VigorACS3

Unified Management System



V1.5

VigorACS 3

Unified Management System User's Guide

Manual Version: V1.5 Date: September 2, 2024 Software Version: V3.6.1 © 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	
	1.2 System Architecture	
	1.3 Web Service	3
	Chapter 2 Install & Startup	5
	2.1 Platform for Windows 10	F
	2.1.1 Installation for Java	
	2.1.2 Installation for MariaDB	
	2.1.3 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	33
	2.2.5 Start VigorACS Chatbot	35
	2.2.6 Edit VigorACS IP	36
	2.3 Registering VigorACS	
	2.3.1 Registration for VigorACS via Windows Platform	
	2.3.2 Troubleshooting for Unstable CPE Status	42
	Chapter 3 Getting Started	46
	3.1 Accessing Web Page of VigorACS	
	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	
	3.2.4 Meru Bar	
	3.2.6 Capture Packets	
	3.2.7 Set Password, Two-factor Authentication, Manage Notification, 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.2 How to Create a New Network?	
	A.3 How to Assign a New Added CPE to a Network?	74
	A.4 How to Create a New User Group?	75
Part II		77
	Chapter 4 SD-WAN Solution	78
	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 Network Group	
	4.4.2 VPN (SD-WAN)	
	4.4.2 VFN (3D-WAN)	
	4.4.4 Data Usage (SD-WAN)	
	Chapter 5 SD-WAN CPE	97

	5.1 Dashboard for SD-WAN CPE	
	5.2 Statistics for SD-WAN CPE	
	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	
	ter 6 System Menu	
Chapt	-	
	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 Legacy Report Tasks (Deprecated) 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 & Service Management	
	6.4.1 Network Management	
	6.4.2 Service Management	
	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 Storage Management	
	6.5.6 Upload Serial Number	
	6.5.7 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	
	6.5.16 App Server	
	6.5.17 License Key Pools 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	

6.6.10 Notifications & Events	
6.6.11 Syslog Server	
6.6.12 Group Parameter	
6.6.13 Link with Router App	
6.7 About VigorACS	
6.7.1 Software Information	
6.7.2 License Information	
6.7.3 License Mail Notify	
6.7.4 License Agreements	
6.7.5 System Resource Notify	
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	284
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 Configuration	
7.3.1 VPN Wizard	
7.3.2 AP Profile	
Chapter 8 Network Group Menu	
8.1 Dashboard for the Network Group	200
· ·	
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 Wizard	
8.4.2 AP Profile	
8.4.3 Load Balance	
8.4.4 Route Policy	
8.4.5 Link Health Check	
8.4.6 Interface Settings	
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 PIN Generator	
8.5.5 Analytics	
Applications	
A.1 How to apply an AP profile to AP device(s)?	
Part V	351
Chapter 9 Device Menu	253
9.1 Dashboard for CPE	

9.2 Statistics for CPE	
9.3 Monitoring	
9.3.1 Alarm	
9.3.2 Logs	
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	
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	
9.4.12 VPN	
9.4.13 Mesh	
9.4.14 Wireless LAN	
9.4.15 Bandwidth Management	
9.4.16 USB Applications.	
9.4.17 System	
9.4.18 Switch	
9.5 Advanced	
9.5.1 Parameter Tree	
9.5.2 Exclude Parameter	
9.5.3 Common UI Status	
9.5.4 Test Inform	
Chapter 10 DrayTek Chatbot	
10.1 Installation	541
10.2 Overview	





Chapter 1 Introduction

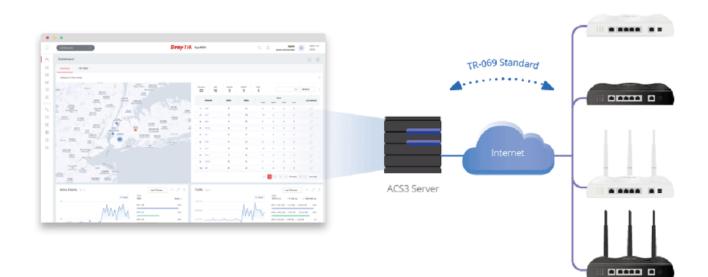
VigorACS 3 is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway, wireless AP **and switch**. VigorACS 3 has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore 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 Vigor 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.

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

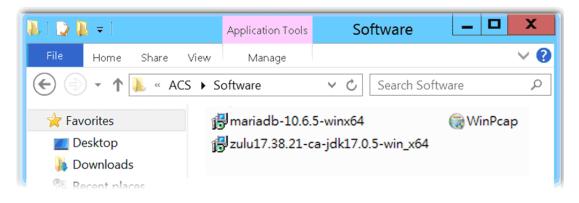
2.1 Platform for Windows 10

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

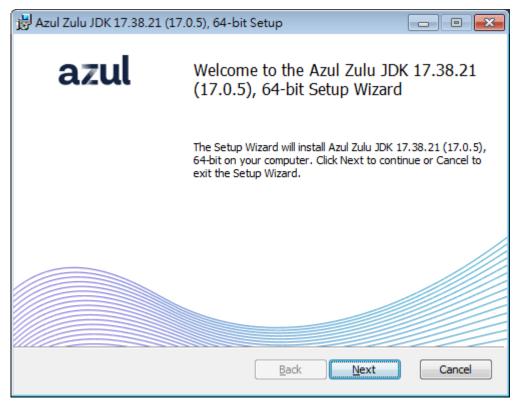
- (I) Installation for Java,
- (II) Installation for MariaDB
- (III) Installation for VigorACS 3
- (IV) Start MySQL/MariaDB Database.
- (V) Edit VigorACS ip.
- (VI) Start VigorACS.

2.1.1 Installation for Java

1. Install Java by clicking "zulu-17.38.21-ca-jdk-17.0.5-.win_x64" (or later) to execute the installation.



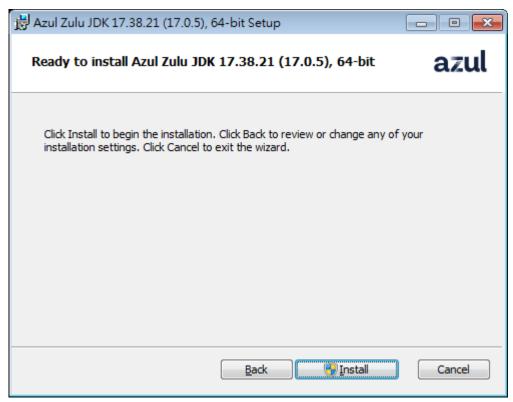
2. The first page will be shown as follows. Click **Next** to get into next page.



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

😸 Azul Zulu JDK 17.38.21 (17.0.5), 64-bit Setup	
Custom Setup Select the way you want features to be installed.	azul
Click the icons in the tree below to change the way	/ features will be installed.
Azul Zulu JDK 17.38.21 x64 Add to PATH Set JAVA_HOME variable JavaSoft (Oracle) registr	This feature requires 308MB on
< +	your hard drive. It has 2 of 3 subfeatures selected. The subfeatures require 1KB on your hard drive.
Location: C:\Program Files\Zulu\zulu-17\	Browse
Re <u>s</u> et Disk <u>U</u> sage	Back Next Cancel

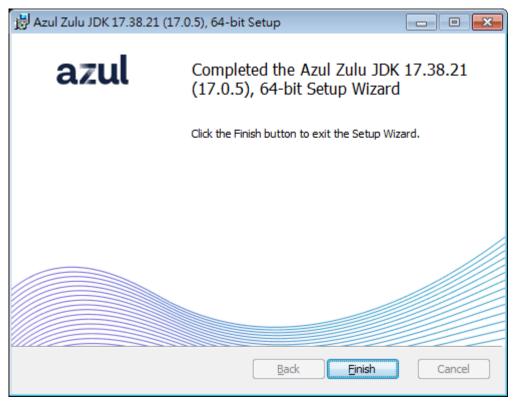
4. In the following page, just click **Install.**



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

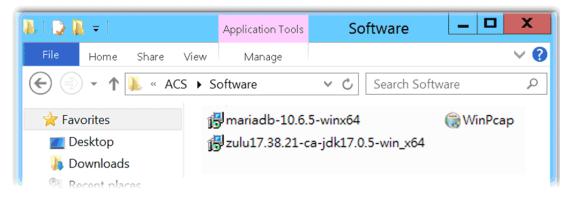
岃 Azul Zulu JDK 17.38.21 (17.0.5), 64-bit Setup	- • 💌
Installing Azul Zulu JDK 17.38.21 (17.0.5), 64-bit	azul
Please wait while the Setup Wizard installs Azul Zulu JDK 17.38.21 (17.0.5)	, 64-bit.
Status: Updating component registration	
<u>B</u> ack Next	Cancel

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

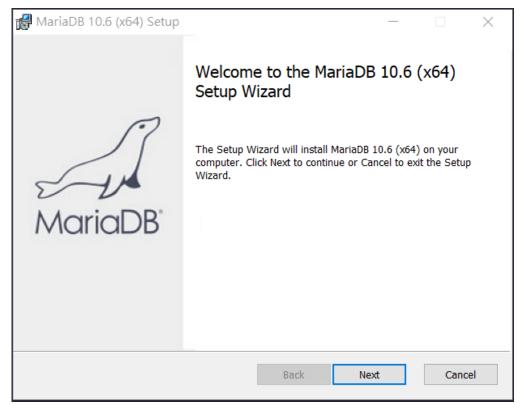


2.1.2 Installation for MariaDB

1. Install MariaDB by clicking "mariadb-10.6.5-winx64" (based on your PC condition) it to execute the installation.



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



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

🚮 MariaDB 10.6 (x64) Setup	- 🗆	×
End-User License Agreement Please read the following license agreement carefully	MariaDB Server	2
GNU GENERAL PUBLIC LICENSE		^
Version 2, June 1991		
Copyright (C) 1989, 1991 Free Software Foundatio Street, Fifth Floor, Boston, MA 02110-1335 USA Ev to copy and distribute verbatim copies of this licens changing it is not allowed.	veryone is permitted	
Preamble		
The licenses for most software are designed to take	away your freedom	~
\checkmark I accept the terms in the License Agreement		
Print Back	Next Can	cel

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

🖟 MariaDB 10.6 (x64	4) Setup			_		×
Custom Setup Select the way you want features to be installed.				Maria Se	DB rver 🗹	A
Click the icons in th	Click the icons in the tree below to change the way features will be installed.					
MariaDB Server Database instance Client Programs Packup utilities Development Components Third party tools HeidiSQL			hard drive selected.	ver ure requires 14 e. It has 3 of 3 The subfeatur your hard drive	subfeature es require	
Location: C:\Program Files\MariaDB 10.6\ Browse						
Reset	Disk Usage		Back	Next	Can	cel

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	– 🗆 X
Default instance properties MariaDB 10.6 (x64) database configuration	MariaDB Server
 Modify password for database user 'root' New root password: Confirm: Enable access from remote machines for user Use UTF8 as default server's character set 	
	Back Next Cancel

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

🖟 Database settings			_		\times
Default instance properties		Maria	DB	R	
MariaDB 10.6 (x64) (latabase configuration		Se	rver 🗹	-2
✓ Install as service Service Name:	MariaDB				
🗹 Enable networking					
TCP port:	3306				
Innodb engine set	tings				
Buffer pool size:	1004 MB				
Page size:	16 ~ KB				
		Back	Next	Can	cel

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

🖟 MariaDB 10.6 (x64) Setup	- 🗆 X
Ready to install MariaDB 10.6 (x64)	MariaDB Server
Click Install to begin the installation. Click Back to review or ch settings. Click Cancel to exit the wizard.	ange any of your installation
Back	Install

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

🕼 MariaDB 10.6 (x64) Setup	_		×
Installing MariaDB 10.6 (x64)	Maria Serv	DB ver ⊄	A
Please wait while the Setup Wizard installs MariaDB 10.6 (x64).			
Status: Updating component registration			
Back	Next	Can	cel

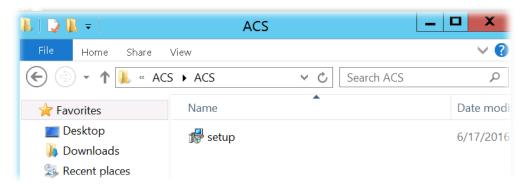
9. After finishing the configuration, please click **Finish** to exit the wizard.

ᡒ MariaDB 10.6 (x64) Setup	- 🗆 X	
	Completed the MariaDB 10.6 (x64) Setup Wizard	
MariaDB'	Click the Finish button to exit the Setup Wizard.	
	Back Finish 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.



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

🔂 Setup - VigorACS	_		×
Database Access Type Selection		¢	
Please select Local Database if you want to update or install the TR the local MySQL, or select Remote Database if the MySQL database host. You will be asked for the connection details later.			
Choose the one you need, and click Next.			
O Local Database			
 Remote Database * Connect to an existed database after finishing the installation 	on proced	dure.	
<u>N</u> ex	ct >	Can	ncel

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

🛃 Setup - VigorACS	_		×
Select MySQL/MariaDB Install Path		Q	
Please specify the installation folder of MySQL/MariaDB and then click	Next	outton.	
C:\Program Files\MariaDB 10.6	Bį	owse	
\searrow			
< <u>B</u> ack <u>N</u> ext	>	Can	icel

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

👸 Setup	- VigorACS	_		×
VigorA	CS Install Type Selection		G	
Plea	se select Install or Upgrade, then click Next.			1
۲	Install This will remove exisiting data and create a new VigorACS Da the "tr069.keystore" file.	tabase, a	nd renew	
0	Upgrade This will keep existing data and update your VigorACS Databa "tr069.keystore" file.	se, and k	eep the	
	< <u>B</u> ack <u>N</u> ex	(t >	Can	cel

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**.

dia , yr aco			
🔂 Setup - VigorACS		_	
MySQL/MariaDB Account Setting			
			a s
Please specify password of root of MySQL/	MariaDB, this step	can be ignored	dif
MySQL/MariaDB database has not been con	figured.	-	
root password			
••••			
confirm root password			
••••			
		Check pa	assword
		_cneck pe	333/010
	< <u>B</u> ack	<u>N</u> ext >	Cancel
👸 Setup - VigorACS		_	□ ×
The VigorServiceController Install Path			
			a s
			Car
E-H			
Folder			
C:\supervisord		Bi	rowse
	N.		
	ß		
	< <u>B</u> ack	<u>N</u> ext >	Cancel

6. Set the passwords. Click **Next**.

😼 Setup - VigorACS	_	□ ×
The InfluxDB User Settings		
Please create a new user with access to InfluxDB, then click Next.		
username:		
password:(Min length is 8)		
•••••		
confirm password:		
•••••		
< <u>B</u> ack	ext >	Cancel

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

😽 Setup - VigorACS	_		\times
System Settings			Ð
By default, the port number is same for the VigorACS portal and CF	E commu	nication.	
 Use same port number for the VigorACS portal and CPE communication Use different port for the VigorACS portal and CPE communication 			
6			
< <u>B</u> ack <u>N</u> e	xt >	Ca	ncel

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			
B setup Mgoixes		—	
HTTP And HTTPS Port			
What is your HTTP and HTTPS port?			して
Please specify your HTTP and HTTPS port, th	en dick Next.		
HTTP Port:			
80			
HTTPS Port:			
443			
HTTPS Chatbot Port:			
18443			
	2		
	12		
	< <u>B</u> ack	Next >	Cancel
		Mext >	Cancel
😽 Setup - VigorACS		_	×
Jg coup ingenies			_ ^
Netflow, STUN And Syslog Port			
Netflow, STUN And Syslog Port What is your Netflow, STUN and Syslog port?	,		
What is your Netflow, STUN and Syslog port?			Ð
		ext.	Ð
What is your Netflow, STUN and Syslog port?		ext.	
What is your Netflow, STUN and Syslog port? Please specify your Netflow, STUN and Syslo		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port:		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port:		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514	g port, then click N		
What is your Netflow, STUN and Syslog port Please specify your Netflow, STUN and Syslo STUN Port: 3478 Syslog Port: 514		ext.	Cancel

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

9. Specify the server domain.

😽 Setup - VigorACS			
		_	
Server Domain			
What is your server domain?			al A
Please specify your server domain.			
Server Domain:			
acs.draytek.com			
	\searrow		
	< <u>B</u> ack	<u>N</u> ext >	Cancel
🔂 Setup - VigorACS		_	
		_	
Setup - VigorACS		_	
		_	×
System Settings	VigorACS portal a	and CPE commu	
System Settings By default, the port number is same for the	e VigorACS portal a	and CPE commu	
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the	from VigorACS po		
System Settings By default, the port number is same for the			
System Settings By default, the port number is same for the	from VigorACS po		
System Settings By default, the port number is same for the	from VigorACS po		

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

🛃 Setup - VigorACS	_	
JBoss Configuration Selection		
The JBoss configuration which VigorACS used for Web and CPE of	ommunicatio	^{m.}
For enhanced security select TLS 1.3 (standalone-secure.xml) For security and compatibility with existing CPEs we recommend T (standalone.xml) For compatibility with older legacy CPEs use TLS 1.0 (standalone-		xml)
Choose the one you need, then click 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>l</u> ext >	Cancel

11. Determine the home path and click **Next**. The default directory used by this program is *C*:*IUsers*. 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 This folder is for storing the statistics and configurations	click N	lext butt	on.
C: \Users \User \AppData \Roaming		B <u>r</u> owse	
< <u>B</u> ack <u>N</u> ext	t >]	Cancel

12. Determine the destination folder and click **Next**. The default directory used by this program is *C*:1*Program Files*1*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, dick Next. If you would like to select a different folder, d	ick Bro	wse.
C:\Program Files\VigorACS	Br	owse
At least 998.0 MB of free disk space is required.		
< <u>B</u> ack <u>N</u> ext	>	Cancel

13. 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	—		\times
Select Start Menu Folder Where should Setup place the program's shortcuts?			
Setup will create the program's shortcuts in the following Sta	art Menu	folder.	
To continue, click Next. If you would like to select a different folder, o	lick Brov	vse.	
VigorACS	Bro	wse	
2			
< <u>B</u> ack <u>N</u> ext	>	Cano	el

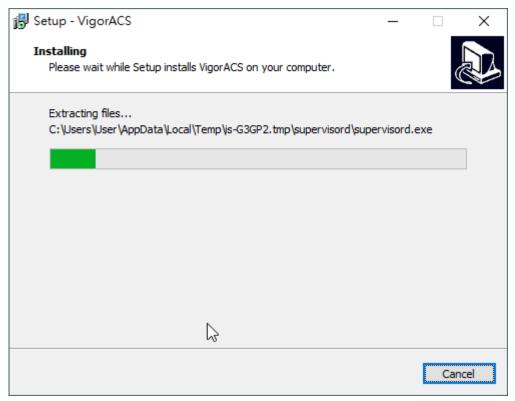
14. In this dialog, check the box of "Create a desktop shortcut" for your necessity. Click Next.

