection first.

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

Send via Gateway	Default Gat	eway	Specific Gateway	1	
Packet Forwarding to WAN/LAN	Force NAT	Force	Routing		
via					
Failover	\bigcirc				
Failback	\bigcirc				
	-	Basic Mod	e		

ltem	Description					
Send via Gateway	 Default Gateway - Traffic will be sent to the default gateway address of the specified interface. Specific Gateway - Traffic will be sent to the specified gateway address instead of the default gateway address. 					
	• Specific Gateway -	Enter an IP address.				
Packet Forwarding to WAN/LAN		P address will not be used to connect to the ork Address Translation (NAT) will be used, ess will be used.				
	Force Routing - The sour to the remote destination	ce IP address will be preserved when connecting n.				
Failover	Click the icon to enable / disable the failover function.					
	Failover					
		✓ Failover to Default WAN ✓ when				
		interface offline.				
	Failover to Gateway	Default Gateway Specific Gateway				
	Failover to - If the interface specified above loses connection, traffic can be forwarded to an alternate interface or be scrutinized by an alternate route policy. Use the drop down list to choose an interface as an auto failover interface.					
	Failover to Gateway - The failed-over traffic can be sent to the gateway.					
	• Default Gateway - Click to use the default gateway.					
	• Specific Gateway - Click to use a specific gateway.					
		r Gateway - Enter an IP address. o enable / disable the failback function.				
Basic Mode		ration page with less options.				
Save and set to CPEs		tion and set to CPE devices.				

4. Click Save and set to CPEs.



5. A route policy has been set successfully.

rdð	×)			Dray Tel	VigorACS 3	Ex Capture Paci	Carrie System Administrator	C
Configuration / Rout	e Policy							C
+ Add New Route Policy	1							
App Service Profile	in Use O	Remaining 32	Maximum 32	© Note App service profiles are currently managed	by Vigor ACS, unused profiles will be removed au	umaticatiy.		
				17 Source	Jit Destination	17 interface	Action	
e at Status	1º Comme	-				a line ave		

8.4.5 VoIP WAN (SD-WAN)

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



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

8 ~	Dray Tek VigorACS 3	Capture Packets ~	carrie System Administrator
Configuration / VoIP WAN			C
Enable VoIP WAN			
Change VoIP WAN when current WAN MOS score is less than	3.5 💌		
And another WAN is better by	0.3 *		

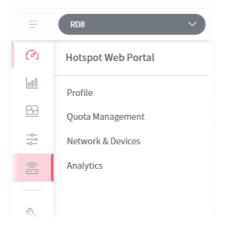
(1) It is available only when SD-WAN feature is enabled for current used network group. If not enabled, a notification will appear to ask for SD-WAN activation.



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

8.5 Hotspot Web Portal for SD-WAN Network Group

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



8.5.1 Profile

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

RDB	~			Dray Te	k VigorACS 3	📾 Captare Packets –	System Adm	carrie inistrator
	Web Portal / Profile							1
÷Add							Profile	Number Limit: 2,
Index 41	Profile Name	† Enable it	Hotspot Server Mode	41 Login Method	21 Applied Interfaces	41 Action		
1	NYF_Carrie	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	e" Edit 🗇 Delet	e O Copy	R ViewLog
2	dsadas	(Disabled)	AC53 as Hotspot Server	Click Through	LAN (1)	d' Edit II Delet	e Copy	WiewLog

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

Copy Profile					
New Profile Name	Please er	nter a profile n	ame		
Copy Item	🗹 Configu	uration			
	□ Locales				
ew Log – Click to	o review detail	Car ed informat		elected prof	īle.
Tiew Log – Click to	o review detail			elected prof	file.
Hotspot Web Portal / Hotspot Profile	o review detail			elected prof	file.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup *	o review detail	ed informat		elected prof	file.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup * A Back To Profile List	o review detail	ed informat	tion for the se	elected prof	file.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup •		ed informat	tion for the se	elected prof	file.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup • + Back To Profile Las Profile Information Profile ID 9 Profile Name NVF_C		ed informat	tion for the se	elected prof	file.
Hotspet Web Pertal / Hotspet Profile User Group : RootGroup * * Beck Torpfile List Profile Information Profile Name NYF_C Comments (ACS) Login Method Variou	Carrie Just for test us Hospot Lagin	ed informat	tion for the se		file.
Idespet Web Pertal / Hospot Profile Jare Group: Rool(Group	Carrie just for test	ed informat	tion for the se		
tspot Web Portal / Hotspot Profile er Group : RootGroup •• Back To Profile Lis: Profile Information Profile ID 9 Profile Name NYF_C Comments (ACS), Login Method VAS, Applied Interfaces LAN (1	Cerrie just for test Us Mospor Login 1) WLAN 2.4G (1) WLAN 5G (1)	ed informat	tion for the se	Satus	
otspot Web Portal / Hospot Profile ser Group : RootGroup • Back To Profile List Profile Information Profile ID 9 Profile Name NYF_C Comments (ACS) Login Method Vario Applied Interfaces LAN (1	Cerrie just for test Us Mospor Login 1) WLAN 2.4G (1) WLAN 5G (1)	ed informat	tion for the se overview	Status Il Noryet ageled II Compiles I	

To create a new hotspot web portal profile:

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

+ Create New Profile	2		
New Profile Name	NYF_Carrie		
		Cancel	Create

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

lotspot	Web Portal / Profile								C
User Gro	RootGroup	¥							
+Add								Profil	e Number Limit: 3/
Index 41	Profile Name	at Enable at	Hotspot Server Mode	27 Login Method	Applied Interfaces	48 Action			
	NYF_Carrie	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	et Edit	E Deleta	Copy	E View Log
2	dsədəs	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	d' Edit	8 Delete	C COPY	W View Log
2	NYF_carrie	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	e Edit	E Delete	C Copy	W View Log

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

lotspot Web Portal / Hotspot Profile Jser Group: RootGroup *	с
1 Profile St	Tup Splash Page Customitation Whiteliti Setup (Optional)
Basic Settings	
Enable Profile	
Profile Name	NYF_Carrie
Comments	just for test
Hotspot Server Mode	ACS3 as Hotpot Server ACS3 as Hotpot Server The 34P April
Applied Interfaces	
Subnet	G LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 LAN7 LAN8
WLAN 2.4G	SSID1 SSID2 SSID3 SSID4
WLAN 5G	SSID1 SSID2 SSID3 SSID4
External RADIUS Server	
External RADIUS Server	No External RADIUS Server 🖉 Edit
RADIUS MAC Authentication	D
RADIUS MAC Format	aa.bb.cc:dd:ee:ff +
RADIUS NAS-Idenfifier	
Portal Server	
Login Method	Click Through 🛛 Facebook 🗇 Google 📄 RADIUS Account 📄 Leave Info
Captive Portal URL	
	Example:https://Your VigorACS Server/ACSServer/HotspotPortal/home
Redirection URL	Hitp:// v portal.draytek.com
HTTPS Redirection ()	
Captive Portal Detection 🔀	
Landing Page Method	Fixed URL *
Landing Page URL	http://draytolc.feeod.url
	B Note: Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.
Quota Policy	
Quota Profile	Default -
	Expired Time After 1 st Login Idle Timeout Bandwidth Limit
	0d 6h 0m Disabled Unlimited
	Cancel Continue

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

External RADIUS Server	Displays the IP address of the external RADIUS Server. Edit - If required, Click to modify the RADIUS Server.				
	External RADIUS Server				
	Enable				
	Enable Accounting				
	Primary Server				
	Server 172.16.3.88				
	Destination Port				
	Retry 2				
	2 ×				
	Secondary Server				
	Server IPv4 format (EX : 123.12.1.1) Destination Port 1942				
	Secret O				
	Retry 2				
	Cancel Confirm				
RADIUS MAC Authentication	If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server.				
RADIUS MAC Format	Select the MAC address format.				
RADIUS NAS-Identifier	Enter the server's ID.				
	Portal Server				
Login Method	There are several methods to be selected as for portal server.				
	Click Through -				
	 Facebook - 				
	 Google - 				
	 RADIUS Account - 				
	Leave Info -				
Captive Portal URL	Enter the captive portal URL.				
Redirection URL	Enter the URL to which the client will be redirected.				
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.				
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet.				
Landing Page	Specify the landing page for the client after passing the authentication.				
Method	• Fixed URL - Specify a landing page URL.				
	 User Request - The user will be redirected to the URL they initially 				
	requested.				
	 Bulletin Message - Show a message on Bulletin. 				
· · · -					
Landing Page	It is available when Fixed URL is selected as Landing Page Method .				
URL	Specifies the webpage that will be displayed after the user has successfully authenticated.				

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

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

	Profile	Setup Splash Page Custon (Optional)	mization Whitelist Setup (Optional)
Layout	Components	Login Method	
Background Layout	Color Image		
Background 1 Color 🔗	#4a4972	5	Dray Tek
Background 2 Color 🔗	#FFFFFF	5	
Login Method Background Color 🔗	#4a4972	C	Welcome! Please log in to enjoy Wi- Fi.
Login Method Opacity 🔗	97		Connect
Browser Tab Title	Draytek Hotspot		
Enable Browser Tab Icon	\bigcirc		
Enable Logo			
Splash Page Logo 🔗	DrayTek Red Image Uplo	be	
	Dray Tek		
			Cancel Previous Continue

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

Color	the predefined color list, or e	enter the RGB value (with the format of HEX).			
Login Method Background Color		Select the background color of the login panel from the predefined color list, or enter the RGB value (with the format of HEX).			
Login Method Opacity	Adjust the opacity (1-100) of	the login panel.			
Browser Tab Tit	Enter the text to be shown as	s the webpage title in the browser.			
Enable Browser Tab Icon	Click to enable / disable the b	prowser tab icon for VigorACS WUI.			
Browser Tab lcc	, , , , , , , , , , , , , , , , , , ,	age by using Browse and upload to VigorACS.			
Enable Logo	Click to enable / disable the l	ogo display on the login window.			
Splash Page Log	Image Upload - Select an im	 DrayTek Red - It is default setting. Image Upload - Select an image by using Browse and upload to VigorACS. It will be used as the logo display on the login window. 			
	Components				
Layout	Components Login Method				
Welcome Message 🔗 Terms & Conditions Text 🔗 Content 🔗	S Terms & Conditions Marketing Language Option Wi-Fit Wi-Fit Fit information on the data Draytek collects and how it is used please see the Draytek Privacy Policy. User must tick to get the Internet access	English (UK) Welcome! Please log in to enjoy Wi- Fi. Connect			
		Terms Marketing For information on the data Draytek collects and how it is used please see the Draytek Privacy Policy.			
		I have read and accept the Terms and Conditions. I Vould like to receive emails about the latest events, products, and services from you. Reject Accept			
Splash Page Components	 Defines the content of the splogin page. Welcome Message Terms & Conditions Marketing 	plash page. Select the one(s) to show on the			

	Language Option					
Welcome Message	Enter the text to be displa	Enter the text to be displayed as the welcome message.				
Terms & Conditions Text	-	If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.				
	Enter the text which will b Conditions.	e shown after the checkbox for Terms and				
Content	If it is enabled, it will be sh Connect / Submit button o	nown on the second page after clicking the on the login page.				
	Enter the text to be displa	yed in the Terms and Conditions window.				
Marketing Text	Connect / Submit button o					
	information.	e shown after the checkbox for marketing				
Marketing Content	lf it is enabled, it will be sh Connect / Submit button o	nown on the second page after clicking the on the login page.				
	Enter the text to be displa	yed in the Terms and Conditions window.				
Language	Use the drop down menu					
	Browse - Select a propert					
	Upload - Click to upload a					
	Download - Click to down	lload a language file.				
	Login Method					
Layout	Components Login Method					
Connect Button Color 🔗	linear-gradient(to right, #ef5568	Dray Tek				
Connect Button Text 🔗	Connect 5					
	Click to Get Internet Access	¢≑ English (UK)				
		Welcome! Please log in to enjoy Wi- Fi.				
		Click to Get Internet Access				
		Connect Connect				
	#edfdD8					
	HEX	Cancel Previous Continue				
Connect		Through is selected as Landing Page Method.				
		Select the color of the connect button from the sing the RGB value (entered with the format of				
	button. The color of the te	nter the text to be displayed on the connect ext can be set from the predefined color list or red with the format of HEX).				
	Connect Button Color 🔗	linear-gradient(to right, #ef5568 0)				
	Connect Button Text 🔗	Connect 5				
	Enable Hint Message 🔗					
		Click to Get Internet Access				

	Welcome! Please log in to enjoy Wi- Fi.
	f Log in with Facebook
	Facebook Login (Login with Facebook) - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
Google	It is available when Google is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi.
	G Sign in with Google
	Google Login (Sign in with Google) - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
RADIUS	It is available when RADIUS Account is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi. Username Password
	RADIUS Username - Enter the account name for passing the RADIUS authentication.
	RADIUS Password - Enter the password for passing the RADIUS authentication.
	RADIUS Login Button Color - Select the color of the login button from the predefined color list, or using the RGB value (entered with the format of HEX).
	RADIUS Login Button Text - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
Submit	It is available when Leave Info is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi. information carrie_ni@draytek.com Agree Submit

	+Add		P	rofile Number Limit: 1
	Leave Info Type Text (Max: 170	characters)	Required	
	General Info 🔹 information			Ô
	Email • carrie_ni@dra	ytek.com] 0	Ē
	Checkbox • Agree] •	Ū
	Submit Button Color 🔗	#113100	5	
	Submit Button Text 🔗	Submit	5	
	Enable Hint Message			
	+Add - Click to add gener panel which will be show Submit Button Color - S	n on the login par elect the color of	nel as entry the submit l	oox or chec outton from
	panel which will be show	n on the login par elect the color of	nel as entry the submit l	oox or chec outton from
	panel which will be show Submit Button Color - S predefined color list, or u	n on the login par elect the color of ising the RGB valu nter the text to be be set from the p	nel as entry the submit l ie (entered v displayed o redefined co	box or chec button from vith the form n the subm
Enable Hint	panel which will be show Submit Button Color - S predefined color list, or u HEX). Submit Button Text - Er The color of the text can	n on the login par elect the color of using the RGB valu nter the text to be be set from the p the format of HEX	nel as entry the submit l ie (entered v displayed o redefined co	box or chec button from vith the form n the subm
Enable Hint Message	panel which will be show Submit Button Color - S predefined color list, or u HEX). Submit Button Text - Er The color of the text can RGB value (entered with	n on the login par elect the color of using the RGB valu nter the text to be be set from the p the format of HEX he hint message.	nel as entry the submit l ue (entered v displayed o redefined co ().	box or chec button from vith the form n the subm
	 panel which will be show Submit Button Color - S predefined color list, or u HEX). Submit Button Text - Er The color of the text can RGB value (entered with Click to enable / disable to 	n on the login par elect the color of using the RGB valu nter the text to be be set from the p the format of HEX the hint message. nce as a hint mess	nel as entry the submit l ue (entered v displayed o redefined co ().	box or chec button from vith the form n the subm
Message	 panel which will be show Submit Button Color - S predefined color list, or u HEX). Submit Button Text - Er The color of the text can RGB value (entered with Click to enable / disable to If enabled, enter a senter 	n on the login par elect the color of using the RGB valu nter the text to be be set from the p the format of HEX he hint message. nce as a hint mess nodification.	nel as entry the submit l ue (entered v displayed o redefined co ().	box or chec button from vith the form n the subm

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

	Profile Setup	Splash Page Customization (Optional)	3 Whitelist Setup (Optional)	
e: All NAT Rules Destin	ation Domain Destination IP Destina	tion Port Source IP Search		+Add
dex Type	Enable	Content		Action

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

		Profile Setup	2 Splash Page Customization (Optional)	3 Whitelist Setup (Optional)	
Type: All	NAT Rules Destination Domain	Destination IP Destination Port Source I	P Search		+ Add 🛛 🗎 Clear All
Index	Туре	Enable	Content		Action
1	NAT Rules 👻	\bigcirc		¥	1 Delete
	NAT Rules Destination Domain Destination IP				Cancel Previous Save

ltem	Description
+Add	Click to add a new whitelist profile.
Clear All	Click to remove all of the whitelist profiles.

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

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

RD8	~			DrayTek VigorACS 3		Capture Packets 👻	carrie System Administrator	С
Hotspot Web	Portal / Hotspot Prof	le						С
User Group :	RootGroup	*						
+Add								
Profile ID	Profile Name	↓↑ Enable	4 Login Method	41	Applied Interfaces	J↑ Action		
9	NYF_Carrie	Enabled	Click Through		LAN (1) WLAN 2.4G (1) WLAN 5G (1)	🖉 Edit 📋 Dele	te 🗅 Copy 📾 View Lo	og

8.5.2 Quota Management

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

(ADH ~		Dray Tek	VigorACS 3	Capture Packets · · System Administra	
Hotspot Web Portal / Quota Ma User Group : RDB	unagement.				ø
+Add Efforts				Profile Numb	er Limit: 1/20
Inde#® Profile Name	27 Expired Time After 128 Login	47 Idle Timeout	-7 Bandwidth Limit	47 Session Limit	10
1 Default	0d 6h 0m	(Unabled)	(Unitraited)	(United)	

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

Bandwidth Limit	Displays the number of bandwidth limit.
Session Limit	Displays the number of session limit.

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

Hotspot Web Portal / Quota Managerr User Group: RootGroup	nent	С
Add Quota Policy Profile		
Profile Name	OP_1	
Account Validity		
Expired Time After 1 st Login	0 days hours minutes	
Enable Idle Timeout		
Idle Timeout	0	
Device Control		
Devices Allowed	Unlimited ~ /account	
Enable Reconnection Restriction		
Restriction Type	Set Particular Time Set Time Period	
	$0 \sim$ hours $0 \sim$ mins	
	Block the same user from reconnecting for the set period	
	Cancel	Save

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

Limit	Download Limit - Enter a value to define the maximum data traffic (downloading) for each client connecting to Vigor device.
	Upload Limit - Enter a value to define the maximum data traffic (uploading) for each client connecting to Vigor device.
	Enable Session Limit - Click to enable and set session limit.
	 Session Limit - Enter a value to define the maximum sessions for each client connecting to Vigor device.
Cancel	Discard current modification.
Save	Save the current settings.

8.5.3 Network & Devices

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

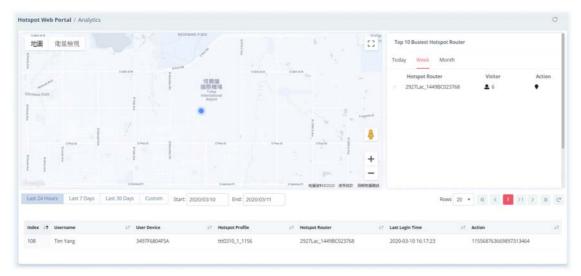
tspot Web Portal / Network & Device				Search Device Name / Model / MAC	C
er Group : rd8 🔹					
ame	Model Name	Hotspot Profile			
₫ rd8		As Parent	Ŧ		
▷ 🚠 rd8-1(0)		As Parent	Ŧ		
d rd8-2(0)		As Parent	•		
810_001DAA7D6514	VigorAP 810	Not Supported			
902_001DAA3D4F16	VigorAP 902	Not Supported			
130_001DAA83A094	Vigor130	As Parent	•		
130_001DAA8411C8	Vigor130	As Parent	•		
130_001DAA854204	Vigor130	As Parent	*		
130_001DAA8D3FA0	Vigor130	As Parent	*		
2120n+_001DAA0FE010	Vigor2120n+	As Parent	*		
2130Vn_001D000000E	Vigor2130Vn	As Parent	*		
2132FVn_001DAAE486C8	Vigor2132FVn	As Parent	•		
2133Vac_001DAA66E020	Vigor2133Vac	As Parent	•		
2620Ln_001DAA926F58	Vigor2620Ln	As Parent	•		
• 2710n_00507F9A3648	Vigor2710n	As Parent	*		
2830V_00507F708028	Vigor2830V	As Parent	*		

These parameters are explained as follows:

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

8.5.4 Analytics

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



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

Applications

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

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

RD8	~	Dray Te
Root Network(241))	a x
	Model	
₩ RD5(9)		AP 910C_001DAA7F5D8C
器 RD6(2)		AP 912C_001DAA72E14A
윪 RD7(15)		AP 918RPD_001DAA3F580C
		AP 920R_001DAA632C78
묾 RD999(3)		BX 2000ac_001DAAD7EC88
욺 SEG1(1)		Español_2832n_001DAAE60E00
😸 Shanghai(15)		▲ G2500_001DAA4C194F

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

(7)	Configuration / AP Profile				
000	Configuration				
<u>-</u>	VPN		Action		
	AP Profile		🖉 Edit 🗴 🛍 Delete	Duplicate	🗇 Сору То
ţţţ	Load Balance (SD-WAN)				
	Route Policy (SD-WAN)				
	VOIP WAN (SD-WAN)				
Z					
	Device Provisioning				
\$	Name	Model Name	Last Provisioned	Status	AP Profile
	🖌 🧰 RD8				T
-	AP 1000C_001DAA04F06C				

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

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

AP 920R_001DAA632C78	VigorAP 920R		Marketi •
VigorAP900	VigorAP 900		(As Parent) Root Network-UK-Copy-edit Marketing_came
			Refresh Sav

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

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

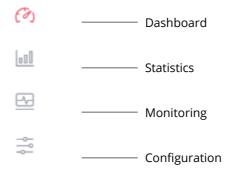


Device Menu



Chapter 9 Device Menu

On the dashboard for CPE, the Device menu contains:



9.1 Dashboard for CPE

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

Root Network(241)				
	Model			
& RD8(49)		品 jaytest(4)		
島 RD999(3)				
& SEG1(1)		& robin_test(2)		
🍇 Shanghai(15)		쑳 yrc_testing(2)		
💑 Test1 & Test2(1)			E486C8	
		2133Vac_001DAA	66E020	
& USA(1)				
ñ				

2862Vac_001DAAF7C0E0	Dray Tek	VigorACS 3	🖬 Captore Paci	carrie C System Administrator
2862Vac_001DAAF7C0E0		Device Status: online	Alarms: 0 Active Clients	0 Auto Refresh: 1 Minute 🗸 🖓
Port Status		WAN Overview		③ Last 24 hours-
ACT WARL Live SISTING USB DR. Procet Salar 24G IS Passed		1 Byte		0 Total
Device Information		0 Byte	08:00	
Device Name	2862Vac_001DAAF7C0E0 https://0.0.0.443	LAN Overview		③ Last 24 hours-
Network Name	RDS			
Model	Vigor2862Vac	1		Active Clients
Firmware Version				
MAC Address	001DAAF7C0E0			
Up Time		0	08:00	
	~ show more :	LAN	it pymask	31 DHCP
Connectivity and Alerts	0'a		No data available	
Id 🔤 Start Time	it ClearTime It type it Message it			- show more
	An data available	Port Status () Interface : Status : Up Time : Tx Rate: 1	Tx Enabled 🖛 Tx Drops 👌 Rx D	

9.2 Statistics for CPE

Statistics is available for a selected group network or CPE.

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

Statistics					C
Last 24 Hours Last 7 Days	Last 30 Days Custom Start 20	20/09/23 End: 2020/09/24			Export
Usage Overview		- / ×	Wireless Clients Overview		- 2 ×
Total Number of Clients 3	Wireless Clients 0 (0%)	Wired Clients 3 (100%)			
Total amount of Traffic 2.27 GB	Download 2.19 GB (96.6%)	^{Upload} 78.25 MB (3.4%)	Band	SSID	05
Max. Number of Concurrent Clie	nt Avg. Numb 2	er of Daily Client 🚱	2 .46 5 6	No Data	Android IVS Windows
Clients		- 2 ×	Traffic		- 2 ×
		OWired OWireless O2.46 O56			Wired OWireless O2.46 O56
4			119.21 MB		
1		١٨٨٨ ٨٨/	95.37 MB 71.53 MB		
2		VVVVVV	47.68 MB		
1			23.84 MB		
			0 Byte		1 la
16:00 18:00 20:00	22:00 00:00 02:00 04:00 0	6:00 08:00 10:00 12:00 14:00	16:00 18:00 20:00 22:0	0 00:00 02:00 04:00 06:0	0 08:00 10:00 12:00 14:00

9.3 Monitoring

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

(7)	Monitoring	
00	Alarm	
5	Logs	
	Diagnostics	
Z		

9.3.1 Alarm

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

Monitorin	g / Alarm						2020/02/15 to 2020/03/16 ~	search No. / Device Name / MA Q
Alarm	History							
BDelete.	Delete All	d.Download					id	< 1 /1 > N C 0
	No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type
					No data available			

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

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

9.3.2 Logs

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

onitori	ng / Logs						2020/02/15 to 2020	/03/16 v search ID / Device Name / Devi C
CPE Acti	Device Re	boot Reboot By CPE	Reset System Password	Set Parameter	File Transfer Setting Profile	Device SysLog CPE Notify	Device Register	Device Operate
Delete	Delete All	⊌Download						KI < 1 /2 > N C ⊗
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
	2968439	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Set Parameter Values	13923	2020/03/06 05:18:11 PM
	2968051	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Set Parameter Values	13788	2020/02/24 05:25:40 PM
	2968049	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Set Parameter Values	13786	2020/02/24 02:42:06 PM
	2968041	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Set Parameter Values	13783	2020/02/24 02:37:23 PM
	2968040	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	42	2020/02/24 02:37:21 PM
	2968039	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	41	2020/02/24 02:37:20 PM
	2968038	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	40	2020/02/24 02:37:19 PM
	2968037	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	39	2020/02/24 02:37:18 PM
	2968035	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	38	2020/02/24 02:37:16 PM
	2968033	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	37	2020/02/24 02:37:15 PM
	2968031	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	36	2020/02/24 02:37:13 PM
	2968029	2865ac_001DAA41DF78	141326	001DAA41DF	192.168.105.67	Add Object	35	2020/02/24 02:37:12 PM

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

9.3.3 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of Vigor router. Here, Vigor2865 series is used as an example.

9.3.3.1 Ping

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

Ping	2865ac_001DAA41DF78 / Monitoring / Diag	nostics	с
Trace Route	Protocol	•	
Routing Table	IP Address / Domain		
ARP Table			
DHCP Table	Ping Through	•	
Sessions Table		Auto WAN1 WAN2 WAN3 WAN4	Run

These parameters are explained as follows:

ltem	Description
Protocol	Choose IPV4 /IPV6 for ping action.
Ping Through	Use the drop down list to choose the interface (e.g., WAN, LTE) that you want to ping through or choose Auto to be determined by the router automatically.
For IPv4	
Ping To	Enter the IPv4/IPv6 address of the host/IP that you want to ping.
Source IP	Use the drop down list to specify a source IP. If Auto is selected,
IP Address	If Host/IP is selected as Ping To, you have to enter the IPv4 address of the host that you want to ping.
For IPv6	
IP Address	Enter the IPv6 address of the host that you want to ping.
Run	Click to start the ping work. The result will be displayed on the screen.

9.3.3.2 Trace Route

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

← Monitoring	2927Vac_1449BC117B60 / Monitoring	g / Diagnostics	С
Ping	Туре	IPV4 IPV6	
Routing Table	Trace through	Auto ~	
ARP Table	Protocol	ICMP UDP	
DHCP Table	Host / IP Address		
Sessions Table			
		Ra	in
			_

ltem	Description
Туре	Click IPv4 or IPv6 to display corresponding information for it.

Trace through	Select an interface for tracing through. It is available when IPv4 is selected as the Type.
Protocol	Click ICMP or UDP that you want to ping through.
Host / IP Address	Enter the IPv4/IPv6 address or domain name of the host.
Run	Click to start route tracing work.

9.3.3.3 Routing Table

This page displays the routing information for the selected CPE.

2865ac_00						
IPv4 Rou	iting Table					
Index	Destination	Subnet Mask	Gateway		Key	Iface
1	0.0.0.0	0.0.0.0	192.168.105.1		*	WAN2
2	192.168.105.0	255.255.255.0	directly connected		С	WAN2
e 3	192.168.67.0	255.255.255.0	directly connected		C~	LAN1
4	192.168.2.0	255.255.255.0	directly connected		C~	LAN2
	: Connected S: Static R: RIP *: defau Iting Table	It ~: private B: BGP				
IPv6 Rot	uting Table	\square	Flags	Metric	Next Hop	ρ
IPv6 Rou show De	uting Table	\square	Flags U	Metric 256	Next Hop	р
IPv6 Rol Show De Destination	n Prefix Length	n Interface				р
IPv6 Rot Show De Destinatio FE80:	uting Table n Prefix Length 64	n Interface	U	256		p
Destination FEBO:: FEBO::	uting Table n Prefix Lengt 64 64	n Interface LAN1 LAN2	U U	256 256	:	P
Destination FEBO:: FEBO:: FEBO:: FEBO::	uting Table n Prefix Length 64 64 64 64	n Interface LAN1 LAN2 LAN3	U U U	256 256 256	:	p
Destination FEBO: FEBO: FEBO: FEBO: FEBO:	uting Table n Prefix Length 64 64 64 64 64 64	h Interface LAN1 LAN2 LAN3 LAN4	U U U U	256 256 256 256	:	p

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

9.3.3.4 ARP Table

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

<- Configuration	3220n_	001DAA554758 /	Monitoring / Diagnos	tics								1.5
	1 PCuar											
Trace Route	LAN	WAN										
Routing Table												
	Show	MAR .		ALL WANS		¥						
	Index		MAC Address		HOST ID	intertace	YLAN	Port	Device	Description	Comment	
Services Table	1	192.168.305.52	00-10-AA-F8-D8-19			WANI	-	-				
	2	192.168.105.62	00-10-AA-F7-C0-E2			WANL	-	-				
	3	192.168,105.71	00-50-77-F1-00-16			WANL	-	-				
	4	192.168.105.77	00-10-AA-65-33-0A			WANL	-	-				
	5	192.168.105.96	00-10- AA -8A-85-C9			WAN1	-	127				
	6	192.168.105.97	00-10-AA-8A-8E-51			WAN1		140				
	7	192.168.105.100	02-04-08-81-C3-88			WAN1	1.111	221				
		192.148.105.103	00-10-AA-3F-58-0C			WANI	-					
	۰	192.168.105.120	14-49-80-02-37-21			WANI		-				
	10	192.168.105.142	00-50-7F-CC-3E-51			WANI	-	100				
	.11	192.168.105.144	00 1D AN E4-86 CE			WANI	-	-				
	12	192,168,105,145	00-50-7F-70-80-2A			WANI		1.00				
	13	192.168.105.146	00-10-AA-70-9C-CA			WANL	-	1.0				
	14	192.168.105.148	00-10-AA-41-07-7A			WAN1	<u>842</u> 1	144				
	15	192.168.105.149	00-10-AA-41-DF-C2			WANL	-	223				
	15	192.168.105.180	00-10-AA-CB-AO-32			WANI	1776	050				
	17	192.168.105.225	00-18-11-19-6F-70			WANL		-				

These parameters are explained as follows:

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

9.3.3.5 DHCP Table

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

Ping	2865ac_001DAA	2865ac_001DAA41DF78 / Monitoring / Diagnostics						
	IPv4 Addres	s Assignment Table						
	Name	IP	Mask	Start IP	End IP	DHCP Server		
	LAN1	192.168.67.1	255.255.255.0	192.168.67.10	192.168.67.209	On		
	LAN2	192.168.2.1	255.255.255.0	192.168.2.10	192.168.2.109	On		
	IPv6 Addres	s Assignment Table						
	Interface	IPv6 Address	IAID	Link-Layer Address	Leased Time	DUID		
				No data available				

ltem	Description
IPv4 Address Assignment Table	Displays the IP assignment status including LAN number, IP address, mask address, start IP, end IP and DHCP server on/off.

IPv6 Address Assignment Table Displays the IP assignment status including interface, IPv6 address, IAID, link-layer address, leased time and DUID.

9.3.3.6 Sessions Table

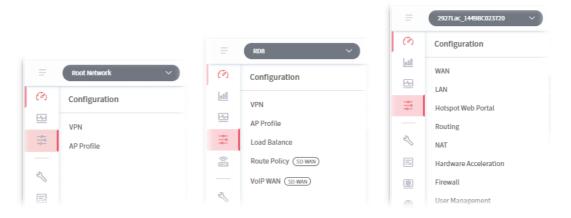
This page displays the private IP, private port number, pseudo port number, the peer IP, the peer port, the connected interface of the remote client communicating with the selected CPE.

2	865ac_001DAA000	000 / Monitoring / Diagnostics					
	Index	Private IP	Private Port	Pseudo Port	Peer IP	Peer Port	Interface
	1	192.168.65.10	64041	65321	17.57.145.21	5223	WAN2
	2	192.168.65.10	31647	32927	8.8.8.8	53	WAN2
	3	192.168.65.10	64497	33009	13.94.40.40	443	WAN2
	4	192.168.65.10	64720	33232	8.8.8.8	53	WAN2
	5	192.168.65.10	49294	50574	52.139.233.255	443	WAN2
	6	192.168.65.10	49675	50955	35.201.124.9	443	WAN2
	7	192.168.65.10	49680	50960	172.16.2.8	5222	WAN2
	8	192.168.65.10	49726	51006	162.247.242.20	443	WAN2
	9	192.168.65.10	49729	51009	139.59.210.197	443	WAN2
	10	192.168.65.10	50015	51295	91.108.56.174	443	WAN2
	11	192.168.65.10	50016	51296	91.108.56.174	443	WAN2
	12	192.168.65.10	50379	51659	52.139.233.255	443	WAN2
	13	192.168.65.10	50381	51661	52.139.233.255	443	WAN2
	14	192.168.65.10	50665	51945	209.206.62.33	443	WAN2
	15	192.168.65.10	50814	52094	209.206.62.33	443	WAN2
	16	192.168.65.10	50844	52124	3.222.91.6	443	WAN2
	17	192.168.65.10	50845	52125	3.222.91.6	443	WAN2
	18	192.168.65.10	50886	52166	192.229.232.200	443	WAN2
	19	192.168.65.10	50896	52176	3.222.91.6	443	WAN2
	20	192.168.65.10	50913	52193	14.226.250.7	8888	WAN2
	21	192.168.65.10	50917	52197	14.186.47.236	8080	WAN2
	22	192.168.65.10	50922	52202	52.114.132.23	443	WAN2
	23	192.168.65.10	50924	52204	14.226.250.7	8888	WAN2

9.4 Configuration

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

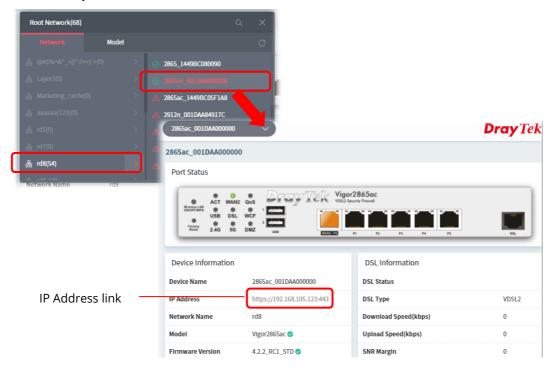
Available configuration settings will vary for root network, group network and specified CPE.



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

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

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



The menu items for Configuration will vary based on the selected CPE (AP / router). Here, we take Vigor2865ac as an example.

=	2865ac_001DAA000000 ~	
(3)	Configuration	
000	WAN	
<u></u>	LAN	
*#	Hotspot Web Portal	1
	Routing	
Z	NAT	
	Hardware Acceleration	
	Firewall	
	User Management	
\$ \$ \$	Objects Setting	

(1) If the administrator wants to access into the web user interface of the selected CPE, click the IP address link of the selected CPE on the CPE dashboard.

9.4.1 WAN

WAN settings relate to access Internet for CPEs.

9.4.1.1 Internet Access

<- Configuration	2865Lac_1	4498C0D8	FOO / Configurat	ion / WAN							с
States Since	Alarm	index	Display Name	Physical Mode	Access Mode		Status	Bandwidth(kbps) DownLink/UpLink	Ping Latency	Ping Jitter	Ping Pkt Loss
	Disable	WAN1		DSL	PPPoE		Enable	0/0	0	0	0
Connection Detection	Disable	WAN2		Ethernet	Static or Dynamic I	P	Enable	0/0	648	776	0
Multi-PVC/MLAN	Disable	WAN3		Wireless 2.4G	None		Enable	0/0	0	0	0
WAN FVG	Disable	WAN4		Wireless 5G	None		Enable	0/0	0	0	0
WAN Budget	Disable	FLE		USB	3G/4G USB Modern	(DHCP mode)	Enable	0/0	0	0	0
DHCP Client Option IPv6	Disable	WAN6		USB	3G/4G USB Modern	(DHCP mode)	Enable	0/0	0	0	0
	Mode Line Spe Weight 1 Downloa Latency Jitter We Pit Loss	Type Weight ad Weight Weight Weight Weight Latency		Au Con Low Low Low Low Low Low		V V High High High High High High High	er ange. No as LAR.				Ø Save

ltem	Description						
Table	Alarm - Display if the alarm function is enabled or disabled.						
	Index - Displays the index number of the WAN interface.						
	Display Name - Displays the description for the WAN interface.						
	Physical Mode - Display the physical mode (e.g., Wireless 2.4G / Wireless 5G) of the interface.						
	Access Mode - Displays the access mode for the WAN interface.						
	Status - Displays if the WAN interface is enabled or disabled.						
	Bandwidth(Kbps)DownLink/UpLink - Displays the downlink / uplink bandwidth ratio.						
	Ping Latency / Ping Jitter / Ping Pkt Loss - Displays the latency / jitter / packet loss value.						
Load Balance Setup	Mode - The default is IP Based. Choose Session Based to get better transmission speed.						
	Line Speed - Choose Auto Weight to let the router reach the best load balance. According to Line Speed to let the router reach the best load balance based on line speed.						
	Weight Type - Choose Bandwidth-Based / Quality-Based / Reliability-Based as the weight type. Or choose Custom to define Upload Weight, Download Weight, Latency Weight, Jitter Weight, Pkt Loss Weight respectively.						
	 Upload / Download Weight- The higher the weight is, the WAN interface with higher bandwidth will get higher usage. 						
	• Latency Weight - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower latency will get						

	 higher usage. Jitter Weight - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage.
	 Pkt Loss Weight - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower packet loss will get higher usage.
Save	Save the current settings.

To modify the general setup settings for each WAN, move the mouse cursor on the WAN# under Index and Click to open the following page.