🔂 Setup - VigorACS	_		\times
Select Additional Tasks Which additional tasks should be performed?		C	
Select the additional tasks you would like Setup to perform while inst then click Next.	alling Vig	orACS,	
Additional shortcuts:			
✓ Create a <u>d</u> esktop shortcut			
Other tasks:			
Allow VigorACS access through Windows Firewall (Recommende	d)		
Allow VigorACSChatbot access through Windows Firewall (Reco	mmende	d)	
5			
< <u>B</u> ack <u>N</u> ex	t >	Car	ncel

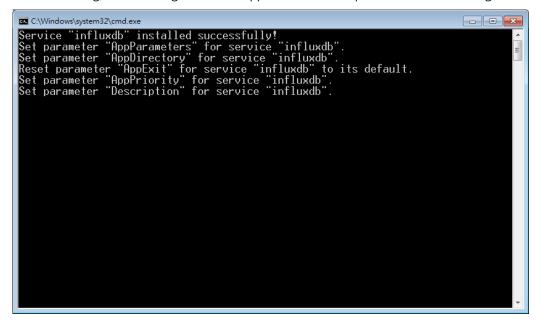
15. Now, the program is ready to install necessary features and files to your computer. Please click **Install** to start.

ß	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 revie change any settings.	ew or	
	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)		
	<	>	~
	< <u>B</u> ack <u>I</u> nstall	С	ancel

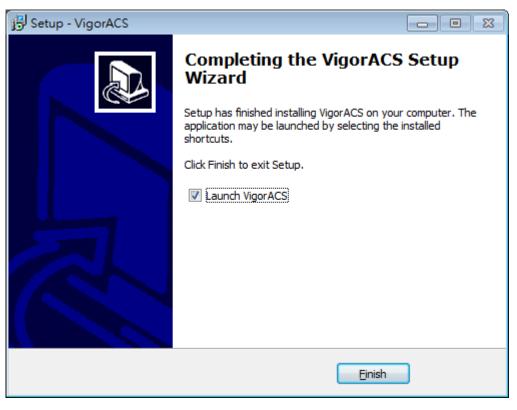
16. Please wait for a while to complete the installation.



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



18. 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.

VigorA User Name root Password	CS ©
root Password	۵
	۵
Validation Code 5817	
Remember me	5817
Login	n
	Remember me

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.

® VIHEISGREAT		Close Adv	erts
		⊕ EN ~	
Warning : Your ACS is still set to the default part root is still using the default password. For security reasons, changing it is stro	assword. Please ch ngly recommended. Wige	nange it ASAP.	
		Change password	Cancel
	root		
	Password	٩	

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

	Root Network 🗸 🗸	Dray	Tek VigorAC	S 3			El Ca	pture Pac	kets 👻	Syst	carrie em Administrator	C
(¹)	Dashboard								Aut	o Refresh	: 1 Minute 💌	С
	Map Overview		×	Network Overvie	ew						-	23
		raissens verderdiepe Zuidwolde lepoel	[]	Network 53	Online 68				Q Netv	work •		
		Beijum	Ga	Network	Online	Offline Total W	ine		Alarm			
Z	兩置倫 Zuidhorn Slaperstil		NOORDDIJK	Network	Unline		WAN	VPN	LAN	Go To Dashboard	3	
E.	Zuiderburen Hoogemeeden	DE HOOGTE KORREWEGWLIK Paddepoel	Lewenborg	Root Network	68	172	172	0	0	0		
	Den Horn	axHuizen 格羅寧根		RD8	27	22	22	0	0	0	0	
\$	Enumatil Lagemeeden HoodKERK	合維寧根 Groningen	9	RD7	0	15	15	0	0	0	θ	
	De Poffert		Oude Roodehaan	Shanghai	0	15	15	0	0	0	8	
ŝ	Gem Leek Matsloot	Helpman		dvcom_kuwait	2	10	10	0	0	0	0	
Ag		Esse Gronin	ien, 🦂 🧍	RD3	4	9	9	0	0	0	0	
	ettelbert		1 m	AnPhat_VN	2	7	7	0	0	0	8	
i	Sandebuur Roderwolde	Eelderwolde Nijveensterkolk	+ aren Oos - r	VISUS	1	4	4	0	0	0	8	
		Hoomsedik 20 GeoBasis-DE/BKG (©2009) 使用條款	次 回報地圖錯誤									_
	Active Clients Top 20	③ Last 24 hours ~	×	Traffic - Top 20						() L	ast 24 hours 🕤 —	20
	Total 25 100 %	RD3 / 0	0%	Total 258.79 GB	î 31.23 (GB ↓ 227. GB	56	RD:	3 / 177.58	GB↑ 30.4	40 GB↓ 147.17 GB 6	996
	125 • Total	RD2 / 14	56%	9.31 GB		 Tota 		200	2 / 70 05 /	CD 1 404	40 MB↓ 79.38 GB	
	75 MMW WWWWWWWW	attel / 9	36%	7.45 GB				KD.	2779.031	GD 404.		196
	50	RD1/2	8%	5.59 GB 3.73 GB	.11	AL		RD	1 / 820.90	MB↑ 47.	21 MB↓ 773.69 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. Start VigorACS Chatbot
- 8. Shutdown VigorACS Chatbox
- 9. Edit bind IP of VigorACS Server (please keyin IP or servername).
- 10. Memory Configuration.
- 11. Port/Domain Configuration.
- 0. 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:

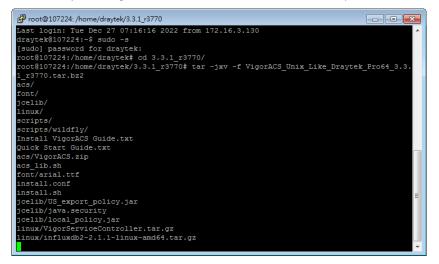
#bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2 | tar xvf -

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 -

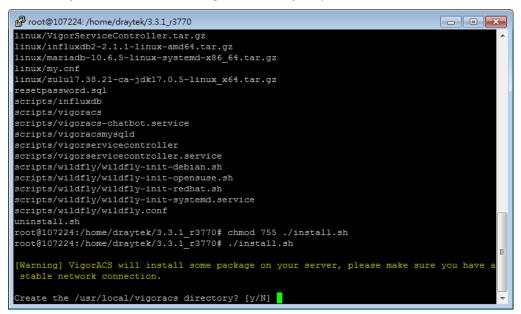


4. Change the permissions mode of install.sh and uninstall.sh.

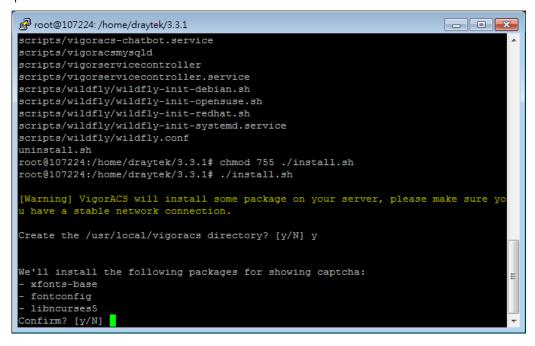
chmod 755 ./install.sh

chmod 755 ./uninstall.sh

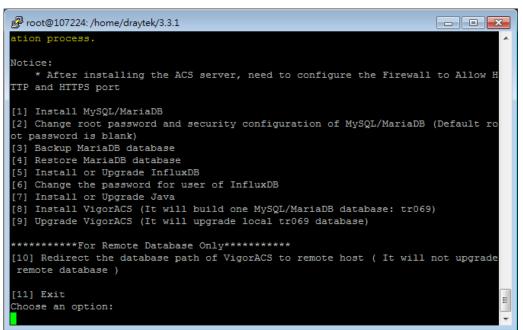
- 5. Enter "y" to execute ./install.sh installation file.
- 6. Later, the system will ask to create vigoracs, enter "y" to proceed.



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 MySQL/MariaDB
- (3) Backup MariaDB database
- (4) Restore MariaDB database
- (5) Install or Upgrade InfluxDB
- (6) Change the password for user of InfluxDB
- (7) Install or Upgrade Java
- (8) Install VigorACS
- (9) Upgrade VigorACS
- (10) Redirect the database path of VigorACS to remote host
- (11) Exit
- Choose an option :
- (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.

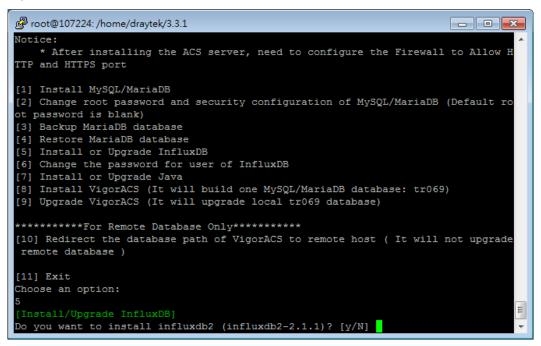
#/usr/local/mysql/bin/mysqladmin --defaults-file=/usr/local/mysql/my.cnf -u root password 'new password'

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

🕑 root@107224: /home/draytek/3.3.1
* After installing the ACS server, need to configure the Firewall to Allow H
TTP and HTTPS port
[1] Install MySQL/MariaDB
[2] Change root password and security configuration of MySQL/MariaDB (Default ro
ot password is blank) [3] Backup MariaDB database
[4] Restore MariaDB database
[5] Install or Upgrade InfluxDB
[6] Change the password for user of InfluxDB [7] Install or Upgrade Java
[8] Install VigorACS (It will build one MySQL/MariaDB database: tr069)
[9] Upgrade VigorACS (It will upgrade local tr069 database)
*********For Remote Database Only*********
[10] Redirect the database path of VigorACS to remote host (It will not upgrade
remote database)
[11] Exit
Choose an option:
1 [Install MariaDB]
Do you want to install mariadb ()? [y/N]

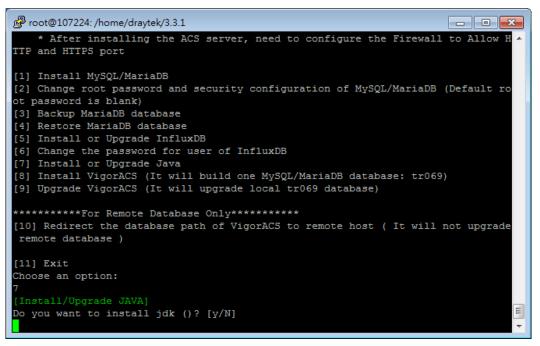
Follow the instructions on the screen to finish the MariaDB installation.

10. Input 5 to install InfluxDB.



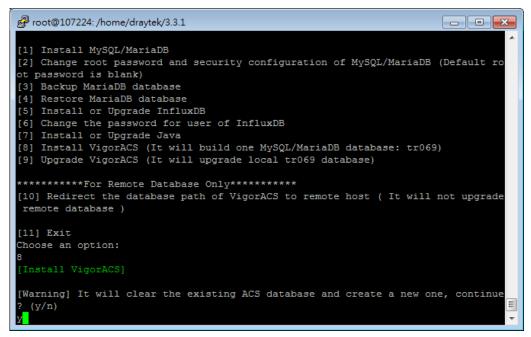
Follow the instructions on the screen to finish the InfluxDB installation.

11. Input 7 to install Java.

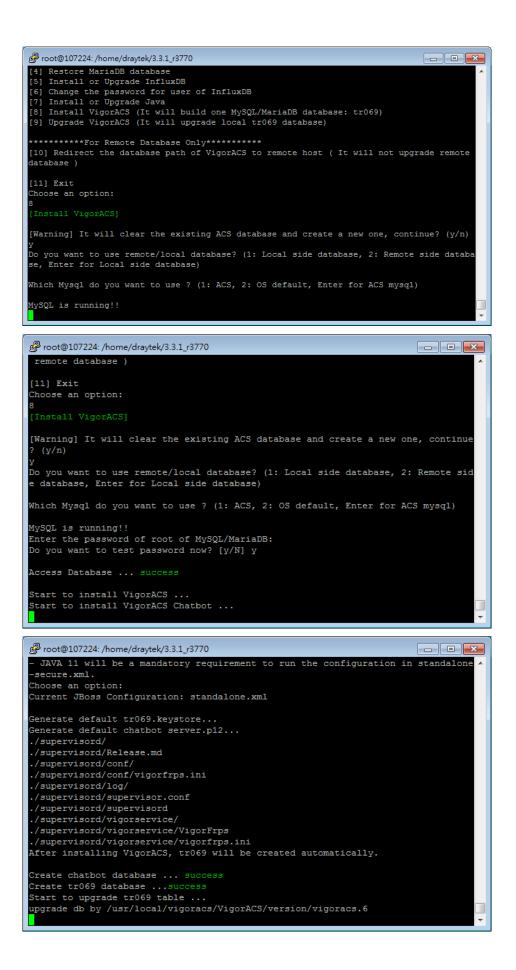


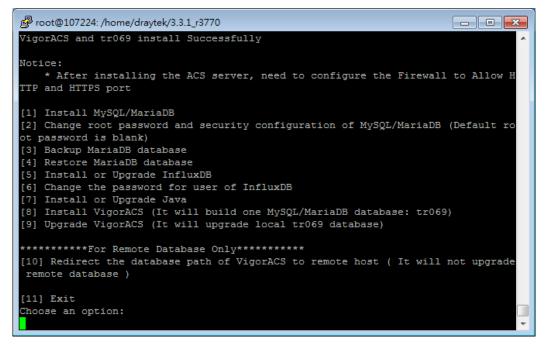
Follow the instructions on the screen to finish the Java installation.

12. Input 8 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.



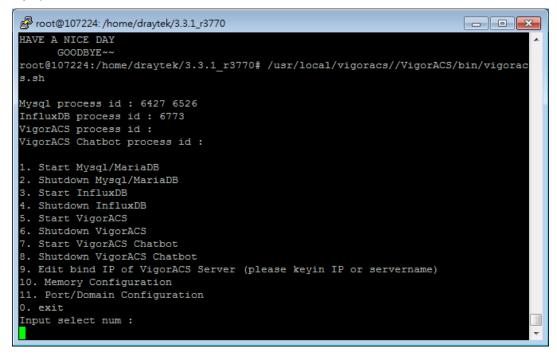


- 13. Input 11 to finish and exit the installation.
 - () Step 14 is required for establishing remote database only. You can ignore it while building local database.

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

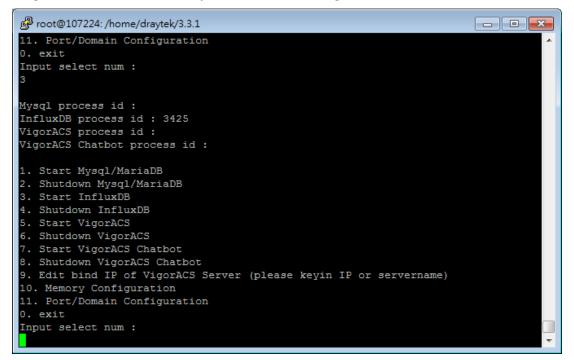
2.2.2 StartMySQL/MariaDB Databse

After installing VigorACS, mysql/mariadb daemon has started. You can check it using " /usr/local/vigoracs//VigorACS/bin/vigoracs.sh" instruction. Use the menu item 1/2 to start / shutdown mysql/mariadb.



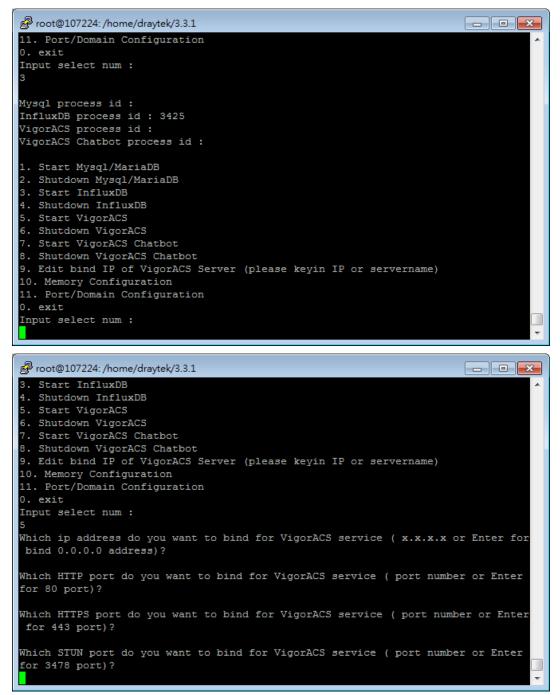
2.2.3 Start InfluxDB

After installing InfluxDB, access "/usr/local/vigoracs//VigorACS/bin/vigoracs.sh" and execute "./vigoracs.sh". Next, it is necessary to start InfluxDB for VigorACS. Select item 3 to start InfluxDB.

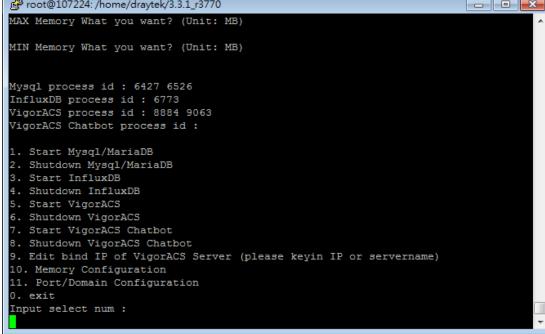


2.2.4 Start VigorACS

After installing VigorACS, access "/usr/local/vigoracs//VigorACS/bin/vigoracs.sh" and select item 5 to start VigorACS.