2865Lac_1449BC0D8F00 / Configuration /	WAN	C
General Setup		
Alarm	Show alarm message when this WAN interface disconnects.	
Enable		
Display Name		
Physical Mode	DSL	
DSL Mode	Auto ~	
DSL Mode Code	Default ~	
Enable Load Balance		
Active Mode	Always On Failover	
VLAN Tag Insertion	0	
VDSL2 VLAN Tag Insertion	0	
VDSL2 Service VLAN Tag Insertion	\bigcirc	
Access Mode	None PPPoE Static or Dynamic IP	
PPPoE MTU	1492	
Path MTU Discovery	D	
	Cancel	Save

ltem	Description
	General Setup
Alarm	Click to show/hide an alarm message.
Enable	Click to enable/disable settings of the WAN interface.
Display Name	Enter the description for the interface.
Physical Mode	Display the physical mode (e.g., DSL) of the interface.
DSL Mode	Specify the physical mode (Auto, VDSL or ADSL) for the router manually.
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection. If you have no idea about the selection, simply choose Default or contact the dealer for assistance.
Enable Load Balance	Click to enable auto load balance function for this WAN interface.
Active Mode	Always On - Make the WAN connection being activated always. Failover - Make the WAN connection as a backup connection.
Failover	It is available when Failover is selected as Active Mode.

	Backup WAN - When the active WAN failed, such WAN will be activated as the main network connection.
	Active When - It is available when Failover is selected as Active Mode.
	• Any - The backup WAN will be activated when any master WAN interface disconnects.
	• All - The backup WAN will be activated only when all master WAN interfaces disconnect.
	Backup Type - Choose Fails to connect or Meet Any/all of the following condition. When Meet Any/all of the following condition is selected:
	 Meet of the following conditions - If the packet meets any one of the conditions, the failover WAN will be enabled; if the packet meets All of the conditions, the failover WAN will be enabled.
	• Upload traffic / Download traffic - Set the values for upload and download respectively.
	• Latency - After selecting Check Latency, enter a value as a threshold.
	• Jitter - After selecting Check Jitter, enter a value as a threshold.
	 Packet loss After selecting Check Packet loss, enter a value as a threshold.
	When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
VLAN Tag Insertion / VDSL2 VLAN Tag Insertion / VDSL2 Service VLAN Tag Insertion	Click to enable the function of VLAN with tag.
Access Mode	Set the access mode for this WAN.
	None - No mode used.
	PPPoE - Click to select PPPoE as the accessing protocol of the Internet.
	• PPPoE MTU - Set a number as the Max Transmit Unit for packet.
	Static or Dynamic IP - Click to select a static IP or use dynamic IP as the accessing protocol of the Internet.
	• Static IP MTU - Set a number as the Max Transmit Unit for packet.
Path MTU Discovery	Click to enable the path MTU discovery function for this WAN interface.
	• Path MTU to – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox.
	 MTU size start from – Determine the starting point value of the packet.
	• MTU reduce size by – Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached.
	Modem Settings (for ADSL only)
Multi-PVC channel	The selections displayed here are determined by the setting page of Multi-PVC/VLAN . Select M-PVCs Channel means no selection will be chosen.
VPI/VCI	Enter the value provided by ISP.
· · · _	
Encapsulating Type	Choose the type provided by ISP.

Protocol	Choose the one (PPPoE or PPPoA) provided by ISP.		
Modulation Type	Default setting is Multimode.		
	Choose the one that fits the requirement of your router.		
	PPPoE (available when PPPoE is selected as the Protocol		
For Wired LAN / For Wireless LAN	 For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN – It is available for <i>n</i> model. If you check this box, PCs on 		
	the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.		
PPP Service Name / PPP User Name / PPP Password	Enter the service name, username and password provided by ISP.		
Schedule Setup(1-15)	Enter four sets of time schedule for your request.		
PPP Authentication	Select PAP only or PAP or CHAP for PPP.		
Fixed IP Enable	Click Yes to enable the fixed IP setting.		
	Or, click No to disable the fixed IP setting.		
Fixed IP Address	Enter a fixed IP address in the box.		
	Static or Dynamic IP (available when Static or Dynamic IP is selected as the Connection Mode)		
Connection Type	 DHCP - Click to obtain the IP address automatically. Router Name - Enter the router name provided by ISP. Domain Name - Enter the domain name that you have assigned. DHCP Client Identifier - Click to enable and specify username and password as the DHCP client identifier for some ISP. Static - Click to specify some data. 		
	 IP Address - Enter the private IP address. Subnet Mask - Enter the subnet mask. 		
Primary DNS Server / Secondary DNS Server	• Subnet Mask - Enter the subnet mask.		
Secondary DNS	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary 		
Secondary DNS Server	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. 		
Secondary DNS Server Enable RIP	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. Click to enable the RIP function. Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded. Enable Firewall - If enabled, all of the filter rules defined and 		
Secondary DNS Server Enable RIP Enable Bridge Mode Enable Full Bridge	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. Click to enable the RIP function. Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded. Enable Firewall - If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. Click to make the router work as a bridge modem which is able to 		
Secondary DNS Server Enable RIP Enable Bridge Mode Enable Full Bridge Mode	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. Click to enable the RIP function. Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded. Enable Firewall - If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. Click to make the router work as a bridge modem which is able to forward incoming packets with VLAN tags. 		
Secondary DNS Server Enable RIP Enable Bridge Mode Enable Full Bridge Mode	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. Click to enable the RIP function. Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded. Enable Firewall - If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. Click to make the router work as a bridge modem which is able to forward incoming packets with VLAN tags. Make a bridge between the selected LAN subnet and such WAN interface. 		
Secondary DNS Server Enable RIP Enable Bridge Mode Enable Full Bridge Mode Bridge Subnet	 Subnet Mask - Enter the subnet mask. Gateway IP Address - Enter gateway IP address. Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. Click to enable the RIP function. Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded. Enable Firewall - If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. Click to make the router work as a bridge modem which is able to forward incoming packets with VLAN tags. Make a bridge between the selected LAN subnet and such WAN interface. 		

Cancel	Discard current modification.
Save	Save the current settings.

9.4.1.2 Connection Detection

This page displays physical mode and access mode for each WAN interface.

2865ac_001DAA41DF78	~	Dray Tek VigorACS 3	Carrie Capture Packets > System Administrator
	2865ac_001DAA41DF	78 / Configuration / WAN	Ø
	Index	Physical Mode	Access Mode
	WAN1	DSL	PPPoE
	WAN2	Ethernet	Static or Dynamic IP
	WAN3	Wireless 2.4G	None
	WAN4	Wireless 5G	None
	WAN5	USB	None
	WAN6	USB	None

These parameters are explained as follows:

ltem	Description		
Index	Displays the index number of the WAN interface.		
Physical Mode	Displays the physical connection for WAN interfaces according to the real network connection.		
Access Mode	Displays the accessing mode of the Internet.		

To modify the setting, move the mouse cursor to any entry and click to open the setting page.

Configuration	2865ac_001DAA000000 / Configur	ation / WAN	
met Accesa	WAN Connection Detection		
FINCMLAN	Index	1	
	Mode	Ping Detect ~	
Budget	Primary Ping IP	PPP Detect Ping Detect	
	Secondary Ping IP	0.0.0	
	Ping Gateway IP	0	
	m	255	
	Ping Interval	1	
	Ping Retry	10	
	Link Condition Detection		
	Mode	Ping Detect ~	
	Primary Ping IP	8.8.8.8	
	Secondary Ping IP	8.8.4.4	
	Ping Interval	10	
			Cancel Save

ltem	Description	
WAN Connection Detection		

Index	Displays the index number of the WAN interface.		
Mode	Choose PPP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.		
	• Primary / Secondary Ping IP - Enter the Primary or Secondary IP address in this field for pinging.		
	 Ping Gateway IP - Use the WAN gateway IP address for pinging. Vigor router can check if the WAN connection is on or off. 		
	• TTL - Set TTL value of PING operation.		
	• Ping Interval - Enter the interval for the system to execute the PING operation.		
	• Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.		
	Link Condition Detection		
Mode In order for the system to detect the latency, jitter, and packet- for each WAN interface, you have to specify the IP transmitting through the interface.			
	Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option.		
Primary Ping IP	Enter an IP address.		
Secondary Ping IP	Enter an IP address.		
Ping Interval	Set a time interval (unit: second) for the system to ping the IP address specified above.		
Cancel	Discard current modification.		
Save	Save the current settings.		

9.4.1.3 Multi-PVC/VLAN

This page allows you to configure multiple permanent virtual circuits (PVCs) and ATM QoS for channels using ADSL.

Configuration	2865ac_001DA	A000000 / Configuration / WAN							c (
Internet Access	Channel	General Enable	WAN Type	V71	VCI	Qo5 Type	Protocol	Encapsulation	
nemet Access	7	false	VDSL	1	47	UBR	PPPoA	VC_MUX	
Connection Detection	8	talse	VDSL	1	48	UBR	PPPoA	VC_MUX	
	9	talse	VDSL	1	49	UBR	PPPoA	VC_MUX	
WAN IPv6	10	false	VDSL	1	50	UBR	PPPoA	VC_MUX	
	11	talse	VDSL	1	51	UBR	PPPoA	VC_MUX	
NAN Budget	12	talse	VDSL	1	52	UBR	PPPoA	VC_MUX	
	11	talse	VDSL.	1	53	UBR	PPPoA	VC_MUX	
	14	talse	VDSL	1	54	UBR	PPPoA.	VC_MUX	
	15	false	VDSL.	1	55	UBR	PPPoA	VC_MUX	
	16	false	VDSL.	1	56	UBR	PPPoA	VC_MUX	

To modify the setting, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / WAN		C
Channel	7	
Enable	•	
General Settings		
WAN Type	VDSL ~	
VLAN Tag	0	
Priority	0 ~	
Port-based Bridge		
Open Port-based Bridge Connection	D	
WAN Interface for this Channel		
Open WAN Interface	\Box	
		Cancel Save

Item	Description			
Channel	Display the number of the channel.			
Enable	Click to enable or disable the channel.			
	General Settings			
WAN Type	Specify a WAN type of the PVC Channel/VLAN.			
VLAN Tag	Enter the value as the VLAN ID number.			
Priority	Choose the number to determine the packet priority for this VLAN. The range is from 0 to 7.			
	Port-based Bridge			
Open Port-based	Click to enable or disable the function.			
Bridge Connection	If enabled, you have to enter required settings for the following items.			
	Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.			
	WAN Interface for this Channel			
Open WAN Interface	Click to enable or disable the function.			
•	If enabled, you have to enter required settings for the following items.			
	WAN Application -			
	 Management - The configuration for this VLAN will be effective for Web configuration/telnet/TR069. 			
	• IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.			
	Mode - Select ARP Detect or Ping Detect. If Ping Detect is selected, you			
	have to set the following options.			
	• Primary Ping IP / Secondary Ping IP - Enter Primary or Secondary IP address in this field for pinging.			
	• Ping Gateway IP - Enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.			

	• TTL - Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
	 Ping Interval - Set a time interval (unit: second) for the system to ping the IP address specified above.
	• Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
	WAN Setup - Choose Static_or_Dynamic_IP or PPPoE/PPPoA.
WAN IP Network	It is available when Static_or_Dynamic_IP is selected as WAN Setup.
Settings	Auto IP - Click to enable / disable the settings.
	If Auto IP is enabled, you have to enter required settings for the following items.
	• Router Name - Enter the router name provided by ISP.
	• Domain Name - Enter the domain name provided by ISP.
	If Auto IP is disabled, you have to enter required settings for the following items.
	• IP Address - Enter the IP address.
	• Subnet Mask - Enter the subnet mask.
	• Gateway - Enter gateway IP address.
	Primary DNS IP - Enter the primary IP address for the router if you want to use Static IP mode.
	Secondary DNS IP - If necessary, Enter secondary IP address for necessity in the future.
ISP Access Setup	It is available when PPPOE/PPPOA is selected as WAN Setup.
	ISP Name - PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank.
	Username - Name provided by the ISP for PPPoE/PPPoA authentication.
	Password - Password provided by the ISP for PPPoE/PPPoA authentication.
	Authentication - Choose the protocol used for PPP authentication.
	Always On - The router will maintain the PPPoE/PPPoA connection.
	Fixed IP - If enabled, the IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN.
	Fixed IP Address - Enter an IP address.
Cancel	Discard current modification.
Save	Save the current settings.
	-

9.4.1.4 WAN IPv6

This page allows to configure IPv6 settings for each WAN interface.

Internet Access	2865ac_001DAA151EB8 / Configuration / WAN			
	Index	Physical Mode	Connection Type	
	WAN1	DSL	Offline	
	WAN2	Ethernet	PPP	
	WAN5	USB	Offline	
	WAN6	USB	Offline	

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the WAN interface.
Physical Mode	Displays the physical connection for WAN interfaces according to the real network connection.
Access Mode	Displays the accessing mode of the Internet.

To modify the IPv6 setting, move the mouse cursor to any entry (WAN1/WAN2/WAN5/WAN6) and click to open the setting page.

2865ac_001DAA151EB8 / Config	uration / WAN		
Basic			
Connection Type	Offline	•	
	Offline		
	TSPC AICCU DHCPv6 Client		Cancel Save
	Static IPv6 6in4 Static Tunnel 6rd		

Offline

When Offline is selected, the IPv6 connection will be disabled.

PPP

2865Lac_1449BC0D8F00 / Configuration / WAN		
Basic		
Connection Type	ppp v	
RIPng Protocol	O	
WAN Connection Detection		
Mode	Ping Detect ~	
Ping IP/Hostname		
TTL(1-255,0:Auto)	0	
		Cancel Save

TSPC

2865Lac_1449BC0D8F00 / Configuration / WAN		
Basic		
Connection Type	TSPC ~	
TSPC		
Username		
Password	•	
Tunnel Broker		
WAN Connection Detection		
Mode	Ping Detect ~	
Ping IP/Hostname		
TTL(1-255,0:Auto)	0	
		Cancel Save

AICCU

2865Lac_1449EC0D8F00 / Configuration / WAN	
Basic	
Connection Type	AICCU ~
connection type	ACCU
AICCU	
Always On	D
Username	
Password	↓
Tunnel Broker	Ec.shos.net
Turnal ID	
Suhnet Prefix	/ 0
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
T⊤L(1 255,0:Auto)	0
	Cencel Save

DHCPv6 Client

2865Lac_1449BC0D8F00 / Configuration / WAN	
D :	
Basic	
Connection Type	DHCPv6 Client ~
IAID	0
DUID	000300011449bc0d8f01
Authentication Protocol	None ~
RIPng Protocol	
Enable Bridge Mode	0
Enable Firewall	\bigcirc
Bridge Subnet	LANI ~
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

Static IPv6

2865Lac_1449BC0D8F00 / Configuration / WAN				
Basic				
Connection Type	Static IPv6	~		
Static IPv6				
Current IPv6 Address Table				
Index IPv6 Address		Prefix Length	Action	
1			+ Add	
IPv6 Gateway Address	:			
RIPng Protocol	\bigcirc			
Enable Bridge Mode				
Enable Firewall	\bigcirc			
Bridge Subnet	LAN1	Ý		
WAN Connection Detection				
Mode	Ping Detect	~		
Ping IP/Hostname				
TTL(1-255.0:Auto)	n			
				Cancel Sav

6in4 Static Tunnel

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Dasic	
Connection Type	6in4 Static Tunnel V
Remote Endpoint IPv4 Address	IPv4 format (IX: 123.12.1.1)
6in4 IPv6 Address	/ 64
LAN Routed Prefix	/ 64
Tunnel TTL	255
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

6rd

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Connection Type	6rd ~
6rd	
Mode	Static_6rd v
IPv4 Border Relay	IPv4 format (EX: 123.12.1.1)
IPv4 Mask Length	0
6rd Prefix	
6rd Prefix Length	64
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

The parameters for connection type (PPP to 6rd) are explained as follows:

ltem	Description
	PPP
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	• Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	• TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	TSPC
TSPC	Username - Enter the name obtained from the broker.
	Password - Enter the password assigned with the user name.
	Tunnel Broker - Enter the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	• Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	• TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	AICCU

AICCU	Always On - Check this box to keep the network connection always.
Alco	Username - Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.
	Password - Enter the password assigned with the user name.
	Tunnel Broker - It means a server of AICCU. The server can provide IPv6
	tunnels to sites or end users over IPv4.
	Tunnel ID - One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394). Enter the ID offered by Tunnel Broker.
	Subnet Prefix - Enter the subnet prefix address obtained from service provider.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	DHCPv6 Client
DHCPv6 Client	IAID - Enter a number as IAID.
	Authentication Protocol - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key , Delayed and None . In general, the default setting is None.
	 Key ID – Enter a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.
	 Realm – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.
	• Secret –Enter a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.
	RIPng Protocol - RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.
	• Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.
	Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

	 TTL (Time to Live) – If you choose Ping Detect as detection mode, you have to type TTL value.
Cancel	Discard current modification.
Save	Save the current settings.

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

9.4.1.5 WAN Budget

WAN Budget determines the data *traffic volume* for each WAN interface respectively to prevent overcharges for data transmission by the ISP.

nlornet Access	Gener	al Setup Status											
onnection Detection	Index	WAN Budget Enable	Quota Limit	Limit Unit	Shutdown WAN interface	Cycle Mode	Monthly Cycle Day	Monthly Cycle Hour	User Defined Cycle Days	User Defined Cycle Hours	User Defined Current Day	Notification Object	US
ILI PVCMLAN	WAN1	false	0	MD	false	Monthly	1	00.00	1	0	1		w
	WAN2	fatse	0	MB	false	Monthly	1	00:00	3	0	1	-	w
AN 1946	WAN3	fatse	0	MB	false	Monthly	1	00-00	1	D	1		w
	WAN4	false	0	MB	false	Monthly	1	00:00	1	0	1		w
HCP Client Option IPv6	LTE	false	0	MB	false	Monthly	1	00:00	1	0	1		W
	WANG	false	0	MB	false	Monthly	1	00:00	1	0	1	-	w
	0.	otec											
		1. The budget traf											
		• 2. When hardware	r acceleration (hered have by ser	sed, the monitored WAH Is	affic of Elliser	ned WAN Interferen in	may be slightly inacco					

To modify the budget profile setting, move the mouse cursor to any entry (index 1 to index 6) and click to open the setting page.

able		
iota Limit	0 M ~	
utdown WAN Interface		
otification Object	v	
cle Mode	Monthly Custom	
able	Use Cycle in hours Use Cycle in days 🗸	
er Defined Cycle Days	1 ~	
er Defined Current Day	1 ~	
er Defined Reset Hours	00:00 ~	
 Note: 1. Please make sure the Time an 2. SMS message and mail will be 	d Date of the router is configured. sent when the usage reaches 95% and 100% of quota.	

ltem	Description
Enable	Click to enable the budget function.
Quota Limit	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
Shutdown WAN Interface	Click to let all the outgoing traffic through such WAN interface be terminated.
Notification Object	The system will send out a notification based on the content of the

	notification object.
Cycle Mode	 Choose Monthly or Custom to define the billing cycle according to request. Monthly is default setting. If long period or a short period is required, use Custom. The period of cycle duration is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.
Monthly Cycle Day /	It is available when Monthly is selected as Cycle Mode.
Monthly Cycle Hour	Set the day and time in a month.
Enable	It is available when Custom is selected as Cycle Mode.
	Use Cycle in hours - Set a time cycle (including days and hours) for Vigor CPE to reset the data record automatically.
	 User Defined Cycle Days - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.
	 User Defined Cycle Hours - Select a number (0~23) of the hours for a cycle. For example, 12 means 12 hours. Based on the cycle days and cycle hours settings, Vigor CPE will reset the data record once reaching 7 days and 12 hours.
	• User Defined Current Day - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.
	Use Cycle in days - Set a cycle (with days) for Vigor CPE to reset the data record on a particular hour automatically.
	 User Defined Cycle Days - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.
	 User Defined Current Day - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.
	• User Defined Reset Hours - Select a particular time (00:00~23:00). For example, choose 15:00. Later, the CPE will reset the data record at 15:00 for every cycle.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.1.6 DHCP Client Option IPv6

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

← Configuration	2865Lac_1449BC0D8F00) / Configuration / WAN			Set to Factory Default	C
Internet Access	Enable	interface	Option	Туре	Data	
Connection Detection	false		٥	ASCII		
Multi PVC/M AN WAN IN46 WAN Rudget	Note: LOption 1, 2, 3, LOption 1, 2, 4, Loption 1, 2, Loption 1, 4,	4, 5, 8, 13, 20, 23, 23, 26 are reserved. re the setting in "WAN == internet Access" page's "IPvG =	- DHCP-6 Client Configuration >> Authentication Pr	ntaccil" if you configure option 11 in		

To modify the setting, move the mouse cursor to the entry and click to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / WAN		Set to Factory De	efault C
Index	1		
Enable			
Interface	WAN1 ~	✓	
Option Number	0		
Туре	ASCII Hex Address 🗸		
Data			
👚 Clear		Cancel	Save

ltem	Description
Index	Displays the index number for the DHCP option.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.
Interface	The interface(s) to which this entry is applicable.
Option Number	DHCP option number (e.g., 100).
Туре	Type of data in the Data field:
	ASCII Character - A text string. Example: /path.
	Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
	Address List - One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2 LAN

6.3.2.1 General Setup

This page provides you the general settings for LAN.

865_1449BC080090 / Configuration / LAN				(
Index	Status	DHCP	IP Address	
LAN1	Enable	Enable	192.168.1.1	
LAN2	Disable	Enable	192.168.2.1	
AN3	Disable	Enable	192.168.3.1	
AN4	DIsable	Enable	192.168.4.1	
AN5	DIsable	Enable	192.168.5.1	
ANG	Disable	Enable	192.168.6.1	
AN7	DIsable	Enable	192.168.7.1	
AN8	DIsable	Enable	192.168.8.1	
MZ Port	DIsable	Enable	192.168.254.1	
Force router to use "DNS server IP address"	Disable	\sim		
				Save

To modify the LAN or DMZ Port setting, move the mouse cursor to any entry and click to open the setting page.

2865_1449BC080090 / Configuration / LAN		C
General Setup		
Index	1	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
RIP Protocol Control	Disable ~	
DHCP Server Setup		
DHCP Server Enable		
IP Pool Start	192.168.1.10	
IP Pool End	192.168.1.209	
Gateway IP Address	192.168.1.1	
DHCP Lease Time	86400	
Clear DHCP lease for inactive clients periodically		
DHCP Relay	\bigcirc	
DNS Server IP Address		
Primary IP Address	IPv4 format (EX : 123.12.1.1)	
Secondary IP Address	IPv4 format (EX : 123.12.1.1)	
		Cancel Save

ltem	Description	
	General Setup	
Index	Display the index number of LAN item.	
IP Address	Display the IP address of the router.	
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet.	

RIP Protocol Control	It is available for LAN Port only.
	Click to enable / disable the function. If enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
Usage	It is available for DMZ Port only.
	NAT - Click to invoke NAT function.
	Routing - Click to invoke routing function.
	DHCP Server Setup
DHCP Server Enable	Click to enable / disable the DHCP server settings. If enabled:
	IP Pool Start - Enter an IP address. The beginning LAN IP address that is given out to LAN DHCP clients.
	IP Pool End - Enter an IP address. The ending LAN IP address that is given out to LAN DHCP clients.
	Gateway IP Address - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN.
	DHCP Lease Time - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.
	Clear DHCP lease for inactive clients periodically - If enabled, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool.
DHCP Relay	Click to enable / disable the DHCP Relay settings. If enabled:
	DHCP Relay IP Address - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
	DHCP 2nd Relay IP Address - Set the second IP address for the DHCP server.
	DNS Server IP Address
Primary IP Address	Specify a DNS server IP address.
Secondary IP Address	Specify secondary DNS server IP address.
Cancel	Discard current modification.
Save	Save the current settings.

7.3.2.2 IP Routed Subnet

2865Lac_001DAA1FB090		Dray Tek VigorACS 3	Capture Packets Captur
General Setup	2865Lac_001DAA1FB090 / Configuration	n / LAN	Ø
IP Routed Subnet	General Setup		
VLAN	Enable		
Bind IP to MAC DHCP Option Setup	IP Address	192.168.0.1	
InterLAN Routing	Subnet Mask	255.255.255.0	
LAN IP46	RIP Protocol Control	Disable •	
Port Mirror Wired 802.1X	DHCP Server Setup		
	IP Pool Start	192.168.0.100	
	IP Pool Counts	32 max. 32.	
	DHCP Lease Time	300	
	Use LAN Port	\bigcirc	
	Use LAN Port1		
	Use LAN Port2		
	Use MAC Address		
	MAC Address Table	Index Matched MAC Address Given IP Address Action	
		1 + Add	
			Cancel Save

ltem	Description
	General Setup
Enable	Click to enable / disable the IP routed subnet configuration.
IP Address	It is the IP address of the router.
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0)
RIP Protocol Control	Enable - The router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
	DHCP Server Setup
IP Pool Start	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses.
IP Pool Counts	Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to.
DHCP Lease Time	Enter the time to determine how long the IP address assigned by DHCP server can be used.
Use LAN Port / Use LAN Port 1 /2	Specify an IP for IP Route Subnet. If Use LAN Port is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of Use LAN Port 1 and Use LAN Port 2 .
Use MAC Address	Click to specify MAC address.
MAC Address Table	It displays the a list of MAC addresses. +Add - Enter the MAC address in the boxes and click this button to add. +Edit - Click to modify the address of the selected entry. Delete - Click to remove the selected entry.
Cancel	Discard current modification.

Save

9.4.2.3 VLAN

AN Configuration				
VLAN Enable				
Permit untagged device	e in P1 to access router			
Name	Subnet	VLAN Tag Enable	VLAN Tag ID	VLAN Tag Priority
VLANO	LAN1 🗸		0	0 🗸
VLAN1	LAN1 🗸		0	0 🛩
VLAN2	LAN1 🗸		0	0 🗸
VLAN3	LAN1 🗸		0	0 🗸
VLAN4	LAN1 🗸		0	0 🗸
VLAN5	LAN1 🗸		0	0 🗸
VLAN6	LAN1 🗸		0	0 🗸
VLAN7	LAN1 🗸		0	0 🗸
VLAN8	LAN1 🗸		0	0 🗸
VLAN9	LAN1 🗸		0	0 🗸
VLAN10	LAN1 🗸		0	0 🗸
VLAN11	LAN1 🗸		0	0 🛩
VLAN12	LAN1 🗸		0	0 🛩
Clear VLAN setup				Cancel Sa

ltem	Description
	VLAN Configuration
VLAN Enable	Click to enable / disable the VLAN configuration.
Permit untagged	Click to enable / disable the function.
device P1 to access router	If enabled, it allows untagged hosts connected to LAN port P1 to access the router.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only.
VLAN Tag Enable	Check to enable the function of VLAN with tag.
VLAN Tag ID	Enter the value as the VLAN ID number. The range is form 0 to 4095.
	VIDs must be unique.
VLAN Tag Priority	Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.
	VLAN Member(LAN)
P1 ~ P5	Check the LAN port(s) to group them under the selected VLAN.
	VLAN Member(Wireless 2.4G/5G)
SSID1~SSID4	Check the SSID boxes to group them under the selected VLAN.
Clear VLAN Setup	Discard the modification and return to the original configuration of this page.
Cancel	Discard current modification.

Save Save the current settings.

9.4.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network.

Bind IP to MAC				
Enable	\bigcirc			
Strict Bind	\bigcirc			
Strict Bind Interface				
				Cancel Save
IP Bind List				
Index	IP Address	MAC Address Comment	Action	
1	192.168.1.11	B0-6E-BF-C9-96-DE	🖉 Edit 💼 Delete	
2			+ Add	
			+ Add	
2 ARP Table			+ Add	
			+ Add	
ARP Table	IP Address	MAC Address	+ Add Host ID	
ARP Table	IP Address 192.168.1.11	MAC Address B0-6E-BF-C9-96-DE		

ltem	Description
	Bind IP to MAC
Enable	Click to enable or disable the function.
Strict Bind	Click to enable or disable the function. If enabled, the router will block the connection of the IP/MAC which is not listed in IP Bind List.
Strict Bind Interface	Choose the interface(s) for applying the rules of Bind IP to MAC.
Cancel	Discard current modification.
Save	Save the current settings.
	IP Bind List
Delete All	Delete all entries in IP Bind List.
+Add	After entering the IP address, MAC address and comment for a new entry, click +Add to create a new IP bind.
Edit	If IP address, MAC address and comment have been modified, click the Edit button to save the change.
Delete	Click the button to remove the selected index entry.
	ARP Table
+Add to Bind List	ARP table is the LAN ARP table of this router.
	Click to add the ARP table onto the Bind List.

9.4.2.5 DHCP Server Option IPv4/IPv6

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

	0		
	0	ASCII	
urved by OS which are not allowed to config	ure in this name: Ontion 1 2 3 4 5 6 8 11 13 20 2	2. 25 and 26	
nfigured from DNS server field of LAN >> Ger	neral Setup >> LAN {x} IPv6 Setup page.		
I be configured from LAN >> General Setup a	>> LAN {x} IPv6 Setup >> DHCPv6 Server >> Advance	e setting page.	
1	nfigured from DNS server field of LAN >> Ge	nfigured from DNS server field of LAN >> General Setup >> LAN {x} IPv6 Setup page.	erved by OS which are not allowed to configure in this page: Option 1, 2, 3, 4, 5, 6, 8, 11, 13, 20, 23, 25 and 26. nfigured from DNS server field of LAN >> General Setup >> LAN [4] IPv6 Setup page. d be configured from LAN >> General Setup >> LAN [4] IPv6 Setup >> DHCPv6 Server >> Advance setting page.

ltem	Description
+Add	Click to add a new option profile.
Delete	Click to remove a selected option profile.

To modify the option setting, move the mouse cursor on the entry and click to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / LAN		Set to Factory I
Index	1	
Enable		
Interface	Nothing selected ~	
Data Type	ASCII Hex Address SIAddr	
Option Number	0	
Data		
🗎 Clear		Cancel

ltem	Description
Index	Displays the index number of the profile.
Enable	Click to enable or disable the DHCP option entry.
Interface	Select the LAN interface(s) to which this entry is applicable. Select All - Select all LAN interfaces.
Data Type	 Select the type of data in the Data field. ASCII - A text string. Example: /path. Hex - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468. Address - One or more IPv4/IPv6 addresses, delimited by commas. SIAddr - It is available for DHCP Server Option IPv4 only. Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	Enter a DHCP option number (e.g., 100).
Data	Enter the data for this DHCP option based on the data type selected.
Next Server IPAddress/SIAddr	Enter the DHCP next server IP address. It is available for DHCP Server Option IPv4 only.
Cancel	Discard current modification.

9.4.2.6 InterLAN Routing

Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	2								
LAN 2	•								
LAN 3	•	•	8						
LAN 4			0						
LAN 5	0	0	0	0	8				
LAN 6	0	0	0	0	D				
LAN 7	0		0	0		0	8		
AN 8			0			0			
DMZ Port		0	0			0	0	0	

ltem	Description
LAN1 to DMZ PortCheck the box(es) to let the 2 intersecting LANs can communicate each other.	
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.7 LAN IPv6

This page allows to configure IPv6 settings for each LAN.

ndex	Status	DHCPv6 Enable	DNS Enable	
LAN1	Enable	true	Deploy_when_WAN_is_up	
LAN2	Enable	true	Deploy_when_WAN_is_up	
LAN3	Enable	true	Deploy_when_WAN_is_up	
LAN4	Enable	true	Deploy_when_WAN_is_up	
LAN5	Enable	true	Deploy_when_WAN_is_up	
LAN6	Enable	true	Deploy_when_WAN_is_up	
LAN7	Enable	true	Deploy_when_WAN_is_up	
LAN8	Enable	true	Deploy_when_WAN_is_up	
DMZ	Enable	true	Deploy_when_WAN_is_up	

To modify the IPv6 setting for each LAN, move the mouse cursor on the entry and click to open the setting page.

Basic Setup					
LAN Name		LAN1			
Enable					
WAN Primary Interface		WAN1	~		
Static IPv6					
ULA Config		Off	~		
ULA Config Address					
		Preftx Length: 64			
IPv6 Address Table	Index	IPv6 Address	Prefix Length	Action	
	1	FE80::B9A1:14C0:2AB4:900B	64	1 Delete	
	2			+ Add	
DNS Server IPv6					
DNS Enable		Deploy_when_WAN_Is_up	~		
Primary DNS		2001:4860:4860::8888			
Secondary DNS		2001:4860:4860::8844			
Management					

ltem	Description
	Basic Setup
LAN Name	Display the name of the LAN interface.
Enable	Click to enable or disable the configuration of LAN IPv6 Setup.
WAN Primary Interface	Specify a WAN interface for IPv6.
	Static IPv6
ULA Config	Select the ULA mode (off, Auto_ ULA_Prefix, Manually_ULA_Prefix).
ULA Config Address	LAN clients will be assigned ULAs generated based on the prefix manually entered.
IPv6 Address Table	Display current used IPv6 addresses.

	DNS Server IPv6
DNS Enable	Select Deploy_when_WAN_is_up, disable or enable.
	Deploy when WAN is up - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.
	Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.
	Disable - DNS server will not be used.
Primary DNS	Enter the IPv6 address for Primary DNS server.
Secondary DNS	Enter another IPv6 address for DNS server if required.
	Management
Management	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.
	Off - No configuration information is sent using Route Advertisements. SLAAC(stateless) - M-bit is unset.
	DHCPv6(stateful) - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor2865, or a separate DHCPv6 server.
Other Option (O-bit)	Click to enable or disable the function. If enabled, the O-bit will be enabled for obtaining additional information (e.g., DNS) from DHCPv6.
	DHCPv6 Server
DHCPv6 Server Enable	Click to enable DHCPv6 server.
Auto IPv6 Range	If enabled, Vigor router will assign the IPv6 range automatically.
Start Address	Enter the start address for IPv6 server.
End Address	Enter the end address for IPv6 server.
	Router Advertisement
Enable	Click to enable or disable the router advertisement server.
Hop Limit	The value is required for the device behind the router when IPv6 is in use.
Min/Max Interval Time(sec)	It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.
Default Lifetime(sec)	Within the period of time, Vigor router can be treated as the default gateway.
Default Preference	It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.
MTU Auto	If enabled, the router will determine the MTU value for LAN.
	RIPng Protocol
Enable	If enabled, RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	Extension WAN
Selected WAN	Additional WANs selected to carry IPv6 traffic.

Save the current settings.

9.4.2.8 Port Mirror

The LAN Port Mirror function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis.

The parameters are explained as follows:

ltem	Description
Enable	Enables or disables LAN Port Mirroring.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Tx Port	Port(s) whose outbound traffic will be forwarded to the mirror port.
Mirrored Rx Port	Port(s) whose inbound traffic will be forwarded to the mirror port.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.9 Wired 802.1X

Wired 802.1X provides authentication for clients wishing to connect to the LAN by Ethernet.

2.1X Ports P1 P2 P3 P4	Enable LAN 802.1X									
P5 Note: • 802.1X enabled LAN ports only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN port	Authentication Type	External	RADIUS			~				
6 Note: • 802.1X enabled LAN ports only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN port	802.1X Ports	🗆 P1	🗆 P2	🗆 P3	🗆 P4					
802.1X enabled LAN ports only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN port		🗆 P5								
	 BO2.1X enabled LAN ports of you need an 802.1X-capabl 	only support a single attach e switch. Then configure 80	ed device usi)2.1X on the a	ng EAPOL aut ttached switc	hentication. h Instead.	To authenticate multip	le devices throug	gh a LAN port		

ltem	Description
Enable LAN 802.1x	Check the box to enable LAN 802.1x function.
Authentication Type	External RADIUS - An external RADIUS server is to be used for 802.1X

	authentication. Local 802.1X - Use the user database on the router to authenticate clients.
802.1X ports	802.1X authentication will be available for the selected LAN ports.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.3 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

9.4.3.1 Profile Setup

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

Index	Enable	Comments	Login Mode	Applied Interface
1	Disable		Click-through	None
2	Disable		Click-through	None
3	Disable		Click-through	None
4	Disable		Click-through	None
		e Internet before webpage redirection will wo other DNS server on LAN, please make sure th		k.com" will be resolved by the router.

To configure the profile, move the mouse cursor to any entry and click to open the setting page. Follow the on-screen steps to set the profile.

Step (1) Login Method

1 Login Method	2 Background	3 Login Page Setup	4 Whitelist Setting	5 More Options			
Step 1- Login Method							
Enable							
Comments							
Portal Server							
Portal Method		Various Hotspot Login	~				
Captive Portal URL		http:// ~ portal.dray	tek.com				
Login Methods							
Choose Login Method		Login with Facebook					
		Login with Google					
		Receive PIN via SMS					
		Receive PIN via Mail					
		PIN with Voucher					
		Login with RADIUS					
		Leave Info Login					
					Cancel	Previous	Save and Next

ltem	Description
Enable	Check to enable this profile.
Comments	Enter a brief description to identify this profile.

	Portal Server
Portal Method	 There are four methods to be selected as for portal server. Skip Login, landing page only Click Through Various Hospot Login
	 Leave Info Login
	External Portal Server
	When Skip Loging, landing page only or Click through is selected as Portal Method
Captive Portal URL	Enter the captive portal URL.
	When Various Hotspot Login is selected as Portal Method
Captive Portal URL	Enter the captive portal URL.
Login Methods	This setting is available when Various Hotspot Login is selected as the portal method.
	Choose Login Method - Select one or more desired login methods.
	 Login with Facebook
	Login with Google
	Receive PIN via SMS
	Receive PIN via Mail
	PIN with Voucher
	 Login with RADIUS
	Leave Info Login
Facebook (Login with Facebook)	This setting is available when Login with Facebook is selected as the logi method.
-	Facebook APP ID - Enter a valid Facebook developer app ID.
	Facebook APP Secret - Enter the secret configured for the APP ID entered above.
Google (Login with Google)	This setting is available when Login with Google is selected as the login method.
	Google App ID - Enter a valid Google app ID.
	Google App Secret - Enter the secret configured for the APP ID entered above.
SMS Provider (Receive PIN via SMS)	This setting is available when Receive PIN via SMS is selected as the login method.
	Receiving PIN via SMS Provider - Select the SMS Provider used to send PIN notifications SMS providers.
Mail Server (Receive PIN via Mail	This setting is available when Receive PIN via Mail is selected as the login method.
Server)	Receiving PIN via Mail - Select the SMS Provider used to send PIN notifications SMS providers.
Radius Server (Login with RADIUS)	This setting is available when Login with RADIUS is selected as the login method.
- ·	Authentication Method – Click link to configure the external RADIUS server for authenticating web portal clients.
	RADIUS MAC Authentication – Check Enable to activate user authentication by MAC address.

	MAC Address Format – Select the MAC address format that is used by the RADIUS server.			
When External Portal Server is selected as Portal Method				
Redirection URL	Enter the URL to which the client will be redirected.			
RADIUS Server	Authentication Method - To configure the RADIUS server, click the <u>External RADIUS Server</u> link and you will be presented with the configuration page.			
	RADIUS MAC Authentication - If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server.			
	MAC Address Format - Select the MAC address format.			
	RADIUS NAS-Identifier - Enter the ID (string) for RADIUS NAS-Identifier.			
Cancel	Discard current modification.			
Previous	Return to previous page.			
Save and Next	Save the current settings and get into next page.			