🔓 root@107224: /home/draytek/3.3.1_r3770 📃 📼 💌
bind 0.0.0.0 address)?
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 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 Ente r for 514 port)?
Which Netflow port do you want to bind for VigorACS service (port number or Ent er for 20314 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)
P root@107224: /home/draytek/3.3.1 r3770
MAX Memory What you want? (Unit: MB)

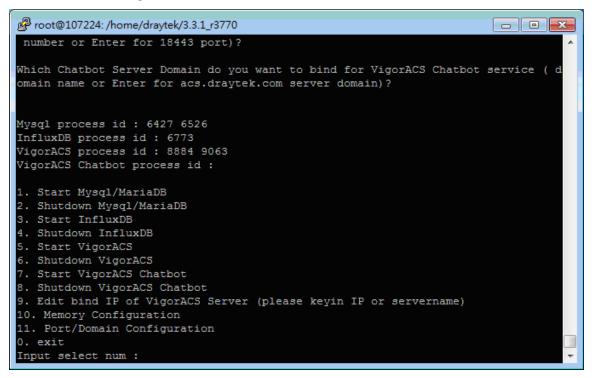


If you ever reboot the machine after installing VigorACS, just select item 1 to start mysql/mariadb first. Then, select item 5 to start VigorACS.

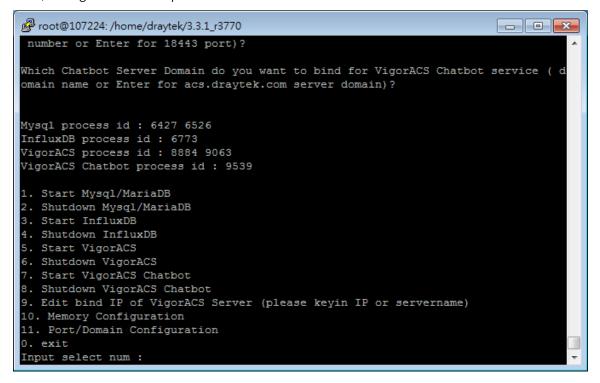
2.2.5 Start VigorACS Chatbot

Activate the chatbot server. The user account can check general information of VigorACS server through specific mobile phone device and/or PC.

Select item 7 to start VigorACS Chatbot.



Later, the VigorACS Chatbot process ID will be shown on the screen.



2.2.6 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 9 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**.

	⊕ en
	VigorACS
	User Name
	root
	Password
	••••••
Dray Tek	Validation Code
	5817
	Remember me .5.8.1.7
	Login

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

		⊕ EN ∽ VigorACS	
LiC Please go	ense Warning : Your license is invalid or ex to license server to activate your license.	pired toot Password	Activate
	Dray Tek	Validation Code 7354 Remember me 7354 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.**

	oes not record any personal identifiable inform	nation with the exception of your IP Address which is recorded after login for security purposes.
The MyVigor website d	oe not record any periodal identificate inform Dray Tek MyVigor	ENGLISH Usemane carrieri Password Login
	Cognight & DrayTek Corp.	Cirette Account / Get Help Return to old MyVigor Terms of Service / Privacy Policy

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 Device)	
el	Device Name Model	VigorACS3_carrie	Ser
	MAC Serial Number	ACS3200100013 ACS3200100013	_ 1
		Cancel Submit	_

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

My Product > VigorACS3_carrie > Service Status		
	ACS	
	License Status License Action Activate License Force Sync	
	License History	
	• Today 2000-01-01	
	Product Registration 2003-01-31	

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

		License Agreement for ACS 3
rie	> Service Status	Insumation, reproduction, display or discussion of the Supplier obtained or any documentation by the officed 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. You will not export, reexport, divert, transfer or disclose, directly or indirectly, the Supplier Software, 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.
		Cancel Accept

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

		A	ctiv	vate	Lice	ense	of A	CS :
Service Status	License				Trial			
	Activate Date			202	0-01	1-31		
				Janu	ıary	2020		*
		Su	Мо	Tu	We	Th	Fr	Sa
								4
			6			9		
				14				
							31	
					Reset	t		
	C	Cancel						

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

PRODUCI	HIGH AVAILABILITY SETTING CUSTOMER SURVEY AU	SENT V	
	Activate Lice	nse of ACS 3	
Service Status	Please confirm the below infor	nation then activate the license.	
	Service	ACS	
	Service Provider	DT-ACS-3	
	License	Trial	
	Activate Date	2020-01-30	
	Expire Date	2020-02-29	
	ſ		
	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	Þ
OPERATION 1000 : License Key OK	
LICENSE ID 0002b097	
START DATE 2020-01-30	
EXPIRE DATE 2021-02-29	
MAX NODE 00000020	
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**.

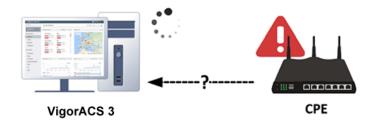
Vig User Name root Password ••••••• Validation Code 5817	orACS
root Password ••••••• Validation Code	
Dray Tek	
	۵
Remember me	5817

Dashboar	d erview		×	Network Overview					Auto Rel	fresh :]	Minute V C	rvi
+		US 75 CONVASSO		Sub Network Online 123 6	Alarm 100136						New Devices Reset to defail	
				Network Members	Online	Offline		Ala	arm		Go To Dashboard	
> Z		US 100	OK 167	Network Members	Onune	Ontune	Total	WAN	VPN	LAN	Go to basilboard	
		Mohank Park	OK 266	Ø directly-under-Root Network	0	13	13	0	0	0		
16-	A Shafe OKI		×	Ø AutoTestNetwork	1	0	2	2	0	0	8	
	CRG US75	408		Ø AutoTest_Dev	2	7	7	0	0	0	Ø	
	1 1			Ø AutoTest_SD-WAN	0	2	2	0	0	0	8	
				Ø AutoTest_VPN	1	0	0	0	0	0	Ø	
US 64			an and a start	Ø Hotspot_Web_Portal	0	2	2	0	0	0	в	
US 412 OK 51	Tulsa	1 1 1 1		Router_App_Network	0	2	2	0	0	0	8	
				T_2024-07-22_Wholesale_GA_D	0	0	0	0	0	0	8	
New De	vices		- 2 ×									
Action	IP Address	Device Name	Device Type									
	192.168.143.10:80	2120n 001DAA7FF2A4 stun	Vigor2120n+									
	192.168.106.144:80	2865Lac 1449BC3D7A08	Vigor2865Lac									
•	192.168.106.143:80	2952Pn 001DAAF8D818 https	Vigor2952Pn									
•	192.168.106.143:80	2962P 1449BC39F110 https	Vigor2962P									
	192.168.105.22:80	3220n 001DAA554758	Vigor3220n									

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.

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name DrayTek		
Default:Disable Auto-Logout	Management P	Port Setup
Enable Validation Code in Internet/LAN Acc	ess Oser Define	e Ports 🔘 Default Ports
Note: IE8 and below version does NOT suppor	t 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 Internet	FTP Port	21 (Default: 21)
Domain name allowed	TR069 Port	8069 (Default: 8069)
FTP Server	SSH Port	22 (Default: 22)
HTTP Server Enforce HTTPS Access	Note:	
HTTPS Server	Ports 8001 and	8043 are used for Hotspot Web Portal.
Telnet Server	Brute Force Pr	otestion
✓ TR069 Server		
SSH Server		e force login protection

System Maintenance >> Management

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.

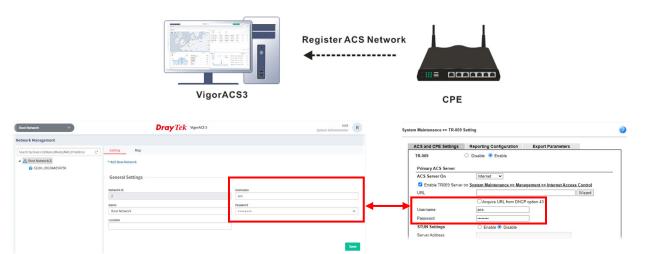
Protocol	●HTTP ○HTTPS		
URL			
Port	8069		
Username	vigor		
Password	•••••		
Note: Please page.		w access from li	nternet on <u>System Maintenance >> Management</u>
page. Periodic Infor		w access from I	nternet on <u>System Maintenance >> Management</u>
page. Periodic Infor Enable	m Settings	w access from h	ternet on <u>System Maintenance >> Management</u>
page. Periodic Infor © Enable Time I	m Settings e O Disable		
page. Periodic Infor © Enable Time I Apply Setting	rm Settings e O Disable nterval		
Page. Periodic Infor © Enable Time I Apply Setting © Enable	m Settings • O Disable nterval Is to APs/Switches		

Check TR-069 authentication

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

- Register to the network of VigorACS 3

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



- Get CPE information

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

		Get CPE Information	
	VigorACS3	1	CPE
lanagement			System Maintenance >> TR.069 Setting
levice ID/Name/Model/MAC/IP Address C	Setting Map		
t Network(1)	Delete This Device & Change Network		ACS and CPE Settings Reporting Configuration Export Parameters
3220n_001DAA554758			TR-069 Obisable Enable
	General Settings		
			Primary ACS Server
	Status Disable Enable	Known Device Known Unknown	ACS Server On Internet V
	Disable Enable	Khown Unknown	Enable TR069 Server on System Maintenance >> Management >> Internet Access Control
	Device ID	Network ID	URL Wizard
	1	2	
	Model Name	Device Name	
	Vigor3220n	3220n_001DAA554758	
	Note 1	Note 2	CPE Client
			Protocol HTTP OHTTPS
	Serial number	MAC Address	URL
	2019090309412601	001DAA554758	
			Username vigor
	Location	CPE Client IP	Password
		192.168.105.22	Note: Please enable TR-069 server to allow access from Internet on System Maintenance >> Management
	Phone No.	CPE Client Port	page.
		8069	Periodic Inform Settings
	Domain Name	CPE Client URI	
		/cwm/CRN.html	C Enable Disable
	Management Protocol	CPE Client User Name	Time Interval 900 second(s)
	CPE default (https) http https	vigor	
	Management Port	//Edit	
	443	CPE Client Password	
levices		/Edit	

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		
D			
Primary ACS Server			
ACS Server On	Internet 🗸		
Enable TR069 Server	on <u>System Maintenance >> Mar</u>	agement >> Internet Acces	s Control
URL			Wizard
	□ Acquire URL from DHC	P option 43	
Username	acs		
Password	•••••		
STUN Settings	● Enable ○ 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.

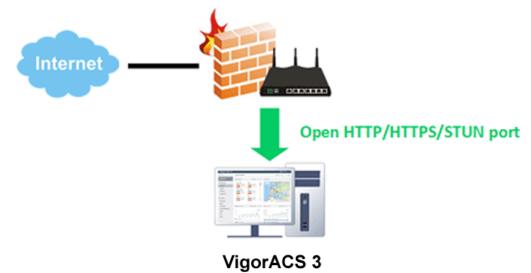
4 👬 Roo

Access List from the Internet	CVM Access Control
✓ Apply Access List to PING List Type Index Description 1 ✓ 1-acs 11.22.33.44/255.255.255.255 2 IP Object ▼ None ✓ 3 IP Object ▼ None ▼	CVM Port 8000 (Default: 8000) CVM SSL Port 8443 (Default: 8443)
4 IP Object V None V 5 IP Object V None V 6 IP Object V None V 7 IP Object V None V 8 IP Object V None V 9 IP Object V None V 10 IP Object V None V	Device Management Respond to external device

• Check the firewall on ACS server

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

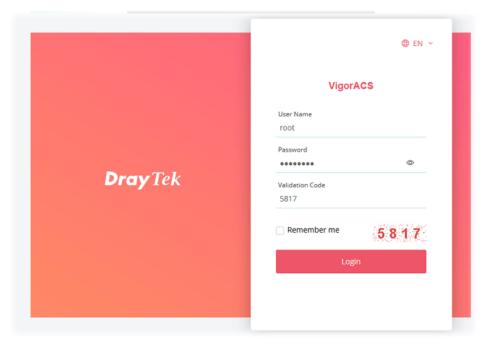
- HTTP port (Default tcp port 80)
- HTTPS port (Default tcp port 443)
- STUN port (Default udp port 3478)



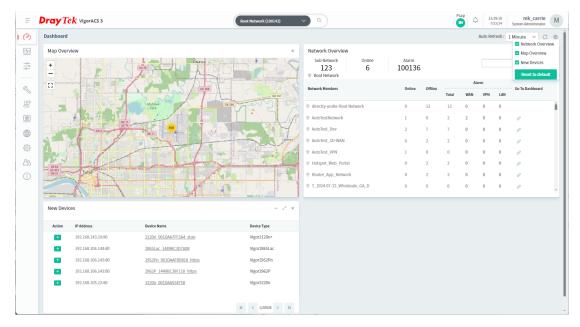
Chapter 3 Getting Started

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.

	-	ek VigorACS 3		Root Network (100142)) (7/2		mk_carrie System Administrator
(P)	Dashboard								(Auto Ref	resh: 1	Minute ~ C
<u>-</u>	Map Over	view		×	Network Overview							Map Overview
	+		US75 Chasso		Sub Network Online 123 6	Alarm 100136						New Devices
					Root Network				AL	arm		Reset to default
Z	Ľ.		05 100		Network Members	Online	Offline	Total	WAN	VPN	LAN	Go To Dashboard
F			Michain Port	04.266	directly-under-Root Network	0	13	13	0	0	0	
	16-	flant 11			AutoTestNetwork	1	0	2	2	0	0	B
	a line	04.11 16.75			AutoTest_Dev	2	7	7	0	0	0	8
		1	The state	Calor	<pre>@ AutoTest_SD-WAN</pre>	0	2	2	0	0	0	8
{\$}		11/1			Ø AutoTest_VPN	1	0	0	0	0	0	B
<u>4</u> 8	US 64 US 412 OK 51		and the second s	and any and any day	Hotspot_Web_Portal	0	2	2	0	0	0	8
()	OK SI	Tuisa			Router_App_Network	0	2	2	0	0	0	Ø
_					© T_2024-07-22_Wholesale_GA_D	0	0	0	0	0	0	8
	New Devi	ces		- ~ ×								
	Action	IP Address	Device Name	Device Type								
		192.168.143.10:80	2120n_001DAA7FF2A4_stun	Vigor2120n+								
			2865Lac_1449BC3D7A08	Vigor2865Lac								
		192.168.106.144:80										
		192.168.106.144:80 192.168.106.143:80	2952Pn 001DAAF8D818 https	Vigor2952Pn								
			2952Pn 001DAAF8D818 https 2962P 14498C39F110 https	Vigor2952Pn Vigor2962P								

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.

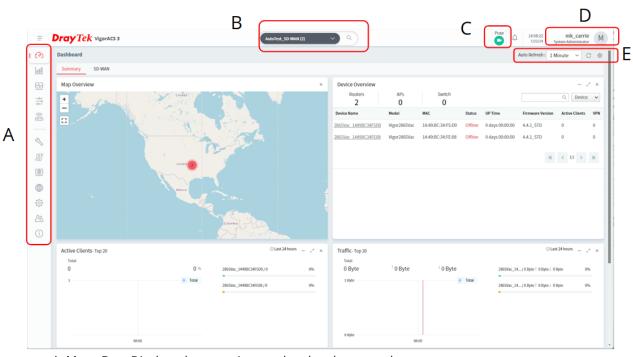
D: Selections - Display current used account and offer selections for setting password, two-factor authentication, manage notification, theme change and logout.

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

Overview - There are three types (Network Overview, Map Overview, New Devices) of overview under the Root Network.

Рсар

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.

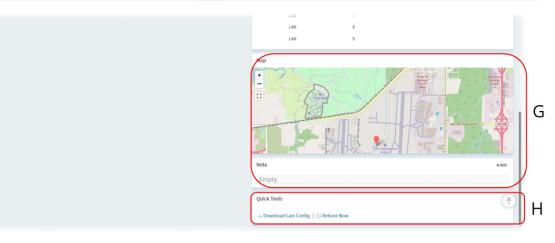
Overview - There are five types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview for the Network Group.

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.

		В				C	Pcap	
=	Dray Tek VigorACS 3		2865Vac_14498C34FE08	✓		-	φ	14:29:53 mk_carrie 7/22/24 System Administrator
0	2865Vac_1449BC34FE08				Device Status: ① Offline	Alarms: 1	Active Clients: 0	Auto Refresh: 1 Minute 🕤
[et]	Port Status			WAN Overview				© Last 24 hours-
E	ACT WANZ OUS DRAYTE	Vigor2865Vac		1 Byte				o Total
	USB DSL Phone1							
	Tatany ALC IC Discus		Hand Preset Eds.					
٥,				0 Byte				
2	Device Information			Total (↑0Byte ↓0B	Byte)	08:00		0.%
	Device Name	2865Vac_1449BC34FE08		WAN1 (†0Byte +0)				0 %
F	IP Address Network Name	http://192.168.106.148:80 AutoTest_SD-WAN		• WAN2 (↑0Byte ↓01	Byte)			0 %
	Model	Vigor2865Vac		■ WAN3 (↑0Byte ↓01	Byte)			0 %
	Firmware Version	4.4.1_STD		■ WAN4 (↑0Byte ↓0)	Byte)			0 %
✨	MAC Address	14:49:BC:34:FE:08		≪ WAN5 (↑0Byte ↓01	Byte)			0 %
පී	Up Time			≪ WANG (↑0Byte ↓01	Byte)			0 %
1			~ show more	•				
_	Connectivity and Alerts			LAN Overview				© Last 24 hours-
	ld ↓† Start Time ↓† Clear Time	10 Terrs 10 1	Message J↑					 Active Clients
	37465130 2024/07/22 05:26:04 ·		Device Loss Connection					·
				0				
						08:00		1
				LAN J†	Status Ut	IP/Mask		41 DHCP 41



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., Vigor2865 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, manage notification, theme change and logout.

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

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

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

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

3.2.4 Menu Bar

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

Menu Bar for Root Network.		Menu Bar for Network Group.	Menu Bar for Selected CPE.
 Dashboard Monitoring Configuration Configuration Maintenance Reports Provisioning Network & Service Management System User About 		 Dashboard Statistics Monitoring Configuration Hotspot Web Portal Maintenance Reports Provisioning Network & Service Management System User About 	 Dashboard Statistics Monitoring Configuration Advanced Advanced Maintenance Reports Provisioning Network & Service Management System User About
RDB ✓ Configuration ✓ VPN AP Profile Load Balance Foute Policy (SD-WAN) VoIP WAN (SD-WAN) ✓	icon to open t list. Select the me	use cursor to each the drop down menu enu item and access guration web page.	