If you have chosen **Skip Login**, **landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

Step (2) Background

Select a background for the login page.

1 Login Method	2 Background	3.1 Login Page Setup	32 Login Page Setup	() Whitelist Setting	S More Options
Step 2 - Background Choose Login Background		Color Background	Image Background		
Dray Tel	Lution Partner	Tab Title Background Color ethods Background Color			
Browser Table Title		Draytek Hotspot			
Logo Image		Default Draytek Logo			
Logo Background Color		Vigor Red	v		
Login Method Background Col	lor	Vigor Grey	v		
					Cancel Previous Save and Next

ltem	Description
Choose Login Background	Select either Color Background or Image Background as the login page background scheme.

Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

If you have selected **Skip Login**, **landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

Step (3) Login Page Setup

Login Method	Background	3.1 Login Page Setup	3.2 Login Page Setup	4 Whitelist Setting	More Options	
Step 3.1 - Login Page Setu	qu					
Configure Login Method and D	etails					
Welcome Message		Welcomel Please	log in to enjoy Wi-Fi.			
Privacy Policy & Terms and Cor	nditions	Default				
Terms and Conditions						
		User must tick to ge	t the internet access			
Description		By clicking the button t Terms and Conditions.	elow you agree to the			
		Default				
Content		Internal Content	External Content			
		(Max 1360 characters)				
Data Collection for Marketir	18	Ð	Ri			
		User must tick to ge	t the internet access			
Description		I would like to receive e	emails about the latest			

ltem	Description
	if you have selected Click Through as the Portal Method.
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions	Click to enable/disable the function. User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.
Description	Enter the text to be displayed in the Terms and Conditions pop-up window.

Content	If enabled, a check box with a description will be shown on the web portal login page.
	Internal Content - Click it for displaying the message that you want the user knows on the web portal login page.
	• Enter the text on the box below the Internal Content button.
	External Content - Click it for opening another URL web page.
	• External Content URL - Enter the URL.
Data Collection for Marketing	If enabled, a check box with a description will be shown on the web portal login page.
	User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.
	Description - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier.
Enter PIN Description	Enter the existing PIN code.
Submit Button Description	Enter the text to be displayed on the Submit button
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
	if you have selected Various Hotspot Login as the portal method.
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and	Click to enable/disable the function.
Conditions	User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.
Description	Enter the text to be displayed in the Terms and Conditions pop-up window.
Content	If enabled, a check box with a description will be shown on the web portal login page.
	Internal Content - Click it for displaying the message that you want the user knows on the web portal login page.
	 Enter the text (maximum 1360 characters) on the box below the Internal Content button.
	External Content - Click it for opening another URL web page.
	• External Content URL - Enter the URL.
Data Collection for Marketing	If enabled, a check box with a description will be shown on the web portal login page.
	User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.
	Description - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier.
Facebook Login Description	Enter the text to be displayed on the Facebook login button.
Google Login Description	Enter the text to be displayed on the Google login button.

Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <pin></pin> within the message.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Hint Message for RADIUS	Enter the text used to prompt the user to login.
RADIUS Account Description	Enter the text to prompt the user to enter the username.
RADIUS Password Description	Enter the text to prompt the user to enter the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

if you have selected **Various Hotspot Login** as the portal method and selected **Receive PIN via SMS** as the login method, you will also need to configure (3.2 Login Page Setup) page.



Login Page Setup

			32		
Login Method	Background	Login Page Setup	Login Page Setup	Whitelist Setting	More Options
Step 3.2 - Login Page Setup					
onfigure Login Method and Details					
	-				
	Back Button				
< Back					
PIN Code will be sent over via SMS.	PIN Code Messa	age			
	Defends Country	, Enter Mobile Number De			
+ 885 enter your mobile number		-	escription		
Send PIN	Send Button De	scription and Color			
	Send Succeede	d Message			
Enter PIN Submit	Enter PIN and S	ubmit Button			
Back Button Description					
Back Button Description		Back			
			10		
		Default			
PIN Code Message		PIN code will be sent ov	ver via SMS.		
		Default	10		
		O CTOOL			
Default Country Code		+ 93 Afghanistan	*		
Enter Mobile Number Description		enter your mobile numb	er		
		2000 2000 100000 100100			

The parameters are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country Code	Select the default country code to be displayed using the dropdown menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

Step (4) Whitelist Setting

Configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

1 Login Method	2 Background	3.1 Login Page Setup	3.2 Login Page Setup	4 Whitelist Setting	More Options
Step 4 - Whitelist Setting					
NAT Rules Dest Domain		Source IP			
Always allow outbound conr	nections from hosts in	NAT >> Port Redirection			
		NAT >> Open Ports			
		NAT >> DMZ			
					Cancel Previous Save and Nex

ltem	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

Step (5) More Options

						- 3
Login Method	Background	Login Page Setup	Logir	Page Setup W	hitelist Setting Me	ore Options
Step 5 - More Options						
oota Management						
Login Method	Quota Policy Profile		Valid Time	Device Allowed	Bandwidth Limit	Session Limit
Facebook Login	1. Default	¥	0d 5h 0m	Unlimited	Unlimited	Unlimited
Google Login	1. Default	•	0d 5h 0m	Unlimited	Unlimited	Unlimited
SMS Login	1. Default	•	0d 5h 0m	Unlimited	Unlimited	Unlimited
	settings, please go to Hotspot \	Web Portal >> <u>Quota Manag</u>	<u>tement</u>			
To modify the quota		Web Portal >> <u>Quota Manag</u>	20202			
To modify the quota leb Portal Options HTTPS Redirection Note: When an unauthenti		Coage, redirect will work but o	ertificate errors may			
To modify the quota Veb Portal Options HTTPS Redirection Note: When an unauthenti	settings, please go to Hotspot l	Coage, redirect will work but o	ertificate errors may			
To modify the quota Veb Portal Options HTTPS Redirection Vien an unauthent Disable this function Captive Portal Detection Inset Trigger the unauther	settings, please go to Hotspot icated client opening a HTTPS p to redirect only HTTP pages. H nticated client to automatically	e redirect will work but o TIPS browsing will timeout u D pop-up the Web Portal page	ertificate errors may without redirection a	ind also no certificate errors. ñ-FL	5 balls in Captive Portal Detection.	
To modify the quota Web Portal Options HTTPS Redirection Note: When an unauthent Disable this function Captive Portal Detection Note: Tigger the unauther	settings, please go to Hotspot cated client opening a HTTPS p to redirect only HTTP pages. H nticated client to automatically valiable when using Social Logi	e redirect will work but o TIPS browsing will timeout u D pop-up the Web Portal page	ertificate errors may without redirection a	ind also no certificate errors. ñ-FL	i built-in Captive Portal Detection.	

Item	Description
	Quota Management
Quota Policy Profile	Choose a policy profile to apply to web portal clients.
	JSON API
Enable JSON API	If enabled, information (e.g., string, number, object and so on) will be saved as a text file on the JSON server.
Server URL	Enter the URL of the server which will store the JSON information.
Get JSON and Update user status every	Specify the time period for the JSON server sending the JSON information to other devices automatically.
Update Information	 The information sent out by JSON server might include the following types: NAS-Identifier (router's ID) MAC Address (routers' MAC address) All User Number (total number of the users connecting to the router) Wi-Fi User Number (total number of the wireless users connecting to the router)
	Web Portal Options
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login , as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.

	Landing Page After Authentication
Landing Page Type	Fixed URL - Specifies the webpage that will be displayed after the user has successfully authenticated.
	The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
	User Requested URL - The user will be redirected to the URL they initially requested.
	Bulletin Message - The message configured here will be briefly shown for a few seconds to the user.
	Bulletin Message Type - Select HTML or Image Upload.
	• Default – This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox.
Force Landing Page Stay Enable	If enabled, the landing page will stay until you close it.
	Applied Interfaces
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN 2.4G / 5G	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Cancel	Discard current modification.
Previous	Return to previous page.
Finish	Complete the configuration.

9.4.3.2 Users Information

This page displays information of users accessing the Internet through the web portal.

6.3.3.2.1 User Info

Select Columns to Filter Users					^
Profile	Profile 1	Profile 2	Profile 3	Profile 4	
Login Method	Skip	Facebook		Google	
	PIncode	Click		RADIUS	
					Apply
					Apply
ser Table					Apply
ser Table vrtive User ~ 0 Online Users / 0 Ali Users				Auto Refresh (per	
				Auto Refresh (per i	
	rr ↓† Login Method	J↑ IP J↑ MAC J↑ Ema	sil J↑ Phone Nu		min): off ~
votive User -> 0 Online Users / 0 All Users	-	⊥া IP টা MAC টা Ema এ D data available	all ↓↑ Phone Nur		nin): off ~

These parameters are explained as follows:

ltem	Description

Select Columns to Filter Users	Select the profiles and the login methods to filter the displayed users. Apply - Save the settings.
User Table	Details of users accessing the Internet via Hotspot Web Portal will be displayed.
Active User / All Database	Displays the information for active user only or for all users in database.
Auto Refresh	On/off - Refresh current page automatically or not.
Go	Where there are more than one page, Click to open the page with specified number.

7.3.3.2.2 Database Setup

This page allows the user to configure settings for database on USB disk.

ser Info Database Setup		
Enable database		
Enable automatic database recovery		
Backup database every	1 v hours 0 v	
Enable sending user information to syslog		
File Path	No USB Disk Detected	
Database Usage	N/A	
	Clear User Info	
Intification and Artion when Storage Ever		
Notification and Action when Storage Exce Notification	Don't send notification	
	Don't send notification +	

ltem	Description
Enable database	Check the box to record user information on router's database.
Enable automatic database recovery	Check the box to enable the functionality of the database recovery on the USB disk. Backup database every Set the interval to backup the database.
Enable sending user information to syslog	Check the box to send user information to syslog.
File Path	If a USB disk has been inserted into the USB port of Vigor router, the file path will be shown in this area.
Database Usage	Display the usage and remaining space on the database. Clear User Info – The user information will be displayed on the page of User Info. You can delete the information by clicking this button.
	Notification and Action when Storage Exceeded

Notification	Don't send notification - Vigor router system will not send any notification to any recipient.
	Send notification - Vigor router system will send a notification e-mail to specified recipient(s) that selected from Email Notification Object and SMS Notification Object .
	Email Notification Object
	SMS Notification Object
Action	Stop recording user information - Vigor router system will stop to record the user information onto USB disk.
	Backup and clean up all user info, and start a new record - Vigor router system will backup all existed information on the USB disk onto the host and clean up the information from USB disk. Later, it will start a new record.
	Advanced Options
Database Encryption	Select to have the router create a new encrypted database. Once this is done, you will not be able to revert to an unencrypted database.
Password	Enter a password for encryption.
Confirm Password	Enter the password again for confirmation.
Save	Save the current settings.

9.4.3.3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

nable Bandwidth Lim	nit 🔿				
nable Session Limit	\bigcirc				
ta Policy Profile			Profile Nur	nber Limit: 20	± 20
Index Name E	Expired Time After First Login	Device Allowed Per Account	Reconnection Time Restriction	Bandwidth	dth
1 Default 0	0d 6h 0m	Unlimited	Unlimited	Unlimited	ed

Item Description			
	Web Portal Bandwidth and Session Limit		
Enable Bandwidth Limit	Click to enable / disable the function. If enabled, it will override the policy configured in Bandwidth Management >> Bandwidth Limit.		
Enable Session Limit	Click to enable / disable the function. If enabled, it will override the policy configured in Bandwidth Management >> Sessions Limit.		
	Quota Policy Profile		

+Add	Create up to 20 policy profiles.
Delete	Delete the selected policy profile.
Save	Save the current settings.

To create a new policy profile, click **+Add** to create a new profile and display on the table.

uota Policy Profile						
+Add Delete Profile No.				Profile Number	mber Limit: 20	
	Index	Name	Expired Time After First Login	Device Allowed Per Account	Reconnection Time Restriction	Bandy
	1	Default	0d 6h 0m	Unlimited	Unlimited	Unlim
0	2	level 2	0d 5h 0m	Unlimited	Unlimited	Unlim

Check the box in front of the new entry and click to open the following page.

2865ac_001DAA41DF78 / Configuration / H	otspot Web Portal	Ø
Index	2	
Profile Name	level 2	
Account Validity		
Expired Time After 1 st Login	0 v 5 v 0 v days hours minutes	
Enable Idle Timeout	0	
Idle Timeout	0	
Device Control		
Devices Allowed per account	Unlimited 💌	
Enable Reconnection Time Restriction	\bigcirc	
Time Restriction	Set Time Set period	
	0 v hours 0 v mins	
	Block the same user from reconnecting for the set period	
Bandwidth and Session Limit		
Enable Bandwidth Limit	D	
Download Limit	0 Kbps 💌	
	Cancel	ave

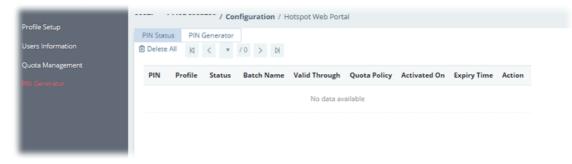
ltem	Description	
Index	Display the index number of the profile.	
Profile Name	Enter a name for a new profile.	
Account Validity		
Expired Time After 1st Login	Sets the days, hours, and minutes. After the login has expired, Vigor router will block the client from accessing the network/Internet.	
Enable Idle Timeout	If enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.	
Idle Timeout	Enter a time value (unit: minutes).	

	Device Control		
Devices Allowed per account	Select the maximum number of devices that can be connected to the network using the same account.		
Enable Reconnection Time Restriction	Click to enable / disable the function.		
Time Restriction	Blocks the account from being used to connect devices to the network in one of two ways:		
	Set Time (At Everyday) - After the login expires, the account cannot be used to connect devices to the network until the set time of day.		
	Set Period (Hours min) - After the login expires, the account cannot be used to connect devices to the network for a set period of time.		
	Bandwidth and Session Limit		
Enable Bandwidth Limit	Click to enable / disable the function.		
Download /Upload Limit	Set the maximum upload and download speeds.		
Enable Session Limit	Click to enable / disable the function.		
Session Limit	Set a maximum session limit for web portal clients.		
Cancel	Discard current modification.		
Save	Save the current settings.		

9.4.3.4 PIN Generator

9.4.3.4.1 PIN Status

This page displays the detailed information for PIN codes generated by PIN Generator.



9.4.3.4.2 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.

PIN Status PIN	N Generator	
Profile		¥
Batch Name		
PIN code len	agth	v
PIN Validity	Days 0	×
PIN Validity	Hours 0	*
	The period of database.	time the PIN will be kept in the
Quantity	0	
Quota Mana	gement Policy	*

These parameters are explained as follows:

ltem	Description		
Profile	Use the drop down menu to specify an index number (from 1 to 4).		
Batch Name	Enter a string as a batch name.		
PIN code length	Specify the length of PIN code.		
PIN Validity Days	Set the days for the period of validity.		
PIN Validity Hours	Set the hours for the period of validity.		
Quantity	Set the quantity of the PIN code.		
Quota Management Policy	Use the drop down list to choose policy profile.		
Generate	Click to generate a PIN code as a voucher.		

9.4.4 Routing

9.4.4.1 Load Balance/Policy Route

This page lists the configured policies coming from Vigor CPE.

								System Administrator	
286	365ac_001DAA000000 / Configuration / Routing								
8	Delete								
		Index	Enable	Comment	Protocol	Interface	Src IP	Dest IP	
		1	Disable	cnn	Any	WAN1	Any	Domain Name	
	0	2	Enable	SIP	Any	VoIP_WAN	Any	VoIP	
	0	3	Disable		Any	WAN1	Any	Any	

Item Description	
Delete Click to remove the selected routing policy.	
Index Displays the index number of the routing policy.	
Enable	Displays the status (enable / disable) of the routing policy.
Comment Displays the description for the routing policy.	
Protocol Displays the protocol used for this policy.	
Interface Displays the interface to send packets to once the policy is m	

Src IP	Displays the mode for the source IP.		
Dest IP	Displays the mode for the destination IP.		

To configure the policy, move the mouse cursor to any entry and click to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / Rout	ing	C
Index	1	
Enable	0	
Comment		
Criteria		
Protocol	Any ~	
Source IP	Any ~	
Destination IP	Any ~	
Destination Port	Any ~	
Send via if Criteria Matched		
Interface	WAN1 ~	
Gateway IP	Default Gateway \vee	
Priority		
Priority	200	
More Options		
		Cancel Save

ltem	Description		
Index	Displays the index number of the routing policy.		
Enable	Click to enable / disable the routing policy.		
Comment	Enter a brief explanation for the routing policy.		
	Criteria		
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.		
Source IP	Select the mode (Any, IP Range, IP Subnet, IP Object or IP Group) of the source IP.		
	Enter the IP address(es), network, mask, or select IP object/group as the source IP based on the source IP mode used.		
Destination IP	Select the mode (Any, IP Range, IP Subnet, Domain Name, IP Object, IP Group or Country Object) of the destination IP.		
	Enter the IP address(es), network, mask, domain name, or select an object/group as the destination IP based on the destination IP mode used.		
Destination Port	Select the mode (Any or Range) for the destination port.		
	Enter the port values as the destination port based on the destination port mode used.		
	Send via if Criteria Matched		
Interface	Use the drop down list to choose a WAN or LAN interface or VPN profile.		
Gateway IP	Default Gateway - Default Gateway is selected in default.		
	Specific Gateway - It is used only when you want to forward the packets		

	to the desired gateway.	
	Priority	
Priority	The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.	
	More Options	
Packet Forwarding Via	When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose Force NAT or Force Routing .	
Enable Failover	Click to enable / disable the failover function.	
Failover to	If enabled, it will lead the data passing through specific interface (e.g., WAN/LAN) automatically when the selected interface is down.	
Failover to Gateway IP	Specific gateway is used only when you want to forward the packets to the desired gateway.	
	Default Gateway - Usually, Default Gateway is selected in default.	
	Specific Gateway - Enter a gateway IP address.	
Cancel	Discard current modification.	
Save	Save the current settings.	

9.4.4.2 Static Route IPv4

The router offers IPv4 for you to configure the static route.

Index	Destination IP Address	Mask	Gateway	Interface	Status
1	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
2	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
3	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
4	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
5	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
6	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
7	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
8	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
9	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
10	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
11	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
12	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
13	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
14	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
15	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
16	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
17	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
18	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
19	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
20	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
21	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable

To configure the profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuratio	n / Routing	ç
Static Route IPv4		
Index	2	
Enable	Œ	
Destination IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
Network Interface	LAN1 r	
🗊 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description		
Index	Displays the index number of the static route policy.		
Enable	Click to enable or disable the static route policy.		
Destination IP Address	Enter an IP address as the destination of such static route.		
Subnet Mask	Enter the subnet mask for such static route.		
Gateway IP Address	Enter the IP address of the gateway.		
Network Interface	Specify an interface for this static route.		
Clear	Click to return to factory default setting.		
Cancel	Discard current modification and return to previous page.		
Save	Save the current settings and return to previous page.		

9.4.4.3 Static Route IPv6

The router offers IPv6 for you to configure the static route.

Index	Destination IPv6 Address	Prefix Len	Gateway IPv6 Address	Interface	Status
1	:	0	:	LAN1	Disable
2	:	0	::	LAN1	Disable
3	**	0		LAN1	Disable
4	:	0		LAN1	Disable
5	**	0	::	LAN1	Disable
6		0		LAN1	Disable
7	:	0		LAN1	Disable
8	::	0	::	LAN1	Disable
9		0		LAN1	Disable
10	:	0		LAN1	Disable
11		0	::	LAN1	Disable
12		0		LAN1	Disable
13	:	0		LAN1	Disable
14	:	0	::	LAN1	Disable
15		0		LAN1	Disable
16	:	0		LAN1	Disable
17	:	0	::	LAN1	Disable
18		0		LAN1	Disable
19	:	0		LAN1	Disable
20		0		LAN1	Disable
21		0		LAN1	Disable
22	**	0		LAN1	Disable
23		0		LAN1	Disable

To configure the profile, move the mouse cursor to any entry and click to open the setting page.

865ac_001DAA000000 / Configuration	n / Routing	ß
Static Route IPv6		
Index	1	
Enable	\bigcirc	
Destination IPv6 Address		
Prefix Len	0	
Gateway IPv6 Address		
Network Interface	LAN1 *	
D Clear		Cancel Save

These parameters are explained as follows:

ltem	Description				
Index	Displays the index number of the static route policy.				
Enable	Click to enable or disable the static route policy.				
Destination IPv6 Address / Prefix Len	Enter the IP address with the prefix length for this entry.				
Gateway IPv6 Address	Enter the gateway address for this entry.				
Network Interface	Specify an interface for this static route.				
Clear	Click to return to factory default setting.				
Cancel	Discard current modification and return to previous page.				
Save	Save the current settings and return to previous page.				

9.4.4.4 BGP

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

2865ac_001DAA000000 ~			DrayTek VigorAC	5 3		Capture Packets ~	carrie System Administrator		
Load Balance/Policy Route	2865ac_001DAA000000 / Configuration / Routing								
Static Route IPv4	Basic Settings								
Static Route IPv6	Enable Local BGP	C	D						
BGP	Local AS Number Hold Time Connect Retry Time		(1~4294967295)						
			80						
			20						
	Router ID	1	92.168.1.1						
	+ Add 💼 Delete						Cancel Save	•	
	Enable	Index	AS Number	Profile Name	IP Address	MD5 Auth	Status		
	Disable	1				Disable	None		
	Static Network								
	+ Add 🝈 Delete								
	Index IP Addre		ress S		Subnet Mask	Subnet Mask			
	0 1								

ltem	Description
Enable Local BGP	Click to enable / disable the BGP function.
Local AS Number	Enter the value as local AS nubmer.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect.
Router ID	Specify the LAN subnet for the router.
Cancel	Discard current modification.
Save	Save the current settings.
Basic Settings	 Displays general settings for for local router and neighboring routers. +Add - Add a new neighbor profile. Delete - Remove a selected neighbor profile. Enable - Displays the status of the BGP profile. Index - Displays the index number of the BGP profile. AS Number - Displays the value of AS number. Profile Name - Displays the name of the BGP profile. IP Address - Displays the IP address of the BGP profile. MD5 Auth - Displays the status (enabled / disabled) of MD5 Auth.
	Status - Display the connection status for local router and neighboring router.
Static Network	 Displays the neighboring routers for exchanging the routing information with the local router. +Add - Add a new static network profile by giving IP address and subnet mask. Delete - Remove a selected neighbor profile. Index - Displays the index number of the BGP profile. IP Address - Displays the IP address of the router. Subnet Mask - Displays the subnet mask of the router.
Cancel	Discard current modification.
Save	Save the current settings.

To configure the BGP profile with basic settings, move the mouse cursor to any entry and click to open the setting page.

Index	1
Enable	\bigcirc
Profile Name	
AS Number	(1~4294967295)
IP Address	IPv4 format (EX : 123.12.1.1)
MD5 Auth	
Password	\$
4-Byte As Number	\bigcirc

These parameters are explained as follows:

ltem	Description
Basic Settings	Index - Displays the index number of the profile.
	Enable - Click to enable / disable the profile.
	Profile Name - Enter the name of the profile.
	AS Number - Enter a value for AS number.
	IP Address - Enter the IP address for the profile.
	MD5 Auth - Click to enable / disable the MD5 authentication.
	Password - Enter the password for authentication.
	4-Byte As Number - Click to enable / disable the setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

To configure the BGP profile for static network, click **+Add** to open the setting page. Or move the mouse cursor to any existed entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Rou	ting		ß
Index	1		
IP Address	IPv4 format (EX : 123.12.1.1)		
Subnet Mask			
		Cancel Save	

ltem	Description
Static Network	Index - Displays the index number of the profile.
	IP Address - Enter the IP address for a router.
	Subnet Mask - Specify a subnet mask for the IP address.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5 NAT

9.4.5.1 Port Redirection

This page lists the configured Port Redirection policies coming from Vigor CPE.

2865ac_001DAA0000000 ~				Dray	Tek Vigo	orACS 3			Capture Pad	kets × Sy	stem Admir	carrie nistrator	С
Part Redirection	2865ac_0	01DAA00	0000 / Configuration /	NAT								Ŕ	3
DMZ Host										5	Set to Fac	tory Default	
Open Ports	Index	Status	Port Redirection Mode	Service Name	Protocol	Public Port Start	Public Port End	Private IP Start	Private IP End	Private Port	WAN IP	Source IP	F
Port Triggering	1	false	Single			0	0		0	0	All	0	f
ALG													

To configure the NAT profile, move the mouse cursor to any entry and click to open the setting page.

NAT	
Enabled	\bigcirc
Port Redirection Mode	Single Range
Service Name	
Protocol	TCP UDP
WAN IP	~ ~
Public Port Start	0
Public Port End	0
Source IP	Any IP Object IP Group
Private IP Start	IPv4 format (EX : 123.12.1.1)
Private Port	0
 Bote: in "Range" Mode the End IP will be calcu 	lated automatically once the Public Port and Start IP have been entered.
💼 Clear	Cancel

ltem	Description
Enabled	Click to enable / disable the port redirection profile.
Port Redirection Mode	Two options (Single and Range) are provided here for you to choose. Single / Range - To set a range for the specific service, select Range . Otherwise, select Single .
Service Name	Enter the description of the specific network service.
Protocol	TCP/UDP - Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN interface used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port Start / End	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will need to enter the required number on the first box (as the starting port) and the second box (as the ending port).
Source IP	Select the source IP mode. Any - It means any IP address. IP Object -

	IP Object - Specify an IP object profile.
	IP Group -
	• IP Group - Specify an IP group profile.
Private IP Start / End	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.2 DMZ Host

DMZ Host allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

2865ac_001DAA000000	~	Dray Tek VigorACS 3	Carrie Capture Packets Y System Administrator
Port Redirection	2865ac_001DAA000000 / Cor	figuration / NAT	S
	Index	Profile Name	
	1	WAN1	
Port Triggering	2	WAN2	
	3	WAN3	
	4	WAN4	
	5	WAN5	
	6	WAN6	

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the DMZ host profiles.
Profile Name	Displays the interface of the DMZ host profile.

To configure the DMZ host profile:

1. Move the mouse cursor to any entry (1 to 6) and click to open the following page.

T DMZ Host						
nterface		WAN1				
Index	WAN Type	Mode	Enable	Private IP	WAN IP	
1	0	None	false	0.0.0.0		

2. Click the index number of the profile to open the settings page.

/ Configuration / NAT		Q
NAT DMZ Host Setup		
Interface	WAN1	
Mode	Private IP v	
Private IP	0.0.0.0	
WAN IP	192.168.105.120	
		Cancel Save

ltem	Description
Interface	Displays the name of the DMZ host profiles.
Mode	 Select a method to enter the IP address. Private IP None
Private	Enter the private IP address of the DMZ host.
WAN IP	Displays the WAN IP alias for this interface.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

3. After finished the configuration, click **Save** to save the changes.

9.4.5.3 Open Ports

This page lists the configured Open Ports policies coming from Vigor CPE.

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

2865ac_001DAA41DF78				Dray Tek	VigorACS 3			Capture Packets 👻	carrie System Administrator	
Port Redirection	2865ac_0	01DAA41DF78 / Config	uration / NAT							S
DMZ Host									う Set to Factory Defa	ault
	Index	Enable Open Ports	Comment	WAN Interface	WAN IP	Local IP Address	Source IP	Open Ports Factory Defaul	t Source IP Typ	æ
Port Triggering	1	false		WAN1	WAN1_IP_Alias[1]	0.0.00	0	false	Any	
ALG										

To configure the open port profile, move the mouse cursor to any entry and click to open the setting page.

Index		1	
nable		D	
Comment			
WAN Interface		WAN1 *	
Source IP		Any IP Object IP Group	
Local IP Address		0.0.0.0	
en Port List			
ndex	Protocol	Start Port	End Port
		0	0
		0	0
		0	0
		0	0
		0	0
		0	0
		÷	0
5		0	0
5 6 7 8			

ltem	Description
	Open Ports
Index	Displays the index number of the Open Port profile.
Enable	Click to enable / disable the Open Port profile.
Comment	Enter the description for the Open Port profile.
WAN Interface	Choose a WAN interface that will be used for this entry.
Source IP	 Select the source IP mode. Any - It means any IP address. IP Object - IP Object - Specify an IP object profile. IP Group - IP Group - Specify an IP group profile.
Local IP Address	Enter the private IP address of the local host.
Open Port List	It displays 1 to 10 open port profiles. Click any one of the index numbers to configure the settings for the selected open port profile.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.4 Port Triggering

Port Triggering is a variation of open ports function. This page lists the configured Port Triggering policies coming from Vigor CPE.

2865ac_001DAA41DF78	~			Dray Tek	VigorACS 3		Capture	Packets 👻	carrie System Administrator	
Port Redirection	2865ac_00	1DAA41DF7	8 / Configurati	on / NAT						Ø
									ら Set to Factory Defau	ult
Open Ports	Index	Enable	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Source IP	Source IP Type	
	1	false						0	Any	

To configure the port triggering profile, move the mouse cursor to any entry and click to open the setting page.

nable	\bigcirc
Service	User Defined V
Comment	
Source IP	Any IP Object IP Group
Triggering Protocol	↓ v
Triggering Port	
Incoming Protocol	
Incoming Port	
 Note: The legal format of Triggering Port and I 123 123,455 123,455,789 123,455,789 123,455,777-789 The llegal format like this: 123,455-789 	coming Port should like this:

ltem	Description
Enable	Click to enable / disable the Port Triggering profile.
Service	Choose the service type to apply for this triggering profile.
Comment	Enter the text to memorize the application of this rule.
Source IP	 Select the source IP mode. Any - It means any IP address. IP Object IP Object - Specify an IP object profile. IP Group IP Group - Specify an IP group profile.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.

Incoming Port Enter the port or port range for the incoming packets.	
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.5 ALG

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

- Configuration	2865_1449BC080090 / Configuration / NAT						(
Aart Redirection	ALG (Applica	tion Layer Gateway)					
OMZ Host			~				
Open Ports	Enable		0				
Aart Triggering							
	Index	Enable	Protocol	Listen Port	TCP	UDP	
	1	false	SIP	5060	true	true	
	2	false	RISP	554	true	true	
						Cancel	

To configure the ALG profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA41DF78 / Co	figuration / NAT	S
Enable		
Protocol	SIP	
Listen Port	5060	
тср		
UDP		
		Cancel Save

ltem	Description
Enable	Click to enable / disable the ALG profile.
Protocol	Displays the type (SIP, RTSP) of ALG.
Listen Port	Enter a port number for SIP or RTSP protocol.
TCP/UDP	Click to enable/disable the TCP/UDP. If enabled, it will make correspond protocol message packet from TCP/UDP transmit and receive via NAT.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.6 Hardware Acceleration

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself.

2865ac_001DAA000000 / Con	figuration / Hardware Acceleration	
Acceleration	Disable Enable	
NAT		
Protocol	🖸 TCP 🗌 UDP	
IPsec		
Protocol	TCP 🗆 UDP	
		Cancel

ltem	Description	
Acceleration	Disable – The default setting.	
	Enable - The sessions with the heaviest loading and the lower latency traffic will be added into PPA.	
NAT	Click to enable / disable NAT setting.	
Protocol	There are two types supported by this function, TCP and UDP.	
IPsec	Click to enable / disable IPsec setting.	
Protocol	There are two types supported by this function, TCP and UDP.	
Cancel	Discard current modification.	
Save	Save the current settings.	

9.4.7 Firewall

9.4.7.1 General Setup

It allows you to enable / disable Data Filter, determine general rule for filtering the incoming and outgoing data.

Data Filter Data Filter Set Start Deta Filter Set Start Set#2 Inbound Policy Allow pass inbound fragmented large packets (required for certain games and streaming) Enable Strict Security Firewall Block routing connections initiated from WAN Block IPv6 Routing Packet Packets are filtered by frewall functions in the following order: 1. Data Filter Sets and Rules Packets rene filtered by frewall functions in the following order: 1. Data Filter Sets and Rules	Filter Setup		
Inbound Policy Allow pass inbound fragmented large packets (required for certain games and streaming) Enable Strict Security Firewall Block routing connections initiated from WAN Block IPv6 Routing Packet Block IPv6 Routing Packet Note: • Packets are filtered by frewall functions in the following order: • Date filter Sets and Rules. 3. Block routing connections initiated from WAN.	Data Filter		
Allow pass inbound fragmented large packets (required for certain games and streaming) Enable Strict Security Firewall Block routing connections initiated from WAN Block IPv4 Routing Packet Block IPv6 Routing Packet Reference filtered by firewall functions in the following order: 1. Data Filter Sets and Rules. 2. Block routing connections initiated from WAN.	Data Filter Set Start	Set#2 ·	
Allow pass inbound fragmented large packets (required for certain games and streaming) Enable Strict Security Firewall Block routing connections initiated from WAN Block IPv4 Routing Packet Block IPv6 Routing Packet C C C C C C C C C C C C C C C C C C C	Jabourd Policy		
Block routing connections initiated from WAN Block IPv6 Routing Packet Block IPv6 Routing Packet R Note: Packets are filtered by firewall functions in the following order: 1. Data Filter Sets and Rules. 2. Block routing connections initiated from WAN.	Allow pass inbound fragmented large packets (required for certain games		
Block IPv4 Routing Packet Block IPv6 Routing Packet Routing Packet Block IPv6 Routing Packet Block	Enable Strict Security Firewall		
Block IPv6 Routing Packet	Block routing connections initiated from WAI		
 β Note: Packets are filtered by firewall functions in the following order: 1. Data Filter Sets and Rules. 2. Block routing connections initiated from WAN. 	Block IPv4 Routing Packet	\bigcirc	
Packets are filtered by firewall functions in the following order: 1. Data Filter Sets and Rules. Block routing connections initiated from WAN.	Block IPv6 Routing Packet		
	Packets are filtered by firewall function Data Filter Sets and Rules. Block routing connections initiated		Save

ltem	Description
	Filter Setup
Data Filter	Click to enable / disable the function.
	If enabled, choose a Start Filter Set.
Data Filter Set Start	Choose a Start Filter Set.
	Inbound Policy
Allow pass inbound	Click to enable / disable the function.
fragmented large	Certain games and video streaming service use fragmented UDP packets to transfer data. Enabling this option allows these applications to function properly.
Enable Strict Security Firewall	Click to enable / disable the function. If this option and the Web Content Filter (WCF) are both enabled, web traffic will be blocked if the WCF server fails to respond to lookup requests.
	Block routing connections initiated from WAN
Block IPv4 Routing Packet	For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, enable this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.
Block IPv6 Routing Packet	IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN. Enable this option to block WAN hosts from connecting to LAN hosts using IPv6.
Save	Save the current settings.

9.4.7.2 Default Rule

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

Default Action	Pass Block
Session Control	60000
Quality of Service	None *
User Management	None 💌
APP Enforcement	None 👻
URL Content Filter	None 💌
Web Content Filter	None •
DNS Filter	None 💌
Syslog	Default Action Session Control Quality of Service User Management APP Enforcement URL Content Filter Web Content Filter DNS Filter
dvanced Settings	
Codepage	ANSI(1252)-Latin I 💌
Window Size	65535
Session Timeout (min.)	60

ltem	Description
	Default Rule
Default Action	Select Pass or Block for the packets that do not match with the filter rules. When the setting is Block, all other fields on the page are disabled because they are not applicable.
Session Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable.
Quality of Service	Select one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
User Management	This setting is only available when Rule-Based is selected in User Management>>General Setup . The default firewall rule will be applied to the selected user or user group.
APP Enforcement	Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule.
URL Content Filter	Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule.
Web Content Filter	Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule.
Syslog	Select the items to send and store the records to Syslog.

Advanced Settings		
CodepageSelecting the appropriate codepage can increase the accuracy of the Content Filter. The default value is ANSI 1252 Latin I. If the setting is no decoding of URL will be performed.		
Window Size	Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535.	
Session Timeout	Sets the timeout sessions are allowed to idle before they are removed from the system.	
Save	Save the current settings.	

9.4.7.3 Filter Rules

This page displays the filter rule profile and allows to create new filter rule profile(s).

+Add @ Delete			
	Set	Comments	Next Filter Set
	1		None
	2	Default Data Filter	None

These parameters are explained as follows:

ltem	Description
+Add	Click to add a new filter rule set.
Delete	Click to remove the selected filter rule.
Set	Displays the number of filter set.
Comments	Displays the comment of the filter rule.
Next Filter Set	Displays the name of next filter set. None means no filter set is specified for current filter set.

To configure the filter rule set profile, move the mouse cursor to any entry and click to open the setting page. Or, click **+Add** to create a new filter rule profile.

	C C C C C C C C C C C C C C C C C C C		1				
Com	ments		Default Data Filter				
Next	Filter Set		None	~			
Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action
l		xNetBios -> DNS	LAN/RT/DMZ/VPN->WAN	Any	Any	TCP/UDP	Block Immediately
		block_all	LAN/RT/DMZ/VPN->WAN	Any	Any	Any	Block If No Further Match
		open_lp	LAN/RT/DMZ/VPN->WAN	192.168.1.10 ~ 192.168.1.20	Any	Any	Pass Immediately

ltem	Description
	Filter Rules

Index	Displays the index number of the filter rule set. Each filter set contains up to 7 rules.
Comments	Enter a comment to identify the filter rule.
Next Filter Set	Select the filter set for the firewall to process after the current filter set
	Table
Rule	Displays the index number of the filter rule.
Active	Click to enabled or disabled the filter rule.
Comments	Optional comment entered in the settings page to identify the rule.
Direction	Displays the direction of packet.
Src IP	Displays the IP address of source /destination.
Dst IP	Displays the type and port number of the packet.
Service Type	Displays the type and port number of the packet.
Action	Displays the packets to be passed /blocked.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.7.4 DoS Defense

2865Lac_1449BC0D8F00 / Configuration / Firev	wall	C
DoS Defense		
DoS Defense	D	
	White/Black List Option	
DoS defense Log	Enable ~	
Flood Defense		
SYN Flood Defense	\odot	
SYN Flood Threshold (pkts/sec)	2000	
Session Time-Out (sec.)	10	
UDP Flood Defense	\bigcirc	
UDP Flood Threshold (pkts/sec)	5000	
Session Time-Out (sec.)	10	
ICMP Flood Defense	\odot	
ICMP Flood Threshold (pkts/sec)	250	
Session Time-Out (sec.)	10	
Port Scan Detection		
		Cancel

ltem	Description	
	DoS Defense	
DoS Defense	Click to enable / disable the DoS Defense.	
White/Black List Options	Click to set white or black list.	