3.2.5 Root Network, Group Network, and Selected CPE

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

3.2.5.1 The Display Tab, Root Network

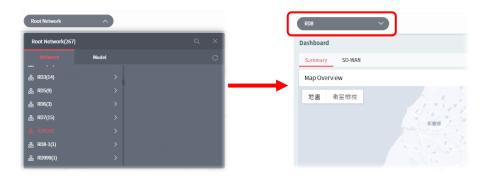
Click the **Display Tab** to display a drop-down list. This tab will display the name of the network group or the name of the selected CPE based on your selection. In default, Root Network will be shown on the Display Tab.

Root Network		
Root Network(267)		Q X
Network	Model	
器 RD3(14)	>	
융 RD5(9)	>	
윪 RD6(3)		
器 RD7(15)		
26 RD8(58)		
묾 RD8-1(1)		
묾 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

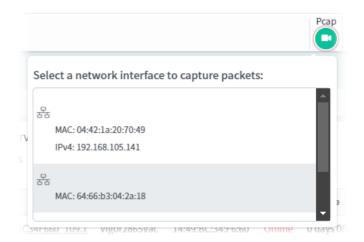
Click the **Model Tab**. Next, click the > button to list other CPE devices with the same model as the selected device. Select the device you want, then the selected CPE will be shown on the Display Tab.

RD8	^			2862Vac_001DAAF7C0E0 V
Root Network(267)		Q X		
Network				2862Vac_001DAAF7C0E0
ය. Vigor2830(1)			1	Port Status
ය. Vigor2832(1)		A 2862Vac_001DAAF1C701		Port Status 🎲
ය. Vigor2860(16)		A 2862Vac_001DAAED3840		DrayTek
ය. Vigor2862(9)				Mireless LAR
ය. Vigor2865(9)		A 2862Lac_001DAA621018		USB DSL Phone1
ය. Vigor2866(1)		A 2862n_001DAAEA38A8		Reset 2.4G 5G Phone2 DSL LAN+1
器 Vigor2912(6)		🛆 DrayTek		
-S. Vienr7915/3)		▲ 2862Vac_001DAAF7C0C0	1	

3.2.6 Capture Packets

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

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



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

(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. 3

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.

< Select anot	her network Interface	
Capture Setting	js	
Selected Netwo	rk Interface	
88		
MAC: 04:42:1	a:20:70:49	
IPv4: 192.168	3.105.141	
Filter Examples		
	er normally, for more expr AP-FILTER	 ✓ ession syntax
You can type filt		 v ession syntax
You can type filt please visit: <u>PC/</u> Custom Filter		<pre> v ession syntax </pre>
You can type filt please visit: <u>PC/</u>	AP-FILTER	ession syntax

These parameters are explained as follows:

ltem	Description
Capture 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.
Timer	Switch the toggle to enable/disable the setting. If enabled, VigorACS server will capture the packets within the time limit defined below. Timer (1-15 Minutes) – 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.

© Pcap 4:45
• When the time is up or stop the job manually, the status of Pcap will be stored as a file on the hard disk. Later, use the tool of Wireshark to check the content of the file.
 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.
f A 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.

_		118-10-23.175419.pcap pture <u>A</u> nalyze <u>S</u> tatistics		Tools Help			- 0
		C Q ← → S T &					
	y a display filter … «Ctrl-/						Expression
	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	192.168.50.10	192.168.105.59	TCP		[SYN] Seq=0 Win=64240 Len=0	
	2 0.001467	192.168.105.59	192.168.50.10	TCP		[SYN, ACK] Seq=0 Ack=1 Win=3	
	3 0.001608	192.168.50.10	192.168.105.59	TCP		[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		
	5 0.004302	192.168.105.59	192.168.50.10	HTTP	· · · · · · · · · · · · · · · · · · ·	Authentication Failed	
	6 0.004673	192.168.50.10	192.168.105.59	TCP		[FIN, ACK] Seq=102 Ack=209 N	
	7 0.005244	192.168.50.10	192.168.105.59	TCP		[SYN] Seq=0 Win=64240 Len=0	
	8 0.005541	192.168.105.59	192.168.50.10	TCP		[ACK] Seq=209 Ack=103 Win=2	
	9 0.005630	192.168.105.59	192.168.50.10	TCP		[FIN, ACK] Seq=209 Ack=103 N	
	10 0 005600	100 168 50 10	107 168 105 50	TCD	51 61750 - 8060	[ACV] Sog-103 Ack-210 Win-6	1032 Lon-0
Tra	nsmission Contro	Version 4, Src: 192. Dl Protocol, Src Por Protocol			l, Ack: 1, Len: 101		
Tra		ol Protocol, Src Por			l, Ack: 1, Len: 101		
Tra	nsmission Contro	ol Protocol, Src Por			l, Ack: 1, Len: 101		
Tra	nsmission Contro	ol Protocol, Src Por			l, Ack: 1, Len: 101		
Tra	nsmission Contro	ol Protocol, Src Por			l, Ack: 1, Len: 101	_	
Tra	nsmission Contro	ol Protocol, Src Por			l, Ack: 1, Len: 101		
Tra	nsmission Contro	ol Protocol, Src Por			l, Ack: 1, Len: 101		
Tra Hyp	nsmission Contro	ol Protocol, Src Por Protocol	t: 64750, Dst Port:	8069, Seq: 1			
Tra Hyp 00	nsmission Contro ertext Transfer 00 1d aa 69 4a	e8 88 d7 f6 56 f7	t: 64750, Dst Port:	8069, Seq: 1	Е.		
Tra Hyp 00 10	nsmission Contro ertext Transfer 00 1d aa 69 4a 00 8d 10 fa 40	e8 88 d7 f6 56 f7 00 80 06 00 00 c0	t: 64750, Dst Port: 99 08 00 45 00 a8 32 0a c0 a8	8069, Seq: 1	Е. 		
Тга Нур 00 10 20	nsmission Contro ertext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f	e8 88 d7 f6 56 f7 00 80 06 00 00 c6 55 3c 14 c0 8e 65	t: 64750, Dst Port: 99 08 00 45 00 a8 32 0a c0 a8 83 a5 64 50 18 i;	8069, Seq: 1	Е. 		
Tra Hyp 00 10 20 30	nsmission Contro ertext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 16 fa f0 1d 16 00	e8 88 d7 f6 56 f7 00 80 06 00 00 c0	<pre>t: 64750, Dst Port: 99 08 00 45 00 a8 32 0a c0 a8 83 a5 64 50 18 1; 63 77 6d 2f 43</pre>	8069, Seq: 1	E- 		
Tra Hyp 00 10 20 30 40	00 1d aa 69 4a 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	e8 88 d7 f6 56 f7 00 80 06 00 c0 85 3c 14 c0 8e 65 00 47 45 54 20 2f	<pre>99 08 00 45 00 a8 32 0a c0 a8 33 a5 64 50 18 i; 63 77 6d 2f 43 62 f 31 2e 31 RN</pre>	8069, Seq: 1	E. JP. n/C 1.1		
Tra Hyp 00 10 20 30 40 50	nsmission Contro ertext Transfer 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	e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5 00 47 45 54 20 2f 6d 6c 20 48 54 54	<pre>t: 64750, Dst Port: 99 08 00 45 00 a8 32 0a c0 a8 33 a5 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RN 74 3a 20 4a 61</pre>	*iJ V •@2 	Е. ;;; л/С 1.1]а		
Tra Hyp 00 10 20 30 40 50 60	00 1d aa 69 4a 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ea 16 69 3b fc ea 16 69 24 e2 68 74 0d 0a 55 73 65 6b 61 72 74 61	e8 88 d7 f6 56 f7 Protocol e8 88 d7 f6 56 f7 00 80 06 00 c0 85 3c 14 c0 08 e5 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 66	99 08 00 45 00 a8 32 0a c0 a8 a3 35 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RN 74 3a 20 4a 61 66 73 2d 48 74 ka	*1J	Е. Jp. "/С I.1 Ja -Ht		
Tra Hyp 20 20 20 50 60 70 80	00 1d aa 69 4a 00 1d aa 69 4a 00 8d 10 fa 40 09 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 d0 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 93 1	e8 88 d7 f6 56 f7 Protocol 88 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e 65 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e 39 32 2e 31 36 38	99 08 00 45 00 a8 32 0a c0 a8 a8 32 0a c0 a8 a8 36 50 18 i; i; a7 76 2f 31 20 a 61 50 2f 31 20 4a 61 6e 73 2d 48 74 ka 31 04 0a 46 f	*1JV .@	Е. p. л/С і Ja Ht Ho		
Tra Hyp 20 20 20 50 60 70 80	00 1d aa 69 4a 00 1d aa 69 4a 00 8d 10 fa 40 09 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 d0 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 93 1	e8 88 d7 f6 56 f7 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 d6 cc 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e	<pre>99 08 00 45 00 99 08 00 45 00 83 25 04 c0 a8 83 a5 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RN 74 3a 20 4a 61 6e 73 2d 48 74 ka 31 0d 0a 48 6f tp 2e 31 30 35 2e st</pre>	*iJ V •iJ v •@ 2 	Е. p. л/С і Ja Ht Ho		
Tra Hyp 00 10 20 30 40 50 60 70 80	00 1d aa 69 4a 00 1d aa 69 4a 00 8d 10 fa 40 09 3b fc ee 1f fa f0 1d 16 00 52 4e 2e 68 74 d0 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 93 1	e8 88 d7 f6 56 f7 Protocol 88 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e 65 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e 39 32 2e 31 36 38	<pre>99 08 00 45 00 99 08 00 45 00 83 25 04 c0 a8 83 a5 64 50 18 i; 63 77 6d 2f 43 50 2f 31 2e 31 RN 74 3a 20 4a 61 6e 73 2d 48 74 ka 31 0d 0a 48 6f tp 2e 31 30 35 2e st</pre>	*iJ V .@	Е. p. л/С і Ja Ht Ho		

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

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

	15:16:21 7/22/24	mk_carrie M System Administrator				
ut	Auto Log	gout 🛛 💽				
	🔊 Engl	ish ~				
	🔒 Set	Password				
	ိစ္ Two Factor Authentication					
	⇔ Man	age Notification				
	🖌 Cha	nge Theme				
	[→ Log	out				

3.2.7.1 Change Language

The web pages of VigorACS can be expressed with different languages. Select the one you want.

t Auto Logout 😧	
▲ English ✓	
Cr 中文 (简体)	ange language
Deutsch	
English	
Nederlands	
中文 (正體)	

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	٩
Confirm Password	٩
	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
	Passward 💿
Dray Tek	Validation Code 5817
	Remember me 6.8 1 7
	Login

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

wo-factor authentication	
Enable two-factor authenticat	lon 💽
Choose 'Default' me Get and Install Goog Scan the QR-Code o Click the save butto	Authentication please follow the instructions below. ans Two Factor Authentication is based on TOTP Authenticator. Je Authenticator (IOS Android) r manual input secret key n to verify the code generated from APPs fou should backup the secret key or QR-Code
Description	mk_carrle@WgorACS
QR-Code	Display in Argen Vignal/CS(mic_carring)Wignah/CS)
Manual Input	3HKBRJLHI6LR03GM
Verification Code	
	Cancel Save

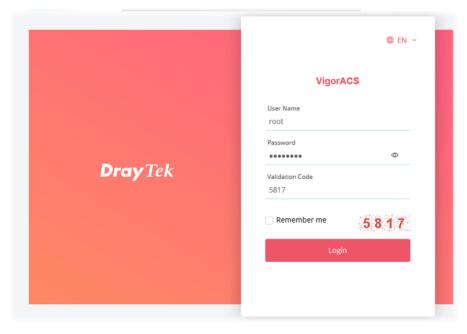
4. Use your cell phone to scan the QR-Code shown on the Two-factor Authentication page.

4:52 ◀ App Store	📲 4G 🔳
	or
VigorACS (root@VigorACS)	
443 987	
	\frown
	+

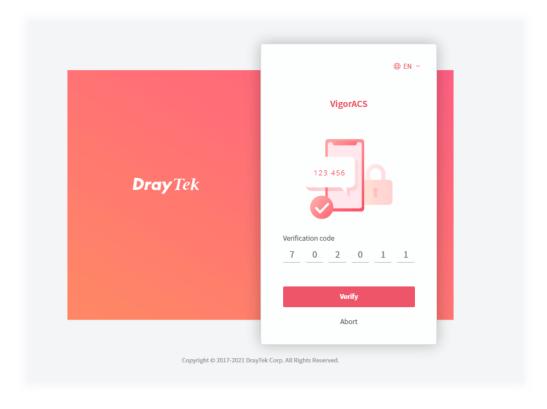
5. A key will be created randomly on the cell phone. Enter that key on the box of **Verification Code** and click the **Save** button.

	n C	
Choose 'Defauit' mee Get and install Googi Scan the QR-Code or Click the save button	athentication please totion the instructions below. ns Two Factor Authentication is based on TOTP Authenticator. e Authenticator (OS Androd) manual Input secret key to werkly the code generated from APPs us hand Dackup the secret key or QB Code	
escription	mk_carrie@VigorACS	
	Display in App: VigorACS(mk_carrie@VigorACS)	
IR-Code		
fanual Input	3HKBRJLHI6LRO3GM	
turiuu input		

- 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 Manage Notification

This option is available when the role of the user accessing the VigorACS server is the System Administrator.

Manage Notification		C
Email Notification		
Email	examplo@gmail.com	
SMS Notification		
Telephone		
Chatbot Notification		
App Notification		
		Save

These parameters are explained as follows:

ltem	Description			
Email Notification	Switch the toggle 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 Notification	Switch the toggle 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.			
Chatbot Notification	Switch the toggle to enable / disable the function.			
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications and information related to VigorACS.			
	If enabled, this user account can check general information of VigorACS server through specific mobile phone device and/or PC.			
App Notification	Switch the toggle to enable / disable the function.			
	If enabled, use the DrayTek Router App to scan the QR-Code for APP Notification.			
Save	Save the settings.			

3.2.7.5 Change Theme

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

eme					
Automatically detect sy	stem or browser theme (Detected: Light The	ame)			
y Automatically detect sy.	terror browser theme (bettetted. Eight fin				
) Light Theme			O Dark Theme		
) tight meme			O bark meme		
E Root Network	Dray Tek VigorACS3	root R	E Root Network ^	Dray Tek VIDUACS 3	root System Administrator
Root Network(74)	a x	Auto Refresh : 1 Minute 👻 🔿 🗇	(%) Root Network(?4)		Auto Refresh : 1 Minute V C
Referent Mode	C twork Overview	- 2 ×	Retwork Model	C work Overview	
÷	Network Online	Alarm Q. Network ~	幸 & SD WAN(D) >	Network Online Alarm 12 2 72	
& mana(123)(5)	Poot Network	12	& assass(123)(7) >	LZ Z IZ Poot Network	
م الله ed1(2)	> work Members	Alarm Online Offline Gr	ஆ ஃார₂) >	work Members 0	Alarm Nine Offine
윤 #d8(50)	•	Total WAN VPN LAN	≗ rd8(50) >		Total WAN VPN LAN
di 149-100	rectly-under-Root Notwo	nk 0 7 7 0 0 0	å (48-1,0) →	rectly-under-Root Network 0	
🕮 💩 rd8-2(1)	>	0 0 0 0 0 0		s\$%^&*_+()*?>+/→ 0	
a rd8-3(1)	> yer2	0 0 0 0 0 0			
	arketing_carrie			orketing_carrie 0	
Part and a second	O SD-WAN	0 0 0 0 0 0		V T T A SD WAN 0	
28	() zazaza(123)	0 0 0 0 0 0		() aaaaaa(123) 0	
O and here a	* ®n3	0 2 2 0 0 0	0	Kun + 0m7 0	
and a subscription	_ @ rd8	2 48 48 0 0 0	and the second s	_ (9 rd3 2	48 48 0 0 0

3.2.7.6 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.

Auto Logout 😧
Image: Anglish ∨
🔒 Set Password
🗁 Two Factor Authentication
Manage Notification
🖉 Change Theme
[→ Logout

3.2.8 Auto Refresh, Manual Refresh, and Widget

ltem	Description
Auto Refresh	Select the time interval for refresh the web page automatically.
	Auto Refresh : 1 Minute 🗸
	1 Minute
	5 Minute
	10 Minute Disable
	Disable
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 💉 🔿 🗇
	Vetwork Overview
	Map Overview
	Clients
	Traffic
	New Devices
	Reset to default
	Available quick overviews on the dashboard will vary according to the roo network, selected group network and selected CPE.

3.2.9 Overviews

There are several types (Network Overview, Map Overview, Active Clients, Traffic, New Devices) of overview. The types will vary according to the root network, selected group network and selected CPE. Use the Widget drop menu to select or deselect the type of the overview.

Active Clients	Top 20		③ Last 24 hours ∨ = 🖉 ×	Traffic - Top 20	③ Last 24 hours ∽ =
Total 27 125 100 75 50 25 20:00	11 • Tr • Tr • 0 00:00 04:00 08:00 12:00	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 8.59 GB 1.86 GB 0 Byte 20.0000.40008.00 12.0016.00	RD3 / 172.67 GB † 29.52 GB 143.15 G RD2 / 77.24 GB † 518.84 MB 76.74 GB RD1 / 818.54 MB † 47.23 MB 771.31 N ettel / 453.14 MB † 245.69 MB 207.46
New Devices	IP Address	Device Name	- 🖉 X		RD6712946 MB 73.36 MB (30.10 MB
+	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	2912_001DAA88040C	Vigor2912		
+	192.168.11.5:443	AP 810_001DAA0F3320	VigorAP 810		
			KI < 1/45 > DI		

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.
- / 2	- (Minimize) - Hide the page.
×	x (Close) - 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.