	2MSLec, 3408C008181 / Configuration / Toronat
	Parlo Address White I
	No. P 1 600 2 600 3 600 4 600 5 600 6 600 6 600 6 600 7 600 8 600 8 600 9 600 10 600 10 600 10 600 10 600 10 600 10 600 10 600 10 600 10 600
DoS defense Log	Click to enable / disable the function of recording DoS defense log onto Syslog.
	Flood Defense
SYN Flood Defense	 Click to enable / disable the SYN flood defense. If enabled, SYN Flood Threshold - Set a threshold value. The default values of threshold is 2000 packets per second. Session Time-Out - Set a threshold value. The default value of
	timeout is 10 seconds.
UDP Flood Defense	 Click to enable / disable the UDP flood defense. If enabled, UDP Flood Threshold - Set a threshold value. The default values of threshold is 2000 packets per second. Session Time-Out - Set a threshold value. The default value of
	timeout is 10 seconds.
ICMP Flood Defense	 Click to enable / disable the ICMP flood defense. If enabled, ICMP Flood Threshold - Set a threshold value. The default values of threshold is 250 packets per second. Session Time-Out - Set a threshold value. The default value of timeout is 10 seconds.
	Port Scan Detection
Port Scan Detection	 Click to enable / disable the port scan defense. If enabled, Port Scan Threshold - Set a threshold value. The default values of threshold is 2000 packets per second.
	Others
Select All	Click to select and enable all items under Others.
	Spoofing Defense
ARP Spoofing Defense Log	Click to enable / disable the store the ARP log to Syslog.
ARP Spoofing Defense	 There are two types for spoofing defense. Block ARP replies with inconsistent source MAC address Block ARP replies with inconsistent Decline VRRP MAC into ARP table

IP Spoofing Defense	There are two types for spoofing defense.	
	Block IP packet from WAN with Inconsistent source IP addresses	
	Block IP replies from LAN with Inconsistent source IP addresses	
Cancel	Discard current modification and keep current configuration.	
Clear All	Discard current modification and return to factory default setting.	
Save	Save the current settings.	

9.4.7.5 APP Enforcement

The APP Enforcement Filter can be used to prevent users from using undesirable or inappropriate network applications such as online chat and peer-to-peer programs. The filter works by detecting and blocking network traffic of applications by means of traffic patterns.

General Setup	2865ac_001DAA41DF78 / Configuration	on / Firewall	Ø
Default Rule	+Add 📋 Delete		
Filter Rules	Index	Profile Name	
DoS Defense			
APP Enforcement			
URL Content Filter			

To create a new profile, click **+Add** to open the following page.

2865Lac_1449BC0D8F00 / Configuration / Firewall			Set to Factory Default 🛛 🖓
Index	1		
Profile Name			
Instant Message	🗌 AIM Login	□ AliWW	Ares
Select All Clear All	🗌 BaiduHi	Facebook/Instagram	E Fetion
	🗌 GaduGadu Protocol		□ iSpQ
	🗆 КС	LINE	LinkedIn
	Paltalk	PocoCall	Qnext
	Signal	Slack	Snapchat
	Telegram	Tencent QQ	🗆 UC
	WebIM URLs	U WhatsApp	U WhatsApp Call
VoIP	RC Voice	Skype/Teams	TeamSpeak
Select All Clear All	TelTel	U WeChat	
P2P	Ares	BitTorrent	ClubBox
Select All Clear All	eDonkey	FastTrack	Gnutella
	Huntmine	🗌 Kuwo	OpenFT
	OpenNap	Pando	SoulSeek
	🗌 Vagaa	Xunlei(Thunder)	
Protocol	BGP	DNS	FTP
Select All Clear All	🗌 GIT	□ H.323	□ HTTP
	IRM Informix	IRM DR2	
			Cancel Save

These parameters are explained as follows:

ltem	Description	
Index	Displays the index number of the profile.	
Profile Name	Displays the name of the profile.	
Select All	Click to select all of the items on this page.	
Clear All	Click to deselect all selected items.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings.	

9.4.7.6 URL Content Filter

The URL Content Filter scans URL strings in HTTP requests for predefined keywords to restrict browsing activities.

General Setup	2865ac_001DAA41DF78 / Configuration /	Firewall			Set to Factory Default
Default Rule	+Add 🗇 Delete				
Filter Rules	Index Profile Name	URL Access Control	URL Access Control Action	Web Feature	Web Feature Action
DoS Defense	D 1	false	Pass	false	Pass
Web Content Filter	Administration Message	<body><center> >The request page has been blocked by URL Control of the second s</center></body>			
DNS Filter		Filter.Please contact your system	1		
Diagnose		administrator for further information.	<pre>//center> ;</pre>		
					Default Message Save

These parameters are explained as follows:

ltem	Description	
+Add	Click to create a new UCF profile.	
Delete	Click to remove the selected UCF profile.	
Default Message	Click to reset the administration message to the factory default.	
Save	Save the current settings.	

To create a new UCF profile, click **+Add** to open the following page.

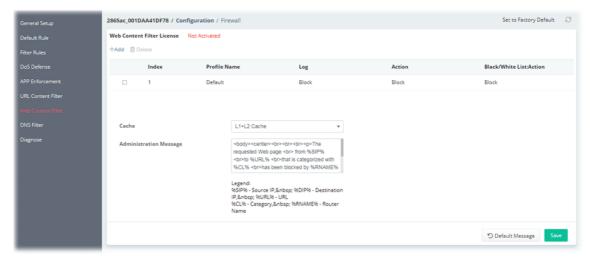
bac_001DAA41DF	78 / Configuration / Firewall	Set to Factory Default	
RL Content Filter F	Profile		
Index	1		
Profile Name			
Priority	E	ther: URL Access Control First	
Log	BI	ock 🔹	
RL Access Control			
URL Access Cont	rol)	
Prevent web acc	ess from IP address)	
Action	P	ass Block	
Index	Keyword Object	Action	
1	None	▼ + Add	
Index	Keyword Group	Action	
1	None	✓ + Add	
Exception List	Q		
		Cancel Sav	ve
	I		

ltem	Description
	URL Content Filter Profile
Index	Displays the index number of the UCF profile.

Profile Name	Displays the name of the UCF profile.
Priority	Select the order of evaluation of URL Access Control and Web Feature.
Log	Select the access attempts (None, Pass, Block or All) to be recorded on Syslog.
	URL Access Control
URL Access Control	Click to enable or disable the URL access control.
Prevent web access from IP Address	Click to enable or disable the function of preventing users from circumventing URL Access Control.
Action	This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First.
	Pass - Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked
	Block - Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed.
Keyword Object	Index - Displays the index number of keyword object profile.
Table	Keyword Object - Displays the name of the keyword object profile.
	Action - +Add - Click to add a new entry to specify a keyword object profile.
Keyword Group Table	Index - Displays the index number of keyword group profile.
	Keyword Group - Displays the name of the keyword group profile.
	Action (+Add) - Click to add a new entry to specify a keyword group profile.
Exception List	lt is available when URL Access Control is enabled.
	Index - Displays the index number of exception object profile.
	Exception Keyword Object /Group - Displays the name of the exception keyword object/group profile.
	Action (+Add) - Click to add a new entry to specify an exception keyword object / group profile.
	Web Feature
Web Feature Restriction	Click to enable or disable the web feature restriction function.
Action	Pass - Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects.
	Block - Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects.
File Extension	Choose one of the profiles for passing or blocking the file downloading.
Cookie, Proxy,	Click to enable or disable cookie function.
Upload	If enabled, it can block cookies from Internet websites.
Proxy	Click to enable or disable proxy function.
	If enabled, it can block web proxy servers that relay HTTP traffic.
Upload	Click to enable or disable upload function.
	If enabled, it can block HTTP uploads from the LAN to the Internet.
Cancel	Discard current modification and return to previous page.

9.4.7.7 Web Content Filter

Users can also be prevented from browsing certain types of websites by using the Web Content Filter. This filter classifies website domain names into different categories, which can be selectively blocked.



ltem	Description
Set to Factory Default	Clear all profile settings.
+Add	Click to create a new WCF profile.
Delete	Click to remove the selected WCF profile.
Index	Displays the index number of the WCF profile.
Profile Name	Displays the name of the WCF profile.
Log	Displays the type (Pass or Block or All) of the log to be recorded.
Action	Displays the type (Pass or Block) of the action selected.
Black/White List	Displays the action to be taken when a WCF matches keyword group and object selections.
Cache	None – The router verifies every HTTP URL requested by communicating with the WCF server on the Internet.
	L1 – The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs.
	L2 – After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server.
	L1+L2 Cache – The router will utilize both L1 and L2 caches.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box.
Default Message	Click to reset the administration message to the factory default.

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

To create a new WCF profile, click **+Add** to open the following page.

2865ac_001DAA41DF78	/ Configuration / Firewall		Set to Factory Default 🛛 📿
Web Content Filter Pro	file		
Index	2		
Profile Name			
Syslog	Block	•	
Action	Pass Block		
White/Black List			
Black/White List	\bigcirc		
Action	Pass Block		
Index	Keyword Object	Action	
1	None *	+ Add	
Index	Keyword Group	Action	
1	None	+ Add	
Category Selection	Select / Clear All		
Child Protection	C Alcohol & Tobacco	Criminal Activity	
			Cancel Save

ltem	Description			
item	Description			
	Web Content Filter Profile			
Index	Displays the index number of the WCF profile.			
Profile Name	Displays the name of the WCF profile.			
Syslog	Displays the type (Pass or Block or All) of the log to be recorded.			
Action	Pass - Only passed access attempts will be recorded in Syslog.			
	Block - Only blocked access attempts will be recorded in Syslog.			
White/Black List				
Black/White List	Click to enable or disable the function of Black/White List. Keyword objects and groups can be applied to the URL to override WCF category filtering.			
Action	Action to take when a URL matches keyword group and object selections.			
	Pass - Allow access to the URL.			
	Block - Disallow access to the URL.			
Keyword Object	Index - Displays the index number of keyword object profile.			
Table	Keyword Object - Displays the name of the keyword object profile.			
	Action - +Add - Click to add a new entry to specify a keyword object profile.			
Keyword Group Table	Index - Displays the index number of keyword group profile.			
	Keyword Group - Displays the name of the keyword group profile.			
	Action (+Add) - Click to add a new entry to specify a keyword group			

profile.		
	Category Selection	
Select/Clear All	Click to select or deselect all items under Category Selection.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.7.8 DNS Filter

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames.

 Configuration 	2865ac_001DAA000000 / Configur	2865ac_001DAA000000 / Configuration / Firewall			Set to Factory Default 📿
General Setup	+ Add D below 1				
Default Rule	Index	Profile Name	DNS Sysleg	DNS WCF	DNS UCF
Filter Rules.			Block	None	None
DoS Defense					
APP Enforcement	DNS Filter Local Setting				
URL Content Filter	DNS Filter	CD			
Web Content Filter	Syslog	None			
ONS THE	WCF	None			
Diagnose					
	UCF	None	~		
	Administration Message	Web page «br» from % «br»that is categorize blocked by %RNAME%	d with %CL% 6 DNS Filter. p Please dimenstrator for further		
					D Default Message Save

ltem	Description
+Add	Click to add a new DNS filter profile.
Delete	Click to remove the selected DNS filter profile.
Index	Displays the index number of the DNS filter profile.
Profile Name	Displays the name of the DNS filter profile.
DNS Syslog	Displays the filtering type (Block, Pass, All or None) of the DNS syslog.
DNS WCF	Displays the name of the WCF profile.
DNS UCF	Displays the name of the UCF profile.
	DNS Filter Local Setting
DNS Filter	Click to enable / disable the DNS filter function.
Syslog	Select the filtering type (Block, Pass, All or None) of the DNS syslog.
WCF	Select a WCF profile.
UCF	Select a UCF profile.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box.
Default Message	Click to reset the administration message to the factory default.

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

To create a new DNS profile, click **+Add** to open the following page.

DNS Filter		
Index	1	
Profile Name		
Syslog	Block	~
WCF	None	~
UCF	None	~

ltem	Description
Index	Displays the index number of the DNS filter profile.
Profile Name	Enter a name of the DNS filter profile.
Syslog	Select the filtering type (Block, Pass, All or None) of the DNS syslog.
WCF	Select a WCF profile.
UCF	Select a UCF profile.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.7.9 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet.

← Configuration	2865ac_001DAA000000 / Configuration / Firewall			C		
General Setup	Firewall Diag	gnose				
Default Rule						
Filter Rules	Mode		UDP	۷.		
DoS Defense	Direction		From LAN	3		
APP Enforcement	IP Ver		IPv4	9		
URI. Content Filter	LAN IP		192.168.1.12			
Web Content Filter	LAN Port		0			
DNSHiller	LAN MAC		00.00.00.00.00.00			
Rapate	WAN IP		80.0.0			
	WAN Port					
	HAR POR		0			
					Analyze Reset Save	
	Note: Please					
	Packet & Pay	load				
	Index	Enable	Direction	Payload Type	Payload Data	TCP Flag
	1	Enable	AtoB	CUSTOMIZE		
	2	Disable	AtoB	CUSTOMIZE		
	() Note:	0 - 1050 (2007) - 00				
	 This is 	firewall live test which need s	etup WAN and plug cable in.			

These parameters are explained as follows:

ltem	Description
------	-------------

	Firewall FwDiagnose			
Mode	Specify the service type (ICMP, UDP, TCP) of the packet.			
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test.			
IP Ver	Select the type of the IP address (IPv4/IPv6).			
LAN IP	Enter the IPv4/IPv6 address of the packet's source.			
LAN Port	Enter the port number of the packet's source.			
LAN MAC	Enter the MAC address of the packet's source.			
WAN IP	Enter the IPv4/IPv6 address of the packet's destination.			
WAN Port	Enter the IPv4/IPv6 address of the packet's destination.			
Analyze	Execute the test and analyze the result.			
Reset	Reset the diagnose settings.			
	Packet & Payload			
Index	Displays the index number of the profile.			
Enable	Displays if the profile is enabled or disabled.			
Direction	The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet.			
Payload Type	Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET).			
Payload Data	It is available when Customize is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transferred with protocol (ICMP/UDP/TCP) which is different to Type setting.			
Save	Save the current settings.			

Click the index number (1 - 5) to configure detailed settings for Packet & Payload.

365ac_001DAA41DF78 / Configuration / Firewall Diagnose					
Packet & Payload					
Packet	1				
Enable	Enable Disable	~			
Direction	AtoB BtoA	~			
Payload Type		•			
			Cancel Save		
Note: • This is firewall live test which need setup WAI	iote: This is firewall live test which need setup WAN and plug cable in.				

ltem	Description			
Packet	Display the index number of the profile.			
Enable	Enable - Enable this profile. Disable - Disable this profile.			
Direction	Select the direction for the second packet.			

	AtoB				
	• BtoA				
Payload Type	Displays the mode selected above and the state.				
Cancel	Discard current modification and return to previous page.				
Save	Save the current settings and return to previous page.				

9.4.8 User Management

9.4.8.1 General Setup

Global settings for User Management can be configured in this section.

Configuration	2865ac_001DAA000000 / Configuration / User Management		C
General Schop User Profile User Group	Mode Selection Mode Rule-Based User-Based		
	Authentication page		
	Web Authentication HTTP HTTP5		
	Display IP Enable		
	Landing page		
	Landing Page +body stats=1+-script Language* (wtodew.location="http://www.dired t=+/body=	sscrigt** k.com <th></th>	
		Cancel Sine	

ltem	Description			
	Mode Selection			
Mode	Rule-Based - Router applies filter rules configured in Firewall>>General Setup and Filter Rule.			
	User-Based - Router applies filter rules configured in User Management>>User Profile.			
	Authentication page			
Web Authentication	 Set the Web protocol for the web authentication page. HTTP HTTPS 			
Login Page Greeting	Click to be redirected to Configuration>>Admin Account >> Login Page Greeting ,			
Display IP Enable	Click to enable or disable the function.			
	If enabled, the IP address of the client will be shown on the tracking window.			
	Landing page			
Landing Page	HTML code to be shown on the Login Page Greeting.			
Cancel	Discard current modification.			

9.4.8.2 User Profile

This page allows you to create up to 200 user profiles for use with User Management.

2865ac_001DAA151EB8 / Configuration / User Management						ß				
Index	Enable This Account	User Name	Password	Idle Timeout	Max User Login	External Server Authentication	Log	Pop Browser Tracking Window	Authentication:Web	Au
1	true	admin		0	0	None	None	false	true	tr
2	true	Dial-In User		0	0	None	None	false	true	fa
3	true	999		10	0	None	None	true	true	tru
4	false			10	0	None	None	true	true	tri

To configure the user management profile, move the mouse cursor to any entry and click to open the setting page.

← Configuration	2865Lac_1449BC0D8F00 / Configuratio	/ User Management	e
General Setup	General Settings		
There Broudfile User Genups	Index	1	
	Enable This Account	©	
	Usernamie	admin	
	Password		
	Log	None-	
	External Server Authentication	None	
	Login Settings		
	Idle Timeout	0	
	Max User Login		
	Authentication:Web	C	
	Authentication:Alert Tool	•	
	Authentication:Telnet	0	
	Landing Page	0	
	Auto Logout(minutas)	0	
		0	Cancel Save

ltem	Description		
	General Settings		
Index	Displays the index number of the user profile.		
Enable This Account Click to enable or disable this user profile.			
Username Enter the login name of this user profile.			
Password	Enter the password of this user profile.		
Log	Select which activities (None, Login, Event or All) of the user can be recorded by Syslog.		
External ServerThe router will authenticate dial-in users using either a built-in (NAuthenticationexternal service (LDAP, Radius or TACACS+).			
	Login Settings		
Idle Timeout	If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will need to re-authenticate before Internet access is once again allowed.		

Max User Login	Enter the maximum number of concurrent logins allowed for this profile.
Authentication:Web	Click to enable or disable the function.
	If enabled, user will need to authenticate by entering a username and password when attempting to access an external website for the first time The user will be redirected to the external website after a successful authentication.
Authentication:Alert	Click to enable or disable the function.
ΤοοΙ	If enabled, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed.
Authentication:Telne	Click to enable or disable the function.
t	If enabled, the user can authenticate by logging in to the router using telnet.
Landing Page	Click to enable or disable the function.
	If enabled, when a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in 6.3.8.1 General Setup.
Auto Logout(minutes)	This account will be forced to logout after a certain time set here.
Pop Browser	Click to enable or disable the function.
Tracking Window	If enabled, a browser window will pop up showing the session time remaining.
	Quota Policy
Login Permission Schedule 1/2/3/4	Enter four sets of time schedule for your request.
Time Quota Enable	Click to enable or disable the function.
Time Quota:Mins	Specify the amount of time (after a successful authentication).
	Click + / - to increase / decrease the time quota for this profile.
Data Quota Enable	Click to enable or disable the function.
Data Quota Value	Specify the amount of data (after a successful authentication).
	Click + / - to increase / decrease the data quota for this profile.
	Reset Quota Automatically
Enable	Click to enable or disable the function.
Default Time Quota(Mins)	Enter value for default time quota.
Default Data Quota(MB)	Enter value for default data quota.
Quota reset	When login permission schedule expired - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.
	At the start time of Schedule -
	• Quota reset schedule - Specify a time schedule index number for this profile.

Internal RADIUSClick to enable or disable the function.			
Local 802.1xClick to enable or disable the function.			
Cancel	Discard current modification and return to previous page.		
Save	Save the current settings and return to previous page.		

9.4.8.3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in **Firewall>>General Setup**.

General Setup		2865ac_001DAA15	2865ac_001DAA151EB8 / Configuration / UserManagement				
User Profile		Index	Name	Selected User Objects			
User Group		1					
	_						

To configure the user group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration /	UserManagement	Ø
User Group		
Name		
Selected User Objects		
🖹 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description
Name	Enter a name for identifying this user group.
Selected User Objects	Use the drop down menu to select the user object(s).
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9 Object Setting

9.4.9.1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently.

IP Object	2865ac_001DA	AA151EB8 / Configura	ation / Objects Setting			
	Index	Name	Interface	Address Type	Information	
	1		Any	Subnet Address		
	2		Any	Subnet Address		
	3		Any	Subnet Address		
	4		Any	Subnet Address		
	5		Any	Subnet Address		
	6		Any	Subnet Address		
	7		Any	Subnet Address		
SMS Service Object	8		Any	Subnet Address		
Mail Service Object	9		Any	Subnet Address		
Notification Object	10		Any	Subnet Address		
String Object	11		Any	Subnet Address		
Country Object	12		Any	Subnet Address		
	13		Any	Subnet Address		
	14		Any	Subnet Address		
	O Note:Excla	amation mark (!) on Inf	ormation column means that Inv	ert Selection is enabled.		

To configure the IP object profile, move the mouse cursor to any entry and click to open the setting page.

65ac_001DAA000000 / Configu	uration / Objects Setting		Set to Factory Default
Index	1		
Name	RD Department		
Interface	Any	~	
Address Type	Range Address	~	
Start IP Address	192.168.1.9		
End IP Address	192.168.1.9		
Invert Selection			
			Cancel

ltem	Description
Index	Displays the index number of the IP object profile.
Name	Enter the name of the IP object profile.
Interface	Select the network interface on which the IP address or addresses are to be found.
Address Type	Any Address - Object covers all IP addresses.
	Mac Address - Object contains a MAC address.
	• MAC Address - Enter the MAC address.
	Range Address - Object covers a range of IP addresses.
	• Start IP Address - Enter an IP address as the starting point.
	• End IP Address - Enter an IP address as the ending point.
	Single Address - Object covers one IP address.
	• Start IP Address - Enter an IP address as the starting point.
	Subnet Address - Object covers a range of IP addresses specified in subnet notation.
	• Start IP Address - Enter an IP address as the starting point.

	• Subnet Mask - Enter the subnet mask.
Invert Selection	Click to enable or disable the function. If enabled, all addresses except the ones entered above will be used.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.2 IP Group

Multiple IP Objects can be placed into an IP Group.

IP Object	2865ac_001D	AA151EB8 / Config	uration / Objects Setting		Ø
	Index	Name	Interface	Selected IP Objects	
	1		Any		
	2		Any		
	3		Any		
	4		Any		
	5		Any		
	6		Any		
	7		Any		
SMS Service Object	8		Any		
	9		Any		
Notification Object	10		Any		
String Object	11		Any		
	12		Any		
	13		Any		
	14		Any		
	15		Any		
	16		Any		

To configure the IP group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration /	Objects Setting	ß
Index	1	
Name		
Interface	Any 👻	
Selected IP Objects		
		Cancel Save

ltem	Description	
Index	Displays the index number of the IP object profile.	
Name	Enter the name of the IP object profile.	
Interface	Select WAN, LAN or Any to filter IP objects.	
Selected IP Objects	Use the drop down menu to select the IP object(s).	
Cancel	Discard current modification and return to previous page.	

Save

9.4.9.3 IPv6 Object

Up to 64 IPv6 Objects can be created.

Index product Index Name Address Type Inormation Match Sympe Inde diges 1 Subnet Address	2865ac_00	A151EB8 / Configuration / Objects Setting			Ê
Indeferred Indeferred <th>Index</th> <th>Name Address T</th> <th>ype Information</th> <th>Match Type</th> <th>Prefix Len.</th>	Index	Name Address T	ype Information	Match Type	Prefix Len.
Image: Control Dependence on the Control Dependence o	1	Subnet A	ddress ::	-	0
Service Type Group 4 Subnet Address :: Keyword Object 5 Subnet Address :: File Extension Object 7 Subnet Address :: SNS Service Object 8 Subnet Address :: Mail Service Object 9 Subnet Address :: Notification Object 10 Subnet Address :: String Object 10 Subnet Address :: String Object 12 Subnet Address :: String Object 13 Subnet Address :: 13 Subnet Address :: 14 Subnet Address ::	2	Subnet A	ddress ::		0
Køyword Group 5 Subnet Address :: - Køyword Group 6 Subnet Address :: - Pile Extension Object 7 Subnet Address :: - SMS Service Object 8 Subnet Address :: - Mal Service Object 9 Subnet Address :: - Notification Object 10 Subnet Address :: - Notification Object 10 Subnet Address :: - String Object 12 Subnet Address :: - Gouthy Object 13 Subnet Address :: - 14 Subnet Address :: - -	3	Subnet A	uddress ::	-	0
Name File Subnet Address # - File File Subnet Address # - SMS Service Object 8 Subnet Address # - Mull Service Object 9 Subnet Address # - Notification Object 10 Subnet Address # - Notification Object 10 Subnet Address # - String Object 12 Subnet Address # - 12 Subnet Address # - - 13 Subnet Address # - - 14 Subnet Address # - -	4	Subnet A	uddress ::		0
Name Subscription 7 Subscription	5	Subnet A	uddress ::		0
File Extension Object File Extensin Object File Extensin Object F	6	Subnet A	ddress ::		0
Skrive Object P Subnet Address I - Mail Service Object P Subnet Address I - Notification Object 10 Subnet Address I - String Object 11 Subnet Address I - 12 Subnet Address I - 13 Subnet Address I - 14 Subnet Address I -	7	Subnet A	ddress ::		0
Mail Service Object 10 Subnet Address :: Notification Object 11 Subnet Address :: String Object 12 Subnet Address :: 13 Subnet Address :: 14 Subnet Address ::	8	Subnet A	ddress ::		0
Notification Object 10 Subnet Address II	9	Subnet A	uddress ::		0
11 Subnet Address II	10	Subnet A	uddress ::		0
12 Subnet Address 13 Subnet Address 14 Subnet Address	11	Subnet A	uddress ::		0
13 Subnet Address 14 Subnet Address	12	Subnet A	uddress ::		0
	13	Subnet A	uddress ::		0
15 Subnet Address ::	14	Subnet A	uddress ::	-	0
	15	Subnet A	ddress ::		0
16 Subnet Address ::	16	Subnet A	ddress ::		0

To configure the IPv6 object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Object	ts Setting	Set to Factory Default	C
Index	1		
Name			
Address Type	Subnet Address ~		
Start IP Address			
Prefix Length	0		
Invert Selection	\bigcirc		
		Cancel Sa	ve

Item	Description
Index	Displays the index number of the IPv6 object profile.
Name	Enter the name of the IPv6 object profile.
Address Type	Any Address - Object covers all IPv6 addresses.
	• Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	Mac Address - Object contains a MAC address.
	• Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	• MAC Address - Enter the MAC address.
	Range Address - Object covers a range of IPv6 addresses.
	• Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.

	• Start IP Address - Enter an IPv6 address as the starting point.
	• End IP Address - Enter an IPv6 address as the ending point.
	 Invert Selection - If enabled, all addresses except the ones entered above will be used.
	Single Address - Object covers one IPv6 address.
	• Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	• Start IP Address - Enter an IPv6 address as the starting point.
	• Invert Selection - If enabled, all addresses except the ones entered above will be used.
	Subnet Address - Object covers a range of IPv6 addresses specified in subnet notation.
	• Start IP Address - Enter an IPv6 address as the starting point.
	• Prefix Length - Enter IPv6 prefix length, if Address type is Subnet Address.
	• Invert Selection - If enabled, all addresses except the ones entered above will be used.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.4 IPv6 Group

Multiple IPv6 Objects can be placed into an IPv6 Group.

	2865ac_001D	AA151EB8 / Configuration	/ Objects Setting	4
	Index	Name	Selected IPv6 Objects	
	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
Service Object	9			
fication Object	10			
'' ng Object	11			
ntry Object	12			
	13			
	14			
	15			
	16			

To configure the IPv6 group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuratio	865ac_001DAA151EB8 / Configuration / Objects Setting			
Index	1			
Name				
Selected IPv6 Objects				
			Cancel Save	

ltem	Description
Index	Displays the index number of the IPv6 group profile.
Name	Enter the name of the IPv6 group profile.
Selected IPv6 Object	Use the drop down menu to select the IPv6 object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.5 Service Type Object

Up to 96 Service Type Objects can be created.

	2865ac_001DAA151EB8 / Configuration / Objects Setting					g	
	Index	Name	Protocol	Protocol Number	Source Port Option	Source Port From	
	1		Any	0	-	0	
	2		Any	0	-	0	
	3		Any	0	-	0	
	4		Any	0		0	
	5		Any	0		0	
	6		Any	0	-	0	
	7		Any	0	-	0	
MS Service Object	8		Any	0		0	
, Aail Service Object	9		Any	0		0	
	10		Any	0	-	0	
	11		Any	0	=	0	
	12		Any	0	=	0	
	13		Any	0		0	
	14		Any	0		0	
	15		Any	0	-	0	
	16		Any	0	=	0	

To configure the service type object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configurat	ion / Objects Setting	S
Index	1	
Name		
Protocol	Any	
	Any ICMP IGMP TCP UDP TCP/UDP ICMPv6 Other	Cancel Save

ltem	Description
Index	Displays the index number of the service type object profile.
Name	Enter the name of the service type object profile.
Protocol	Choose a protocol to which this profile applies.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.6 Service Type Group

Multiple Service Type Objects can be placed into a Service Type Group.

IP Object	2865ac_001DAA15	1EB8 / Configuration / Objects Setting		Ø
IP Group	Index	Name	Selected Service Type Objects	
IPv6 Object	1			
IPv6 Group	2			
Service Type Object	3			
Service Type Group	4			
Keyword Object	5			
Keyword Group	6			
File Extension Object	7			
SMS Service Object	8			
Mail Service Object	9			
Notification Object	10			
String Object	12			
Country Object	13			
	14			
	15			
	16			

To configure the service type group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration	on / Objects Setting	Q
Index	1	
Name		
Selected Service Type Objects		
		Cancel Save

ltem	Description
Index	Displays the index number of the service type group profile.
Name	Enter the name of the service type group profile.
Selected Service Type Objects	Use the drop down menu to select the service type object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.7 Keyword Object

200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **Web Content Filter Profile**.

IP Object	2865ac_001DAA151EB8 / 0	Configuration / Objects Setting		£
	Index	Name	Contents	
	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	13			
	15			
	16			

To configure the keyword object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration / Objects Setting			
Index	1		
Name			
Contents			
			Cancel Save
L			

ltem	Description	
Index	Displays the index number of the keyword object profile.	
Name	Enter the name of the keyword object profile.	
Contents	Enter the keywords to be matched. Up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

IP Object	2865ac_001DAA151EB8 / Configuration / Objects Setting			
IP Group	Index	Name	Selected Keyword Objects	
IPv6 Object	1			
IPv6 Group	2			
Service Type Object	3			
Service Type Group	4			
Keyword Object	5			
Keyword Group	6			
File Extension Object	7			
SMS Service Object	8			
Mail Service Object	9			
Notification Object	10			
String Object	11			
Country Object	12			
	14			
	15			
	16			

To configure the keyword group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configurat	ion / Objects Setting	Q
Index	1	
Name		
Selected Keyword Objects		
		Cancel Save

ltem	Description	
Index	Displays the index number of the keyword group profile.	
Name	Enter the name of the keyword group profile.	
Selected Keyword Objects	Use the drop down menu to select the keyword object(s).	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.9 File Extension Object

Up to 8 File Extension Objects can be set up for use.

IP Object	2865ac_001DAA151EB8 / Configuration / Objects Setting		C
IP Group	Index	Profile Name	
IPv6 Object	1		
IPv6 Group	2		
Service Type Object	3		
Service Type Group	4		
Keyword Object	5		
Keyword Group	6		
File Extension Object	7		
SMS Service Object	8		
Mail Service Object			
Notification Object			

To configure the file extension object profile, move the mouse cursor to any entry and click to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / Obje	ects Setting	Set to Factory Default	C
File Extension Object Setup			
Index	1		
Profile Name			
Categories			
Index	Categary Name		
1			
2	Video		
3	Audio		
4	Java		
5	ActiveX		
6	Compression		
7	Execution		
8	P2P		
9	Document		
🗓 Clear		Cancel Sa	ave

ltem	Description		
Index	Displays the index number of the file extension object profile.		
Profile Name	Enter the name of the file extension object profile.		
Cancel	Discard current modification and return to previous page.		
Save	Save the current settings and return to previous page.		

9.4.9.10 SMS Service Object

Up to 10 SMS Service Objects can be set up for use.

← Configuration	2865ac_0010	DAA000000 / Configuration / O	ojects Setting	Set to Factory Default
IP Object	Index	Profile Name	Service Provider	
	1	Local number	kotsms.com.tw (TW)	
IP Group	2		kotsms.com.tw (TW)	
IPv6 Object	3		kotsms.com.tw (TW)	
IPv6 Group	4		kotsms.com.tw (TW)	
Service Type Object	5		kotsms.com.tw (TW)	
Service Type Group	6		kotsms.com.tw (TW)	
Keyword Object	.2		kotsms.com.tw (TW)	
Keyword Group			kotsms.com.tw (TW)	
File Edension Object		Custom 1		
2005 Service Object	10	Custom 2		
N. I.P. Children				

To configure the SMS service object profile, move the mouse cursor to index 1 to index 8 and click to open the setting page.

2865ac_001DAA000000 / Configuration / Object	ts Setting	Set to Factory Default	C
Index	1		
Profile Name	Local number		
Service Provider	kotsms.com.tw(TW) ~		
Connection Protocol	HTTP HTTPS		
Username	abc5026		
Password	Φ		
Quota	3		
Sending Interval	3		
 B Note: Only one message can be sent during the ' If the "Sending Interval" was set to 0, there 	Sending Interval [®] time. will be no limitation.		
🗎 Clear		Cancel	Save

ltem	Description		
Index	Displays the index number of the SMS service object profile.		
Profile Name	Enter the name of the SMS service object profile.		
Service Provider	Select a Service Provider from the dropdown list.		
Connection Protocol	Select HTTP or HTTPs.		
Username	Enter a name to log in to the server.		
Password	Enter a password to log in to the server.		
Quota	Set the remaining number of text messages allowed to be sent.		
Sending Interval	Set the minimum amount of time, in seconds, to wait between sending SMS messages.		
Clear	Clear all modifications on this page.		
Cancel	Discard current modification and return to previous page.		
Save	Save the current settings and return to previous page.		

To configure the customized SMS service object profile, move the mouse cursor to index 9 to index 10 and click to open the setting page.

2865ac_001DAA000000 / Configuration / Object	Set to Factory Default	C	
Index	9		
Profile Name	Custom 1		
Service Provider			
Exact URL			
	Wease contact with your SMS provide to get the exact URL String gbuiksmussms.net.5567 (appl/submission/send_sms.p/2.0.0? upsname=###ULDber###dpacsword=###ULDber##dpacsdim=###dutDes####message=###dtMsg###		
Server Response			
Username			
Password	•		
Quota	10		
Sending Interval	3		
 6 Note: Only one message can be sent during the If the "Sending Interval" was set to 0, there 	Sending Internal" time. will be no limitation.		
會 Clear		Cancel	Save

ltem	Description			
Index	Displays the index number of the SMS service object profile.			
Profile Name	Displays the name of the SMS service object profile.			
Service Provider	Enter an identifier for the service provider. Maximum length is 23 characters.			
Exact URL	Enter the URL for the SMS service.			
Username	Enter a name to log in to the service.			
Password	Enter a password to log in to the service.			
Quota	Set the remaining number of text messages allowed to be sent.			
Sending Interval	Set the minimum amount of time, in seconds, to wait between sending SMS messages.			
Clear	Clear all modifications on this page.			
Cancel	Discard current modification and return to previous page.			
Save	Save the current settings and return to previous page.			

9.4.9.11 Mail Service Object

Up to 10 Mail Service Objects can be set up for use.

IP Object	2865ac_001DAA000000 / Configuration / Objects Setting				
IP Group	Index	Profile Name	SMTP Service	SMTP Port	Sender Address
IPv6 Object	1			0	
IPv6 Group	2			0	
Service Type Object	3			0	
Service Type Group	4			0	
Keyword Object	5			0	
Keyword Group	6			0	
File Extension Object	7			0	
SMS Service Object	8			0	
Mail Service Object	9			0	
Notification Object	10			0	
String Object					
Country Object	う Set to Factory Defau	lt			

To configure the mail service object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Objects Setting			Set to Factory Default	C
Index	1			
Profile Name	Mail_Notify			
SMTP Server	192.168.1.98			
SMTP Port	25			
Sender Address	carrie_@draytek.com			
Use SSL	\bigcirc			
Authentication				
Username	John			
Password	٩			
Sending Interval	0			
 β Note: Only one mail can be sent during the "Sent If the "Sending Interval" was set to 0, there 	ling Interval" time. will be no limitation.			
盦 Clear			Cancel	ave

ltem	Description			
Index	Displays the index number of the mail service object profile.			
Profile Name	Enter the name of the mail service object profile.			
SMTP Server	Enter the IP address of the SMTP server.			
SMTP Port	Enter the port number of the SMTP server.			
Sender Address	Enter the e-mail address of the sender.			
Use SSL	Click to enable or disable the function. If enabled, Vigor router will use SMTPS (SMTP over SSL) to communicate with the SMTP server.			
Authentication	Click to enable or disable the function. Username - Enter a name for authentication. Password - Enter the password for authentication.			

Sending Interval	Specify the minimum amount of time, in seconds, to wait between sending e-mail messages.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.12 Notification Object

Up to 8 Notification Objects can be set up for use.

IP Object	2865ac_001DAA0	00000 / Configuration / Object	cts Setting		Ø
IP Group	Index	Profile Name	Settings		
IPv6 Object	1				
IPv6 Group	2				
Service Type Object	3				
Service Type Group	4				
Keyword Object	5				
Keyword Group	6				
File Extension Object	7				
SMS Service Object	8				
Mail Service Object					
Notification Object	Set to Factory	Default			
String Object					

To configure the notification object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Objects	Setting	ø
Index	1	
Profile Name		
WAN	Disconnected	
	Reconnected	
VPN Tunnel	Disconnected	
	Reconnected	
	Sar Trader Provider	
Temperature Alert	OutofRange	
WAN Budget		
WAN Budget	UmitReached	
Central VPN Management	CPE Offline	
	CPE Config Backup Fail	
	CPE Config Restore Fail	
	CPE Firmware Upgrade	
	Fail	
	CPE VPN Profile Setup Fail	
High Availability	Failover Occurred Config	
	Sync Fail Router Unstable	
Security	🗆 Web Login	
	Teinet Login	
	SSH Login	
	C TR069 Login	
	FTP Login	
Gear	0 fut fund	
e clear	Cancel	Save

ltem	Description
Index	Displays the index number of the notification object profile.
Profile Name	Enter the name of the mail service object profile.
Check boxes	Select the states to be monitored.

Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.13 String Object

Set string profiles which will be applied in route policy.

<- Configuration	2865ac_001	DAA000000 / Configuration / Objects Setting	Set to Factory Default
	Index	String	
IP Object	1	Floor_1	
# Group	2	Floor_2	
IPv6 Object	3	server1.draytek.com	
IPv6 Group	4	Draytek Hotspot	
	5	Floor_2	
Service Type Object	6	portal draytek.com	
Service Type Group	7		
Keyword Object	8	portai.draytek.com	
Keyword Group	9		
	10		
File Extension Object.	11		
SMS Service Object	12		
Mail Service Object	13		
	14	Draytek Hotspot	
Notification Object	15		
	16	test1	
Country Object	17	test	
	18	NTP	
	19	NTP	
	20		

To configure the string object profile, move the mouse cursor to any entry and click to open the setting page.

Index 1	
String (Max.253 chars.)	
æ	
Clear Cance	el Save

ltem	Description	
Index	Displays the index number of the string object profile.	
String	nter a string.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.14 Country Object

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

2865ac	001DAA000000 / Configuration / Objects S	letting	
up Index	Name	Selected Objects	
Object 1			
i Group 2			
ervice Type Object 3			
rvice Type Group			
5			
eyword Object 6			
eyword Group 7			
le Extension Object 8			
MS Service Object			
ail Service Object			
11			
12			
tring Object 13			
suntry Object 14			
15			
16			
17			
18			
19			
20			
	to Factory Default		

To configure the country object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Objects Se	etting	Ø
Index	1	
Name		
Selected Country Objects		
 8 Note: The maximum number of Selected Count 	ry is 16.	
🖹 Clear	Can	ncel Save

ltem	Description
Index	Displays the index number of the country object profile.
Name	Enter the name of the mail country object profile.
Selected Country Objects	Use the drop down menu to select the country object(s).
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10 QoS

9.4.10.1 QoS WAN

Configuration	2865ac	001DAA00	00000 / Conf	Iguration / QoS							-
	Index	Status	Direction	Inbound Bandwidth	Outbound Bandwidth	Class 1 Ratio	Class 2 Ratio	Class 3 Ratio	Others Ratio	Enable UDP Bandwidth Control	
	1	false	BOTH	0	0	25	25	25	25	false	
leS Claus	2	false	BOTH	100000	100000	25	25	25	25	fatse	
loS Service Type	3	false	вотн	100000	100000	25	25	25	25	fatse	
olP Prioritization	4	false	BOTH	100000	100000	25	25	25	25	false	
ag Outbound Traffic	5	false	BOTH	100000	100000	25	25	25	25	false	
	6	false	BOTH	100000	100000	25	25	25	25	faise	

To configure the QoS WAN profile, move the mouse cursor to any entry and click to open the setting page.

865ac_001DAA000000 / Configuration / C	QoS		Ø
Interface Settings			
WAN	2		
QoS Policy	Ð		
Direction	BOTH	¥	
Inbound Bandwidth (kbps)	100000		
Outbound Bandwidth (kbps)	100000		
Bandwidth Reserved for each Class			
Class 1 Ratio (%)	25		
Class 2 Ratio (%)	25		
Class 3 Ratio (%)	25		
Others (%)	25		
Advanced Settings			
UDP Bandwidth Control	0		
UDP Bandwidth Ratio (%)	25		
Prioritize Outbound TCP ACK	Ð		
			Court Court
			Cancel Save

ltem	Description
	Interface Settings
WAN	Display the index number of the WAN interface.
QoS Policy	Click to enable or disable this QoS policy.
Direction	Use the drop-down list to set the direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both).
Inbound Bandwidth(kbps)	Set the inbound bandwidth of the WAN.
Outbound Bandwidth(kbps)	Set the outbound bandwidth of the WAN.
	Bandwidth Reserved for each Class
Class 1 ~3 Ratio (%)	Set the percentage of bandwidth reserved for each class.
Others (%)	Set the percentage of bandwidth reserved for others.

	Advanced Settings
UDP Bandwidth Control	Click to enable or disable this function. If enabled, the router will restrict the bandwidth available to UDP traffic.
UDP Bandwidth Ratio(%)	Enter a percentage value.
Prioritize Outbound TCP ACK	Click to enable or disable this function. If enabled, the router will give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10.2 QoS Class

Configure Class 1 to Class 3 with detailed settings.

QoS WAN	2865ac_001DAA000	0000 / Configuration / QoS	4
	Index	Enable Tag Packet AS	Tag Packet AS
QoS Service Type	1	false	Default
	2	false	Default
ag Outbound Traffic	3	false	Default

To configure the QoS class profile, move the mouse cursor to any entry and click to open the following page.

		Local Address Type	Local Start IP	Local End IP	Local Mask	Remote Address Type	Remote Start IP	Remote End IP	Re		
f f	false	Any	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0		
2 t	true	Any	0.0.0.0	0.0.0.0	0.0.0.0	Any	0.0.0.0	0.0.0.0	0.0		
3 t	true	Any	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0		
4 τ	true	Any	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0		
5 f	false		0.0.0.0	0.0.0.0	0.0.0.0		0.0.0.0	0.0.0.0	0.0		

Then, click any index number to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / QoS		C
ACT	D	
IP Version	IPv4 ~	
Local Address Type	~	
Remote Address Type	~	
Diff Serv Code Point		
Service Type	~ ·	
Change to Class	~	
💼 Clear		Cancel Save

ltem	Description
АСТ	Click to enable or disable this function.
IP Version	Select IPv4 or IPv6.
Local Address Type	 Set the remote (WAN) IP address or address range for the rule. Any - The rule covers all IP addresses. Range - The rule covers a range of IP addresses. Local Start IP Address - Enter an IP address as the starting point. Local End IP Address - Enter an IP address as the ending point. Single - The rule covers one IP address. Local Start IP Address - Enter an IP address as the starting point. Single - The rule covers one IP address. Local Start IP Address - Enter an IP address as the starting point. Subnet - The rule covers a range of IP addresses specified in subnet notation.
	 Local Start IP Address - Enter an IP address as the starting point. Local Mask - Enter the subnet mask for the above IP address. Group and Object - The rules covers a range of IP address specified in a group or object profile.
Remote Address Type	 Set the remote (WAN) IP address or address range for the rule. Any - The rule covers all IP addresses. Range - The rule covers a range of IP addresses. Remote Start IP - Enter an IP address as the starting point. Remote End IP - Enter an IP address as the ending point. Single - The rule covers one IP address. Remote Start IP - Enter an IP address as the starting point. Subnet - The rule covers a range of IP address specified in subnet notation. Remote Start IP - Enter an IP address as the starting point. Group and Object - The rules covers a range of IP address specified in a group or object profile.
Diff Serv Code Point	Enable it to set DSCP or ToS precedence of packets to which this rule applies.
Service Type	Choose a service type to which this rule applies.
Change to Class	Specify a class for the QoS class profile.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10.3 QoS Service Type

QoS WAN	2865ac_001DAA0	000000 / Configura	ition / QoS			0
QoS Class	Index	Name	Protocol Type	Port Type	Port Number From	Port Number To
QoS Service Type	1		TCP	Single	0	0
VoIP Prioritization						
Tag Outbound Traffic						

To configure the QoS service type profile, move the mouse cursor to any entry and click to open the following page.

865ac_001DAA000000 / Configuration / QoS		
Index	1	
Name		
Service Type	TCP	×
Port Type	Single Range	×
Port Number Start	0	
Port Number End	0	

ltem	Description
Index	Display the index number of the profile.
Name	Enter a name of this profile.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Type	Single - Set a port number for this profile.
	• Port Number Start - Enter the starting port number.
	Range - You have to set the starting port number and the end porting number on the boxes below.
	• Port Number Start - Enter the starting port number.
	• Port Number End - Enter the end porting number.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10.4 VoIP Prioritization

QoS WAN	2865ac_001DAA000000 / Configuration	/ QoS					g
QoS Class	Enable the First Priority for VoIP SIP/	тр 💽					
QoS Service Type	SIP UDP Port	5060					
VolP Prioritization							
Tag Outbound Traffic							Cancel Save
	VoIP QoS Status						
	VoIP Staus LAN IP VoIP Staus Peer IP	VoIP Staus Interface VoIP Stau	s Delayms VolP Staus Delay Draw	VoIP Staus Jitterms	VoIP Staus Jitter Draw	VoIP Staus Packet Lossms	VolP Staus Loss Draw
				No d	lata available		

ltem	Description
Enable the First Priority for VoIP SIP/RTP	Click to enable or disable the function. If enabled, VoIP traffic will be received with the highest priority.
SIP UDP Port	Set a port number to be monitored for SIP traffic.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.
VoIP QoS Status	Displays current VoIP QoS status.

9.4.10.5 Tag Outbound Traffic

Tag the outgoing traffic with the DSCP or Precedence value.

QoS WAN	2865ac_001DAA000000 / Configuration / QoS	Ø
QoS Class	Enable Tag Packet AS	Tag Packet AS
QoS Service Type	false	Default
VolP Prioritization	false	Default
Teg Outbound Treffic	false	Default

To configure the tag outbound traffic profile, move the mouse cursor to any entry and click to open the following page.

865ac_001DAA000000 / Configuration / QoS		
Class	1	
Enable		
Add DSCP or Precedence Value	Default	•

These parameters are explained as follows:

ltem	Description
Class	Display the index number of the class.
Enable	Click to enable or disable the profile.
Add DSCP or Precedence Value	Use the drop-down list to choose the value for applying the DSCP or precedence value for each class.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11 Applications

9.4.11.1 Dynamic DNS

The Vigor router supports a wide range of DDNS providers, such as DynDNS, No-IP.com, DtDNS, and ChangeIP. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.

<- Configuration	2865a	_001DAA0000	00 / Configuration / Ap	plications									Set to	Factory Defaul	u c
														View Log Foro	e Update
LAN DNS / DNS Forwarding															
	Dyn	amic DNS Se	tup												
Schedule	Enabl	e		0											
External RADIUS	Auto-	Update interval		14400											
Internal RADIUS															
External INCACS+															Save
Active Directory /LDAP															Jave
JPnP	Index	Enable Account	Service Provider	Service Type	Host Name	Domain Name	Login Name	Password	Wildcards	Backup MX	Mail Extender	WAN Interface	Determine WAN IP	Provider Host	Service
	1	false	dyn.com_{www.dyn.com}	Dynamic					false	false		WAN1_First	WAN_IP		
CMP	2	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
Nake on LAN	3	false	dyn.com_(www.dyn.com)	Dynamic					talse	false		WAN1_First	WAN_IP		
SMS / Mail Alert Service	4	false	dyn.com_(www.dyn.com)	Dynamic					talse	false		WAN1_First	WAN_IP		
	5	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
Bonjour	6	faise	dyn.com_(www.dyn.com)	Dynamic					false	faise		WAN1_First	WAN_IP		
High Availability															

To configure the DDNS profile, move the mouse cursor to any entry (1 to 6) and click to open the following page.

2865ac_001DAA000000 / Configuration / Applic	ations		C
Enable Account			
WAN Interface	WAN1 First ~		
Service Provider	dyn.com (www.dyn.com)		
Service Type	Dynamic ~		
Host Name			
Domain Name	~		
Login Name			
Password	٥		
Wildcards	\bigcirc		
Backup MX	\bigcirc		
Mall Extender			
Determine WAN IP	WAN IP ~		
👜 Clear		Cancel S	ive

Item	Description
Enable Account	Click to enable or disable the account.
WAN Interface	Select the WAN interface to monitor for IP address changes.
Service Provider	Select the DDNS provider. If your DDNS provider is not listed, select User-Defined and manually configure the profile.
Service Type	Select the service type (Custom, Dynamic, Static) that matches that of your DynDNS account.
Host Name	Enter the IP address or the domain name of the host which provides related service.
Domain Name	Select one domain name.
Login Name	Enter the login name of the DDNS account.
Password	Enter the password of the DDNS account.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please enter the name in this area. Such mail server will be used as backup mail exchange.
Determine WAN IP	 There are two methods offered for you to choose: WAN IP - The IP address of the router's WAN interface will be used. Internet IP - The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.2 LAN DNS/DNS Forwarding

LAN DNS allows the network administrator to override standard DNS resolutions for selecting domain addresses. The router will respond to queries on matched domain addresses with custom IP addresses.

Dynamic DNS		/ C	onfiguration / Applications			Set to Factory Default ${egin{array}{ccc} {\cal C} \end{array}}$
LAN DNS / DNS Forwarding	Index	Enable	Profile Name	Domain Name	DNS Server IP Address	Set To Factory Default
DNS Security	1	false				false
Schedule						
External RADIUS						
Internal RADIUS						

To configure the profile, move the mouse cursor to any entry and click to open the following page.

2865ac_001DAA000000 / Configurat	ion / Appl	lications				C
Enable						
Profile						
Domain Name						
DNS Server IP Address						
CNAME(Alias Domain Name)						
	Index	CNAME	Acti	ion		
	1		+	Add		
IP Address List						
	Index	IP Address	Same Subnet Reply	Action		
	1		\bigcirc	+ Add		
fi Clear					Cancel Sa	e

ltem	Description
Enable	Click to enable or disable the profile.
Profile	Enter a name to identify this profile.
Domain Name	Enter the domain name for the router to look for in DNS queries to intercept and reply to.
DNS Server IP Address	Enter the IP address of the DNS server you want to use for DNS forwarding.
	CNAME(Alias Domain Name)
Index	Displays the index number of the IP alias.
СЛАМЕ	Enter a domain name alias for the domain name.
+Add	After entering the CNAME, Click to save the setting and create a new entry.
	IP Address List
Index	Displays the index number of the IP address.
IP Address	The IP address entered here will be used for mapping with the domain name specified above.
Same Subnet Reply	Click to enable or disable the function. If enabled, the router will only respond to the DNS request which coming from the same subnet of the IP address specified in this entry.
+Add	After entering the IP address, Click to save the setting and create a new

	entry.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

7.3.11.3 DNS Security

Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

 Configuration 			guration / Applications				1
Dynamic DNS	General	Setup					
LAN DNS / DNS Forwarding	Index	Interface	Enable	Primary DNS	Secondary DNS	Bogus DNS Reply	
	1	WAN1	false	0.0.0.0	0.0.0.0	Pass	
Schedule	2	WAN2	table	0.0.0.0	0.0.0.0	Pass	
External RADIUS	3	WAN3 WAN4	false	0.0.0.0	0.0.0.0	Pass Pass	
Internal RADIUS	5	WANS	false	0.0.0.0	0.0.0.0	Pass	
	6	WANE	false	0.0.0.0	0.0.0.0	Pass	
Active Directory /LDAP	Domain	Diagnosis					
JPnP							
CMP	Domai	in					
Wake on LAN	Domai	in Type	1Pi4	IPv6			
SMS / Mail Alert Service							
lonjour	Interfa	ice	WAN1		*		
High Availability	DNS 5	erver					
Local 807.1X General Setup							
							Diagnose
	Domain N			IP Address	Interface	Verify Besult	

ltem	Description
	General Setup
Index	Displays the index number of the WAN interface.
Interface	Displays the WAN interface name for which DNS security is to be configured.
Enable	Displays if the DNS security is enabled (true) or disabled (false).
Primary DNS	Displays the primary DNS server IP address in effect for this WAN.
Secondary DNS	Displays the secondary DNS server IP address in effect for this WAN.
Bogus DNS Reply	Displays the action to be taken for DNS responses that fail authentication. Pass – Pass DNS result. Drop – Do not pass DNS result.
	Domain Diagnosis
Domain	Enter domain address to be diagnosed.
Domain Type	Select the type of IP address to be looked up. IPv4 IPv6
Interface	Select the WAN port to be used for the lookup.
DNS Service	Enter the IPv4 / IPv6 address of the DNS server to be used for the lookup.
Diagnose	Click to begin DNS lookup.

To configure the profile, move the mouse cursor to any index entry and click to open the following page.

865ac_001DAA000000 / Configu	tion / Applications	C
General Setup		
Enable		
Interface	WAN1	
Bogus DNS Reply	Pass ~ Drop Pass	
		Cancel Save

9.4.11.4 Schedule

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

namic DNS	2865ac_0010	DAA000000 / Configu	aration / Applications		Set to Factory Default	Ø
	Index	Enable	Comment	Time	Frequency	
	1	false		00:00 00:00	Sun.	ə
	2	false		00:00 00:00	Sun.	9
mal TACACS+ e Directory /LDAP	3	false		00:00 00:00	Sun.	9
	4	false		00:00 00:00	Sun.	9
	5	false		00:00 00:00	Sun.	9
	6	false		00:00 00:00	Sun.	9
a Availability al 802.1X General Setup	7	false		00:00 00:00	Sun.	9
	8	false		00:00 00:00	Sun.	9
	9	false		00:00 00:00	Sun.	9
	10	false		00:00 00:00	Sun.	9
	11	false		00:00 00:00	Sun.	9
	12	faise		00:00 00:00	Sun.	9
	13	false		00:00 00:00	Sun.	9
	14	false		00:00 00:00	Sun.	

To configure the schedule profile, move the mouse cursor to any entry (1 to 15) and click to open the following page.

Enable Image: Comment Start Date (yyyy-mm-dd) 2000 - 1 - 1 - 1 - 1 Start Time (hh:mm) 0 - 2 - 0 - 2 Duraton Time (hh:mm) 0 - 2 - 0 - 2 End Time (hh:mm) 0 - 2 - 0 - 2 Action Image: Comment - 2 How Often Weekdays Image: Comment - 2 Image: Comment - 2 Image: Comment - 2 Image: Comment - 2	Enable			
Comment Start Date (yyyy-mm-dd) 2000 - 1 - 1 - 0 - 2000 - 1 - 1 - Start Time (hh:mm) 0 - 2 - 0 - 2 - 1 - 1 - Start Time (hh:mm) 0 - 2 - 0 - 2 - 1 - 1 - Action Force On Weekdays Sun	Enable			
Start Date (yyyy-mm-dd) 2000 - 1 - 1 Start Time (hh:mm) 0 - 200 - 1 0 - 200 - 1 Duration Time (hh:mm) 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 0 - 200 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 1 - 1 0 - 200 - 1 0 - 200 - 1 0 - 200 - 1 1 - 200 - 1 0 - 200 - 1 1 - 200 - 1 0 - 200 - 1 1 - 200 - 1 0 - 200 - 1 1 - 200 - 1 0 - 200 - 1 1 - 200 - 1 0 - 200 - 1 1 - 200 - 1				
Start Time (hh:mm) 0 0 <td>Comment</td> <td></td> <td></td> <td></td>	Comment			
Duration Time (hh:mm) Duration Time (hh:m	Start Date (yyyy-mm-dd)	2000 ~ - 1	~ - <u>1</u> ~	
End Time (hh:mm) 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0	Start Time (hh:mm)	0 ~ : 0	~	
Action Force On How Often Weekdays Sun Mon	Duration Time (hh:mm)	0 ~ : 0	~	
How Often Weekdays ~	End Time (hh:mm)	0 : 0		
Weekdays Sun 🖬 Mon	Action	Force On	~	
	How Often	Weekdays	~	
🗹 Tue 🛛 🗹 Wed	Weekdays	🗆 Sun	Mon	
		🗹 Tue	Wed	
🗹 Thu 🔤 Fri		🛃 Thu	🗹 Fri	
	① Note: Comment can only contain A-Z a-z 0	D-9,.{}()^\$!~`		
① Note: Comment can only contain A-Z a-z 0-9 , . { } () ^ \$! - `				
O Note: Comment can only contain A-Z a-z 0.9,{}() ^ \$!~ `	🗎 Clear			Cano

ltem	Description	
Enable	Click to enable or disable the schedule profile.	
Comment	Enter a name to identify this schedule entry.	
Start Date	Select the date when the entry comes into effect.	
Start Time	Select the time when the schedule is triggered.	
Duration Time	Select how long the action lasts when the scheduled is triggered.	
End Time	It will be calculated automatically when Start Time and Duration Time are configured well.	
Action	Specify the action to take when the schedule is triggered.	
	Force On – The feature with which this schedule is associated will be turned on.	
	Force Down – The feature with which this schedule is associated will be turned off.	
How Often	Specify how frequently the schedule is triggered.	
	 Once - The schedule is triggered once, on the Start Date at the Start Time, for the Duration Time. 	
	 Weekdays - The schedule will be triggered repeatedly, starting on the Start Date at the Start Time, on the selected days of the week, at the Start Time, for the Duration Time. 	
	 Monthly, on date – The router will only execute the action applied such schedule on the date (1 to 28) of a month. 	
	• Cycle duration – Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	

9.4.11.5 External RADIUS

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

Dynamic DNS	2865ac_001DAA000000 / Configuration / Applications		
LAN DNS / DNS Forwarding	Primary Server		
DNS Security	Enable		
Schedule	Enable Accounting	\square	
External RADIUS	Comments		
Internal RADIUS			
External TACACS+	Primary Server		
Active Directory /LDAP	Secret	•	
UPnP	Authentication Port	1812	
IGMP	Retry	2	
Wake on LAN	Secondary Server		
SMS / Mail Alert Service	Secondary Server		
Bonjour	-		
High Availability	Secret	•	
Local 802.1X General Setup	Authentication Port	1812	
	Retry	2	
	🖻 Clear	Since	•

These parameters are explained as follows:

ltem	Description
	Primary Server
Enable	Click to enable or disable the server settings.
Enable Accounting	Click to enable or disable the accounting.
Comments	Enter a brief description for this profile.
Primary Server	Enter the IP address of RADIUS server.
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Authentication Port	Enter the UDP port number that the RADIUS server is using.
Retry	Set the number of attempts to perform reconnection with RADIUS server.
	Secondary Server
Secondary Server	Enter the IP address of RADIUS server.
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Authentication Port	Enter the UDP port number that the RADIUS server is using.
Retry	Set the number of attempts to perform reconnection with RADIUS server.
Clear	Clear all modifications on this page.
Save	Save the current settings and return to previous page.

9.4.11.6 Internal RADIUS

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

Dynamic DNS		/ Configuration	/ Applications			S
LAN DNS / DNS Forwarding	General Setup					
DNS Security						
Schedule	Enable					
	Authent	tication Port	1812			
	Authent	tication Method	PAP Only			
			PAP Only	•		
	Support	802.1X Method	\bigcirc			
UPnP	Authent	tication List				
IGMP	Synchro	nize Internal RADIUS user list	t to			
	Local 80	2.1X user list.				
SMS / Mail Alert Service						
						Save
High Availability	RADIUS Client	Access List				
	Index	Client Access Enable	Client Access Shared Secret	Client Access IP Address	Client Access IP Mask	Client Access IPv6 Address
	1	false		0.0.0.0	0.0.0.0	84 84
	2	false		0.0.0.0	0.0.0.0	
	3	false		0.0.0.0	0.0.0.0	
	4	false		0.0.0.0	0.0.0.0	
	5	false		0.0.0.0	0.0.0.0	:
	6	false		0.0.0.0	0.0.0.0	
	7	false		0.0.0.0	0.0.0.0	
	🗊 Clear					

ltem	Description	
	General Setup	
Enable	Click to enable or disable the internal RADIUS server settings.	
Authentication Port	Enter the UDP port for authentication messages.	
Authentication Method	 Specify the way to authenticate the wireless client. PAP only PAP/CHAP/MS-CHAP/MS-CHAPv2 	
Support 802.1X Click to enable or disable the Support 802.1X Method function. Method EAP_TTLS/PAP EAP_TTLS/MSCHAP EAP_TTLS/MSCHAPv2 EAP_PEAP/MSCHAPv2 EAP_PEAP/MSCHAPv2		
Authentication List	Use the drop down list to choose the use profile.	
Synchronize Internal RADIUS user list to Local 802.1X user list	Users can be authenticated by RADIUS server and local 802.1X to get certain network service. It is not necessary to create new user profiles (containing user accounts and user passwords) for RADIUS and local 802.1X respectively. Simply select to update the 802.1X authentication list to match the RADIUS authentication list.	
Save Save the current settings		
	RADIUS Client Access List	
Client Access Enable	Displays the status (true or false) of the client entry. Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.	
Client Access Shared Secret	Displays the text string that is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them.	

Client Access IP Address	Displays the base address of the IP block.	
Client Access IP Mask	Displays the IP mask to configure the size of the IP block.	
Client Access IPv6 Address	Displays the base address of the IPv6 block.	

To configure the profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

Enable	
Shared Secret	٥
IP Address	0.0.0.0
IP Mask	0.0.0.0
IPv6 Address	
IPv6 Length	0

These parameters are explained as follows:

ltem	Description	
Enable	Click to enable / disable the profile.	
Shared Secret	Enter a text string. It is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them.	
IP Address	Enter the base address of the IP block.	
IP Mask	Enter the IP mask to configure the size of the IP block.	
IPv6 Address	Enter the base address of the IPv6 block.	
IPv6 Length	Enter the prefix length of the IPv6 block.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.11.7 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does.

Dynamic DNS	/ Configuration / Applications		
	Enable	\odot	
	Server IP Address	0.0.00	
	Destination Port		
		49	
	Shared Secret	Φ	
	🛱 Clear		
			Save
UPnP			

ltem	Description	
EnableClick to enable / disable the external TACACS+ server settings.		
Server IP Address Enter the IP address of the TACACS+ server.		
Destination Port Enter a port number used by the TACACS+ server. Port 49 is most common.		

Shared Secret	Enter a text string. It is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters.
Clear	Clear all modifications on this page.
Save	Save the current settings.

9.4.11.8 Active Directory/LDAP

Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

Dynamic DNS		/ Configuration / Applications					Ø	
LAN DNS / DNS Forwarding	General Setup	, ,						
DNS Security	Enable							
Schedule								
External RADIUS	Bind Typ			Simple Mode				
Internal RADIUS	Server A	ddress		IPv4 format (EX : 123.12.1.1)				
External TACACS+	Destinat	tion Port		389				
Active Directory ALDAP	Use SSL			D				
UPnP								
IGMP								Save
Wake on LAN	Active Directo	ry / LDAP Profiles						
SMS / Mail Alert Service								
Bonjour	Index	Name	Common Name Identi	ier Distinguish	d Name	Additional Filter	Group Distinguished Name	
High Availability	2							
Local 802.1X General Setup	3							
	4							
	5							
	6							
	8							

ltem	Description	
	General Setup	
Enable	Click to enable / disable the AD/LDAP function.	
Bind Type	 Select from one of 3 bind types: Simple Mode – Initiate bind operation (authentication) without performing user search. Anonymous – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user search. Regular Mode – Same as Anonymous mode, except that the DN and 	
	password are sent to the server.	
Server Address	Enter the network address of the LDAP server.	
Destination Port	Enter a network port that the LDAP server listens on. The default ports are 389 for unsecured connections and 636 for LDAPS (LDAP over SSL) connections.	
Use SSL	Click to enable or disable SSL.	
	If enabled, the router will use Secure Sockets Layer (SSL) for LDAP traffic.	
Regular DN	Enter the LDAP Distinguished Name for authentication if Bind Type is set to Regular Mode .	
Regular Password	Enter the LDAP Password for authentication if Bind Type is set to Regular Mode .	

Save	Save the current settings.		
	Active Directory / LDAP Profiles		
Index	Displays the index number of the profile. Up to 8 LDAP profiles can be configured.		
Name	Displays the user-defined name that identifies this entry.		
Distinguished Name	Displays the distinguished name (DN) configured in the profile.		

To configure the profile, move the mouse cursor to any entry (1 to 8) and click to open the following page.

Name	
Common Name Identifier	
Base Distinguished Name	
Additional Filter	
Group Distinguished Name	

These parameters are explained as follows:

ltem	Description			
Name	Enter a name that identifies this profile.			
Common Name Identifier	Enter a common name attribute, which is typically "cn" in most LDAP configurations.			
Base Distinguished Name	Enter a starting point of user search in the LDAP directory, for example, dc=draytek,dc=com.			
Additional Filter	Additional filter to be applied to the search request to identify eligible users.			
	For example,			
	 "OpenLDAP: (gidNumber=500)" 			
Group Distinguished Name	The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com.			
Cancel	Discard current modification and return to previous page.			
Save	Save the current settings and return to previous page.			

9.4.11.9 UPnP

The Vigor supports UPnP (Universal Plug and Play), which is a suite of network protocols that simplifies network configuration.

<- Configuration	2865ac_001DAA000000 / Configuration / Applic	tions	C
Dynamic DNS	WAN Interface	Default WAN ~	
LAN DNS / DNS Forwarding	Enable UPnP Service	D	
DNS Security	Enable Connection Control Service	D	
Schedule	Enable Connection Status Service	P	
External RADIUS			
External TACACS+	Note: To allow NAT pass-through to a UPnP of	nabled client the connection control service must also be enabled.	
Active Directory /LDMP			
	E Clear	Sav	
КМР			

ltem	Description	
WAN Interface	Select the WAN port on which ports will be opened in response to UPnP commands.	
Enable UPnP Service	Click to enable or disable the UPnP function.	
Enable Connection Control Service	Click to enable or disable the connection control service.	
Enable Connection Status Service	Click to enable or disable the connection status service.	
Clear	Clear all modifications on this page.	
Save	Save the current settings.	

9.4.11.10 IGMP

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

← Configuration	2865ac_001DAA000000 / C	onfiguration / Application	ons						C
Dynamic DNS	IGMP Proxy	a	0						
LAN DNS / DNS Forwarding	Interface	w	ANI		v				
DNS Security	IGMP version	A							
Scherlule			AD.		•				
Edemal RADIUS	General Query Interval (seco	nds) 12	5						
Internal RADIUS	Add PPP header	a)						
External TACACS+	Encapsulate IGI	(P in PPPoE							
Active Directory /LDAP							1		
UPnP	Enable IGMP syslog	0							
SHP	IGMP Snooping	a							
Wake on LAN									
SMS / Mail Alert Service									Save
Bonjour	Working group								
High Availability	6 6 t								
Local 802.1X General Setup	Index	Group ID		P1	P2	P3	P4	P5	м
					\wedge				
					No data available				
	-								

These parameters are explained as follows:

ltem	Description
IGMP Proxy	Click to enable or disable the IGMP proxy settings.
Interface	Select an interface for packets passing through.
IGMP version	At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe. Or choose

	Auto.
General Query Interval (seconds)	Set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router.
Add PPP header	Click to enable or disable the function. If you have no idea to enable or disable, simply contact your ISP providers.
Enable IGMP syslog	Click to enable or disable the function. If enabled, the router will store the IGMP status onto Syslog.
Enable IGMP Snooping	If enabled, the following option shall be configured. Enable IGMP Fast Leave - If enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message.
Save	Save the current settings.
	Working group
Group ID Displays the ID port of the multicast group, which is within the reserved for IGMP, 224.0.0.0 through 239.255.255.254.	
P1-PX	Displays the LAN ports that have IGMP hosts joined to this multicast group.

9.4.11.11 Wake on LAN

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

← Configuration	2865ac_001DAA000000 / Configuration / App	lications C			
Dynamic DNS	Wake by	MAC Address			
LAN DNS/ DNS Forwarding					
DNS Security	IP Address				
Schedule	MAC Address				
External RADIUS					
Internal RADIUS		Wake Up			
External TACACS+					
Active Directory /LDAP	Result				
UPnP					
IGMP	() Note:				
Walio on LAN	Wake on LAN Integrates with Bind IP to MAC function; only bound PCs can wake up through IP.				
And the state of the state of the					

These parameters are explained as follows:

ltem	Description
Wake by	 To wake up the binded IP, MAC Address - Enter the correct MAC address of the host in MAC Address boxes.
MAC AddressEnter any one of the MAC address of the bound PCs.	
Result	Displays the result of WOL execution.
Wake Up Click to wake up the selected device.	

9.4.11.12 SMS/Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

- Configuration	2865aC_0	001DAA000000 / Cor	nfiguration / Applications				C
Ayturnic DNS	SMS AI	ert					Set to Factory Defau
AN DNS / DNS Forwarding	Index	SMS Enable	SMS Provider	SMS Recipient Number	SMS Notify Profile	SMS Schedule1	SMS Schedula2
WS Security	1	faise	1-Local number		1-		
chedule	2	tatse	1-Local number		1.		
demail RADIUS	3	taise	1-Local number		1-		
	4	talse	1-Local number		1-		
sternal RADIUS	5	false	1-Local number		1-		
isternal TACACS+	6	false	1-Local number		1-		
ctive Directory /LDAP	7	false	1-Local number		1-		
ւթոթ	8	false	1-Local number		1-		
JPoP	9	false	1-Local number		1-		
CMP	10	false	1-Local number		1-		
Wake on LAN	() Not	le:		Interval [®] setting if they use the sar			
	() Not	le: All the SMS Alert pro		Interval" setting if they use the sar			
Yale on LAN ANS - Haat Astro borving Konjour	() Not	le: All the SMS Alert pro		Interval" setting if they use the sar			Set to Factory Defa
Yale on LAN MS ; plant story: Service konjour ligh Availability	() Not	le: All the SMS Alert pro		Interval" setting if they use the sar Mail Address		Mail Schedule 1	Set to Factory Defau Mail Schedule2
Yale on LAN MS ; plant story: Service konjour ligh Availability	Mail Ab	te: All the SMS Alert pro ert	files share the same "Sending		ne SMS Provider.	Mail Schedule 1	~
Yale on LAN MS ; plant story: Service konjour ligh Availability	Mail Ab Index	te: All the SMS Alert pro ert Mall Enable	files share the same "Sending Mail Service		ne SMS Provider. Mell Netty Prefile	Mail Schedule]	~
file on LAN MS / Mail Aller Gereine knjour Igh Avalability	Mail Ab Index	ert Mitthe SMS Alert pro ert Mail Enable False	files share the same "Sending Mail Service 1-Mail Notity		ne SMS Provider. Mail Natly Public J-	Mail Schedule 1	
file on LAN MS / Mail Aller Gereine knjour Igh Avalability	Mail Ald Index 1 2	er All the SMS Alert pro ert Mall Enable false false	Files share the same "Sending Mall Service 1-Mail_Notity 1-Mail_Notity		ne SMS Provider. Mail Natily Portie 1-	Mail Schedule 1	
file on LAN MS / Mail Aller Gereine knjour Igh Avalability	Mail Ale Mail Ale Index 1 2 3	er All the SMS Alert pro ert Mail Enable false false false	Flies share the same "Sending Mail Service 1-Mail, Notify 1-Mail, Notify 1-Mail, Notify		me SMS Provider. Meil Netty Profile I- I-	Mail Schedule 1	~
Yale on LAN MS ; plant story: Service konjour ligh Availability	Mail Ale Mail Ale Index 1 2 3 4	er All the SMS Alert pro- ert Mait Enable failse failse failse failse	flies share the same "Sending Mail Service 1-Mail, Notly 1-Mail, Notly 1-Mail, Notly 1-Mail, Notly		ne SMS Provider. Mail Natily Profile 1- 1- 1-	Mail Schedule 1	~
Yale on LAN MS ; plant story: Service konjour ligh Availability	Mail Ab Mail Ab Index 1 2 3 4 5	All the SMS Mert pro ert faite faite faite faite faite faite faite faite	files share the same "Sending Mail Service 1-Mail_Notify 1-Mail_Notify 1-Mail_Notify 1-Mail_Notify 1-Mail_Notify		ne SMS Provider. Mail Kathy Profile J- J- J- J-	Mail Schedule 1	~
Vale on LAN ANY (Mari Alary Service	Mail Al Mail Al Index 1 2 3 4 5 6	ert Mitthe SMS Alert pro ert false false false false false false false	Files share the same "Sending Mail Service 1-Mail, Notity 1-Mail, Notity 1-Mail, Notity 1-Mail, Notity 1-Mail, Notity 1-Mail, Notity		ne SMS Provider. Mail Natily Profile 1- 1- 1- 1-	Mail Schedule 1	Set to Factory Defau Mail Schedulo 2

ltem	Description
SMS Alert	It allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.
Mail Alert	It allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

To configure the SMS alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

2865ac_001DAA000000 / Configuration / Appl	ications	C
Enable	O	
SMS Provider	1 ~	
Recipient Number		
Notify Profile	1 ~	
Schedule 1		
Schedule 2		
		Cancel Save

ltem	Description
Enable	Click to enable or disable the SMS alert profile.
SMS Provider	Use the drop down list to choose SMS service provider.
Recipient Number	Enter the phone number of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile.
Schedule 1 / 2	Enter the schedule number that the SMS will be sent out.

Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

To configure the mail alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

2865ac_001DAA000000 / Configuration / Ap	plications	C
Enable		
Mail Service	1 ~	
Mail Address		
Notify Profile	1 ~	
Schedule 1		
Schedule 2		
		Cancel Save

These parameters are explained as follows:

ltem	Description
Enable	Click to enable or disable the mail alert profile.
Mail Service	Use the drop down list to choose mail service object.
Mail Address	Enter the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile.
Schedule 1 / 2	Enter the schedule number (0~15) that the notification will be sent out.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.13 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.

Dynamic DNS	2019 - Addateseen / Configuration / Applications		Ø	
LAN DNS / DNS Forwarding	Enable Bonjour Service			
DNS Security	HTTP Server	D		
Schedule				
External RADIUS	Telnet Server	Œ		
Internal RADIUS	FTP Server	D		
External TACACS+	SSH Server	0		
Active Directory /LDAP	LPR Printer Server	D		
UPnP				
IGMP				Save
Wake on LAN				
SMS / Mail Alert Service				
Radiant				

ltem	Description	
Enable Bonjour	Click to enable or disable the Bonjour service.	
Service	With bonjour service enabled, Vigor router can share the service (e.g.,	

	HTTP service, Telnet service, FTP service, SSH service, LRP Printer server and etc.) to the LAN clients.
Save	Save the current settings and return to previous page.

9.4.11.14 High Availability

The High Availability (HA) feature of the router provides redundancy of network resources, and reduces downtime in case of component failure.

← Configuration	2865ac_001DAA000000 / Configuration / Ap	plications		Set to Factory De
namic DNS N DNS / DNS Forwarding	Enable High Availability	0		
NS Security	Redundancy Method	Active-Standby	Ý	
checkule	General Setup			
ternal RADIUS				
itemal RADIUS	Group ID	1		
aternal TACACS+	Priority ID	10		
lctive Directory /LDWP	Authentication Key	draytek		
Rup	Protocol	IPr4	*	
ЭМР	Management Interface	LANI	~	
Yake on LAN	Update DDNS	0		
MS / Mail Alert Service konjour	Systog	0		
	Config Sync			
ocal 802.1X General Setup	Enable Config Sync (Max, Sync to 10 routers)	0		
	Day	0	v	
	Hour	0	¥	
	Minute	15	v	
	WAN Settings	0		

ltem	Description
Enable High Availability	Click to enable or disable the HA function.
Redundancy Method	Select the redundancy method (Hot-Standby or Active-Standby) for high availability.
	General Setup
Group ID	Enter a value (1~255). Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group.
Priority ID	Enter a value (1~30). Different routers must be configured with different IDs.
Authentication Key	Enter an authentication key up to 31 characters long.
Protocol	Select the IP protocol (IPv4 or IPv6) to be used for DARP.
Management Interface	Select the interface to be used for DARP negotiation between routers.
Update DDNS	Click to enable or disable the function. If enabled, the router will update the DDNS server for the secondary device when the primary router fails.
Syslog	Click to enable or disable the function. If enabled, the router will record required information on Syslog.