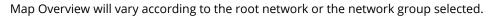
					Auto Ref	resh :	Disable	~ C	~0;
Network Overview Sub Network 123 Root Network	Alarm 100138						Q	- 、 Network	
vetwork Members	0-line		Alarm			Go To Dashboard			
Network Members	Online	Offline	Total	WAN	VPN	LAN	GO TO Da	ISNDOÀľď	
Irectly-under-Root Network	0	13	13	0	0	0			ĺ
AutoTestNetwork	0	1	3	2	0	0	8		
AutoTest_Dev	2	7	7	0	0	0	8		
AutoTest_SD-WAN	0	2	2	0	0	0	8		
AutoTest_VPN	1	0	0	0	0	0	8		
Hotspot_Web_Portal	0	2	2	0	0	0	8		
Router_App_Network	0	2	2	0	0	0	8		
T_2024-07-22_Wholesale_GA_D	0	0	0	0	0	0	8		

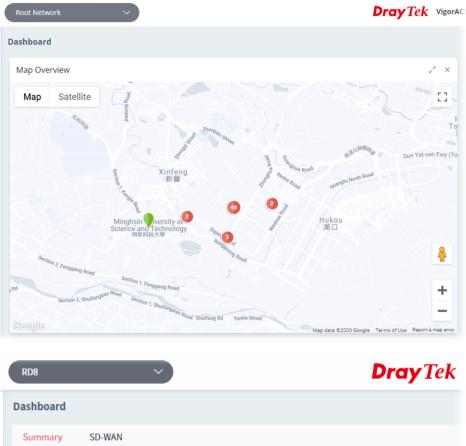
Under **Device Overview**, move the scroll bar left and right to check basic information for each device. Click >> (Next) or << (Previous) arrow to display next page for checking information for other devices.

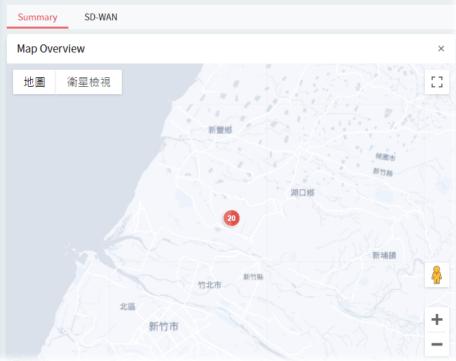
Device Name Model MAC Status UP Time Firmware Version Addition 2927Lac 1449BC023768 Vigor2927Lac 14:49:BC:02:37:68 Online 0 days 02:50:16 4.4.2.3 0 2120n 001DAA7FF2A4 stun Vigor2120n+ 00:1D:AA:7F:F2:A4 Online 41 days 20:00:29 3.8.10 0 2865Lac 1449BC3D7A08 Vigor2865Lac 14:49:BC:3D:7A:08 Offline 0 days 00:00:00 4.4.5_STD 0 2952Pn 001DAAF8D818 https Vigor2952Pn 0:1D:AA:F8:D8:18 Offline 0 days 00:00:00 3.9.7.2 0	
2120n 001DAA7FF2A4 stun Vigor2120n+ 00:1D:AA:7F:F2:A4 Online 41 days 20:00:29 3.8.10 0 2865Lac 14:49:BC:3D:7A:08 Offline 0 days 00:00:00 4.4.5_STD 0	
2865Lac 1449BC3D7A08 Vigor2865Lac 14:49:BC:3D:7A:08 Offline 0 days 00:00:00 4.4.5_STD 0	0
<u>2952Pn 001DAAF8D818 https</u> Vigor2952Pn 00:1D:AA:F8:D8:18 Offline 0 days 00:00:00 3.9.7.2 0	0
	0
<u>962P 1449BC39F110 https</u> Vigor2962P 14:49:BC:39:F1:10 Online 46 days 19:57:10 4.3.2.6 0	1
Vigor3220n 00:1D:AA:55:47:58 Offline 0 days 00:00:00 3.9.7.4 0	0
<u>VIgorAP 810 00:1D:AA:7C:2B:50</u> Offline 0 days 00:00:00 1.3.4 0	0
<u>P 902 001DAA3F150E stun</u> VigorAP 902 00:1D:AA:3F:15:0E Offline 0 days 00:00:00 1.3.4 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.



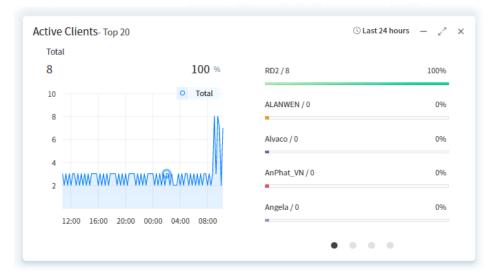




3.2.9.3 Active Clients

It is available for Group Network and CPE Device selected.

This area displays the top 10 clients or top 20 clients accessing into VigorACS 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.
- / 2	- (Collapse) - Hide the page. (Fullscreen) - Display the page in fullscreen.
×	x (Delete) - Delete this widget.

3.2.9.4 Traffic

It is available for Group Network and CPE Device selected.

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

	RD2 / 5.54 GB↑ 101.25 MB↓ 5.44 GB	100%
		15.74 -
3.26 GB O Total	ALANWEN / 0 Byte ↑ 0 Byte ↓ 0 Byte	0%
2.79 GB		
2.33 GB		00/
1.86 GB	Alvaco / 0 Byte↑ 0 Byte↓ 0 Byte	0%
1.40 GB		
53.67 MB	AnPhat_VN / 0 Byte↑ 0 Byte↓ 0 Byte	0%
76.84 MB	•	
	Angela / 0 Byte↑ 0 Byte↓ 0 Byte	0%
53.67 MB	■ AnPhat_VN / 0 Byte ↑ 0 Byte ↓ 0 Byte	

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	Nigor2926Vac
+	192.168.105.81:443	810_001DAA7D6514	2862Vac_001, 438C0
+	192.168.105.89:8442	902_001DAA3D4F16	
			Port Status
			ACT WAN2 Line Use of the second s
			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.	
H	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

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

3.3 Operation Procedure

Follow the instruction listed below to operate VigorACS 3:

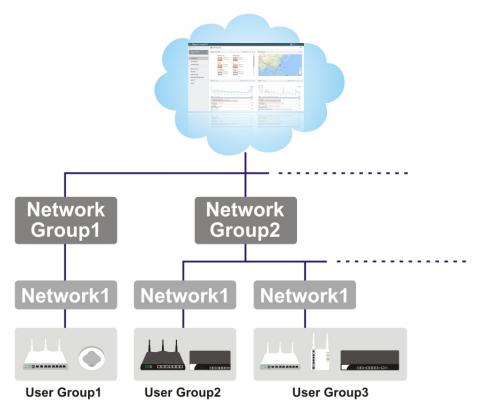
- Create networks.
- Create users and user groups.

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 Validation 	Auto-Logout on Code in Internet/LAN	Access Management Port Setup User Define Ports Defa Telnet Port
Internet Access Control Allow management from the Internet Domain name allowed FTP Server HTTP Server HTTPS Server Telnet Server Telnet Server TR069 Server		SSH Port Note: Ports 8001 and 8043 are used
 SSH Server SNMP Server Disable PING fr 	r om 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.

CS and CPE Settings	Reporting Configuration Export Parameters	
TR-069	O Disable 💿 Enable	
ACS Server On	LAN/VPN *	
ACS Server		
URL	http://192.168.1.110:8011/ACSServer/services/ACSServle Wizard	
	Acquire URL from DHCP option 43	
Username	acs	
Password		
	Test With Inform Event Code PERIODIC *	
Last Inform Response	Time :Sat Jan :(NA) 🥌	
CPE Client		
Protocol		
Protocol URL	http://192.168.1.1:8069/cwm/CRN.html	
	http://192.168.1.1:8069/cwm/CRN.html 8069	
URL		

- 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 🥌

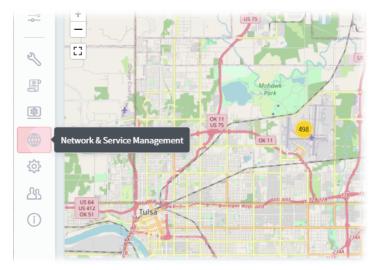
- 5. Open the homepage of VigorACS 3.
- 6. Now, Vigor2927Vac has been registered onto VigorACS 3 and displayed on the homepage.

ew Devi	ces		- 2
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
		K	1 < 1/1 > 🕅

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 & Service Management.



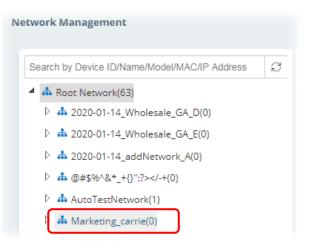
3. Select Network Management. When the following page appears, click the link of +Add New Network.

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

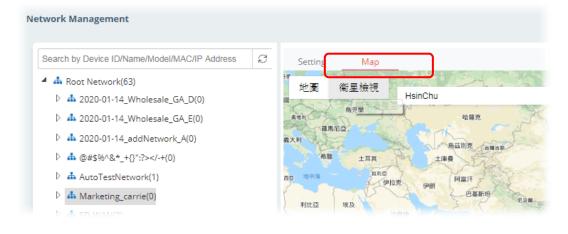
4. A pop-up window appears. Type the required information.

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.



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					Total				
27			RD2 / 14	52%	35.96 GB	↑479.24 MB	↓ 35.49 GB	RD2 / 34.04 GB † 369.37 MB ↓ 33.68 GB	95
30 25	•	MM	attel / 10	37%	3.26 GB		• Total	RD1 / 1.80 GB † 46.13 MB ↓ 1.76 GB	51
20			RD1 / 3	1196	2.33 GB			attel / 80.99 MB † 45.91 MB ↓ 35.08 MB	01
10			1111/0	096	1.40 GB			RD8 / 30.77 MB † 17.82 MB ↓ 12.95 MB	09
			ALANWEN / 0	0%	476.84 MB			1111 / 0 Byte † 0 Byte ↓ 0 Byte	09
12:00	16:00 20:00 00:00 04:00	08:00			0 Byte 12:1	00 16:00 20:00 00:0	00 04:00 08:00	•	
		08:00	•		12:	00 16:00 20:00 00:0	00 04:00 08:00	• • • •	
12:00 lew Devic		08:00	•		12:	00 16:00 20:00 00:0	00 04:00 08:00	• • • •	
lew Devic	ces		•	- 2	12:	20 16:00 20:00 00:0	00 04:00 08:00	• • • •	
lew Devic	CES IP Address	Device Name	• • •	— 🧳 Device Type	12:	DO 16:00 20:00 00:0	20 04:00 08:00	• • • •	
Action	IP Address 172.17.5.151:4433	Device Name 3910_001DA	• • • • • • • • • • • • • • • • • • •	- Z Device Type Vigor 3910	12:	20 16:00 20:00 00:0	00 04:00 08:00	• • • •	
Action	IP Address 172,17,5,151:4433 14,161,2,165:443	Device Name 3910_001DA 2912Fn_0011	AA18E740 DAA8C0F0C AA87FAE4	Device Type Vigor3910 Vigor2912Fn	12:	00 16:00 20:00 00:0	20 04:00 08:00	• • • •	

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

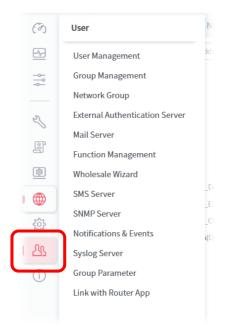
+ Add New Device			×
Add to Network	Root Network		Q
Device name:	3910_001DAA18E740		
Location:			
Emergency phone:			
Set to known device:			
		Cancel	✓ Apply

- 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.

Jser / Group Management						
Setting	Management	UI Customization				
+Add 💼						
+Add 🖄	Delete l≌ Export Group ID ↓↑		J↑ Max Nodes	↓↑ Used Nodes	$\downarrow\uparrow$ Enable Expire Date	

RootGroup is a default setting.

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

User / Group Management				C
Setting Management UI Customizatio	n			
Add Group				
Group name	Marketing2024		~	
Nodes	10 (-1: No Limit Nodes)]	~	
Enable CPE Notify Mail/SMS/SNMP				
Enable Global Mail Server				
Enable Global SNMP Server				
Enable Expire Date				
Expire Date	2024/08/31			
				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.

Jser / Group Management						
Setting Management UI Customization						
+Add [@] De						
	Group ID ↓↑	Group Name	$\downarrow\uparrow$	Max Nodes 41	Used Nodes	Enable Expire Date
	1	RootGroup		200	120.5	Disabled
	2	Marketing2024	٦	No Limit Nodes	12	Disabled

Part II

SD-WAN



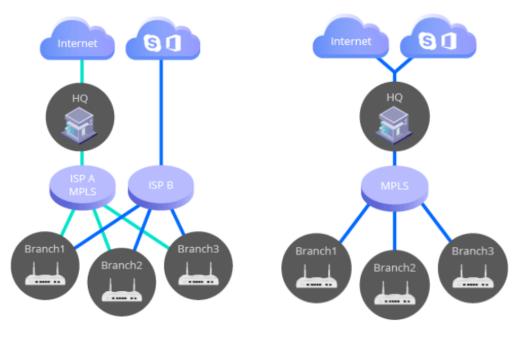
Chapter 4 SD-WAN Solution

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.

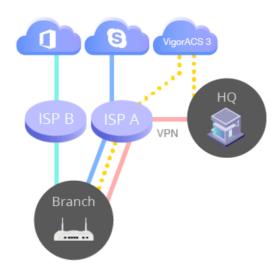


Direct Internet Access with lower cost

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 & Service 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 Vigor	ACS 3	pture Packets ~ mk_team_1 System Administrator
1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	Root Network	Network ID 8 Name draytek_rd8 Location	Username draytek_rd8 Password	
E ■ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		Advanced Settings Enable SD-WAN Enable SD-WAN ENABLY Settings Set the category of data to be collected for statistical analy corresponding profile, and specify the report interval at wf WAN operation.		
	聞Delete Devices	Profile #1 Enable Pro Report Interval (sec) Rep 120 30 Bulk Data Categories Bulk	k Data Categories El Users and Apps Size: 4	Avallable / Disabled Bulk Data Categories

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

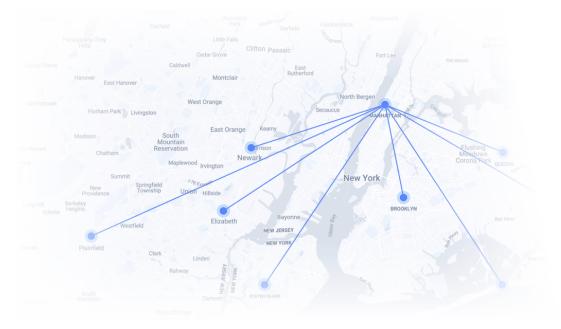
- Auto VPN
- VoIP WAN, and
- Full Traffic Control with SD-WAN Route Policy

4.1.2 Auto VPN

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

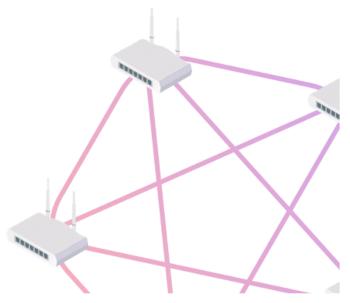
• For Hub and Spoke(s)

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

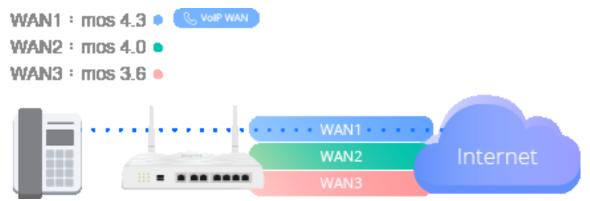
VigorACS server will create tunnels between each router automatically. If a subnet conflict occurs, VigorACS server is capable to design and suggest LAN subnets for all devices.



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

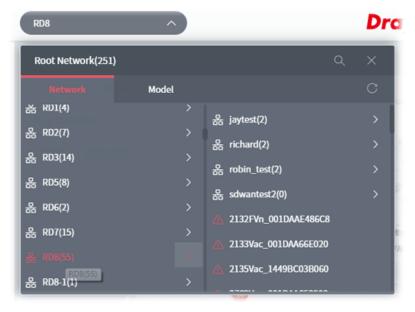
SD-WAN provides complete routing control by allowing Network Admin to specify the desired route for selected applications/domains to make sure the specific routing scenarios can be accomplished.

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

	_				
Enable					
Comment	For_MKT_education				
Source	Any			~	
Destination	App Services			~].
App Service Profile	Create a new profile	From an existing	g profile		
Selected App Service	WhatsApp (8)				٦.
Send via Interface ① Note If you want to send via VPN	WAN 1 (to the Hub), please of	iial VPN Hub and S	Spoke conn	~ lection	
(i) Note	WAN 1 (to the Hub), please of	Jial VPN Hub and S	Spoke conn		
③ Note If you want to send via VPN	WAN 1 (to the Hub), please of	iial VPN Hub and S Specific Gateway	Spoke conn		
① Note If you want to send via VPN first. Go to SD-WAN VPN Set	WAN 1 (to the Hub), please of tings Default Gateway		Spoke conn		
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway	WAN 1 (to the Hub), please of tings Default Gateway	Specific Gateway	Spoke conn		
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway Packet Forwarding to WAN/LAN	WAN 1 (to the Hub), please of tings Default Gateway	Specific Gateway	Spoke conn		
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway Packet Forwarding to WAN/LAN via	WAN 1 (to the Hub), please of tings Default Gateway	Specific Gateway	Spoke conn		

4.2 Dashboard for SD-WAN Network Group

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



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

0	Dashboard		\bigcirc Auto Refresh: $\$ 5 minutes \checkmark
<u>lat</u>	Summary SD-WAN		
11+ EB	Wirdwan O 24 hrs Wireless Walt O 7 days	IPsec VPN 024 hrs Other VPN 024 hrs	VolP (O 7 days
-	Average MOS MOS Compliancy No Data	Average MOS MOS Compliancy No Data	Average MOS MOS Compliancy 3.9 33 % > 40
<u> </u>	3.2 26 % ≥ 4.0	3.4 31 % ≥ 4.0	
2	~ 3.2 ~ 20%	~ 3.4 ~ 31%	
Ē	Active Physical WAN	Active VPN	Active VoIP Call _ Detected 67117 _ Failovered 33451
۲	• Wired 10	• IPSec 9	Last 1 hour
	10 • Wireless 2.4G / 5G 0	9 • SSL 0	
	WAN Online LTE 0	VPN Online L2TP 0	
©	• USB 0	• PPTP 0	0 0 225 pm 2.35 pm 2.45 pm 2.55 pm 3.05 pm 3.15 pm
28			אין פרג אין פר
0	Active Physical WAN Quality	Active VPN Quality	Active Call Quality
	Great 4.3-5.0 2	Great 4.3-5.0 3	Great 4.3~5.0 + 360
	Good 4.0~4.2 0	Good 4.0~4.2 1	Good 4.0-4.2 30098
	Okay 3.6~3.9 1	Okay 3.6-3.9 1	Okay 3.6-3.9 36513
	Poor 3.1-3.5 2 Bad 1.0-3.0 5	Poor 3.1~3.5 0 Bad 1.0~3.0 4	Poor 3.1~3.5 146 Bad 1.0~3.0 0
	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_001DMA000001,2552Pn_001DAA000007 5 Routers are Having Bad Active Physical WAN Quality. 2952Pn_001DMA00009,2552Pn_001DMA00008,2552Pn_00	4 Tunnels are Having Bad Acthe VPN Quality. 2952Pn_001DA4000009,2952Pn_001DA4000008,2952Pn_00…	10 Routers are Having Poor Active Call Quality. 2952Pn_001DA4000009, 2952Pn_001DA4000008, 2952Pn_00
	More	More	More
1			
1			
(

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 VPN	Displays the quality levels (Great, Good, Okay, Poor and Bad) for active 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.