	Config Sync
Enable Config Sync	Click to enable or disable the Config Sync function.
Day / Hour / Minute	The primary router will synchronize its configuration with secondary routers at every specified time interval.
WAN Settings	Click to enable or disable the WAN settings. WAN settings will be excluded when executing configuration synchronization.
Enable Config Inherit	 Click to enable or disable the function. The configuration inherits will be executed only when the device (router) plays the role of the master device. Once another device with the priority ID higher than this device is ready to take over the management as the master device, after acting as the primary master for a while, this device will sync the configuration to all members in the same group and return to the role of the backup device (secondary master). Config Inherit for () minute - Enter a value.
IPv4	Set IPv4 virtual IP for each LAN interface.
IPv6	Set IPv6 virtual IP for each LAN interface.
Save	Save the current settings and return to previous page.

To configure the IPv4 profile, move the mouse cursor to any entry and click to open the following page.

2027 Configuration / Applications			ß
Index	LAN1		
Enable			
Virtual IP	192.168.27.2		
		Cancel	Save

To configure the IPv6 profile, move the mouse cursor to any entry and click to open the following page.

/ Configuration / Applications		
Index	LAN1	
Enable		
Virtual IP	FE80::200:5EFF:FE00:101	

9.4.11.15 Local 802.1X General Setup

It allows you to configure general settings for Local 802.1X server built in Vigor router.

Dynamic DNS	/ Configuration / Applicatio	s	ø
LAN DNS / DNS Forwarding	Enable		
DNS Security	EAP_TTLS/PAP	\odot	
Schedule	EAP_TTLS/MSCHAP	D	
External RADIUS	EAP_TTLS/MSCHAPv2	0	
Internal RADIUS			
External TACACS+	EAP_PEAP/MSCHAPv2		
Active Directory /LDAP	Authentication List		
UPnP	Sync User Profile Setting to Internal Radius	0	
IGMP			
Wake on LAN		Save	
SMS / Mail Alert Service			
Bonjour			
High Availability			
Local 802.1X General Setup			

ltem	Description	
Enable	Click to enable or disable the function.	
EAP_TTLS/PAP	Click to enable or disable the EAP_TTLS/PAP server certificate.	
EAP_TTLS/MSCHAP	Click to enable or disable the EAP_TTLS/MSCHAP server certificate.	
EAP_TTLS/MSCHAPv2	Click to enable or disable the EAP_TTLS/MSCHAPv2 server certificate.	
EAP_PEAP/MSCHAPv2	Click to enable or disable the EAP_PEAP/MSCHAPv2 server certificate.	
Authentication List	Select user profiles.	
Sync User Profile Settings to Internal Radius	Click to enable or disable the function. It will enable/disable setting for both Internal RADIUS and Local 802.1X synchronize for all of the user profiles.	
Save	Save the current settings.	

9.4.12 VPN

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

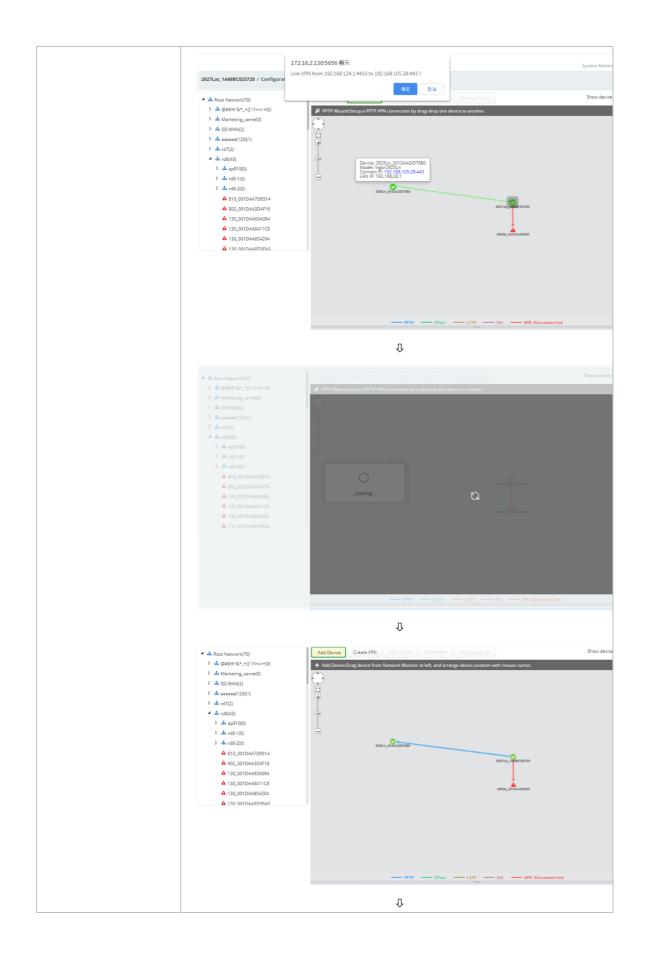
9.4.12.1 VPN Wizard

This page displays the VPN status related to the specified device.

/ Configuration	/ VPN	ø
/ Configuration A & Root Network(70) b & @#\$\%^&_+()^:?> -(0)</p b & Marketing_carrie(0) b & SD-WAN(2) b & assass(123)(1) b & drd7(2) 4 & drd8(42) b & drd8(42) <pb &="" drd8(42)<="" p=""> b & drd8(42) b &</pb>		

These parameters are explained as follows:

ltem	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.			
Add Device Create VPN Edit LAN PPTP Wizard PPTP Wizard C L2TP Wizard S SSL Wizard C LSTO Wizard C LSTO Wizard C LSTO Wizard	To build a quick VPN connection with PPTP/IPsec/L2TP/SSL/customized settings , simply click this button and choose one of the wizards for establishing VPN. Then, drag and drop one device to another. Here we take PPTP Wizard as an example.			



	VPN Name: p_5B0_720 VPN Type: PPTP Encryption: MPPE TX Packets: 10 RX Packets: 1 TX Rate(Bps): 24 Up Time: 0:03:14
Edit LAN IP	If there is LAN IP segment conflict in VPN connection, please select that device and click this button to change LAN IP setting.
Unlink VPN	To disconnect a VPN connection, Click this button and move the mouse cursor to the VPN connection that you want to disconnect.
Remove Device	Click to remove the selected device without VPN connection.
Show device name	Click to display / hide the name of the device.

9.4.12.2 LAN to LAN

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

- Configuration	Configuration /	VPN						Set	to Factor	y Defau	ilt	G
PN Wusant	Alarm Enable	Index	Enable	Always On	Default Route	Name	Remote Network	Remote Network Mask		\$	utus	
	disable	1	true	true	false	1_720_000	192.158.124.1	255.255.255.0		0	nine	
	disable	2	false	faise	false	772	0.0.0.0	255.255.255.0		0	mine	
lemote Dial-In User												
lemote Access Control									10	< 1/	1-2	DK.
PN Matcher	Pass packets from	LAN in Routing										
Ipen/VPN	Pass Packets to W	IAN when VDN dis	connects.									
					-							
												Save

To create a new LAN to LAN profile, click the bottom one entry. To configure the LAN to LAN profile, move the mouse cursor to any entry and click to open the following page.

← Configuration	Configuration / VPN		Set to Factory Default 🛛 📿
VPN Warned	Common Settings		
1 AN IN LAN	Index	1	
Remote Access Control	Enable this profile		
VPN Matcher	Enable ACS Alarm	00	
OpenVPN	Profile Name	1_720_000	
	Call Direction	Both Dial-Out Dial-In GRE Tunnel	
	Dial-Out Through	WANI First 👻	
	Always on		
	Idle Timeout	-4	
	Quality Monitoring/Keep Alive		
	Netbios Naming Packet	Pass Block	
	Multicast via VPN	Pass Block	
	() (for some IGMP,IP-Camera,DHCP	Relayetc.)	
	Dial-Out Settings		
	VPN Server Type	iPSec_Tunnel v	
	IPsec Tunnel Type	IKEvi v	
	Server IP/Host Name	192.168.105.120	
	fi Clear		Cancel Save

ltem	Description		
	Common Settings		
Index	Displays the index number of the profile.		
Enable this profile	Click to enable or disable this profile.		
Enable ACS Alarm	Click to enable or disable the function.		
Profile Name	Enter the name of the profile.		
Call Direction	 Specify the allowed call direction of this LAN-to-LAN profile. Both Dial-Out Dial-In 		
	GRE Tunnel		
Dial-Out Through	Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.		
Always On	Click to enable or disable the function to maintain an always on dial-out connection. However, if disabled,		
	Idle Timeout - Set a value if Always On is disabled. The router will close connection if no activity is observed in the VPN connection for this many seconds.		
Quality Monitoring /Keep Alive	Click to enable or disable the function.		
Netbios Naming Packet	Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.		
	• Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.		
	 Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. 		

Multicast via VPN	Specifies whether to allow multicast packets to traverse through the VPN tunnel.			
	• Pass – Click this button to let multicast packets pass through the router.			
	• Block – This is default setting. Click this button to let multicast packets be blocked by the router.			
	Dial-Out Settings			
VPN Server	Select the VPN protocol to be used.			
IPsec Tunnel Type	Select IKEv1 or IKEv2.			
Server IP/Host Name	Enter an IP address or DNS host name of remote VPN host.			
Dial-Out Schedule	Connect and disconnect according to schedule profiles.			
Profile	Up to four schedule profiles can be specified.			
	IKE Phase 1 Settings			
Mode	Select IKE phase 1 mode. Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session. Main Mode			
	 Aggressive Mode 			
Authentication	Select PSK (IKE Pre-shared key) or X509 (X.509 digital signature).			
Pre-Shared Key	It is available when PSK is selected as Authentication.			
Tre-Sharea Key	Enter the PSK.			
Local ID	Enter a string.			
Proposal Encryption	Select an proposal encryption mode.			
Proposal ECDH Group	Select an proposal ECDH group (e.g., G14).			
Proposal Authentication	Select SHA256 or SHA1.			
	IKE Phase 2 Settings			
Security Protocol	Select the dial-out protocol.			
	ESP(High)			
	AH(Medium)			
Proposal Encryption	Select an proposal encryption mode.			
Proposal Authentication	Select All, SHA256, SHA1 or None.			
	IKE Advanced Settings			
Phase 1 Key Lifetime	For security reason, the lifetime of key should be defined. The default value is 28800 seconds.			
Phase 2 Key Lifetime	For security reason, the lifetime of key should be defined. The default value is 3600 seconds.			
Phase 2 Network ID	In Aggressive mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.			
Enable Perfect	Click to enable or disable the function.			
Forward Secret	If enabled, the IKE Phase 1 key will be reused to avoid the computation			

	complexity in phase 2.			
Ping to Keep Alive	Click to enable or disable the transmission of PING packets to a specified IP address.			
	PING Target IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.			
	TCP/IP Network Setting	gs		
Local Network IP / Mask	Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.			
Remote Network IP / Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection.			
More Remote Subnet	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection.			
	More Remote Subnet	Index Network IP	Netmask	Action
		1	0.0.0.0 / 0	▼ + Add
	Enter the IP address and	l the mask address	. Click +Add to sav	
	and create a new entry.			
Mode	 If the remote network only allows one IP address for the local network, select NAT; otherwise, select Routing. Routing NAT 			
RIP via VPN	Specifies the direction of	f Pouting Informati	on Protocol (PIP) r	ackets
	-			
Translate Local Network	It is available when Routing is selected as Mode. Click to enable or disable the function. This is usually used when you find there are several subnets behind the remote VPN router.			
	If enabled, the function of Change Default Route to this VPN tunnel will be disabled. And please configure the following options.			
	Type - There are two types (Translate Whole Subnet, Translate Specific IP) for you to choose.			
	For Translate Whole Sub			
	 Local Subnet - Select the LAN whose IP addresses are to be translated. 			
	 Translated IP - Sp 	ecify an IP address		
	 More Local Subne 	et - Add more subn	ets.	
	More Local Subnet	Index Translated To	Local Network	Action
	More Local Subnet	Index Translated To	Local Network	Action + Add
		1		
	For Translate Specific IP,	1	LAN1	▼ + Add
	For Translate Specific IP, • Virtual IP Mappin	1 g - Specify the loca	LAN1	• + Add
	For Translate Specific IP, • Virtual IP Mappin virtual IP address.	1	LAN1	▼ + Add
Change Defeuti	For Translate Specific IP, Virtual IP Mappin virtual IP address.	1 g - Specify the loca Index Local IP 1	LAN1	 + Add ne mapping Action
Change Default Route to this VPN	For Translate Specific IP, • Virtual IP Mappin virtual IP address.	1 g - Specify the loca Index Local IP 1	LAN1	+ Add he mapping Action + Add

Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.12.3 Remote Dial-In User

The system administrator can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

 Configuration 	2865ac_001DAA0000	00 / Configuration / VPN			Set to Factory Default	С
VPN Wissed	Index	Enable	Username	Status		
LAN to LAN	1	Disable	m	Disable		
Remain Dist in User					$ 0\rangle = (-1/1) \rightarrow$	91
Remote Access Control						
VPN Matcher						
Oper/VPN						

To configure the remote dial-in user profile, move the mouse cursor to any entry and click to open the following page.

Configuration	2865ac_001DAA000000 / Configuration	Ion / VPN			Set to Fact
N Wuard	Remote Dial In User				
N Ko LAN Manda Digit Ki Kang I	User account and Authenticat	tion			
mote Access Control	Index	1			
Matcher	Enable	0			
nVPN	Idle Timeout	200			
	Username	m			
	Password				
	Mobile One-Time Passwords(mOTP)	0			
	OpenVPN tunnet does not sup Allowed Dial-In Type	part mOTP.			
	pptp	(\overline{O})			
	IPsec Tunnel				
		E MAN MAN	IKEV2 EAP	IPsec XAuth	
		IKEv1/IKEv2			
	L2TP				
	L2TP L2TP with IPsec Policy				
			*]		

ltem	Description	
	User account and Authentication	
Index	Displays the index number of the user account profile.	
Enable	Click to enable or disable the user account profile.	
Idle Timeout	Set the allowed idle time before the router disconnects the VPN connection.	
Username	Set a username used for PPTP, L2TP or SSL Tunnel dial-in type	
Password	Set a password used for PPTP, L2TP or SSL Tunnel dial-in type	
Mobile One-Time Passwords (mOTP)	Click to enable or disable one-time passwords (Mobile-OTP). If enabled, please PIN Code - Enter the code for authentication (e.g, 1234).	

	Secret - Enter the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
	Allowed Dial-In type
PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel	Click to enable (select) or disable (deselect) the PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel protocol.
Specify Remote Node	Click to enable or disable the function. The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified. Remote Client IP - Enter the IP address for remote client. Or Peer ID - Enter the string for peer ID.
Netbios Naming	It is available when Specify Remote Node is disabled.
Packet	Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.
	 Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
	 Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	 It is available when Specify Remote Node is disabled. Specifies whether to allow multicast packets to traverse through the VPN tunnel. Pass – Click this button to let multicast packets pass through the router. Block – This is default setting. Click this button to let multicast packets be blocked by the router.
	Subnet
Subnet	Select an interface.
Assign Static IP	Click to enable or disable the function. IP Address - Enter a static IP address.
Digital Signature(X.509)	It is available when Specify Remote Node is disabled. Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please
	Digital Signature(X.509) Index - Select an X.509 profile.
	IKE Authentication Method
Enable Pre-Shared Key	It is available when Specify Remote Node is enabled. Click to enable or disable the function. If enabled, please Pre-Shared Key - Enter an IKE PSK.
Digital Signature(X.509)	Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please
	Digital Signature(X.509) Index - Select an X.509 profile.
	IPsec Security Method
Medium(AH)	Click to enable or disable the function that data will be authenticated, but not be encrypted.

High(ESP)	The payload (data) will be encrypted and authenticated.	
Local ID (optional)	Click to enable or disable the setting. Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.12.4 Remote Access Control

The Vigor router supports several protocols for VPNs, all of which can be enabled or disabled independently of one another.

← Configuration	2865ac_001DAA000000 / Configurati	2865ac_001DAA000000 / Configuration / VPN	
VPN Wizard	Remote Access Control Setup		
LAN to LAN Remote Dial-In User	PPTP VPN Service Enable	•	
Biomoda Access Control	IPSec VPN Service Enable	•	
VPN Matcher	L2TP VPN Service Enable	0	
OperMPN	SSL VPN Service Enable	C	
	OpenVPN Service Enable	0	
	C Note: • To allow VPM pass through to Ports or Port Redirection is a	a legarate VFN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open bio coordigined	Sove

These parameters are explained as follows:

ltem	Description	
PPTP VPN Service Enable	Click to enable or disable the service. If enabled, this VPN is easy to set up, has low overhead, and moderately secure.	
IPsec VPN Service Enable	Click to enable or disable the service.	
L2TP VPN Service Enable	Click to enable or disable the service.	
SSL VPN Service Enable	Click to enable or disable the service.	
OpenVPN Service Enable	Click to enable or disable the service. If enabled, this VPN offers a convenient way for users to build VPN between local end and remote end.	
Save	Save the current settings	

9.4.12.5 VPN Matcher

The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other.

	2865ac_001DAA000000 / Configuration	/ VPN		
VPN Wurand	VPN Matcher			
LAN to LAN	Enable			
lemote Dial In User				
ernote Access Control	Server Ip	vpn-matcher.draytek.com		
	Server Port	31503		
penVPN	Router List Key	٥		
	Group Device List	Get List		
	Index 41 Description	it MAC it Remote Network	At Model At Role	
		No data available		
				Cancel Save

These parameters are explained as follows:

ltem	Description	
	VPN Matcher	
Enable	Click to enable or disable the function of VPN Matcher Setup.	
Server IP / Server Port	The IP address of the DrayTek VPN Matcher server is defined as "vpn-matcher.draytek.com" with the port number "31503".	
Router List Key	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via VPN wizard.	
STUN Server	Detect - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established.	
	Group Device List	
Get List	After entering the Authkey above, click to get available Vigor router which is within the same group as this device.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings	

9.4.12.6 OpenVPN

9.4.12.6.1 OpenVPN Server Setup

OpenVPN requires the use of certificates. Certificates generated by the third party can be imported to your host and ready for use by Vigor router.

← Configuration	2865ac_001DAA000000 / Configurati	on / VPN		c
VPN Wilcard	OpenVPN Server Setup Client Config			
LAN IoLAN	1177 STATE STATE STATE			
Remote Dial-In Liser	General Setup			
Remote Access Control	Enable UDP			
VPN Matcher	UDP Port	1194		
OpentWH	Enable TCP			
	TCP Port	1194		
	Cipher Algorithm	AE5128	Ŷ	
	HMAC Algorithm	SHA1	~	
	Certificate Authentication	0		
	Certificates Setup			
	Certificate Source	Uploading certificates to Router	~	
	Trust CA	default	u .	
	Server Certificate	None	. *	
	Note: OpenVPN on Vigor Rooter only	support TUN device interface currently. So please sets	ip corresponding configurations on the client side.	
		n a gan an a		
				Save

ltem	Description		
	General Setup		
Enable UDP	Click to enable or disable UDP protocol for OpenVPN connections. If enabled, please UDP Port - Enter the UDP port number.		
Enable TCP	Click to enable or disable the TCP protocol for OpenVPN connections. If enabled, please TCP Port - Enter the TCP port number.		
Cipher Algorithm	Select the desired cipher algorithm.		
HMAC Algorithm	Select the desired HMAC hash algorithm. It is used to validate the data integrity and authenticity of the VPN data.		
Certificate Authentication	Click to enable or disable the settings. If enabled, the router can validate that the client certificate was issued by a trusted CA.		
	Certificates Setup		
Certificate Source	 Select a source for the certificate to be used for OpenVPN. Router generated certificates - Router-generated certificates that will be used for OpenVPN. GENERATE - Click to generate a certificate. Delete all certificates - Click to remove all certificates generated by the router. Uploading certificates to Router - Third-party certificates will be used for OpenVPN. Trust CA - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA 		
	that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the Certificate Management >> Trusted CA Certificate page to perform the operation.		

	 Server Certificate - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the Certificate Management >> Local Certificate page to perform the operation.
Save	Save the current settings

9.4.12.6.2 Client Config

Create and export the configuration required for a remote OpenVPN client to connect to the router.

← Conliguation	2865Lac_1449BC0D8F00 / Configuration / VPN		e
VPN Wound	OpenVPN Server Setup Client Config		
LAN to LAN			
Remote Dial In User	Client Config		
Remote Access Control	Remote Server	IP Domain VIPN Matcher	
VPN Matcher	Transport Protocol		
Corrid PR	Auto Dial-Out	Enable Disable	
	Set VPN as Default Gateway	Enable Disable	
	File Name	19691	
	Client cert	.zt	
	Client key	kny :	
		Epport	
	Note: Please make sum the Client set and the Clie Please make sum that YMM can be used as 0	ed key are located in the same lokder with zegan this periVM same.	

ltem	Description	
	Client Config	
Remote Server	 There are three types of the remote server. IP - Use the numeric IP address as the server address. Domain - Use the domain as the server address. VPN Matcher - Use the VPN matcher as the server. 	
IP	If IP is selected as the remote server, enter the IP address of the server.	
Domain	If Domain is selected as the remote server, enter the domain name of the server.	
Transport Protocol	Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.	
Auto Dial-Out	 Enable - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel. Disable - Select to disable the function. 	
Set VPN as Default Gateway	 Enable - If selected, the Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel. Disable - Select to disable the function. 	
File Name	Enter the filename of the configuration file to be downloaded from the router.	
Client cert	Enter the filename of the client certificate obtained from 3rd party provider.	

Client key	Enter the filename of the private key obtained from the 3rd party provider.
Export	Click to download the settings on this page as a file.

9.4.13 Mesh

9.4.13.1 Mesh Setup

Vigor router is treated as a mesh root. You can search and specify mesh nodes as members under current mesh group.

← Canfqynatum	2865ac_001DAA000000 / C	onfiguration / Mesh				e	
Manch Sattago Add Mesh Node Mena Natars	General Setup Mesh Enable Hole Mesh Group Name Log Level		Mesh Root Vigor/Heah Dask				
	Mesh Group Index 1 Shurd MichiGump	MAC Address 001D/VA000000		Mødst Viger 2865	Vevice Name DrayTek	Carneel Save	ī

These parameters are explained as follows:

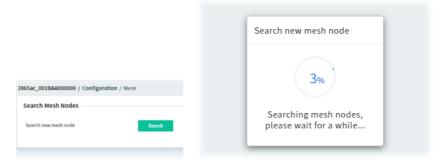
ltem	Description
	General Setup
Mesh Enable	Click to enable or disable the mesh network function.
Role	Displays the role of the router. For Vigor router, it is always Mesh Root.
Mesh Group Name	Displays the name of the current mesh group.
Log Level	Choose Basic or Detailed .
	Mesh Group
Index, MAC Address, Model, Device Name	Basic information including MAC address, model and device name of the members in this Mesh Group will be shown in this area.
Reset Mesh Group	Click it to clear the Mesh Group information. All mesh nodes in the group will become isolated.
Cancel	Discard current modification.
Save	Save the current settings

9.4.13.2 Add Mesh Node

Before a Mesh Node is connected, it is unable to check the device status from Mesh Root. This page can help to discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.

<- Configuration	2865ac_001DAA000000 / Configuration / Mesh	Ċ.
Mesh Setup	Search Mesh Nodes	
Add Health Hade Mesh Status	Search new mesh node Search	
		_

1. Click **Search**. The system will search new mesh node around.



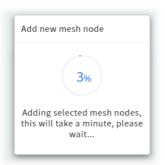
2. Available mesh nodes will be listed on this page.

← Configuration	2865a0	_001DA	A000000 / Con	figuration / M	esh
Mesh Setup	Sea	rch Me	sh Nodes		
Add Block Nucle	Sear	ch new n	nesh node		Search
Mesh Status					
	Add	Index	MAC Address	Model	Device Name
		1	00507FF1918C	VigorAP 903	VigorAP903
		2	1449BC426E1E	VigorAP 960C	VigorAP960C
	-				

3. Select the device(s) you want to group under this mesh group and click **+Add**.

	2865a	_001D/	A000000 / Cont	liguration / Me	esh
Mesh Setup	Sea	rch Me	sh Nodes		
	Sea	rch new r	nesh node		Search
Mesh Status					
	Add	Index	MAC Address	Model	Device Name
		1	00507FF191BC	VigorAP 903	VigorAP903
	Π.	2	1449BC426E1E	VigorAP 960C	VigorAP960C
	-				

4. Wait for a moment.



5. Open **Configuration>>Mesh Setup**. The new mesh node will be added.

IAC Address	Model	Device Name
01DAA000000	Vigor 2865	DrayTek
0507FF191BC	Unknown	VigorAP903
0	01DAA000000	11DAA000000 Vigor 2865

9.4.13.3 Mesh Status

This page shows the mesh status.

One Mesh Group can contain up to 8 devices. A Device with hop 0 is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.

	2865ac_00	1DAA000000 / Co	onfiguration	Mesh					
Mesh Setup	• Online(sync ready) 😐 Onl	ine 😐 Offline						
Add Mesh Node	Index	Status	Device Name	MAC Address (Model)	Нор	Up Link	Up Time	Clients	Disconnect
	1	undefined	DrayTek	001DAA000000 (Vigor 2865)	0		2d 15:22:57	0	
	2	undefined	VigorAP903	00507FF191BC (VigorAP 903)	1	001DAA000000	0d 00:03:36	0	

9.4.14 Wireless LAN

9.4.14.1 General

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

	2865ac_001DAA000000 / Configuration	/ Wireless LAN		C
2.4G SG	General Setup			
General	Index	0		
Security	Wireless LAN Enable	•		
Access Control	Mode	Mixed(11b+11g+11n)	~	
wps	Channel	Channel 6, 2437MHz	×	
Bandwidth Management.				
Artime Falmess				
Advanced Setting				Cancel Save
Band Steering	Index	Schedule		SSID
AP Discovery	1	0		
Station List	2	0		
Station List - Advance	4	a		
Station List - Neighbor				
Roaming	Note: Channel setting should not be d	hanged while Wireless 2.4G WAN mode is in u Ints associated with this SSID from accessing	ie.	
Station Control	 Isolate VPN: Block the wireless c Only the action "Force Down" in 	lients from accessing the VPN network and p the Schedule Profile will be applied to WLAN	event wireless traffic being sent to VPN connection	

ltem	Description
	General Setup
Index	Displays the index number of the WLAN profile.
Wireless LAN Enable	Click to enable or disable the wireless LAN function.
Mode	Select the 802.11 mode allowed on the band.
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting " Auto ".
Cancel	Discard current modification.
Save	Save the current settings.
Index	Displays the index number of the WLAN profile.
Schedule	Displays the number of the schedule profile.

To configure the schedule profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

865ac_001DAA000000 / Configur	ation / Wireless LAN	
WirelessLAN_General_SchSS	ID	
Index	1	
Schedule	None ~	
SSID	Nothing selected ~	
	Select All Deselect All	
	SSID1(AII)	Cancel
	SSID2	
	SSID3	
	SSID4	

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the schedule profile applied to the SSID.
Schedule	Select a name of the schedule profile.
SSID	Select a number of SSID.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.13.2 SSID

Set Service Set Identification (SSID), which shows up as the AP identifier.

2.46 5G	2865ac_001DAA00	0000 / Configuration	/ Wireless LAN			Ø				
	Index	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN				
General	1	true	false	2865_MKHenry	false	false				
590	2	false	false	DrayTek_Guest	false	false				
Security	3	false	false		false	false				
Access Control	4	false	false		false	false				
WPS	Note:									
Bandwidth Management		Isolate Member: Prevent the clients associated with this SSID from accessing each other. Isolate VPN: Block the wireless clients from accessing the VPN network and prevent wireless traffic being sent to VPN connections.								
Airtime Fairness	· ISOIDLE IPTA. C	nook the wireless them	s norm accessing the TPA netw	ork and prevent wireless dame deing sent i	o vrit connectoris.					

To configure the SSID profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

2865ac_001DAA000000 / Configu	rration / Wireless LAN	C
General Setup		
Index	1	
Hide SSID		
SSID	DrayTek	
Advance Setup		
Isolate Member		
Isolate VPN		
		Cancel Save

These parameters are explained as follows:

ltem	Description
	General Setup
Index	Display the index number of SSIDs. There are four SSIDs.
Hide SSID	Click to enable or disable the SSID settings.
SSID	Enter or display the name of SSID.
	Advance Setup
lsolate Member	Click to enable or disable the function. If enabled, the router disallows communication between wireless clients (stations) on the same SSID.
Isolate VPN	Click to enable or disable the function. If enabled, the router blocks wireless clients (stations) from accessing VPN clients.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.13.3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to the bottom of the router. For extra security, you can set your own wireless password

- Configuration	2865ac_0	01DAA000000 / Conf	Iguration / Wireless LAN		c
2.4G 5G	Index	Mode	WPA Encryption Mode	WEP Encryption Mode	WEP Key Index
30	1	WPA2/PSK	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
General	2	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
	3	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
	4	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
WPS					
Banchwidth Management					
Artime Fairness					

To configure security settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

2865ac_001DAA000000 / Configuration	Wireless LAN	C
General Setup		
Index	1	
Mode	WEP/802.1x_Only ~	
WEP		
WEP Encryption Mode		
WEP Key Index	1	
WEP Key	Φ	
Note: Please configure the <u>Wireless LAN</u>	(2.4GHz) 802.1X Setting,	
		Cancel Save

These parameters are explained as follows:

ltem	Description
	General Setup
Index	Displays the index number of SSID1 to SSID4.
Mode	Disable - Encryption mechanism is disabled. WEP or WEP/802.1x_Only- Allows only connections from WEP clients. WPA/802.1x_Only or WPA2/802.1x_Only or Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE - Allows only connections from WPA clients.
	WEP or WEP/802.1x_Only
WEP Encryption Mode	Select 64-bit or 128-bit.
WEP Key Index	Select an index number to configure the WEP setting.
WEP Key	Enter the encryption key.
	WPA/802.1x_Only or WPA2/802.1x_Only or Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE
WPA Encryption Mode	Displays the encryption mode used for WPA.
WPA Pre-shared Key	Enter 8~63 ASCII characters.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.13.4 Access Control

In the Access Control web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

<- Configuration	2865ac_001DAA000000 / Configura	tion / W	ireless LAN							C
2.4G 5G	General Setup									
Ceneral SSID	SSID 1 Enable		Ð							
Security	SSID 1 Policy		White_List			v				
Report Continue	SSID 2 Enable		0							
WPS	SSID 2 Policy		White_List			÷				
Bandwidth Management	SSID 3 Enable		Ø							
Airtime Fairness	SSID 3 Policy		White_List			÷				
Advanced Setting	SSID 4 Enable		Ø							
Band Steering AP Discovery	SSID 4 Policy		White_List							
Station List	CLASE LASTA KANSA									
Station List Advance	🛱 Clear									Cancel Save
Station List - Neighbor										
Roaming	MAC Address Filter List									
Station Control		Index	MAC Address	Attribute	55ID 1	55ID 2	55ID 3	SSID 4	Action	
		1							+ Add	

ltem	Description
	General Setup
SSID 1 Enable ~ SSID 4 Enable	Click to enable or disable the MAC filter.
SSID 1 Policy ~ SSID 4 Policy	White List - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list.
	Black List - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list.
Clear	Clear all modifications on this page.
Cancel	Discard current modification.
Save	Save the current settings.
	MAC Address Filter List
Index	Displays the index number of entry.
MAC Address	Enter the MAC address of wireless client.
Attribute	Select to isolate the wireless client from LAN.
SSID1 ~ SSID4	Select the SSIDs to which the above MAC address filter will be applied.
Action +Add	After entering MAC address and select SSIDs, click +Add to save the settings and create an additional setting entry.

9.4.13.5 WPS

It provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.

← Conliguration	2865ac_001DAA000000 / Configuration / Wire	less LAN	C
2.46 36	Enable WPS	•	
General	WPS Status	Configured	
SSID	WPS SSID	DrayTek	
Security	WPS Authentication Mode	WFM2/PSK	
Access Control			
Bandwidth Management		Cance	Save
Artane Fairness			_

ltem	Description
Enable WPS	Click to enable or disable the WPS function.
WPS Status	Displays system information related to WPS. The message "Configured" means that the wireless security (encryption) function of the router is properly configured and functioning properly.
WPS SSID	Displays the name of SSID1. WPS is supported on SSID1 only.
WPS Authentication Mode	Displays the current authentication mode of the router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.13.6 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.

Configuration		DAA000000 / Configuration / Wi					
46 56	Index	SSID	Enable	LimitType	UploadLimit	DownloadLimit	
	1	DrayTek	false	Auto_Adjustment	30000	30000	
	2	DrayTek_Guest	false	Auto_Adjustment	30000	30000	
	3		false	Auto_Adjustment	30000	30000	
	4		faise	Auto_Adjustment	30000	30000	
una Control							
ame Fairness							
anced Setting							

To configure the bandwidth management settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

ltem	Description			
SSID	Displays the specific SSID name.			
Enable	lick to enable or disable the function.			
Bandwidth Limit Type	 Auto_Adjustment - Bandwidth limit is determined by the system automatically. Total Upload - Enter a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to this router. Total Download - Enter a value to define the maximum data client(stations) connecting to this router. Per_Station_Limit - Bandwidth limit is determined according to the 			
	 Upload Limit(Kbps) - Enter a value to define the maximum data traffic (uploading) for each wireless client connecting to this router. Download Limit(Kbps)- Enter a value to define the maximum data traffic (downloading) for each wireless client connecting to this router. 			
Cancel	Discard current modification and return to previous page.			
Save	Save the current settings and return to previous page.			

9.4.13.7 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

← Configuration	2865ac_001DAA000000 / Configuration / Wireless IAN	c
2,4G SG	Enable Airtime Fairness	
General	Triggering Client Number 2	
SSID	(2 - 64, Selault: ?)	
Security		
Access Control	Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.	
WPS	Airtime: • Airtime is the time where a wireless station occupies the wireless channel. Airtime Fairness function tries to assign similar airtime to	
Bandwidth Management	each station by controlling TX traffic. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance	
Aletherie Falture III	 Suitable environment: (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection. 	
Advancest Setting	wreiess connection. Triggering Client Number: Airtime Fairness function is applied only when active station number achieves this number.	
Rand Streeting		
AP Discovery		
Station List		Cancel Save

These parameters are explained as follows:

ltem	Description
Enable Airtime Fairness	Click to enable or disable the airtime fairness.
Triggering Client Number	Airtime Fairness function is applied only when there are at least this many active wireless stations.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.13.8 Advanced Setting

This page allows you to configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

← Configuration	2865ac_001DAA000000 / Configuratio	n / Wireless LAN		
2.46 SG	Operation Mode	Mtxed_Mode	20	
	Channel Bandwidth	20/40		
SSID	Guard Interval	auto	~	
Security	Aggregation MSDU(A-MSDU)	•		
Access Control	Long Preamble	0		
WFS Bandwidth Management	TX Burst	0		
Airtime Fairness	Antenna	2T2R	0	
	Tx Power	100%	3	
Band Steering	WMM Capable	•		
AP Discovery	APSD Capable	0		
Station List Station List - Advance	Rate Adaptation Algorithm	New	_	
Station List - Neighbor	Fragment Length	2346		
Roaming		(256 - 2346 bytes)		
Station Control	RTS Threshold	2347		
		(1 - 2347 bytes)		
	Country Code		(Reference)	
				c

ltem	Description
Operation Mode	Mixed_Mode - The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless

	transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected.
	Green_Field - Select this mode to achieve the highest throughput. This mode supports data transmission between 802.11n systems only.
Channel Bandwidth	20 MHz - Vigor Router will utilize 20 MHz channels for data transmission and reception between the AP and wireless stations.
	40 MHz - Vigor Router will utilize 40 MHz channels for data transmission and reception between the AP and wireless stations.
	20/40 MHz - Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of nearby wireless APs.
Guard Interval	If you choose auto as guard interval, the router will choose short guard interval (which increases wireless performance) or long guard interval for data transmit depending on the station capability.
Aggregation MSDU	Click to enable or disable the function.
	If enabled, it will combine frames of different sizes to improve performance at the MAC layer for clients from certain manufacturers.
Long Preamble	Click to enable or disable the function.
-	This option determines the length of the sync field in an 802.11 packet.
TX Burst	Click to enable or disable the function.
	If enabled, this feature can enhance the performance in data transmission about 40%*.
Antenna	Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.
TX Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.
WMM Capable	Click to enable or disable the function.
	It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard.
APSD Capable	Click to enable or disable the function.
	It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old".
Fragment Length	
	Set the Fragment threshold. You are advised to leave the default value, 2346.
RTS Threshold	-
RTS Threshold Country Code	2346. Minimize the collision (unit is bytes) between hidden stations to improve
	2346.Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.Vigor router broadcasts country codes according to the 802.11d standard.
Country Code	 2346. Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Vigor router broadcasts country codes according to the 802.11d standard. Click Reference to get detailed information.
Country Code Isolate 2.4GHx and	 2346. Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Vigor router broadcasts country codes according to the 802.11d standard. Click Reference to get detailed information. Click to enable or disable the function. If enabled, the wireless client using 2.4GHz band is unable to connect to

9.4.13.9 Band Steering (for 2.4G only)

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

Configuration	286Sac_001DAA000000 / Configuration / Wireless LAN	c
2.46 56	Enable Band Steering	
General	5G Capability Check Timer 15	
SSID	(1 - 60 seconds, Default 15)	
Security		
Access Control	Note: Prease setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.	
WPS	Band Steering Note: Band Steering is used to detect if the wireless client is capable of dual-band or not. If dual-band is detected, the AP will let the wireless	
Bandwidth Management	 client connect to less congested wireless LAN, such as SGRz to prevent from network congestion. 	
Airtime Fairness	 Band steering would actively block the client's attempts to associate with 2.4GHz Wireless LAN. So the setting of "Check time for WLAN client 5G capability" would cause the delay of 2.4G WLAN connection. 	
Advanced Setting		
Bend Sherring		Cancel Save
AP Discovery		Canton Conto
- The second		

These parameters are explained as follows:

ltem	Description
Enable Band Steering	Click to enable to disable the Band Steering function.
5G Capability Check Timer	Set a check time value. When a wireless client attempts to connect, the router will block attempts to connect to the 2.4 GHz band for the specified period of time (default is 30 seconds), which hopefully will entice the client to connect to the 5 GHz band. If the client fails to connect to the 5 GHz band within the specified interval, it will then be able to connect to the 2.4 GHz band.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.13.10 AP Discovery

Vigor router can scan all regulatory channels to find working APs in the neighborhood.

	Index	SSID	BSSID	Channel	RSSI	Auth
General	1	FAE_AP903_Victor	00:1D:AA:3F:36:74	11	10%	WPA1PSKWPA2PSK
	2	Vigor2927 PQC Tang Test	16:49:BC:42:37:D8	9	10%	WPA2P5K
	3	staffs_5F	02:50:7F:C1:7F:1F	1	096	WPA1PSKWPA2PSK
Access Control	4	RD8_GW_24G_s1	00:1D:AA:5B:A0:C8	13	83%	WPA1PSKWPA2PSK
WPS	5	DrayTek04F06C	00:1D:AA:57:5D:38	11	096	WPA1PSKWPA2PSK
	6	DrayTek-LAN-B	06:1D:AA:3F:36:74	11	10%	WPA1PSKWPA2PSK
Bandwidth Management	7	DrayTek_24G_2862_Cole	00:1D:AA:F7:C0:E0	11	7196	WPA1PSKWPA2PSK
	8	FAE-Wendy-2925-BS	00:1D:AA:F0:6D:F0	11	096	WPA2P5K
Advanced Setting	9	DrayTek04F06C	00:1D:AA:04:F0:6C	11	7196	WPA1PSKWPA2PSK
Band Steering	10		12:1D:AA:04:F0:6C	11	7196	WPA2PSK
	11	DrayTek-E48E80	00:1D:AA:E4:8E:80	11	096	WPA2PSK
	12	FAE2925_Guest	02:1D:AA:F0:6D:F0	11	096	WPA2
Station List	13	guests	02:50:7F:D1:7F:1D	11	3196	WPA2P5K
Station List - Advance	14	staffs	02:50:7F:C1:7F:1D	11	3196	WPA2P5K
Station List - Neighbor	15	AP902_RD8_Tim	00:1D:AA:3D:4F:16	10	2196	WPA1PSKWPA2PSK
Roaming	16	2927_RD8_tim	16:49:BC:42:37:68	9	096	WPA1PSKWPA2PSK
Station Control	17	V2865-PQC-Tang	02:1D:AA:48:E8:08	9	26%	WPA2P5K
Station Control	18	PQC WiFi WAN Test	02:50:7F:C1:91:EA	9	24%	WPA2P5K
	10	RD8 rim 2865 24#	02:1D:AA:41:DE:78	0	3,496	WPA1PSKWPA2PSK

9.4.13.11 Station List

Station List provides an overview of all currently connected wireless clients and their status.

<- Configuration	2865ac_001DAA000000 / Configuration / Wireless LAN	C
2.40 50	Station List	
General	Status Codes ; • C.Connected, No encryption.	
550	E Connected, WEP.	
Security	P: Connected, WPA K:Connected, WPA2.	
Access Control	B: Blocked by Access Control.	
wis	N Convecting.	
Bandwidth Management	Fe Fail to pass W94,050K authentication.	
Artime Fairness	Add to Access Control :	
Advanced Setting		
Band Steering	MAC	
AP Discovery	55ID (1-4)	
Station List		
Station List - Advance	Add	
Station List Neighbor	Note: • After a station connects to the router successfully, it may be turned off without action. In that case, it will still be on the that until the connection expires.	
Roaming		

These parameters are explained as follows:

ltem	Description		
Station List	Displays wireless stations connected to the Vigor router.		
Add to Access Control	MAC - Enter the MAC address.		
	SSID - Specify the number of SSID.		
Add	Click to add a new entry to Access Control.		

9.4.13.12 Station List - Advance

Displays wireless stations connected to the Vigor router with more detailed information.

← Configuration	2865ac_001DAA00	2865ac_001DAA000000 / Configuration / Wireless LAN									
2.46 SG	Index	MAC Address	AID	RSSI	Rate	BW	PSM	WMM	PhMd	MCS	
General					\triangle						
SSID					No data available						
Security											
Access Control	Add to Access	Control:									
WIS	MAC										
Bandwidth Management	SSID		(1-4)								
Airtime Fairness											
Advanced Setting								Add			
Band Skeering	• After a station										
AP Discovery										_	
Station List											
Station List - Advance											
Station List - Neighbor											
Roaming											
Station Control											

9.4.13.13 Station List - Neighbor

This page displays the nearby wireless stations connected to other access points that are detected by the Vigor router.

 ← Configuration 	2865ac_001DA	A000000 / Configuration /				e			
2.46 56	index	MAC Address	Vendor	RSSI	Apprex Distance		SSID	Visit Time	
General	Add to Acce	ss Control :							
SSID			60						
Security	MAC		00:1D:AA:00:00:00		~				
Access Control	SSID		1		×				
wrs									
Bandwidth Management	Note:					Add			_
Airtime Faimesa			Ignal strength of device detected. Inac						
Advanced Setting			or different devices, the calculated values of their respective owners.		ce also might be different.				
Band Steering	· · · · ·	and should be also be a	penns of men respective owners.						_
AP Discovery									
Station List									
Station List - Advance									
Station List - Heighbor									

These parameters are explained as follows:

ltem	Description
Station List	Displays wireless stations connected to the Vigor router.
Add to Access Control	MAC - Enter the MAC address.
	SSID - Specify the number of SSID.
Add	Click to add a new entry to Access Control.

9.4.13.14 Roaming

WiFi roaming allows wireless stations to switch connections between access points within an area to achieve better coverage and signal quality.

← Configuration	2865ac_001DAA000000 / Configuration / Win	eless LAN	C
2.45 56	Roaming Type	Minimum_RSSI ~	
General	Minimum RSSI	-46	
SSID Security	Adjacent AP RSSI over	60% (Default: 46 dBm) \$	
Access Control		(Default: 5 dbm)	
WPS	AP-assisted Client Roaming Note: When AP detects that a station may a	need to marm, AP disconnects the station	
Bandwidth Management	 This feature helps those stations with sticky to the original AP and with bac 	bad roaming ability. Avoid the situation that a station is already close to the other AP but still	
Airtime Faimesa	 Please notice that RSSI Requirement 		
Advanced Setting	Minimum RSSI with Adjacent AP RSSI or Disconnect clients with had signal to	ver X encourage roaming only when they can have better signal through another DrayTek AP.	
Band Steering	All APs must be DrayTek APs which a	upport this feature. The LANs assigned by the SSID of all APs must be connected by Ethernet and	
AP Discovery.	under the same subnet.		
Station List	-		
Station List - Advance			Cancel Save
Station List - Neighbor			
here's			
Station Control			

These parameters are explained as follows:

ltem	Description
Roaming Type	 Disable RSSI Requirement - The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations. Strictly Minimum RSSI

	Minimum RSSI
Strictly Minimum RSSI	The Vigor router will immediately disconnect the wireless station if its RSSI falls below the configured value. Specify a value as a threshold.
Minimum RSSI	The Vigor router will disconnect wireless clients whose RSSI falls below the minimum threshold only if there is also a neighboring wireless host (router or AP) that has an RSSI value (defined in the field of With Adjacent AP RSSI over) higher than a certain threshold.
	In order for this option to work, other wireless hosts connected to the same LAN subnet need to support the exchange of RSSI information with peer wireless hosts via Ethernet.
	Specify a value as a threshold.
Adjacent AP RSSI over	Specify a value as a threshold.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.13.15 Station Control

Station Control is used to specify the duration that the wireless client can connect to the Vigor router. If this function is disabled, wireless clients can connect to the router as long as the router is powered on and the wireless feature is enabled.

 ← Configuration 	2865ac_001	DAA000000 / Configuration / Wire	less LAN			C
2.46 56	Index	SSID	Enable	Connect Time	Reconnect Time	
30	1	DrayTek	false	0 days:1 hours:0 min	1 days:0 hours:0 min	
	2	DrayTek_Guest	faise	0 days:1 hours:0 min	1 days:0 hours:0 min	
	3		false	0 days:1 hours:0 min	1 days:0 hours:0 min	
	4		faise	0 days:1 hours:0 min	1 days:0 hours:0 min	
Bandwidth Management						
Airtime Fairness						
Advanced Setting						
Band Steering						
AP Discovery						
Station List						
Station List - Advance						
Station List - Neighbor						
Reaming						

To configure the station control settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

dex	1	
SID	DrayTek	
nable		
onnect Time	0 ~ days hours 0 ~	
econnect Time	1 ~ 0 ~ days hours minutes	
<u>play All Station Control List</u> t <u>spot Web Portal</u>		
Note: Once the feature is enable	d, the connection time quota will apply to each wireless client (identified by MAC address).	

ltem	Description
Index	Displays the index number of SSID profile.
SSID	Displays the name of the SSID.
Enable	Click to enable or disable the station control function for this SSID.
Connect Time /	Enter the time in days, hours and minutes.
Reconnect Time	In the Connection Time dropdown box, select the maximum amount of time that a wireless client is allowed to connect within the period of time selected in the Reconnection Time dropdown box.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14 Bandwidth Management

9.4.14.1 Sessions Limit

When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is a finite number of sessions that can be tracked by the router. By setting session limits will ensure that the router does not run out of resources.

← Configuration	2865ac_001DAA000000 / Configuration / Bandwidth Management	c
C Cordigoration Constant Line Bandwidth Line AIPPQuS	IPv4 Enable Default Max Sessions Limitation Lb1 Index Start IP End IP Max Sessions I 0.0.0.0 0.0.0 0 Clear Al IPv6 Enable Default Max Sessions I00 Limitation Lb1 Index Start IP End IP Max Sessions I00 Limitation Lb1 Index Start IP End IP Max Sessions I00 Limitation Lb1 Index Start IP End IP Max Sessions	c
	I 0	Cancel Save

ltem	Description
	IPv4 / IPv6
Enable	Click to enable or disable the sessions limit function.
Default Max Sessions	The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List.
Limitation List	Displays specific limitation entries.
Clear All	Clear all modifications on this page.
	Administration Message
Administration Message	Enter a message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached.
	Time Schedule
Schedule 1 ~ 4	Specify up to 4 time schedule entries to enable or disable the WAN. Specify up to 4 time schedule entries to apply the sessions limit management.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.14.2 Bandwidth Limit

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

- Configuration	2865ac_001DAA000000 / Configura	tion / Bandwidth Management	
essions Limit	IPv4		
andweddi Clinif IPP Qess	Enable	0	
	IP Routed Subnet	Ø	
	Default TX Limit Per User	2000 Kbps ~	
	Default RX Limit Per User	8000 Kbps ~	
	Limitation List	Index Start IP End IP TXLimit EXClimit Eact	
		1 None None 0 0 Eac	
		© Char Al	
	IPv6		
	Enable	\odot	
	Default TX Limit Per User	2000 Kbps ~	
	Default RX Limit Per User	8000 Kbps ~	
	Limitation List	Index Start IP End IP TX.Limit RX.Limit Eact	
		1 None None 0 0 Eac	
		ft: Clear All	
		Cance	t Sa

ltem	Description	
	IPv4 / IPv6	
Enable	Click to enable or disable the bandv	vidth limit function.
	IP Routed Subnet - It is available for	or IPv4 only.
Default TX Limit Per User	Set default upstream speed limit for	r each LAN client.
Default RX Limit Per User	Set default downstream speed limit	for each LAN client.
Limitation List	Displays specific limitation entries.	
	To add a new profile, click the last ir	ndex number to open the setting page.
	IPv4 Bandwidth Limitation List Add Entry By IP Group IP Object Each or Shared TX Limit RX Limit Clear After finishing the settings, click Sav	IP Range IP Object None ~ Each Shared 0 Mbps ~ 0 Mbps ~

	displayed on the limitation list.					
	Limitation List	Index	Start IP	End IP	тх	
		1	192.168.1.55	192.168.1.65	10:	
		2	None	None	0	
		💼 Clear A	.11			
Clear All	Clear all profiles in the limitation list.					
Allow user to use	Click to enable or disable this fur	iction.				
more bandwidth than the assigned	If enabled, it lets the router automatically adjust the upstream and downstream limits based on available bandwidth.					
Smart Bandwidth	Click to enable or disable this function.					
Limit	If enabled, it restricts the bandwidth of LAN clients that are not in the limitation list when the network sessions exceed a predefined threshold.					
Apply the below limit to users not in	Enter the number of sessions that a LAN client is allowed to have before Smart Bandwidth Limit activates.					
TX Limit	Upstream speed limit for each LAN client. Unit can be either Kbps or Mbps					
RX Limit	Downstream speed limit for each LAN client. Unit can be either Kbps or Mbps.					
	Time Schedule					
Schedule 1 ~ 4	Specify up to 4 time schedule en management.	tries to a	apply the ba	ndwidth lin	nit	
Cancel	Discard current modification.					
Save	Save the current settings.					

9.4.14.3 APP QoS

APP QoS allows QoS to be applied to select protocols and applications. Protocols and applications fall into two categories: Traceable and Untraceable.

← Configuration	2865ac_001DAA000000 / Configuration / Bandwidth Management	C
Sesion Unit Bandwidth Lmit Al ^{age} Quis Traceable	APP QoS Enable	
Traceable Unimacnable		Save

Click the **Enable** button to enable or disable the APP QoS function. Then click **Save** to save the settings.

Traceable

Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class.

← Configuration	2865ac_001DAA000000	/ Configuration / Bandwidth Management	c
Sealors Limit	Index	Type Name	
Bandwidth Dimit	1	Instant Message	
APP Qua	2	VolP	
	3	Protocol	
Tracade	4	Tunneting	
Uetroceable	5	Stream	
	6	Remote Control	
	7	Web HD	
	8	Game	
	0	Apple Services	
	10	Google Services	
	11	Amazon Services	
	12	E-Life	
	Note: Please rememb This will help Q	nt to adjust tabound. On facund bandwidth of your network in "Quality of Service". S is work more efficient.	

Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.

← Configuration	2865ac_001DAA000000 / Configu	ration / Bandwidth M	anagement		c
Sessions Limit Bandwidth Limit Allth Quil	index Type Name	1 Instan	it Message		
	Select All Clear All			← Apply to all	
Untraceable	Арр Name	Enable	Version	Action	
	Facebook/Instagram	Ø		QoS Class 1 (High) ~	
	UNE	D	5.23.0.2134	QoS Class 1 (High) ~	
	Linkedin	Ø		QoS Class 1 (High) ~	
	Signat	Ø	1.26.2	QoS Class 1 (High) ~	
	Stack	Ø	4.0.0	QoS Class 1 (High) ~	
	Snapchat	0	10.79.5.0	QoS Class 1 (High)	
	Telegram	Ø	1.7.10	Qo5 Class 1 (Hgh) ~	
	WhatsApp	0	0.3.2848	Qo5 Class 1 (Hgh) ~	
				Car	ncel Sawe

These parameters are explained as follows:

ltem	Description	
Enable	Click to enable or disable the bandwidth limit function.	
Action	Select a QoS class to be applied to the application.	
Cancel	Discard current modification.	
Save	Save the current settings.	

Untraceable

Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

<- Configuration	2865ac_001DAA000000 /	Configuration / Bandwidth Management	C
Sessions Limit Bandwidth Limit	Action	QoS Class 1 (High) v	
APP QuS	Index 1	Type Name Instant Message	
ListnenMe	2	VolP 1929	
	4 5 6	Protocol Tunneling Striam	
	1	Remote Control	
	8 (*) Motes - Please neinvender - This with help Oo	Web HD r to adjust inbound /Duthound bandwidth of your network in "quality of Servicer". 5 to work more efficient.	Save

Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.

Configuration	2865ac_001DAA000000 / Configura	tion / Bandwidth Management		
essions Limit	Index	1		
andwidth Limit	Type Name	Instant Message		
PP QoS				
Inaccable	Select All Clear All			
	App Name	Enable	Version	
	AIM Login	CD	8	
	AUWW	0	2008	
	Ares	0	2.0.9	
	BaiduHI	D	37378	
	Fetton	0	2010	
	GaduGadu Protocol	0)		
	ICQ	0	7	
	ISpQ	Ø	8.0.60	
	ĸc	D	2008	
	Paltalk	0	9	
	PocoCall	0	2007	
	Qmext	0	3.0.1	
	Tencent QQ	Ø	2012/2009 beta3	
				Cancel Sav

These parameters are explained as follows:

Item	Description
Enable	Click to enable or disable the bandwidth limit function.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.15 USB Applications

9.4.15.1 General Settings

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

← Configuration	2865ac_001DAA000000 / Configuration /	USB Application	e
General Settings	Simultaneous FTP Connections	\$	
User Management	Default Charset	English ~	
Dek Status Modern Status	SMB File Sharing Service		
Modern Status	Access Mode	LAN Only LAN And WAN	
Sensor Status	Workgroup Name	WORKGROUP	
	Host Name	Vigor	
	Printer Server	0	
	limit client connections to 1 to impro	anned by Bouter FTP server. If your FTP client has a multi-connection mechanism, such as FIR/ZIIIa, you should we performance. I rom the host name. The workgroup name can have up to 15 characters and the bost name can have up to 15	San

ltem	Description
Simultaneous FTP Connections	Enter the maximum number of simultaneous FTP sessions allowed.
Default Charset	Select the character set for file and directory names.
SMB File Sharing Service	Click to enable / disable the function.
Access Mode	LAN Only - Only users on the LAN can connect access the shared USB disk. LAN and WAN - Both LAN and WAN users can access SMB server of the router.
Workgroup Name	Enter the workgroup name. Maximum allowed length is 15 characters.
Host Name	Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters.
Printer Server	Click to enable / disable the function. If enabled, the Vigor router can act as a print server for printers connected the USB.
Save	Save the current settings.

9.4.15.2 User Management

This page allows you to set up profiles for FTP/SMB users.

← Configuration	2865ac_001DAA000000 / Configuration / USB Application		Set to Factory Default 📿			
General Settings	Index	Username	FTP/SMD User	Home Folder	File Access Rule	Directory Access Rule
	1		talse			
And Managements						
ther Heragonisti Disk Status						
Modem Status						
Printer Status						

To configure the user management settings, move the mouse cursor to any entry and click to open the following page.

2865ac_001DAA000000 / Configuration /	USB Application	Set to Fact	ory Default	C
A No USB disk Connected ! Please Insert t	he disk.			
Index	1			
FTP/SMB User	\bigcirc			
Username	(Max. 11 characters allowed)			
Password	(Max. 11 characters allowed) $$\Phi$$			
Confirm Password	•			
Home Folder				
Create New Home Folder				
	+ Create			
Note: The folder name can only contain the	e following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! () and space.			
Access Rule				
File	Read			
	Write			
	Delete			
Directory	🗆 List			
	Create			
🖻 Clear		Ca	ncel Sa	ave

ltem	Description	
Index	Displays the index number of USB application profile.	
FTP/SMB User	Click to enable / disable the function. If enabled, this profile (account) for FTP service and / or SMB service will be activated.	
Username	Enter the username for this user profile.	
Password	Enter the password for this user profile.	
Confirm Password	Enter the password again to confirm.	
Home Folder	Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile.	
Create New Home Folder	Enter a name as a new folder name. + Create - Click to create a new folder.	
	Access Rule	
Access Rule	File – Check the items (Read, Write and Delete) for such profile. Directory –Check the items (List, Create and Remove) for such profile.	

Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.15.3 Disk Status

This page displays the status information for the USB disk connecting to Vigor router.

+- Configuration	2865ac_001DAA000000 / Configu	aration / USB Application			¢
General Settings User Management	Connection Status	No Disk Connected			
Mick Status	Write Protect Status	NULL.			
Modern Status Printer Status	Disk Capacity Free Capacity	0 MB			
Sensor Matia	 Only support to mount si Single file size can be up 	Al 32 format, FAT32 Is recommended. opti partition, maximum apacity is 500CB. If them are more then one 6.42, which is been instruction of 14312 format. 6.42, which is been instruction of 14312 format. For a second second second second second second second second of USB disk is turned on, the USB disk is in READ-ONLY mode. No defined to the second se			
	Index Service	IP Address (Port)	Username	Drop	
	8				

These parameters are explained as follows:

ltem	Description
Connection Status	Displays if the USB is connected or disconnected. Disconnect USB Disk - If connected, click to disconnect USB disk with the router.
Write Protect Status	Displays the total capacity of the USB storage disk.
Disk Capacity	Displays the disk capacity.
Free Capacity	Displays the free space on the USB storage disk.
USB Disk Users Connected	Displays the clients that are connected to the SMB/FTP server.

9.4.15.4 Modem Status

General Settings		/ Configuration / USB Application			Ø
User Management	Index	Connection Status	Manufacturer	Model	
Temperature Sensor	2	No Modem Connected			
Disk Status					
Modern Status					
Printer Status					
Sensor Status					

Click the index number to open the following for viewing detailed information for parameter settings.

/ Configuration / USB Appl	ication	
Index	2	
Connection Status		
Manufacturer		
Model		
Revision		
Serial Number		
IMSI		
Signal Quality (CINR)		
RSSI Signal		
Hardware		
SIMPIN	٥	
Link Speed		

9.4.15.5 Printer Status

This page displays current status for the USB printer connecting to Vigor router managed by VigorACS 3.

← Configuration	2865ac_001DAA0	00000 / Configuration / U	SB Application		e
General Settings	Connection Stat	us:	No Printer Connected		
User Management	Manufacturer		No Printer		
Disk Status	Model		No Printer		
Modern Status	and a second				
	Serial Number		No Printer		
Sensor Status	Printer Queue				
	Index	User	Files Name	Status	
	1	No Printer	No Printer	No Printer	
	2	No Printer	No Printer	No Printer	
	3	No Printer	No Printer	No Printer	
	4	No Printer	No Printer	No Printer	

9.4.15.6 Sensor Status

This page displays current status for the USB thermometer connecting to Vigor router managed by VigorACS 3.

← Configuration	2865ac_001DAA000000 / Configuration / USB Ap	2865ac_001DAA000000 / Configuration / USB Application	
General Settings	Connection Status	Thermometer Connected	
User Management Disk Status	Manufacturer	RDing	
Modern Status	Product	TEMPerLFV2.4	
Printer Status			-
Senari Mahis			

9.4.16 System

9.4.16.1 Maintenance

This page can be used for backup configuration for specified CPE, restoring configuration for specified CPE, making firmware upgrade for CPE, and even reboot the specified CPE via VigorACS 3.

	2865ac_001DAA000000 / Configuration	/ System	c
Watersteine	Configuration Backup		
Time Settings			
Admin Account	Backup Config	Backup	
Admin Local Liser	Restore Config	Last Config Local File Shared Folder	
SNMP Settings		Kinstore Now	
Managyement	Download Config	Download	
111069 Settings			
Systog Settings			
Mail Alert	Firmware Upgrade		
Internal Service User List			
Panel Control	Model Name	Vigor2865ac	
	Modern Firmware Version	(null_STD	
	Firmware Version	4.2.2, RC1_5TD	
	Choose a Firmware File From	Locat File Shared Folder	
		Bronna	
		Upgrade Now	
		Save	
12			

ltem	Description
	Configuration Backup
Backup Config	Backup - Click to backup the configuration from CPE to VigorACS server.
Restore Config	Select the type of configuration file.
	Last Config
	Local File
	Shared Folder
	Restore Now - Click to initiate restoration of configuration immediately.
Download Config	Download - Click to download the lastest configuration backup file from VigorACS server.
	Firmware Upgrade
Model Name	Displays the model name of the CPE.
Modem Firmware	Displays the modem version of the CPE.
Version	No DSL - It indicates the selected CPE is non-DSL device.
Firmware Version	Displays the firmware version used by the CPE.
Choose a Firmware	Local File - Select a firmware from the host by clicking Browse.
File From	Shared Folder - Select a firmware from the database by click Browse.
	Upgrade Now - Click to upgrade the firmware immediately.
	Automatic Firmware Recovery
Enable	Click to enable or disable the function.

	If enabled, when the router unexpectedly reboots three times in a row then the backup firmware will be restored to the unit on the third reboot.
	Backup Setting
Backup Mode	Backup after reboot - The backup will be executed after the router reboot.
	Backup after system uptime - The backup of current running firmware will be executed after a period of time. The default is 24 hours (1 day).
	Backup manually - The backup will be executed manually according to your request.
Backup Firmware	Displays the backup firmware version of the CPE.
Last backup	Displays the time for the last backup for the CPE.
	Device Reboot
Restart the device	Reboot Now - Click to reboot the router immediately.
	Reset
Reset to factory default	Reset Now - Click to reset the router with factory default setting immediately.
Save	Save the current settings.

9.4.16.2 Time Settings

This page allows you to configure settings related to the system date and time.

← Configuration	2865ac_001DAA000000 / Configuration	n / System	
Maintenance	Current System Time	2020-11-09707:43:37	
	Local Time Zone	+00.00	
Admin Account	Time Setup	Use_Browser_Time Use_Internet_Time	
idmin Local User	NTP Server	pooLntp.org	
NMP Settings	An and a second at the		
lanagement	Priority	Auto 🗸	
R069 Settings	Time Zone	(GMT) Greenwich Mean Time : Dublin 🔍	
yslog Settings	Daylight Savings	0	
	Daylight Saving Type	Default By Date By Weekday	
	Start	Yearly on March last Sun	
anel Control	End	Yearly on October last Sun	
	Automatically Update Interval	30 mins 🗠	
	Send NTP Request Through	Auto ~	

ltem	Description
Current System Time	Displays the current time obtained from the time server.
Local Time Zone	Displays the time zone where the router is located.
Time Setup	 Use_Browser_Time - Click to let the router set its system time using the time reported by the web browser. Use_Internet_Time - Click to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).
NTP Server	Enter the address of the time server.

Priority	Select Auto or IPv6 First as the priority.
Time Zone	Select the time zone where the router is located.
Daylight Savings	Click to enable or disable the Daylight Saving Time (DST) if it is applicable to your location.
Daylight Savings Type	Default - Uses the default DST schedule for the time zone.
	By Date - Select this option if DST starts and ends on fixed dates.
	By Weekday - Select this option if DST starts and ends on certain days of the week.
Start	It is available when By Date is selected as Daylight Saving Type.
	Use the drop down list to select month, day and hour settings as the starting point.
End	It is available when By Date is selected as Daylight Saving Type.
	Use the drop down list to select month, day and hour settings as the ending point.
Automatically Update Interval	Select the time interval at which the router updates the system time.
Send NTP Request Through	Select a WAN interface to send NTP request for time synchronization.
Save	Save the current settings.

9.4.16.3 Admin Account

This page allows you to set or change the administrator password.

<- Configuration	2865ac_001DAA000000 / Configuration / Syste	m	C
Maintenance	Admin Account		
Time Settings	Admin Password	•	
Admin Accusol)			
Admin Local User	 Diverse Password can contain only a-z A-Z 0-9	.*~**= ?@x*I()\$%&	
SNMP Settings	Enable 'admin' account login to Web UI from the	•	
Management	Internet		
TR069 Settings	Use only advanced authentication method for	0	
SysLog Settings	Admin "WAN" login		
MallAlet	User Account		
Internal Service User List	- OAT ACCOUNT		
Panel Control	Enable User Account	0	
	User Password	•	
	Note: Password can contain a 2.4-2.0.9; . * < Password can't be all asterbics(*). For each other in the second can't be all asterbics(*).	-**= j ? @ # *1 () mple, ** ar **** is thegot, but ? 123** or **65* Is OK.	
	Login Greetings		
	Login Page Logo	Default ~	
	Enable Login Greetings	0	
			Cancel Save

ltem	Description	
	Admin Account	
Admin Password	Enter the new password.	
Enable admin account login to	Click to enable or disable the function. If enabled, it allows the administrator to log in from the Internet. This	

	option is enabled when Administrator Local Account is enabled (see below).		
Use only advanced authentication	Click to enable or disable the function. If enabled,		
	Advanced Authentication - Advanced authentication method can offer a more secure network connection. Select to require mOTP or 2-step authentication when logging in from the WAN.		
	• Mobile one-Time Password (mOTP) - Enter the PIN Code and Secret settings for getting one-time passwords.		
	 2-Step Authentication - Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. 		
	User Account		
Enable User Account	Click to enable or disable the function.		
	If enabled, other users are allowed to administer the router.		
User Password	Enter a string as the password for the user account.		
Login Greetings			
Login Page Logo	Default - Choose it to use the default image.		
	Blank - Choose it to discard the logo image.		
	Upload a file - Choose it to specify an image as the logo.		
Enable Login Greetings	Click to enable or disable the function.		
Logo Image Upload	It is available when Upload a file is selected as Login Page Logo.		
	Browse - Click to select an image file.		
	+Upload - Click to upload the selected image file to VigorACS.		
Title	Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.		
Message	Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom.		
Cancel	Discard current modification.		
Save	Save the current settings.		

9.4.16..4 Admin Local User

Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router.

- Configuration	2865ac_001DAA000000	0 / Configuration / System			
wintenance	Local User	a	D.		
ime Settings	Use only advanced aut	hentication method for Admin 🥥	5		
dmin Account.	"WAN" login				
	Local User List				
MP Settings	Index	Username	Password	Action	
Ganagement R069 Settings	1			+ Add	
n Log Settings all Alert	Administrator LDA	AP Setting			
emal Service Diser Dist	Enable LDAP/AD login f	for Admin users	0		
	① Note: * 17 Local Use	er is enabled, you will need to s	elect 'admin' group when log into We	u UL	

ltem	Description		
Local User	Click to enable or disable the local user setting.		
Use only advanced authentication method for Admin "WAN" login	Advanced authentication method can offer a more secure network connection. Select to require mOTP or 2-step authentication when logging in from the WAN.		
Local User List	Index - Displays the index number of local user profile.		
	User Name - Displays the name of the local user profile.		
	Password - Displays the password of the local user profile.		
	Action +Add - Click to create a new user profile.		
	Username Image: Module one-Time Pasawork(m017) Authentication method Image: Module one-Time Pasawork(m017) 2-Step Authentication - Pasaword - Confirm Pasawork -		
	Note: * Max.15 characters for Unemanne and Pessword Cancel Cancel Save		
	Canor Srm		
	Index - Displays the index number of the profile.		
	Index - Displays the index number of the profile.		
	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step 		
	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step Authentication. 		
	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step Authentication. If Basic is selected - Enter the password. If Mobile one-Time Password (mOTP) is selected- Enter the 		
	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step Authentication. If Basic is selected - Enter the password. If Mobile one-Time Password (mOTP) is selected- Enter the PIN Code and Secret settings for getting one-time passwords. If 2-Step Authentication is selected- Select the SMS and/or Mail profiles and the destination SMS number and/or email 		
Enable LDAP/AD login for Admin users	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step Authentication. If Basic is selected - Enter the password. If Mobile one-Time Password (mOTP) is selected- Enter the PIN Code and Secret settings for getting one-time passwords. If 2-Step Authentication is selected- Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. 		

9.4.16.5 SNMP Settings

This page allows you to configure settings for SNMP and SNMPv3 services.

Configuration	2865ac_001DAA000000 / Configurati	Ion / System	c
Maintenance	Enable SNMP Agent	0	
Time Settings	Enable SNMPV1 Agent		
Admin Account	Enable SNMPV2C Agent		
Admin Local User	Get Community	public	
SIGNP Settings Management	Set Community	private	
TR069 Settings	Trap Community	public	
Syslog Settings	Trap Timeout	10	
Mail Alert Internal Service-User List	Manager Host IP (IPv4)		
Panel Control	Index I: IP	0.0.0.0	
	Index 1: Subnet Mask		
	Index 2: IP	0.0.0.0	
	Index 2: Subnet Mask	~	
	Index 3: IP	0.0.0	
	Index 3: Subnet Mask		
	Manager Host IP (IPv6)		
			Save

ltem	Description	
Enable SNMP Agent / Enable SNMPV1 Agent / Enable SNMPV2C Agent	Click to enable or disable the SNMP function.	
Get Community	Enter the Get Community string. The default setting is public.	
Set Community	Enter the Set Community string. The default setting is private.	
Trap Community	Enter the Trap Community string. The default setting is public.	
Trap Timeout	The default setting is 10 seconds.	
	Manager Host IP (IPv4)	
Index #:IP	Enter the IPv4 address of hosts that are allowed to issue SNMP commands.	
Index #: Subnet Mask	Select a subnet mask for IP address configured above.	
	Manager Host IP (IPv6)	
Index #: IP	Enter the IPv6 address of hosts that are allowed to issue SNMP commands.	
Index #: Prefix Length	Enter the fixed value for prefix length.	
	Notification Host IP (IPv4)	
Index #: IP	Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.	
	Notification Host IP (IPv6)	
Index #: IPv6 Address	Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.	
	SNMPV3 Agent	
Enable SNMPV3 Agent	Click to enable or disable the SNMPv3 function.	

USM User	Enter the username to be used for authentication
Auth Algorithm	Select one of the hashing methods to be used with the authentication algorithm.
Auth Password	Enter a password for authentication.
Privacy Algorithm	Select an encryption method as the privacy algorithm.
Privacy Password	Enter a password for privacy.
Save	Save the current settings.

9.4.16.6 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

Configuration / Social State 2865ac_001DAA000000 / Configuration / Social State 2865ac_001DAA0000000 / Configuration / Social State 2865ac_00000000 / Social State 2865ac_000000000000000000000000000000000000	System	
Interance Router Name	DrayTek	
ne Settings Default:Disable Auto-Logout	C	
In Account Enable Validation Code in Internet/LAN Access	Ø	
Local User		
Constant and below version does NOT support Constant and below version does NOT support	HT DrayOS CAPTCHA auth code.	
entent.		
Settings Internet Access Control		
Settings Allow management from the internet		
rt Domain name allowed		
Service User List	FIP Server	
ntral	THIP Server	
	Endorce HTTPS Access	
	HTTPS Server	
	Tetnet Server	
	SR Server	
	SNMP Server	
Disable PING from the internet	0	
LAN Access Control		

ltem	Description
Router Name	Enter the router name as provided by ISP.
Default:Disable Auto-Logout	Click to enable or disable the function. If enabled, the auto-logout function for web user interface will be disabled
Enable Validation Code in Internet/LAN Access	Click to enable or disable the function. If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in.
	Internet Access Control
Allow management from the Internet	Click to enable or disable the function. If enabled, it allows system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered.
Domain name allowed	Enter a domain name. This setting is only available if DNS filtering is enabled, applying DNS filter profile in firewall rules, or enabling DNS Filter Local Setting.

Disable PING from	Click to enable or disable the function.
the Internet	If enabled, it will reject all PING packets from the Internet. For increased security, this setting is enabled by default.
	LAN Access Control
Allow management	Click to enable or disable the function.
from LAN	If enabled, it allows system administrators to login from LAN interface.
	There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply to Subnet	Click to enable or disable the LAN interface.
	If enabled, the selected interface can be used for accessing into web user interface of Vigor router.
	IP Object Enable - Click to enable or disable the IP object setting.
	Index in IP Object - Enter the index number of the IP object profile. Related IP address will appear automatically.
	IPv6 Management Setup
Allow management from the Internet	Click to enable the function. Select the servers that system administrators are allowed to manage from the Internet.
Disable PING from the Internet	Click to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
	IPv6 Address Security Option
Enable Random	Click to enable or disable the function.
Interface Identifiers	If enabled, the IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker.
	Access List from the Internet
Apply Access List to	Click to enable or disable the function.
PING	Access List #: IP Object - Enter the index number of the IP object profile. Related IP address will appear automatically.
	IPv6 Access List
Apply Access List to	Click to enable or disable the function.
PING	Access List #: IPv6 Object - Enter the index number of the IP object profile. Related IP address will appear automatically.
	Management Port Setup
Management Port Setup	User Define Ports - Specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.
	Default Ports - Use standard port numbers for the Telnet and HTTP servers.
	Brute Force Protection
Enable brute force	Click to enable or disable the function.
login protection	If enabled, any client trying to access into Internet via Vigor router will be asked for passing through user authentication.
Maximum login failure	Specify the maximum number of failed login attempts before further login is blocked.
Penalty period	Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed.

	Blocked IP List
Table	Display, in a new browser window, IP addresses that are currently blocked from logging into the router.
	TLS/SSL Encryption Setup
TLS 1.3, 1.2, 1.1, 1.0 Enable, SSL 3.0 Enable	Check the box to enable SSL 3.0/1.0/1.1/1.2 encryption protocols.
	CVM Access Control
Enable CVM Port	Click to enable or disable the function.
CVM Port	Check the box to enable Central VPN Management port setting.
Enable CVM SSL Port	Click to enable or disable the function.
CVM SSL Port	Check the box to enable Central VPN Management SSL port setting.
	AP Management
Enable AP Management	Click to enable or disable the access point management function.
	Device Management
Device Management	Click to enable or disable the device management function.
Respond to external device	Click to enable or disable the function. If enabled, the router will function as a slave device.
Save	Save the current settings.

9.4.16.7 TR069 Settings

CPE device supports the TR-069 standard for remote management by VigorACS.

<- Configuration	2865ac_001DAA000000 / Configuration / Syst	011	C*
Maintenance	Primary		
Time Settings	Tr069 Enable	0	
Admin Account	ACS Server On	Internet ~	
Admin Local User	URL	http://192.168.105.130/#CSServer/services/#CSServ	
SNMP Settings			
Management		Acquire URL from DHCP option 43	
	Username	rd8	
SysLog Settings			
Mail Alert	Password		
Internal Service User List	Client Settings		
Panel Control	Protocol	нтр нтря	
	Client URL	http://192.168.105.123.0060jcwm/CENLhtml	
	Port	8069	
	Username	vigor	
	Password	٥	
	Periodic Inform Settings		
	Enable Periodic Inform	•	
		Sav	

ltem	Description
	Primary

Tr069 Enable	Click to enable or disable the TR-069 functionality.
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.
URL	Enter the URL for connecting to the ACS. Acquire URL from DHCP option 43 - Select to acquire the ACS URL from DHCP option 43.
Username	Enter the username required to connect to the ACS server.
Password	Enter the password required to connect to the ACS server.
	Client Settings
Protocol	Select Https if the connection is encrypted; otherwise select Http.
Client URL	Displays the URL of the client.
Port	In the event of port conflicts, change the port number of the CPE.
Username	Enter the username that the VigorACS will use to connect to the CPE.
Password	Enter the password that the VigorACS will use to connect to the CPE.
	Periodic Inform Settings
Enable Periodic Inform	Click to enable or disable the function. If enabled, the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field.
Inform Interval (sec.)	Set interval time or schedule time for the router to send notification to CPE.
	STUN Settings
Enable STUN	Click to enable or disable the function.
Server Address	Enter the IP address of the STUN server.
Server Port	Enter the port number of the STUN server.
Maximum Keep Alive Period	Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server.
Minimum Keep Alive Period	Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server.
	Advanced
Disable TR069 configuration change from CPE UI	Click to enable or disable the function.
	Apply Settings to APs
Enable	Click to enable or disable the function.
AP Password	Enter the password of the VigorAP that you want to apply Vigor router's TR-069 settings
Apply Specific STUN Settings to APs	Click to enable or disable the function of applying specific STUN settings to AP. If enabled, Enable AP STUN - Click to enable or disable the STUN server settings. Server Address - Enter the IP address of the STUN server.