					-,	
atistics						
Last 24 Hours Last 7 Days Last 30	Days Custom Start: 2020/03/08 E	ind: 2020/03/09				Export
Jsage Overview (.)		- 2 ×	Wireless Clients Overview ()			- 2
Total Number of Clients		ed Clients 50%)				
Total amount of Traffic 270.79 MB	Download Uple 254.05 MB (93.8%) 16	75 MB (6.2%)	Band	SSID	os	
Max. Number of Concurrent Client 2	Avg. Number of Hourly C 1	lient 🕅	100.0%	100.0%	Android iOS	Windows
ients		- 2 ×	Traffic	■ 2320-mk-angela-2		- 2
	Ow	fired OWireless O 2.4G O 5G	Trame		OWired OWireless	
2			190.73 MB		Wired O Wireless (1
1			143.05 MB			
		WVV	47.68 MB		. /	
0 16:00 18:00 20:00 2	22:00 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 04:0	00 06:00 08:00 10:00	12:00 14:00
Device Ranking 🔅		≡Client • - 🖉 ×	Client Ranking {,}		≡Tri	affic 🔹 — 🏒
Device	J↑ MAC	↓↑ Client ↓↑	Host Name	J↑ MAC	4↑ Traffic	\$1
	001DAA000000	1	1 MKHL	406C8F525BFF	269.83 MB (99.6%)	
1 2865ac_001DAA000000	001 DAA000000					

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.

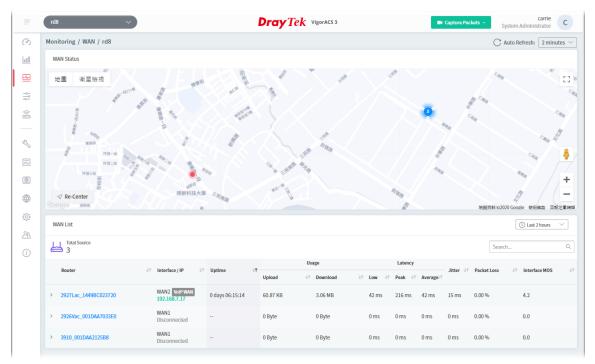
(7)	Monitoring	
1 600	Alarm	
	Logs	
	Devices	e to
~	Clients	
	Cellular Data Usage	N B
	Floor Plan	
Z	Rogue AP Detection	
F	WAN (SD-WAN)	
\$	VPN (SD-WAN)	
<u></u>	VoIP (SD-WAN)	
	Data Usage (SD-WAN)	

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)

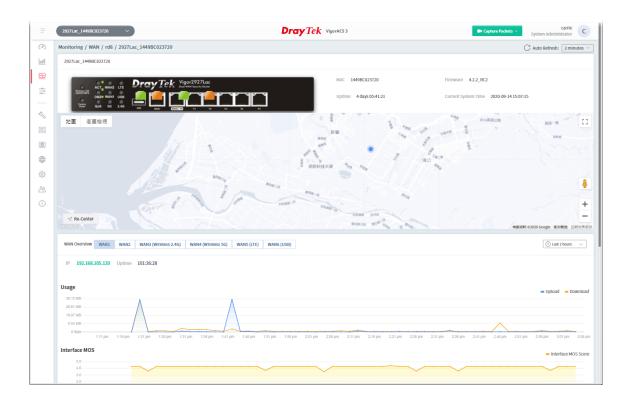
This page displays the location, name, interface/IP, uptime, usage, latency, jitter, packet loss and interface MOS of the routers within the group.



These parameters are explained as follows:

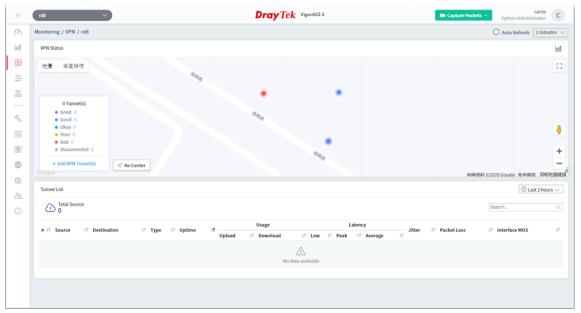
ltem	Description
WAN Status	Displays the location of the network group.
WAN List	Displays the total number of CPEs within the selected group.

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:



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) ⊗ 2927Lac_1449BC0237E8 (Vigor2927Lac) ⊗							
	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.

rd8 V	Dray Tek VigorACS 3	Capture Packets Capture Pack
	Creating VPN Hub and Spoke Connections Please wait for a while.	
	Succeed: 0 Processing: 0 Walting: 0 Falled: 0 + Show Details	

- 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.

VPN Setup	×
Туре	Hub and Spoke Full Mesh
Hub Devices	2927Lac_1449BC023720 (Vigor2927Lac) ③
Support spokes count	64
	+ Advanced Mode
	x Cancel Save and set to CPEs

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	2927Lac_1449BC0237E8 (Vigor2927Lac) ③
VPN Connection Through	WAN1 First ~
Dial Type	IPsec Tunnel PPTP L2TP SSL
IPsec	
Customize IKE Pre-Shared Key	
IKE Pre-Shared Key	Required, Please input IKE Pre-Shared Key (1988)
IPSec Security Mathod	AES v
	— Basic Mode
	× Cancel Save and set to CPEs

These parameters for Advanced Mode are explained as follows:

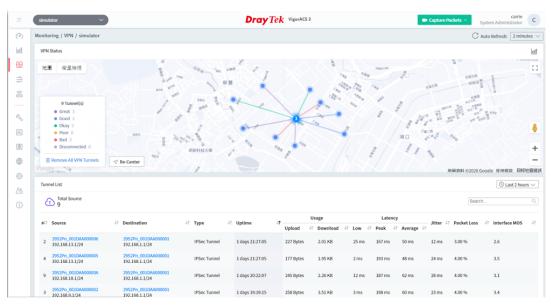
ltem	Description
Spoke Devices	Lists the name of the devices. Select one device as the spoke device.

VPN Connection	Select a WAN interface.									
Through	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.									
	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									
PPTP - PPTP is sele	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 v
	VJ Compression
L2TP - L2TP is select	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 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 🐵
	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.

simulator			Dray1	Tek VigorACS 3			-	Capture Pa	ckets ~ s	carrie System Administrator
Monitoring / VPN / simulator									C	Auto Refresh: 2 minu
Sankey Diagram										
2952Pn_001DAA0000	12									
2952Pn_001DAA0000	13									
2952Pn_001DAA0000	м									
2952Pn_001DAA0000	19				2952Pr 5.28 KB	_001DAA00000A → 2	952Pn_001DAA	000001	295	2Pn_001DAA000001
2952Pn_001DAA0000	18				5.20 10					
2952Pn_001DAA0000	16									
2952Pn_001DAA0000	14									
2952Pn_001DAA0000	07									
	07									
2952Pn_001DAA0000	07									C Last 2 hou
2952Pn_001DAA0000 2952Pn_001DAA0000	07								Search	C Last 2 hou
2952Pn_001DA40000 2952Pn_001DA40000 Tunnel List 0 Total Source 9	77	22 Tone	27 Untine	+ Us	age	Latens	у	litter 12		h
2952Pn_001DAA0000 2952Pn_001DAA0000 Tunnel List	07	J↑ Type	라 Uptime	JT		Latens	,	- Jitter ↓↑	Search Packet Loss	
2952Pn_001DA40000 2952Pn_001DA40000 Tunnel List 0 Total Source 9	77	라 Type IPSec Tunnel	년 Uptime 1 days 21:38:28	JT	Download 41		,	- Jitter J† 12 ms		h
2952Pn_001DA40000 2952Pn_001DA40000 Tunnel List 9 f* Source 2952Pn_001DA400000	77 55 47 Destination 2952Pn_001DAA000001			Upload 41	Download 41 4.34 KB	Low 🕸 Peak	↑ Average ↓↑		Packet Loss	h ↓↑ Interface MOS
295791; 0010A40000 295791; 0010A40000 Tunnel List 0 9 #1* Source 2 2952791; 0010A400006 2 2952791; 0010A400006 2 2952791; 0010A400006 2 2952791; 0010A400006 2 2952791; 0010A400007	27 5 47 Destination 295207, 00104000001 1952108.11/24 2953270, 00104000001	IPSec Tunnel	1 days 21:38:28	496 Bytes	Download 41 4.34 KB 2.21 KB	Low 41 Peak 4	↑ Average ↓↑ 47 ms	12 ms	Packet Loss	J↑ Interface MOS 3.1

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.

VPN Overview													(S Las	t 2 hours 🗸
Search VPN Tunnel List	Q, T	o 2952Pn_001DAA0	00003 IP	192.168.105.52										
Total 1 To 2952Pn_001DAA00000 192.168.105.52	02	Usage 000 Byres											Upload =[ownload
2 To 2952Pn_001DAA00000 192.168.105.52	03	400 Bytes 200 Bytes												
3 To 2952Pn_001DAA0000	04	0 Byte	1:28 pm	1:30 pm	1:45 pm	1:58 pm	2:08 pm	2:16 pm	2:26 pm	2:30 pm	2:46 pm	2:50 pm	3:00 pm	3:16 pm
4 To 2952Pn_001DAA0000	05	5.0 4.0											Interface M	IOS Score
5 To 2952Pn_001DAA0000	06	3.0 2.0											L	
6 To 2952Pn_001DAA0000		0.0	1:28 pm	1:30 pm	1:45 pm	1:58 pm	2:00 pm	2:10 pm	2:28 pm	2:38 pm	2:45 pm	2:50 pm	3.00 pm	3:10 pm
7 To 2952Pn_001DAA0000		Latency (ms)											Low – Average	Peak
. To 2952Pn 001DAA0000	09	150 ms 100 ms												
		🕓 Last 2 ho	urs 🗸											
	Last 1 hour													
	Last 2 hour		~											
	Last 3 hour													
1 Decket Less	Last 6 hour													
Packet Loss L	Last 8 hour	s												

4.4.3 VoIP (SD-WAN)

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

onito	oring / Vol	P / simulator												C
/oIP (Call List												Last 2 hou	irs 🗸
(1414 Total	11 • Great 5.0~4.3		3.9 ~ 3.6		0 • Bad 1.0 ~ 1.0				Rows	5 10 ×	KI < 1	/160 >	N 8
										Latency				
*	Status ↓↑	LAN IP 4	1 Peer IP	↓↑ Call ID↓1	Via Interface	↓↑ Start Time	↓↑ Failovered Interfac	:e ↓↑ Up Time ↓↑	Low $\downarrow \uparrow$	Peak 41	Average		Packet Loss ↓1	MOS
1	ß	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
2	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
3	6	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
4	6	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
5	6	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

These parameters are explained as follows:

Custom..

4.0

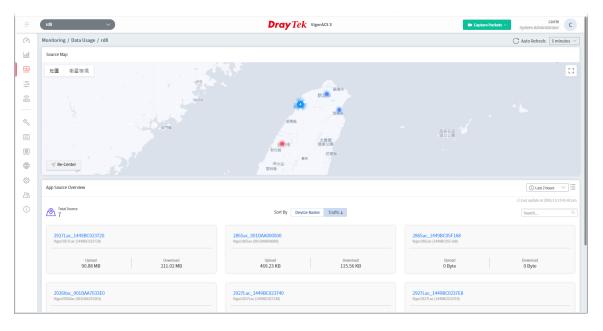
3.00 %

2.00 %

ltem	Description
Great, Good, Okay, Poor, Bad	All the VoIP calls will be separated with different levels according to its quality.
Q	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)



4.4.4.1 Data Usage of Selected CPE

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

	2927Lac_1449BC023720 V	Dray Tek VigorACS 3		E Captur	re Packets v C System Administrator
(⁷)	Monitoring / Data Usage / rd8 / 2927Lac_1449BC023720				\bigcirc Auto Refresh: $\$ 5 minutes \checkmark
100	2927Lac_14498C023720				(i) Last update at 2020/11/13 01:43 pm.
<u>6</u>	Usage Sorting by Application Client Device				🕓 Last 2 hours 🗸 🗸
	TOTAL Search Category or App Q.				
2					
1		Protocol	211.43 MB	 Others 	51.66 MB
		 Instant Message 	24.78 MB	VolP	7.13 MB
	Total 301.89	Apple Services	2.17 MB	 Google Services 	2.17 MB
	501.09 MB	Stream	1.44 MB	Tunneling	928.10 KB
(2)		 Web HD 	195.62 KB	 Remote Control 	3.45 KB
යින					
(i)					
	Traffic Line Chart Upload/Download By Interface				
					💻 Upload 🛛 💻 Download
	38. 15 MB				
	28.61 MB 10.07 MB				
	9.54 MB				
	0 Byte 11:45 am 11:50 am 11:55 am 12:00 pm 12:05 pm 12:10 pm 12:15 pm 12:20 pm 12:25	pm 12:30 pm 12:35 pm 12:40 pm 12:45 pm 12:50 pm	12:55 pm 1:00 pm 1:05 pm 1:10 p	m 1:15 pm 1:20 pm 1:25	pm 1:30 pm 1:35 pm 1:40 pm 1:45 pm
	Harry Haller Application Climb Davids				
	Usage List by Application Client Device				

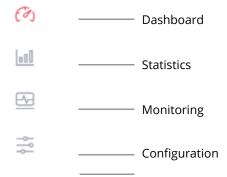
These parameters are explained as follows:

ltem	Description								
Usage Sorting by	Displays a pie chart related	l to various applica	ition usage.						
	Application - Click to display a pie chart for various application								
	Client Device - Click to display a pie chart for the selected CPE.								
Traffic Line Chart	Displays a line chart related to data upload/download, or traffic via the WAN interface.								
	Upload/Download - Click to	o display data uplo	ad/download.						
	By Interface - Click to displainterface.	ay a line chart relat	ted to traffic via th	e WAN					
Usage List by	Displays the data usage for	r common Apps or	for connected clie	ent.					
	Application Click to displa	wtho data informa	ition related to var	rious					
	Application - Click to displa applications, including nan download usage.	-							
	applications, including nan download usage.	-		pload and System Administrator					
	applications, including nan download usage.	ne of application, n		pload and					
	applications, including nam download usage.	ne of application, n		spitom Administration					
	applications, including nam download usage.	e of application, n DrayTek WardS3	2823100 ● Others 5.09108 ● Others 5.09108 ● Tomeling 101.040 ● YuP	pload and optime for the former C Anto Reference To C C Anto Refe					
	applications, including nam download usage.	 Флар об аррисаtion, п Dray Tek ченса Флар Тek ченса Флар бенса <	2823100 ● Others 5.09108 ● Others 5.09108 ● Tomeling 101.040 ● YuP	And Index and Control of Control					

	affic Line Cha	art Upload/Download	By interface						
	20.01 M3							- WANI	WAN2
	19.07 M3							\sim	
	0.54 MB								
	0 Byte 12:50 pm	12.55 pm 1.00 pm 1.05	5pm 1:10pm 1:1	5pm 120pm 125pm 130p	m 1.35.pm 1.40.pm 1.45.pm 1:	50 pm 1.55 pm 2.00	pm 2:05 pm 2:10 p	pm 2:15 pm 2:20 pm 2:25 pm 2:30 pm 2:35 pm 2:40 pm 2:45 pm	n 2.50 pm
Us	age List by	Application Client Devi	ice						
								Usage	
				10					
	# 41 Host	Name 41 IP A	Address	41 MAC Address	41 Connection Type	41 OS 41	Upload	41 Download	41
	# 4° Host		Address	41 MAC Address 8C85902C6662	Connection Type Wireless (5G)	41 OS 41	Upload 108 Bytes		11
		1-MBP 192					Upload	at Download	11
	1 adam	n-MBP 192. Iown 192	.168.124.12	8C85902C6662	⊕Wireless (56)	Ø	Upload 108 Bytes	U Download 132 Bytes	40
	1 adam 2 Unkn	1-MBP 192 Iowin 192 0675 192	168.124.12	8C85902C6662 00507F393EB2	약 Wireless (5G) 옰 Wired	0	Upload 108 Bytes 3.92 KB	Ut Download 132 Bytes 2.14 KB	11
	1 adam 2 Unkn 3 R100	-MBP 192 iown 192 0675 192 -IPhone 192	168.124.12 168.124.20 168.124.10	8C85902C6662 00507F393E82 88D7F656F799	Wireless (5G) 욼 Wired 욼 Wired	0	Upload 108 Bytes 3.92 KB 10.01 MB	07 Download 132 Bytes 2.14 KB 4.44 MB 144 MB	11

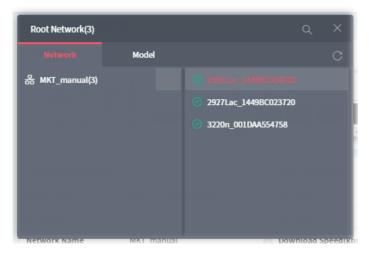
Chapter 5 SD-WAN CPE

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.



Dray Tek vig	orACS 3	2865Vac_14	49BC34FE98	C C Pcap P 11:47:29 mk_car 7/23/24 System Administra
2865Vac_1449BC34	FE98			Device Status: O Online Alarms: 0 Active Clients: 0 Auto Refresh: Disable
Port Status				WAN Overview ©Last 24
ACT WANZ Winternite USB DSL P Party Stany 2.40 50 P	Cos Drocy Tele Vigor hone: hone: bone: use use use use use use use use use use	865Vac	en Paret	781.25 KB 585.94 KB 390.63 KB 195.31 KB
Device Information	n	DSL Information		0 Byte 12:00 16:00 20:00 00:00 04:00 08:00
Device Name	2865Vac_1449BC34FE98	DSL Status	TRAINING	Total (↑2.69 MB ↓22.10 MB)
IP Address	http://192.168.106.141:80	DSL Type	VDSL2	WAN1 (↑0 Byte ↓0 Byte)
Network Name	AutoTest_VPN	Download Speed(kbps)	0	WAN2 (↑2.69 MB ↓22.10 MB)
Model	Vigor2865Vac 🤣	Upload Speed(kbps)	0	WAN3 (↑0 Byte ↓0 Byte)
Firmware Version	4.4.2_STD 😒	SNR Margin	0	WAN4 (↑0 Byte ↓0 Byte)
MAC Address	14:49:BC:34:FE:98	Loop Attenuation(0.1dB)	0	WAN5 (↑0 Byte ↓0 Byte)
Up Time	95 days 18:42:09	CRC Errors	0	WAN6 (↑0 Byte ↓0 Byte)
4	show more		~ show more	" WAN ∔↑ Line/Mode ↓↑ IP ↓↑ Uptime ↓↑ Active Mor

WAN4 Wireless_5G / ---

WAN5 USB/---

WAN6 USB/---

LAN Overview

1

100% 75% 50% 25% 0%

 $\label{eq:constraint} Id \quad {\downarrow}\uparrow \quad Start Time \qquad {\downarrow}\uparrow \quad Clear Time \qquad {\downarrow}\uparrow \quad Type \quad {\downarrow}\uparrow \quad Message \qquad {\downarrow}\uparrow$

No data available

15:20 20:40

02:00 07:20

15% 10% 5% 0%

Connectivity and Alerts

15:20 20:40 02:00 07:20

0d 00h 00m

0d 00h 00m

0d 00h 00m

Always On

Always On

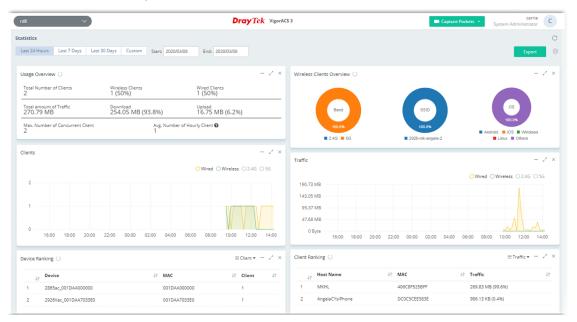
Always On

Active Clients

() Last 24 hours

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 Vigor2927Vac/Vigor2865ac series as an example.

(7)	Monitoring	
1 600	Alarm	:3
	Logs	
	WAN (SD-WAN)	re
	VPN (SD-WAN)	1
E.	VoIP (SD-WAN)	w B
	Data Usage (SD-WAN)	_

5.3.1 Alarm

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

ray	Tek vi	gorACS 3		2927Vac_1449B0	22C438_101.1	✓ Q		Pcap	¢ P	11:59:38 7/23/24 Syste	mk_carr m Administra	
Monito	ring / Aları	m						2024/06/23 to 2024/	07/23 ~	Search No. / D	evice Name	/MAC C
Alarm	• н	Istory										
	te 🛱 Dele	te All	ownload						Ы	< 1 /1	> D	C
	No.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm T	ype	Ack Time	Ack Us
	37554252	Not Ack	2024/07/23 05:29:34	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	🛦 Critical	Device Loss Connection	Device	Lost Connection		

ray	/ Tek vig	orACS 3	2927Vac_14498	3C22C438_101.1	Q	Pa	12	2:01:14 mk_carrle M 7/23/24 System Administrator
Monit	oring / Alarn	n				2024/06/23 to 20	24/07/23 ~	Search No. / Device Name / MAC Q
Alarr	n 🚹 🛛 His	story						
	ete 🔮 Delet	e All 🕹 Download					М < 1	/2 > ▷ ℃ ⊗
	No.	Time	Device Name	Network Name	MAC Address	Clear Time	Alarm Level	Alarm Message
	37465460	2024/07/22 05:26:06	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/23 05:03:49	\Lambda Critical	Device Loss Connection
	37364051	2024/07/21 05:26:03	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/22 05:03:48	\Lambda Critical	Device Loss Connection
	37252574	2024/07/20 05:28:51	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/21 05:03:42	\Lambda Critical	Device Loss Connection
	37215739	2024/07/19 05:36:55	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/20 05:04:08	\Lambda Critical	Device Loss Connection
	37052935	2024/07/18 05:28:57	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/19 05:03:47	🛦 Critical	Device Loss Connection
	36953229	2024/07/17 05:28:53	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/18 05:03:43	\land Critical	Device Loss Connection
	36915323	2024/07/16 17:16:51	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/17 05:04:13	🛦 Critical	Device Loss 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.

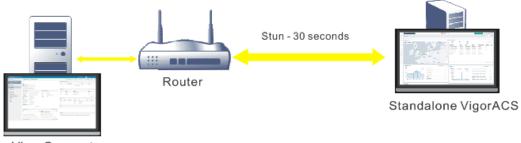
₹	Dr	ay	Tek	/igorACS 3		2865Vac_1449BC34FE98	✓ Q		Pcap	13:11:0 7/23/2		М
(7)	м	Ionitor	ing / Log	gs				202	24/06/23 to 2024/07	r∕23∨ sear	ch ID / Device Name / Device	e Q
	-	All CPE		Device Reboot Reboot By CPE Add Object Delete Object	Reset System Pass	word Set Parameter	File Transfer Setting Pro	file Device Syslog	CPE Notify	Device Register	Device Operate	
			e 🛱 Del	lete All 🕹 Download					12	< 1	/17 → ▷ C	۲
 E2			ID	Device Name	Device ID	MAC Address	Current IP	Logged IP	Action	Action ID	Time	
드랬			212081	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 12:36:41	
Z			212080	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 10:51:39	
			212041	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:21:33	
\$			212038	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:06:31	
			212035	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:00:13	
\$			212034	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 16:36:19	
4			212023	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 14:21:17	
(j)			212000	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 08:51:13	
			211998	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 08:36:13	
			211965	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 05:06:09	
			211962	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 05:00:15	
			211955	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/21 20:36:00	
			211938	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/21 16:35:57	

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

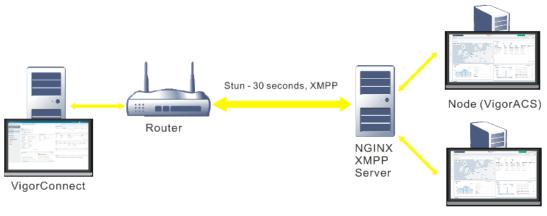
Vigor router adopts the function of NetFlow to collect the quantity and data of incoming and outgoing packets. With analysis of the collected data, the network administrator can get the source and destination IPs of the packets, type of network service, and the reason for network congestion.

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

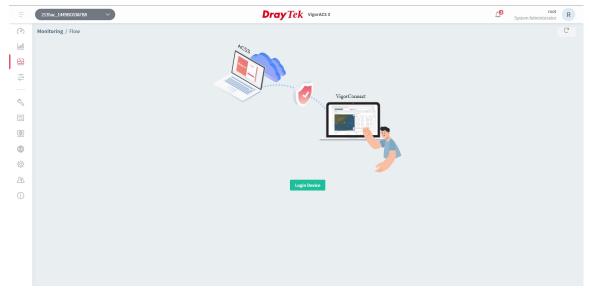


VigorConnect

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

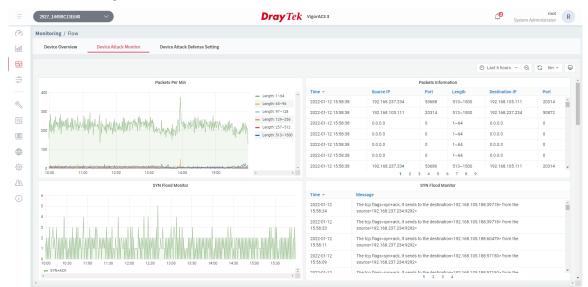
NetFlow uses several types of data to identify the data flow, for example, source IP address, destination IP address, source port number, destination port number, IP protocol, interface, and so on.

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

	2927_1449BC13E640 V	Dray Tek	VigorACS 3	System Administrator
(7)	Monitoring / Flow			
000	Device Overview Device Attack Monitor Device Attack Defe	nse Setting		
	Inspect_SourceIP 102.168.237.234 - Inspect_DestIP 102.168.237.234 -			⑦ Last 6 hours × Q ℃ 5m × ₽
	Top 10 Destinations From 192.168.	237.234	Top 10 Sources To 192.168.23	7.234
2	Destination IP	Usage ~	Source IP	Usage 👻
	192.168.105.111	947.7 kB	192.168.105.180	1.7 MB
	192.168.105.180	842.0 kB	192.168.105.111	1.4 MB
\$	192.168.105.238	139.3 kB	192.168.105.188	296.6 kB
_	192.168.105.188	125.3 kB	192.168.105.238	73.0 kB
	192.168.105.235	8.3 kB	192.168.105.235	0 B
<u>{ô</u> }	8.8.8	6.6 kB	192.168.105.234	0 B
28	192.168.105.234	4.1 kB	8.8.8.8	0 B
255	224.0.0.251	0.8	224.0.0.251	0.8
()	Flow Usage	DownStream 3.5 MB UpStream 3.1 MB	L3 Protocol Visit Rate	UDP 72.8% TOP 22.2% Others 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_1449BC13E640 ~	Dray Tek Vigoracs 3	٢	root System Administrator	R
(?)	Monitoring / Flow				
000	Device Overview Device Attac	ck Monitor Device Attack Defense Setting			
	Device Upstream Flow				
	Enable	\bigcirc			
Z	Frequency	30 min 🗸			
	Volume	1 GB ~			
<u>\$</u>					
۲	Device Downstream Flow				
ζĝ}	Enable	\bigcirc			
쓰	Frequency	30 min v			
(i)	Volume	1 GB ~			
	Inspect Source Flow				
	Enable	\bigcirc			
	Frequency	30 min ~			
					Save

ltem	Description
Device Upstream	Flow / Device Downstream Flow
Enable	Switch the toggle to enable the function of monitoring all upstream flow / downstream flow via this router. - means "Enable". - means "Disable".
Frequency	Set the timeout value.
Volume	Set the threshold value.
12.5 MB	- 1921 43.272 24 23.0 48 - 1921 43.272 25 35 - 1921 43.272 25 - 1921 43.472 25 - 1921 43.474 25 - 1921 43.474 28 -
0 B	1130 1200 1230 1300 1330 1400 1430 1500 1530 1600
35 MB 30 MB 25 MB	Top 10 Up50team Usage EMP +
20 M8	- 192146146220 421146 - 1921662320 421146 - 1921662320 492146 - 19216620 922146 - 1921661001 222146 - 1921661001 222146 - 1921661001 222146
10:30 11:00	1130 1200 1200 1300 1300 1300 1400 1430 1800 1800
Enable	Switch the toggle to enable the function of monitoring the data flow for specified source IP / destination IP.

Frequency	Set the	Set the timeout value.					
Volume	Set the	e threshold va	lue.				
See the following e	example figure	5					
Monitoring / Flow Device Overview Device Attack Monitor	Device Attack Defense Setting						
				② Last 6 hours ∨ Q 🖏 5m ∨ 📮			
Inspect_SourceIP 192.168.237.234 - Inspect_Deat	IP 192.168.237.234 ~			C contentions C, C oni B			
Destination IP	Top 10 Destinations From 192.168.237.234	sage v	Source IP	Top 10 Sources To 192.168.237.234 Usage v			
192.168.105.111	3	4.1 MB	192.168.105.230	227.5 MB			
192.168.105.230		2.1 MB 35.0 kB	192.168.105.111 192.168.105.188	3.6 MB 2.2 MB			
192.168.105.238	9	0.0 kB	192.168.105.238	69.6 kB			
192.168.105.235 8.8.8.8		7 kB 6 kB	192.168.105.235	08			
192.168.105.234		7 kB	8.8.8	0.8			
224.0.0.251	n	R	224 0 0 251	ne.			
APP Flow							
Enable			enable the functi APPs via the rou	ion of monitoring the data flow uter.			
Frequency	Set the	e timeout valu	e.				
Volume	Set the	e threshold va	lue.				
SYN Flood							
Enable	Switch	the toggle to	enable the funct	ion of monitoring SYN flood defense.			
	router as def router The de	 When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources. The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively. 					
Frequency	Set the	e timeout valu	e.				
Volume	Set the	e threshold va	lue.				
ICMP Flood							
Enable	When router as def	the arrival rate will start to ra ined in Timeou	e of ICMP packet indomly discard ⁻ it.	ion of monitoring ICMP flood defense s exceeds the Threshold value, the TCP SYN packets for a period of time			
) seconds, resp		imeout are 250 packets per second			
Frequency	Set the	e timeout valu	e.				
Volume	Set the	e threshold va	lue.				
UDP Flood							
Enable	When router	the arrival rate	e of UDP packets indomly discard	ion of monitoring UDP flood defense. exceeds the Threshold value, the TCP SYN packets for a period of time			
		efault values o) seconds, res _l		imeout are 2000 packets per second			
Frequency	Set the	e timeout valu	e.				
Volume	Set the	e threshold va	lue.				

Land Flood	
Enable	Switch the toggle to enable the function of 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 / Diag	nostics	
Plog	Protocol	IPV4	~
Trace Route	Ping Through	Auto	~
Routing Table	Ping To	DN5-8.8.8.8	~
DHCP Table	Source IP	Auto	~
Sessions Table	IP Address	8.8.8.8	
		on't want to specify which WAN to ping through, p III III Source IP according to the interface you ping	

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	Туре	IPV4 IPV5	
Trace Route	Trace through	WANI	
Routing Table	Protocol	ICMP UDP	
ARP Table DHCP Table	IP Address / Domain		
Sessions Table			
		Ru	
	l		

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.

← Conliguration	2865ac_001DAA000000	2865ac_001DAA000000 / Monitoring / Diagnostics						
Ping	IPv4 Routing Table							
Trace Route	Index Destin	nation	Subnet Mask		Gateway		Key	Iface
	1 0.0.0	0	0.0.00		192.168.105.1			WAN2
	2 192.1	68.105.0	255.255.255.0		directly connected		с	WAN2
ARP Table	3 192.1	68.10.0	255.255.255.255		192.168.1.2		S~	LAN1
DHCP Table	4 192.1	68.1.0	255.255.255.0		directly connected		C~	LAN1
Sessions Table	5 211.1	00.88.0	255.255.255.255		192.168.1.3		S~	LAN1
	Key C: Connected IPv6 Routing Table Show Detail		': default ~: private B:	BGP				
	Destination	Prefix Length		Interface	Flags	Metric	Next Hop	
	FE80::	64		LAN1	U	256		
	FE80::	64		LAN2	U	256	=	
	FE80::	64		LAN3	U	256	=	
	FE80::	64		LAN4	U	256	=	
	FE80::	64		LAN5	U	256	=	
	FE80::	64		LAN6	U	256	=	
	FE80::	64		LAN7	U	256	=	
	FE80::	64		LAN8	U	256	-	
	FE80::	64		DMZ	U	256	=	
	FF00::	8		LAN1	U	256	=	
	FF00::	8		LAN2	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		
	🖯 Clea	r										
Trace Route	LAN	WAN										
Routing Table	Show	LAN		ALL LANS	~							
	Show	/I AN		ALL VLANS	~							
DHCP Table	SHOW	(LAR		ALL VLANS	Ŷ							
Sessions Table	Index	IP N	AC Address	HOST ID	Interface	VLAN	Port	Device	Description	Comment		
	15	192.168.1.10 1	8-D6-C7-01-A2-34	R1000675	LAN1		P3					
 Configuration Ping Trace Route Routing Table ASP Table 	2865ac	ar WAN) / Monitoring / Diag	gnostics ALL WANS	v					c		
Ping Trace Route	Clea	ar WAN	0 / Monitoring / Diag			VLAN	Port	Device	Description	Comment		
Ping Trace Route Routing Table ARP Table	Clear LAN Show	sr I <u>WAN</u> WAN	MAC Address	ALL WANS		VLAN	Port	Device	Description			
Ping Trace Route Routing Table ARP Table DHCP Table	Clea LAN Show	ar WAN WAN	MAC Address 00-1D-AA-F8-D8-19	ALL WANS	ID Interface		Port 	Device	Description			
Ping Trace Route Routing Table ARP Table DHCP Table	Clear LAN Show Index 1	WAN I WAN IP 192.168.105.52	MAC Address 00-1D-AA-F8-D8-19	ALL WANS	ID Interface WAN2		Port 	Device	Description			
Ping Trace Route Routing Table ARP Table DHCP Table	Clear LAM Show Index 1 2	WAN	MAC Address 00-1D-AA-F8-D8-19 00-1D-AA-66-E0-21 00-1D-AA-F7-C0-E2	ALL WANS	ID Interface WAN2 WAN2		Port 	Device	Description			
Ping Trace Route Routing Table ARP Table DHCP Table	Ciec LAN Show Index 1 2 3	WAN WAN IP 192.168.105.52 192.168.105.59 192.168.105.62	MAC Address 00-1D-AA-F8-D8-19 00-1D-AA-66-E0-21 00-1D-AA-F7-C0-E2	ALL WANS	ID Interface WAN2 WAN2 WAN2 WAN2 WAN2 WAN2		Port 	Device	Description			
Ping Trace Route Routing Table ARP Table DHCP Table	Clear LAN Show Index 1 2 3 4	WAN WAN 192.168.105.52 192.168.105.52 192.168.105.62 192.168.105.71	MAC Address 00-1D AA-F8-D8-19 00-1D AA-F8-D8-19 00-1D AA-F8-D8-19 00-1D AA-F7-C0-E2 00-50-7F-F1-00-16 00-1D-AA-7D-65-14 00-1D-AA-8A-8B-C9	ALL WANS	ID Interface WAN2 WAN2 WAN2 WAN2 WAN2		Port 	Device	Description			

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.