	Server Port - Enter the port number of the STUN server.
	Maximum Keep Alive Period - Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server.
	Minimum Keep Alive Period - Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server.
	CPE Notification Settings
Enable	Click to enable or disable the function.
	If enabled, select the notification item(s) by clicking it. Vigor router will send the utilization status to VigorACS.
	Web Login
	Web Configuration
	High Availability
	• SSH Login
	SSH Command
Bandwidth Utilization	Enable - Click to enable or disable this function. To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in medium and high fields), a notification will be sent to VigorACS. After a long time observation, the administrator can determine if it is necessary to increase the bandwidth setting for that CPE or not. The default is disabled .
	Time Period – Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS.
	• Enable / WAN – Choose the WAN interface by clicking Enable for applying the bandwidth utilization notification mechanism.
	• Threshold Level – Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization.
	• Line Speed – Set the transmission rate and receiving rate for specified WAN interface.
Save	Save the current settings.

9.4.16.8 SysLog Settings

SysLog function is provided for users to monitor router.

- Configuration	2865ac_001DAA000000 / Configuration / Syste	em	
intenance	Enable		
ne Settings	Syslog Save to	Systog Server 🗌 USB Disk	
Imin Account	Maximum Syslog folder space	1	G8 ~
	Keep logging when Syslog folder is full (Overwrite		
MP Settings	oldest logs)		
analloweng	Router Name	DrayTek	
R069 Settings		- Conflict	
	Server IP Address		
all Nert	Destination Port	514	
nternal Service User List.	Mall Systog	0	
	Collect Syslog About	Prewall Log	
		VPN Log	
		User Access Log / Hotspot User Information	
		VIAN Log	
		Router/DSL Information	
		VIAN Log	

ltem	Description
Enable	Click to enable or disable the Syslog function.
Syslog Save to	Select Syslog Server and / or USB Disk.
Maximum Syslog folder space	Set a space (unit GB/MB) to store event logs.
Keep logging when Syslog folder is full	Click to enable or disable the function. If enabled, the action of overwriting the olderest logs or stopping logging will be executed.
Router Name	Display the name for this router.
Server IP Address	Enter the IP address of the Syslog server.
Destination Port	Enter a port for the Syslog protocol.
Mail Syslog	Click to enable or disable the function. If enabled, it will record the mail event on Syslog.
Collect Syslog About	Select the type of log to send the corresponding message to syslog.
Save	Save the current settings.

9.4.16.9 Mail Alert

This page allows to configure settings for Mail alert.

- Configuration	2865ac_001DAA000000 / Configu	ation / System	
laintenance Time Settings	Enable	Send A Test E-Mall	
	Interface	Any ~	
	SMTP Server		
MP Settings	SMTP Port	25	
nagement	Mail To		
069 Settings slog Settings	Sender Address		
	Connection Security	Planintext ~	
nel Control			
et Compilia	Force StartTLS - Stop # Star Authentication	In both 19 Junit 15 connection failed. 11 IS connection failed.	
E CLEMIN	Force Start11.5 : Stop If Sta	TTIS connection failed.	
	Force StartTLS - Step If Sta Authentication	TTIS connection failed.	
	Force StartTLS - Stop # Sta Authentication Username	rtTLS connection tabled.	
	Fore StartTLS is legit Sta Authentication Username User Password	ITTLS connection tabled.	
	Fore StartTLS is legit Sta Authentication Username User Password	rtTLS connection tabled.	

Item	Description
Enable	Click to enable or disable the mail alert function. Send Test E-Mail - Make a simple test for the e-mail address specified in this page.
Interface	Specify an interface.
SMTP Server	Enter an IP address of the SMTP server.
SMTP Port	Enter the port number of the SMTP server.
Mail To	Specify a mail address for receiving the mail.
Sender Address	Specify a mail address for sending mails out.
Connection Security	 Select a method (Plaintext, SSL, StartTLS or Force StartTLS) to ensure the connection security. SSL means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. Accept using plain text if StartTLS connection failed. Force StartTLS. Stop if StartTLS connection failed.
Authentication	Click to enable or disable the function. If enabled, the authentication will be activated while using an e-mail application.
Username	Enter the user name for authentication.
User Password	Enter the password for authentication.
Enable E-Mail Alert	Select the item(s) to send the alert message to the e-mail box while the router detecting the item(s) you specify here.
Save	Save the current settings.

9.4.16.10 Internal Service User List

This page allows you to turn on or turn off security authentication service (offered by internal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.

← Canliguration	2865ac_001D	AA000000 / Configuration /	System		
Maintenance	Internal S	ervice User List			
lime Settings	Username		Nothing selected ~		
Imin Account	Internal Ser	vices RADIUS			
04P Settings	Internal Ser	vices Locat8021 X			
anagement					
				Apply	
069 Settings					
	Note:	nly the user profiles which is enable	d in User Management == User Profile will be isled here.		
- stog Settings	+ 1.0			sdy, however, you may change its authentication methods via User Management >>: User Pr	ofile.
- eslog Settings all Mert	+ 1.0			ods, however, you may change its authentication methods via User Management 2-2 User Pr	ofile.
nl og Settings all Alert torinal Sierither Ober 134	+ 1.0			nds, however, you may change its authentication methods via User Management 2-2 User Pr	ofile.
nl og Settings all Alert torinal Sierither Ober 134	+ 1.0			ods, however, you may change its authvestication methods via User Management 2-2 User Pr biternal Services Localit221 X	ofile.
1889 Settings Luil Alert Luil Alert Liternal Set Hop Clart Lid anei Control	- 1.0 - 2.8	you enable NADIUS or Local 802.1X	for a user profile here, it will use the default authentication meth		offie.

These parameters are explained as follows:

ltem	Description
Username	Display the name of the existed user profile.
Internal Services RADIUS	Click to enable (turn on) or disable (turn off) the security authentication service offered by the internal RADIUS server for the user profile.
Internal Services Local802.1X	Click to enable (turn on) or disable (turn off) the security authentication service offered by the Local 802.1X server for the user profile.
Apply	Save the current settings.

9.4.16.11 Panel Control

This page allows you to customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

figuration	2865ac_001DAA000000 / Configu	nuovii / System				
	LED					
ettings						
	Enable LED					
	Enable Sleep Mode	D				
Settings	Turn off LED after (Minutes)	1				
	Button					
Settings	Button					
g Settings	Wireless					
	Factory Reset	•				
	Note:	10.00	actory Reset Button" on the front panel as below: LED On	LED Off		
	Note: Enable the Sleep Mode will make the fu	nctions of "Wireless Button" and "Fa	LED On Wireless On/Off/WPS	LED Off	7	
	Note: Enable the Sieep Mode will make the fu LED Status	nctions of "Wireless Button" and "Fa	LED On		7	
	Note: Enable the Steep Mode will make the fu LED Status Wireless Button	nctions of "Wireless Button" and "Fa	LED On Wreless On/Off/WPS and: Turn LED off Immediately*	LED Off		
	Note: Enable the Steep Mode will make the fu LED Status Wireless Button Factory Reset Button	nctions of "Wireless Button" and "Fa	LED On Wreless On/Off/WPS and: Turn LED off Immediately*	LED Off		
	Note: Erable the Sleep Mode will make the fur UED Status Wreekss Button Factory Reset Button *Soll functional even the buttons are die	nctions of "Wireless Button" and "Fa	LED On Wreless On/Off/WPS and: Turn LED off Immediately*	LED Off		
	Note: Enable the Skep Mode will make the fu LED Status Wreless Button Factory Reset Button "Still functional even the buttons are db USB	nctions of "Wireless Button" and "Fa	LED On Wreless On,/Off,WPS Grant Turn LED off Immediately" ACT light flashing: Reset router	LED Off		
	Note: Enable the Skep Mode will make the fu LED Status Writeless Button Factory Reset Button *Still functional even the buttons are db USB Index	Inctions of "Wireless Button" and "Fa	LED On Wheles OnyOKIVPS and Turn LED off Immediately" ACT light flashing: Beset router Status	LED Off		
	Note: Enable the Skep Mode will make the fur UED Status Writess Button Factory Reset Button *Still functional even the buttons are db USB Intex 1	nctions of "Wireless Button" and "Fi	LED On Wreless ChyO(MPPS and Turn LED Off Immediately" ACT light flashing: Besiet router Status No Device	LED Off		

ltem	Description
	LED
Enable LED	Click to enable or disable the LEDs to function according to the configured settings.
Enable Sleep Mode	Click to enable (turn on) or disable (turn off) the LEDs after the specified number of minutes has elapsed.
Turn off LED after (Minutes)	Enter a number.
	Button
Wireless	Click to enable or disable the ability of the Wireless button to control WLAN and WPS functions.
Factory Reset	Click to enable or disable the reset function of the factory reset button.
	USB
Enable	Click to enable or disable the USB port.
	LAN Port
Enable	Click to enable or disable the LAN port.
Status	Displays the status of the USB port.
Speed	Displays the negotiated speed of the LAN port.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.17 Switch

9.4.17.1 Status

It displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch **connected to** Vigor router.

Switch Status

Status Switch Hierarchy Status IP Address MAC Address Model System Up Time Group Switch Name IP Address Model System Up Time No data available No data available No data available No data available	Port In Use Clients	Firmware Version
Group Switch Name IP Address MAC Address Model System Up Time No data available No Address No <th>Port In Use Clients</th> <th>Firmware Version</th>	Port In Use Clients	Firmware Version
No data available New Switch List +Add Device	Port In Use Clients	Firmware Version
No data available New Switch List -+Add Denice	Port In Use Clients	Firmware Version
New Switch List +Add Device		
+Add Device		
+Add Device		
+hdd Devce		
Index Switch Name IP Address MAC Address		
	Model	Firmware Version
□ 1 G2280 ● 192.168.1.10 00:1D:AA:22:80:AA	G2280	2.5.1_RC5
2 P2500	P2500	2.6.0_RC1

modify the group settings if required. Switch Name - Displays the name link of VigorSwitch. You can click to name link to access into the switch profile. IP Address - Displays the IP address of VigorSwitch. MAC Address - Displays the IP address of VigorSwitch. Model - Displays the model name of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this Vigorwith powered up. Port in Use - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under curr used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status.	tem	Description	<u>ו</u>						
New Switch List The one under New Switch List is allowed to be managed under currused group. • Add ress - Displays the selected VigorSwitch. You can click in name link to access into the switch profile. IP Address - Displays the ime accumulated since this VigorSwitch. Model - Displays the model name of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch. Lients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the firmware version that VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch. Clients - Displays the selected VigorSwitch to be managed under currused group. • Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status.	tatus	Displays the	e switch which is	s managed by V	'iogr router.				
Switch Name - Displays the name link of VigorSwitch. You can click in name link to access into the switch profile. IP Address - Displays the IP address of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorWitpowered up. Port in Use - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. Vew Switch List The one under New Switch List is allowed to be managed under currus degroup. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Setter Head Status New Switch List Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Select a switch list were Switch List on the selected Sylop Orthone Status. Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Were Switch List Here Switch List He		Group - Displays the name link of the group. You can click the link to							
name link to access into the switch profile. IP Address - Displays the IP address of VigorSwitch. MAC Address - Displays the MAC address of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorWitpowered up. Port in Use - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Clients - Displays the firmware version that VigorSwitch current used. The one under New Switch List is allowed to be managed under curr used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Select a switch from New Switch List of Ordew2280aa 0.220 Were Switch List									
IP Address - Displays the IP address of VigorSwitch. MAC Address - Displays the MAC address of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorSwitch. Clients - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch. Clients - Displays the selected VigorSwitch to be managed under currused group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Setter State Setter Name Version - Displays the reactive Version - Displays the firmware version that VigorSwitch current used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Version - Displays the setter VigorSwitch to be managed by Vigor router and be shown under Status. Setter State Setter State Version - Displays the setter VigorSwitch to be managed by Vigor - Displays the setter VigorSwitch List - Displays - Displays the setter VigorSwitch - Displays - Di					-	'ou can click	the		
MAC Address - Displays the MAC address of VigorSwitch. Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorSwitch. Clients - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under currus used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Setter States Setter New Witch List Setter New Witch List and Click +Add Device. Then, the selected switch will be moved and displayed under Status. Setter States Setter New Switch List and Click +Add Device. Then, the selected switch will be moved and displayed under Status.									
Model - Displays the model name of VigorSwitch. System Up Time - Displays the time accumulated since this VigorWitpowered up. Port in Use - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under currused group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Switch List Switch State Switch Ust Herr Switch List Switch State Switch Herrdry Switch State Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch State Switch Herrdry State Switch Herrdry Switch State Switch Herrdry Switch State Switch Herrdry Switch State Switch Herrdry Switch State Switch Herrdry				-					
System Up Time - Displays the time accumulated since this Vigorwit powered up. Port in Use - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under curr used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Settin State Settin State We switch List Settin State					-	h.			
powered up. Port in Use - Displays how many devices connected to VigorSwitch. Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under curr used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Setter States Setter States New Switch List Setter States Setter States<				_					
Clients - Displays the number of LAN ports used in VigorSwitch. Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under currus used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Switch States Switch List Switch List Switch Name Padews Mac Address New Switch List Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Select a switch Hierardy Switch Hie				s the time accur	nulated since	this Vigorwi	tch is		
Firmware Version - Displays the firmware version that VigorSwitch current used. New Switch List The one under New Switch List is allowed to be managed under currus used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Switch Herachy Switch Herachy Switch Herachy Switch Herachy New Switch List Select a switch Name P Address Mac Address No data workble Select a switch from New Switch List and click +Add Device. T		Port in Use	- Displays how	many devices o	onnected to	VigorSwitch.			
current used. New Switch List The one under New Switch List is allowed to be managed under currused group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Settich Status Setti		Clients - Dis	splays the numl	ber of LAN port	s used in Vigo	orSwitch.			
New Switch List The one under New Switch List is allowed to be managed under curr used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status. Switch Herardly Switch List +Add Device 1 02200 1 022100.110 1 02200 1 022100.110 001DAA2220AA Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch Herardly Status Switch List Herardly Status Switch List Switch List Herardly Status Switch List Herardly Status Switch List Herardly Status Switch Status Switch List Herardly Status Switch List Herardly Status Switch List Switch Status Switch Status Switch List Switch Status Switch List Switch Status Switch Status Switch List Switch Status Switch List Switch Status Switch Status Swi		Firmware \	/ersion - Displa	ys the firmware	e version that	VigorSwitch			
used group. +Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status.		current use	d.						
router and be shown under Status.	lew Switch List			List is allowed	to be manage	ed under cur	rent		
Switch Status Switch Hierarchy Status No deta available Foodsta available No deta available New Switch List No deta available Index Switch Name IP Address MAC Address MAC Address MAC Address Index Switch Name IP Address MAC Address Index Switch Name IP Address MAC Address Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22:80-aa G2280 IP Address Model Vex Switch List Switch Name IP Address MAC Address Model Intervently Status Switch Name IP Address Model IP Address Model Default G2280 192.168.1.10 00-1d-aa-22:80-aa G2280 IP Address IP Address <t< td=""><td></td><td>+Add Devic</td><td>e - Make the se</td><td>elected VigorSwi</td><td>tch to be mai</td><td>naged by Vig</td><td>or</td></t<>		+Add Devic	e - Make the se	elected VigorSwi	tch to be mai	naged by Vig	or		
Status MAC Address Model System New Switch List Hoddress MAC Address MAC Address MAC Address MAC Address MAC Address I G2280 192:168.1:10 colspan="2">colspan="2">Colspan="2" Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Hierarchy Switch Status Switch Name IP Address Model Default G2280 IP2:168.1:10 Colspan="2" New Switch List MAC Address Model Default G2280 IP2:168.1:10 Colspan="2" New Switch List Model Default G2280 New Switch List Model New Switch List		router and	be shown unde	r Status.					
Group Switch Name IP Address MAC Address Model System New Switch List		Switch Status	Switch Hierarchy						
New Switch List +Add Device 1 G2280 2 P2500 • 192.168.1.10 00:1D:AA-22:80:AA 0 2 2 P2500 • 192.168.1.12 00:1D:AA-42:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Name Image: Switch Name IP Address MAC Address Model Default G2280 Image: Switch List Model Image: Switch List Mac Address Mace Image: Switch List Image: Switch List Mace Image: Switch List Image: Switch List <		Status							
New Switch List +Add Device 1 G2280 2 P2500 192.168.1.10 00:1D:AA-42:280:AA 2 P2500 92.168.1.12 00:1D:AA-42:280:AA Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Hierarchy Status Switch Name Image: Switch List MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22:80-aa G2280 New Switch List Mac Address Mace Head Device		Group	Switch Name	IP Address MA	C Address Mod	el Syste	ım Up Time		
New Switch List Index Switch Name IP Address MAC Address I G2280 0:192.168.1.10 00:1D:AA.22.80:AA I G2280 0:192.168.1.12 00:1D:AA.4C:18.83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Status Switch Hierarchy Switch Hierarchy Status Switch Name IP Address Model Default G2280 192.168.1.10 00-1d-aa-22:80-aa G2280 New Switch List - - - -					N		-		
+Add Device Index Switch Name IP Address MAC Address I G2280 192.168.1.10 00:1D:AA:22:80:AA I 2 P2500 192.168.1.12 00:1D:AA:4C:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Image: Switch Status Switch Status Switch Status Switch Hierarchy Image: Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00:1d:aa:22:80:aa G2280 New Switch List Image: Switch List Image: Switch List Image: Switch List						o data avaliable			
+Add Device Index Switch Name IP Address MAC Address I G2280 192.168.1.10 00:1D:AA:22:80:AA I 2 P2500 192.168.1.12 00:1D:AA:4C:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Image: Switch Status Switch Status Switch Status Switch Hierarchy Image: Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00:1d:aa:22:80:aa G2280 New Switch List Image: Switch List Image: Switch List Image: Switch List									
Index Switch Name IP Address MAC Address 1 G2280 192.168.1.10 00:1D:AA:22:80:AA 2 P2500 192.168.1.12 00:1D:AA:42:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Hierarchy Status IP Address Mac Address Model Default G2280 192.168.1.10 00-1d-aa-22-80-aa G2280 New Switch List		New Switch List							
I G2280 192.168.1.10 00:1D:AA:22:80:AA I 2 P2500 192.168.1.12 00:1D:AA:4C:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Image: Comparison of the selected switch Hierarchy Status Switch Status Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22:40-aa G2280 New Switch List		+Add Device							
2 P2500 192.168.1.12 00:1D:AA:4C:18:83 Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Status Switch Hierarchy Status Default G2280 New Switch List New Switch List New Switch List Head Device		In	dex Switch Name	IP Address		MAC Address			
Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status. Switch Status Switch Hierarchy Status Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22-80-aa G2280 New Switch List		2 1	G2280	• 192.168.	1.10	00:1D:AA:22:80:AA			
Switch Status Switch Hierarchy Status Switch Name Group Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22-80-aa G2280		□ 2	P2500	• 192.168.	1.12	00:1D:AA:4C:18:83			
Group Switch Name IP Address MAC Address Model Default G2280 192.168.1.10 00-1d-aa-22-80-aa G2280 New Switch List		selected sw	itch will be mov				e		
Default G2280 192.168.1.10 00-1d-aa-22-80-aa G2280 New Switch List		Status							
New Switch List +Add Device		Group	Switch Name	IP Address	MAC Address	Model	Sys		
+Add Device		Default	G2280	• 192.168.1.10	00-1d-aa-22-80-aa	G2280	0:5		
+Add Device									
		New Switch List							
Index Switch Name IP Address MAC Address		+Add Device							
		1	ndex Switch Name	IP Ad	dress	MAC Address			
□ 1 P2500 ●192.168.1.12 00:1D:AA:4C			P2500	• 19	2.168.1.12	00:1D:AA:40	:18:83		

	Switch - Displays the name of the device.
	IP Address - Displays the IP address of the device.
	MAC Address - Displays the MAC address of the device.
	Model - Displays the model name of VigorSwitch.
	Firmware Version - Displays the firmware version that VigorSwitch current used.
Search	Click to search Vigor switch.

Switch Hierarchy

This page displays the hierarchy of VigorSwitch(es) managed under Vigor router.

/ Configuration / Switch	C
Switch Status Switch Hierarchy	
PI	
VigorSwitch G2280 10 102 164 1.10 G2280	
P2	
P3	
P4	
P5	

9.4.17.2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor router. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.

Status			/ Configuratio	n / Switch			
Profile	Profile l	List					
Alert And Log							
Database Setup		Index	Name	Group	IP Address	MAC Address	Model
Group		1	G2280	Default	• 192.168.1.10	00-1d-aa-22-80-aa	G2280
Maintenance							
	New Sw	vitch List					
	+Add De	evice					
		Index	Switch Name	IP Address	MAC Address	Model	Firmware Version
		1	P2500	• 192.168.1.12	00:1D:AA:4C:18:83	P2500	2.6.0_RC1

ltem	Description
	Profile List
Delete	Click to remove the selected entry from the profile list.
Check box	Click to select the device.
Index	Displays the index number of the switch profile.
Name	Displays the name of the switch profile.
Group	Displays the group name of VigorSwitch(es).
IP Address	Displays the IP address of VigorSwitch.
MAC Address	Displays the MAC address of VigorSwitch.

Displays the model name of VigorSwitch.
New Switch List
Make the selected VigorSwitch to be managed by Vigor router and be shown under Profile List.
Displays the index number of the switch device.
Displays the name of the switch.
Displays the IP address of VigorSwitch.
Displays the MAC address of VigorSwitch.
Displays the model name of VigorSwitch.
Displays the firmware version that VigorSwitch current used.

To edit profile for the selected switch:

1. Selecting one device from the Profile List. Click on the entry to open the following page.

Switch Profile 1 : G2280		
General VLAN Port		
Index	1	
Switch Name	G2280	
Comment		
Trap Community Name		
Enable Copy configuration	\bigcirc	
Copy configuration from	None •	
Login Password	©	
IP Address	DHCP 192.168.1.10	
Set General to Factory Default		
U secondence record pendic		Cancel Save Sen

ltem	Description
Index	Displays the index number of the switch profile.
Switch Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Comment	Enter the text in such field if additional explanation for the switch is required.
Trap Community Name	Enter the text in such field as trap community.
Enable Copy configuration	Click to enable or disable the function.
Copy configuration	Check the box to copy configuration from other device. Use the drop down list to choose the one you need.
from	Note, if there is only one VigorSwitch connected and managed by Vigor router, then such field is unavailable.
Login Password	Displays the original login password for the VigorSwitch.

IP Address	Display the dynamic IP address (of the connected switch) assigned by Vigor router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.
Send to Device	Transfers the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately.

2. After finished the settings, click **VLAN** tab to open following page.

Blank page due to LAN>>VLAN not configured previously:

Switch Pro Genera Router VL	il -	: G22 VLAN		Po	rt																												
Group	Su	bnet	v	D	P	riority		P1		P2		P3		P4		P5		SSID1		SSID2		SSID	3	SSID4		SSID1	5G	SSID	2 5G	SSID3	5G	SSID4 5	iG
															N	o data	a availa	able															
External S	Switch	VIAN	- Por	t Mer	nbers																												
	1	2	3	4	5	6	7	8		9	10	11	12	13	1	4	15	16	17	18	1	9	20	21	22	2	3	24	25	26	27	2	8
															N	o data	availa	able															
8 No	te: Th	e rout	er co	nfigu	ration	i will b	be up	dateo	d wh	en ge	tting	profile	settin	gs fron	n exte	rnal s	switch	n.															
🔊 Set Vlan ti	o Facto	ry Defa	ult																								Ca	ncel	Sav	re	Send	to Devi	ce

Setting page with LAN>>VLAN configured previously:

Group	Subne	t	VID	Pri	iority	P1		P2	P3		P4		P5	SSI	D1	SSID2	2	SSID3	s	SID4	SSID	1 5G	SSID2	G	SSID3 5G	SSI	D4 5G
VLAN0	LAN1		0	0								(2							1							
VLAN1	LAN2		10	0							\boxtimes							\boxtimes		1						\boxtimes	
VLAN2	LAN3		20	0							\boxtimes					\boxtimes		\boxtimes	0	1	\boxtimes		\boxtimes			\boxtimes	
ternal Swi	itch Vl	AN - P 2	ort Me 3	mbers 4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
					5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
dan0 [0]	1	2	3	4																							27

General VLAN Port	-			
ort Description	Port Control	Schedule	Ingress Rate (Kbps)	Engress Rate (Kbps)
,	Enable Port	•	•	0
	Enable Port	· 0	•	0
	Enable Port	• 0 . 0		•
Uplink	Enable Port	· 0	0	0
	Enable Port	▼ 0 , 0	0	0
;	Disable Port	• 0 . 0	0	0
j	By Schedule	• 0 , 0	0	0
,	Enable Port	• 0 , 0	0	0
3	Enable Port	• 0 , 0	0	0
	Enable Port	• 0 , 0	0	0
0	Enable Port	• 0 . 0		

3. Click **Save** to save VLAN configuration. Then, click **Port** tab to access the following page:

These parameters are explained as follows:

ltem	Description
Description	If required, enter a brief description to explain the device connected to VigorSwitch via the LAN port.
Port Control	Disable Port – The port (e.g., Port 3 in this case) which is used to connect VigorSwitch and Vigor router will not be shutdown by Vigor router.
	Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Save, the network connection between that device and VigorSwitch will be terminated.
	By Schedule – Two schedule profiles can be specified here to force Vigor router executing specific action to VigorSwitch.
Ingress Rate	Check the box for entering the ingress rate for the selected VigorSwitch. After clicking Save , the value modified in this page will be written to VigorSwitch and enabled.
Egress Rate	Check the box for entering the egress rate for the selected VigorSwitch. After clicking Save , the value modified in this page will be written to VigorSwitch and enabled.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.
Send to Device	Transfers the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately.

4. Click **Save** to save the changes and then click **Send to Device**. Settings will be sent to VigorSwitch immediately.

9.4.17.3 Alert And Log

Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly.

Alert Setup

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

tatus	Enab	le Alert and L	og C)						
vofile										
	Alert	Levels an	d Action							
Switch and Port Setup	Index	Enable	Level Name	Color	Create Log	Send Notification	Object 1	Object 2	Object 3	Object 4
NetLogs	1	2	No Alert	No Color	No Log	No Notification				
latabase Setup	2		Minor Alert	000	Enable	No Notification				
	3		Moderate Alert	000	2		sms 1-Local nu $ \sim$	sms 1-Local nu 🗸	sms 1-Local nu \circ	sms 1-Local nu
aintenance	4	8	Major Alert	000	-		sms 1-Local nu $ \sim $	sms 1-Local nu $ arsigma$	sms 1-Local nu ${\sim}$	sms 1-Local nu
	5			000			sms 1-Local nu ~	sms 1-Local nu 👻	sms 1-Local nu ~	sms 1-Local nu
	6			000			sms 1-Local nu 🗸	sms 1-Local nu 🗸	sms 1-Local nu ~	sms 1-Local nu
	7			000			sms 1-Local nu 👻	sms 1-Local nu 🛩	sms 1-Local nu ~	sms 1-Local nu
	4			000			sms 1-Local nu \sim	sms 1-Local nu \sim	sms 1-Local nu \sim	sms 1-Local nu

ltem	Description
Enable Alert and Log	Click to enable or disable the function.
	Enable Altert and Log
	Index Enable Level Name Color Create Log Send Notification Object 1 Object 3 Object 3 Object 4
	1 D His Alert No Color No Log No Nonfluation
	2 D Mour Net O Enable No Notification
	3 👩 Moderante Alexit 🦉 🤕 🖉 🚳 🔅 annu 1-777 • annu 1-777 • annu 1-777 •
	< □ Major Alent 22 12 0 □ 1010 1-777 • 1010 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7770 1-7700 1-7700 1-7700 1-7700 1-77
	Alert Levels and Action
Index	Displays the index number of alert profile.
Enable	Check it to enable this feature.
Level Name	Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined.
Color	Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed.
Create Log	Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default.
Send Notification	If it is checked, Vigor router's system will send notification to specified phone number via SMS.
Object 1 ~ 4	Select the SMS object which will get the SMS from Vigor router. Up to 4 objects can be selected at one time.

Switch and Port Setup

This page defines enabling switch alert and/or port alert for each switch.

Status		-	Configur	ation / Switch				
	Index	Switch Name		IP Address	Model	Switch Alert	Port	Alert
	1	G2280		192.168.1.10	G2280	Enable	Enal	ble
Maintenance								

ltem	Description
Index	Displays the index number of the alert profile for switch(es).
Switch Name	Displays the name of the switch.
IP Address	Displays the IP address of the switch.
Model	Displays the model name of the switch.
Switch Alert	Displays the switch alert status.
Port Alert	Displays the port alert status.

To configure the switch alert settings, move the mouse cursor to any entry and click to open the setting page.

Index	1			
Switch Name	G2280			
IP Address	192.168.1.10			
Model	G2280			
Switch Alert	Enable Disable			
Port Alert	Enable Disable			
Cold Start	4-Major Alert	•		
Warm Start	4-Major Alert	•		
Disconnect	4-Major Alert	•		
Reconnect	2-Minor Alert	•		
Port Alert				
Port Description	Device Disconnects	Device Reconnects	Schedule On/Off	Shutdown En/Dis
1	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻

ltem	Description		
Index	Displays the index number of the alert profile for switch(es).		
Switch Name	Displays the name of the switch.		
IP Address	Displays the IP address of the switch.		
Model	Displays the model name of the switch.		
Switch Alert	Enable - Click to enable the switch alert function.		
	Cold Start, Warm Start, Disconnect, Reconnect - When VigorSwitch encounters the alert events, alert mechanism will perform corresponding actions based on the servity level of the incident encountererd. Specify the severity level (Minor, Major, or No) for each incident.		

	Disable - Click to disable the switch alert function.	
Port Alert	Enable - Click to enable the port alert function.	
	Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this page. Each port can be confgiured with different alert level for diffent alert event.	
	Disable - Click to disable the port alert function.	
Port Alert table	Port – Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this table. Each port can be confgiured with different alert level for different alert event.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

Alert Logs

The system administrator can get the information by filtering the collective information based on the conditions specified in this page.

Status	/ Configuration / S	vitch		Ø
Profile	Select Columns to Filter Logs		~	
Alert And Log	Level			
Alert Setup	Туре	Switch Alert Port Alert		
Switch and Port Setup	Switch			
Database Setup		•		
Group	Time Period	Last 24 Hours Last 7 Days		
Maintenance			Appły	
	Alert Logs			
	() Logs			KI < 1 /0 > N
	Index 41 Level Name 41 Time	å↑ Type å↑ Switch	J↑ Port J↑ I	incident 41
		No data available		

These parameters are explained as follows:

ltem	Description	
Select Columns to Filter Logs	Level – The alert can be divided into several levels, Minor Alert, Moderate Alert and Major Alert. Check the one(s) you want to check in Alert Logs list.	
	Type – Select the type (switch / port) of the log to be displayed in Alert Logs list.	
	Switch – Switch(es) connecting to Vigor router will be shown in this area. Select the one you need.	
	Time Period - Select Last 24 Hours or Last 7 Days as time period.	
	Apply – Click to save the configuration.	
	Log related to the items selected above will be shown in Alert Logs list.	
Alert Logs	This area displays logs (level name, time, type, switch, port, and incident) related to VigorSwitch managed by Vigor router.	

9.4.17.4 Database Setup

The database of the switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of the switch.

← Configuration	2865ac_001DAA000000 / Configuration / Switch			
Status	Enable Database to Record alert logs and traffic history	•		
Profile	insury			
Nert And Log	File Path	No USB Disk Detected		
	Database Usage	N/A		
	Notification	Send notification	1921 - 1921 - 1922 - 19	
	Email Notification Object	1-Mail_Notify	Ψ.	
	SMS Notification Object	1-Local number	(e)	
	Action	Stop recording user information	w	
		Stop recording user information Backup and clean up all user info, and		

ltem	Description
Enable Database to	Click to enable or disable the function.
Record alert logs and traffic history	If enabled, it will make the database (in USB disk) record the alert logs and traffic history.
File Path	Displays the file path for storing the logs.
Database Usage	Displays the used capacity.
Notification	Send notification - A notification will be sent out when there is no capacity for storage in USB.
	• Email Notification Object - Choose an email notification object profile.
	• SMS Notification Object - Choose a SMS notification object profile.
	Don't send notification - No notification will be sent out when there is no capacity for storage in USB.
Action	Choose an action.
	Backup and clean up all user info, and start a new record - Only the newest events will be recorded by the system.
	Stop recording user information - When the capacity of log is full, the system will stop recording.
Save	Save the current settings.

9.4.17.5 Group

Different switches can be classified into different group(s). There are ten switch groups available for configuration.

← Configuration	2865ac_001DAA000000 / Configuration / Switch		C
	Index Group Name	Member Switch	
	1 Default		
Profile	2		
Nert And Log	3		
Database Setup	1		
	5		
	7		
Maintenance	8		
	9		
	10		

To configure the group settings, move the mouse cursor to any entry and click to open the following page.

2865ac_001DAA000000 / Configuration / Switc	h	C
Index	1	
Profile Name	Default	
Enable Group Password		
Group Password	•	
Member Switch		
		Cancel Save

ltem	Description	
Index	Displays the index number of the profile.	
Profile Name	Enter a name as the group name.	
Enable Group Password	Click to enable or disable the group password.	
Group Password	Enter a password that the system administrator can use to access into the managed VigorSwitch connecting to Vigor router.	
Member Switch	Choose the switches you want to group.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.17.6 Maintenance

This page is able to execute configuration backup, restore, reboot or reset the VigorSwitch devices remotely.

	2865ac_001DAA000000 / Configuration / S	65ac_001DAA000000 / Configuration / Switch			С
Status Profile Alert And Log	Action Type Select Device	Contig Backup	•		
Database Setap Group Virinterment	Switch Name	MAC 00-1d-aa-22-80-aa	8P 192.168.1.10	Download Config	
					Sive

ltem	Description	
Action type	Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor router to perform on VigorSwitch.	
	Config Backup - Perform the configuration backup.	
	Config Restore - Perform the configuration restoration.	
	• Restore Config From - Select Local File or Shared Folder.	
	• File/Path - Click Browse to locate a file.	
	Remote Reboot - Reboot the VigorSwitch devices remotely.	
	Factory Reset - Reset the VigorSwitch devices with factory default settings.	

Select Device		
Switch NameDisplays the name of the switch.		
МАС	Displays the MAC address of the switch.	
IP	Displays the IP address of the switch.	
Download Config	Click to download the configuration file and store on the host.	
Save	Save the current settings.	

9.4.18 Advanced

9.4.18.1 Parameter Tree

All control parameters of the selected CPE will be presented on this page with a tree view that is convenient for the administrator/user to view and select.

- Configuration	2865ac_001DAA000000 / Configuration / Advanced		e
Farameter Tree	Name	Value	DataType
Facture Parameters	🖌 🐼 InternetGatewayDevice.		
	UANDeviceNumberOfEntries	9	
	WANDeviceNumberOfEntries	6	
	p 🐼 DeviceInfo.		
) 🔉 ManagementServer.		
	þ 🐼 Time.		
	þ 💿 Layer3Forwarding,		
	p @ LANDevice.		
	p 💿 WANDevice.		
	p @ X_00507F_InternetAcc.		
	p 🐼 X_00507F_LANL		
	C X_00507F_LoadBalanceFolicyNumberOfEntries	6	
	b Q X 00507F_LoadBalancePolicy.		
	b ⊗ X_00507F_NAT.		
	p ⊗ X_00507F_Freewall.		
	b ⊗ X_00507F_Applications.		
	b ⊗ X_00507F_VPN.		
	b ⊗ X_00507F_WirelessLAN.		
	1. 🔿 ¥ 1058775 Section		
			10 Save

ltem	Description
Name	Lists the name of the parameter.
Value	Displays the setting value (true/false, numbers, selections and etc.) of the selected parameter. Sometime, It might be null.
DataType	It means the data type (e.g., string, boolean or unsignedInt) of the parameter. However, the corresponding information will be displayed in this field only if the parameter allowed to be written.
Сору	Copy the selected parameter with the value. The copied parameter can be added onto the XML template downloaded from Provisioning>>Global Parameters. After that, the completed XML template can be saved as a sampling profile which will be selected and applied to Provisioning>>Global Parameters.
Save	Save the change.

9.4.18.2 Exclude Parameter

The firmware version of the managed CPE might be different from the data stored on VigorACS database. Therefore VigorACS will compare the available parameters of the selected CPE with the one stored in the VigorACS database automatically. When some of the parameters not supported by the CPE, those parameters will be listed on this page.

< Configuration	2865ac_001DAA000000 / Configuration / Advanced	(
Pacameter Tree	II Delute All	
	Parameter	
	InternetGatewayDevice.X_00507F_LTELTEGP5.GP5Position1.ongitude	
	InternetGatewayDevice.X_00507F_LTE.ITEGPS.GPSPosition.Latitude	
	InternetGatewayDevice_X_00507F_InternetAcc.MultiPVCs.GeneraL(x).WAN.(y).	
	InternetGatewayDevice.X_00507F_InternetAcc.WAN.(x).InternetPhysicalType	
	InternetGatewayDevice.X_00507F_Firewall.DoSDefense.BlackWhiteList.WhiteListNumberDIEntries	
	InternetGatewayDevice X. 00507F_FinewalLDoSDefense.BlackWhiteList.BlackListNumberOfEntries	
	InternetGabewayDevice X, 00507F_Finewall.Do5Defense.BlackWhiteList.WhiteListv5NumberOfEntries	
	InternetGatewayDevice.X_00507F_Firewall.DoSDefense.BlackWhiteList.BlackListvSNumberOrEntries	
	InternetGatewayDevice,X_00507F_WirelessLANLWDS.WDSMode	
	InternetGatewayDevice.X 00507F Status.MultIVLANWANNumberOfEntries	
	InternetGatewayDevice.X_00507F_InternetAcc.WAN.(x).MTU	
	InternetGatewayDevice.X_00507F_System.SyslogMail.SysLogAccess.Calllog	
	InternetGatewayDevice.X_00507F_System.SystogMail.SysLogAccess.AlertLogEnable	
	InternetGatewayDevice.X_00507F_System.SystogMail.SysLogAccess.AtertLogPort	
	InternetGatewayDevice.X_00507F_Operation_Mode_AP	
	InternetGatewayDevice.X_00507F_Status.CPUTemperature	
	InternetGatewayDevice X. 00507F_WirelessLAN_AP.General.AvailableChannets	
	InternetGatewayDevice.X_00507F_WirelessLAN_5G_AP.General.AvailableChannels	
	InternetGatewayDevice.X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	
	InternetGatewayDevice.X_00507F_Status.Wireless.	
	InternetGatewayDevice.X_00507F_Status.Wireless_5G.	
	InternetGatewayDevice.X_00507F_WhrelessLAN_SG.General.TxBurst	
	InternetGatewayDevice.X_00507F_WhrelessLAN.General.LongPreamble	
	InternetGatewayDevice X, 00507F_US8Application.DeviceStatus.Modem.(x).SignalStrength	
	Information Providence V ANZATE Ultractional ALL Constant PETR 1-2 Trade-Part	

ltem	Description
Delete All	Click to remove all parameters listed in this page.