	2865ac_001DAA	000000 / Monitoring / Diagn	ostics				C				
Ping	IPv4 Address	I 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 DHCP Table Sessions Table		ck on a specific LAN to display	the detailed information o	i the DHCP client.							
JESHUIS HUIC	IPV6 Address	Assignment Table									
	Interface	IPv6 Address	IAID	Link-Layer Address	Leased Time	DUID					
				No data available							

5.3.4.6 Sessions Table

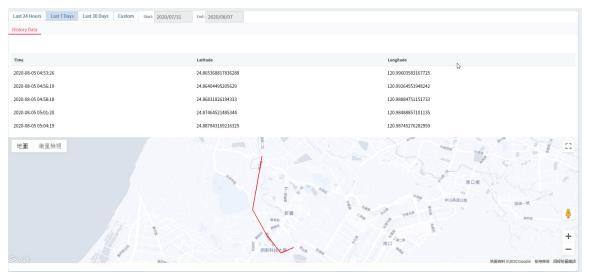
← Configuration	2865ac_00	1DAA000000 / Monitorir	ng / Diagnostics				
	Index	Private IP	Private Port	Pseudo Port	Peer IP	Peer Port	Interface
Ping	1	192.168.1.10	64325	32837	8.8.4.4	53	WAN2
Trace Route	2	192.168.1.10	64325	32837	8.8.8.8	53	WAN2
Routing Table	3	192.168.1.10	65186	33698	216.58.200.227	443	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.

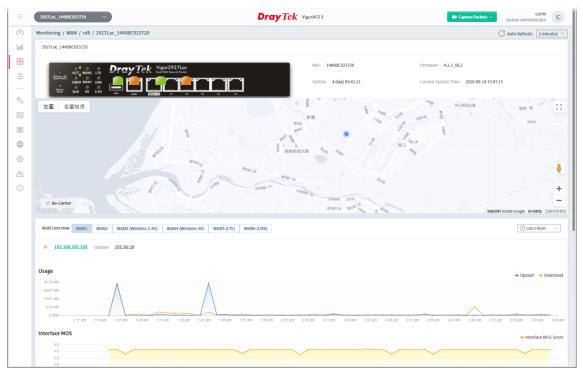
The GPS page will display the moving path (including time and coordinate position, latitude, and longitude) of the Vigor device.



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.



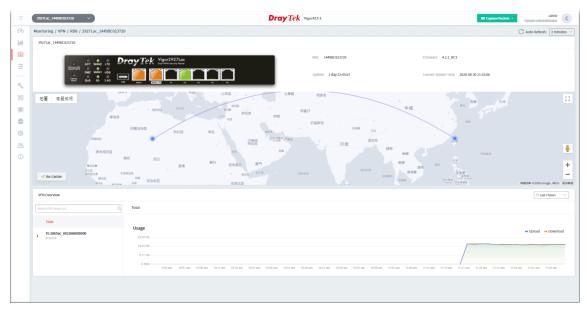
ltem	Description

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

5.3.7 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.

IP (all List													C Last 2 hou	ırs 🗸
	1 414 Total	11 • Great 5.0 - 4.3			4 • Poor 3.5 ~ 3.1	0 • Bad 3.0 - 1.0					Rows	5 10 ×	14 < 1	/160 >	D 1
	Status↓↑	LAN IP	↓↑ Peer IP	↓↑ Call ID	† Via Interfac	e ↓↑ Start Time	↓↑	Failovered Interface 4	Up Time ↓↑		Latency Peak ↓⊺	Average		Packet Loss ↓↑	MOS
	6	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	i		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 96	4
	6	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
	പ	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
	6	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

These parameters are explained as follows:

ltem	Description
Great, Good, Okay, Poor, Bad	All the VoIP calls will be separated with different levels according to its quality.
Q	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.

=	2927Lac_14498C023720 V	Dray Tek VigorACS 3		Capture Packets	C C C C
(?)	Monitoring / Data Usage / rd8 / 2927Lac_1449BC023720				\bigcirc Auto Refresh: 5 minutes \smallsetminus
00	2927Lac_1449BC023720				
•	Usage Sorting by Application Client Device				🕓 Last 2 hours 🗸 🗸
-	Total Search Category or App				
Ľ					
Ŧ		Protocol	97.35 MB	 Others 	5.43 MB
3	Total	Google Services	2.74 MB	Instant Message	1.31 MB
	109.63 MB	VoIP	1.20 MB	Tunneling	826.83 KB
£Ĝ}		Apple Services	769.39 KB	Web HD	40.76 KB
28					
()					
ĺ	Traffic Line Chart Upload/Download By Interface				
					Upload Download
	57.22 MB				
	38.15 MB				
	19.07 MB				
	0 Byte	2:40 pm 2:50 pm 3:00 pm 3:10 pm	3:20 pm	3:30 pm 3:40	pm 3:50 pm 4:00 pm
	Heare List by Application Client Device				
	Usage List by Application Client Device				

ltem	Description			
Usage Sorting by	Displays a pie chart re	ated to various	s application	usage.
	Application - Click to d	isplay a pie cha	ort for various	s applicatio
	Client Device - Click to	display a pie cl	hart for the s	elected CP
Traffic Line Chart	Displays a line chart re interface.	lated to data u	pload/downl	oad, or tra
	Upload/Download - Cli	ck to display d	ata upload/d	ownload.
	By Interface - Click to c	lisplay a line ch	hart related to	o traffic via
	interface.			
Usage List by	Displays the data usag			
Usage List by	Displays the data usag Application - Click to d applications, including download usage.	isplay the data	information	related to
Usage List by	Application - Click to d applications, including	isplay the data	information	related to
Usage List by	Application - Click to d applications, including download usage.	isplay the data name of appli	information	related to ser of users
Usage List by	Application - Click to d applications, including download usage.	e yesterike • erect	entromation cation, numb	related to a er of users Management Manageme
Usage List by	Application - Click to d applications, including download usage.	e yesterike • erect	entromation cation, numb	related to v er of users I de folge I de fol

incl	uding	host nam	•	ess, MAC			ne selected CPE, ection type, ope	
Traffic	ine Chart Uploa	d/Download By Interlace						
25.0	MB						- 1	IAN1 WAN2
19.23								
1.5	1 MB							
			15 pm 1 20 pm 1 25 pm 1 30 pm	1.35 pm 1.46 pm 1.46 pm 1.50) pm 155 pm 2:	:00 pm 2:05 pm 2:10 pm 2:15	pm 2.20 pm 2.25 pm 2.30 pm 2.35 pm 2.40 pm	2:45 pm 2:50 pm
Usaget	ist by Applicatio	n Client Device					Usage	
+ 4	Host Name	41 IP Address	하 MAC Address	41 Connection Type	at os	Upload	at Download	11
1	adam-MBP	192.168.124.12	8C85902C6662	♥Wireless (5G)	0	108 Bytes	132 Bytes	
2	Unknown	192.168.124.20	00507F393EB2	as Wired	0	3.92 KB	2.14 KB	
3	R1000675	192.168.124.10	88D7F656F799	8 Wired	0	10.01 MB	4.44 MB	
4	YRCs-iPhone	192.168.124.11	B019C6DC60E2	Wireless (5G)	0	644.29 KB	38.61 MB	
	gboyQQ	192.168.124.13	E8FBE9C9B2A3	💬 Wireless (5G)	0	4.80 KB	13.03 KB	G

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.

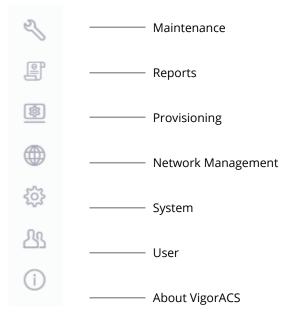


System Menu



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.

10	Maintenance
<u>E</u>	Scheduled Backup
~	Configuration Restore
	Firmware Upgrade
2	Device Reboot
Ē	System Password Reset
E	Schedule Profile
\$	File Manager
	Batch Activation
ŝ	
凸	
(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.

aIntenance / Scheduled Back	sup				
User Group : RootGroup	~				
etworks & Devices Backup Setti	ngs Profile				
lame	File Type	Backup Setting			
🐼 Root Network(123)	Configuration File	Empty	~		
AutoTest_SD-WAN(2)	Configuration File	As Parent	~		
> O U_2133_100(100)	Configuration File	As Parent	~		
VigorSwitch(2)	Configuration File	As Parent	~		
> 🚱 aaa(5)	Configuration File	As Parent	~		
> 🐼 Issue6925(0)	Configuration File	As Parent	~		
Jason_test(1)	Configuration File	As Parent	~		
2133Vac_001DAA66E020	Configuration File	As Parent			
2762Vac_001DAA653308	Configuration File	As Parent	~		
2765Vac_1449BC2C42E8	Configuration File	As Parent	~		
2850V_001DAA7D9CC8	Configuration File	As Parent	~		
2865ac_001DAA4ACFB0	Configuration File	As Parent	~		
2865ac_1449BC143DA0	Configuration File	As Parent	~		
2962_1449BC0D2040	Configuration File	As Parent	~		
@ 3910_1449BC1CA218	Configuration File	As Parent	~		
3910_1449BC6B9178	Configuration File	As Parent	~		
39125_1449BC3072A0	Configuration File	As Parent	~		
P1280_001DAA4E6C33	Configuration File	As Parent	~		
P1282_1449BC43CD19	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 /			
	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.

Maintenance / S User Group : R	icheduled Backup ootGroup ~				
	Backup Settings Profile				
+ Add					
Name	Period(Days)	Туре	Time Interval	Action	
Default	1	The Last 20	Now	🖉 Edit 🝈 Delete	
tttt1	1	The Last 20	Now	🖉 Edit 🝈 Delete	

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.

Maintenance / Scheduled Backup User Group: RootGroup		
Networks & Devices Backup Settings Profile		
Name		
Backup Period(days)	1	
Keep Files	The Last 20 All	
Backup Time	Now Scheduled Schedule Profile	
Schedule Profile	reset_password_wizard ~	
		Cance

Item	Description		
User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.		
Name	Enter a name of the backup profile.		
Backup Period(days)	The number typed here means the interval for the backup executed by VigorACS. The unit is "day". If you type 1, that means the backup will be executed one time by one day.		

Keep Files	Choose to keep all of the files (router's configuration files) or the last 20 files.						
Backup Time	 Set a time interval for executing the backup work for networks and devices. Now - The backup work will be executed immediately after clicking 						
	 the Save button. Scheduled - The backup work will be executed at the specified ti and date after clicking the Save button. 	me					
	 Schedule Profile - The backup work will be executed according to selected schedule profile after clicking the Save button. 	o the					
Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hou and minutes by clicking the number on the clock.	ır					
	50 10 40 20 Profile 5 35 30 25 5 9 5 15 9 10	<u>.</u>					
	Su Mo 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	Choose a trigger profile from the drop down list. In which, VigorACS of						

	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	s nage
5470	Save the changes on the	s 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.

Maintenance / Configuration Restore	2			
User Group : RootGroup ~				
Apply to Devices Restore Settings Profil	e			
Quick Setting				
Name	Apply	File List	Restore Profile	
Root Network(91)				
ALANWEN(3)				
2952n_001DAAE061E8			Empty	
2960_00507FFF3900			Empty restore_wizard	
3910_001DAA18E740	\bigcirc		Default	
AnPhat_VN(8)			^RD8TestTest 1111	
AriesTest(0)			2222 3.333	
Solution State			0.000	
David_Test_n1(3)				
FAE(3)				
Marketing_carrie(0)				
OCTOBER(1)				
RD1(3)				
> 🐼 SEG1(1)				
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	Each user group can be configured with different restore settings profiles. This wizard offers a series of steps to specify configuration file which can be applied to multiple APs / Switches at one time. f Quick Setting Quick Setting Quick Setting Common Config File (AP903_20190715.cfg Notice To apply ALL 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 Device Filter APS Switches Select Devices Name Firmware Version Firmware Version Common Restore Profile Device Filter APS Switches Firmware Version Firmware Version
	$ \begin{array}{c} \bigcirc & \otimes \text{ AnPhat_VN(6)} \\ \bigcirc & \odot \text{ AnFrat_evt(6)} \\ \bigcirc & \odot \text{ AnFrat_evt(6)} \\ \bigcirc & \odot \text{ Cshih(0)} \\ \bigcirc & \odot \text{ David_Test_n1(0)} \\ \bigcirc & \odot \text{ prat_est_n1(0)} \\ \bigcirc & \odot \text{ prat_evt(6)} \\ \bigcirc & \odot \text{ prat_evt(6)} \\ \bigcirc & \odot \text{ of CTOBER(0)} \\ \bigcirc & \odot \text{ SEG1(0)} \\ \end{array} $

	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.
	♥ 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
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. 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.
	5 Select a config file ×
	Filename ↓↑ Property ↓↑ Size Last Modified ↓↑ File Path ↓↑
	▷ Directory 0 Byte 02/19/2020 13:10:11 .
	AP1000C_20190604.cfg cfg file 9.41 KB 06/04/2019 14:09:13 /RootGroup
	AP910C_acl_20181206.cfg cfg file 210 Byte 06/04/2019 11:22:24 /RootGroup
	 Notice: To restore a CFG file from a different model, please make sure the firmware on both devices is up to date. 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.
	X Close
Restore Profile	Choose a profile defined in Restore Settings Profile for applying onto the selected CPE.

	Empty ~	
	Empty	
	restore_wizard	
	Default	
	^RD8TestTest	
	1111	
	2222	
	3.333	
	Empty - No restore setting for the	selected network / device.
	Default - Use the default restore :	setting for the selected network / device.
	Others - In addition to Empty and Settings Profile also will be listed	Default, profiles defined in Restore in this drop-down list.
Save	Save the current settings.	

6.1.2.2 Restore Settings Profile

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

Maintenance / Config User Group : RootGr	-			
Apply to Devices Rest	ore Settings Profile			
Name	Trigger Profile	Time Interval	Action	
Default	default	Now	🖉 Edit 🐵 Delete	
wireless		Now	🖉 Edit 🐵 Delete	
ACL	-	Now	🖉 Edit 🐵 Delete	

These parameters are explained as follows:

Item	Description
User Group	Specify a user group for applying the configuration restore settings profile. Each user group can be configured with different configuration restore settings profiles.
+Add	Click 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.

Maintenance / Configuration Restore		
User Group : RootGroup ~		
Apply to Devices Restore Settings Profile		
Name		
Restore Time	Now Scheduled Schedule Profile	
Start Time	Select time	
End Time	Select time	
Specify Start Date	0	
	Cancel Save	

Description				
Specify a user group for applying the restore settings profile. Each user group can be configured with different restore settings profiles.				
Enter a name of the restore setting profile.				
 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. 				
The configuration restore will be executed after clicking Save .				
Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock. Image: Click to grad the setting of the time setting. Specify Start Date – Click to enable the time setting. Date – Click to pop up a calendar to choose a date as the starting date.				

	_1						
	<	Jan		~ 2	022	~	>
	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					
	C.1						
Schedule Profile		gorACS _passw	offer	s defai zard			
		_passv ot_wiza		vizard			
		ore_wiz up_wiz					
	defa test1	ult					
Save	Save the	curren	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.

laIntenance / Fir	mware Upgrade				
User Group : Roo	vtGroup ~				
irmware Upgra	ide Job List				
+ Add 🖲 Dele	te All Complete Jobs				
	te All Complete Jobs • File Path	$\downarrow\uparrow$ Schedule $\downarrow\uparrow$ Device Cou	int ↓† Status ↓† Resi	alt J↑ Action	
		it Schedute it Device Cou Any 1		alt 3↑ Action cess:0 Fall:0 2 Edit	B Delete € View La

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.
View Log	Click to view the record of the firmware upgrade for the CPE

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

Maintenance / Firmware Upgrade User Group: RootGroup		C
Firmware Upgrade Job Settin	ngs	
Name		
Status	Disable Enable	
Upgrade Time	Now Scheduled	
Date	Select a date	
Start Time	Select time	
End Time	Select time	
Apply Firmware		
Protocol Options	TR069 HTTP	
Note: Firmware Upgrade Job	o will only be performed between start and end time.	
Device to Upgrade 🛛 🖓		
Name	MAC Address Model Name Firmware Version Modem Version	Ì
Root Network(123)		
AutoTest_SD-WAN(2)		
▷ O_2133_100(100)		
VigorSwitch(2)		

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 and devices.
	• Now - The firmware upgrade job will be executed immediately after clicking the Save button.

Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.												
		01:14											
		$\begin{array}{cccccccccccccccccccccccccccccccccccc$											
			21 9 20 ⁸		3	15 16							
			1	76 918	5 17								
		01	1:14	Ö	,∕Sel¢	ect time	Ü						
	Date	Date – Click to pop up a calendar to choose a date as the starting date.											te.
		<	Jan		~ 2	022	~	>					
		Su	Мо	Ти	We	Th	Fr	Sa					
							_	1	le				
	-	2	3	4	5	6	7	8					
	-	9	10	11	12	13	14	15					
	-	16	17	18	19 26	20	21	22					
	-	23 30	24 31	25	26	27	28	29					
									J				
Apply Firmware		Click to open a dialog to select a firmware file. VigorACS will upgrade the selected CPE with the selected file.											
	Sel	lect a fi	rmware										
		Filenam	ne			Pr	operty	† Size	Le	st Modified	ţ	File Path	↓↑
						Di	ectory	0 Byt		/19/2020 13:10		./RootGroup	
		ð	dFirmware			Dir	ectory	0 Byt	e 04				
		 □ Share 	edFirmware		F 8		ectory	0 Byt		/04/2010 13-55		/RootGroup	
		 □ Share 	r2960_001E		E8	Di	ectory ectory ectory	0 Byt	e 06	/04/2019 13:55		./RootGroup	
		 Share Vigor 	r2960_001E		ES	Di	ectory	0 Byt	e 06	/04/2019 13:55		./RootGroup	
		 Share Vigor 	r2960_001E		ES	Di	ectory	0 Byt	e 06	/04/2019 13:55			Close
Protocol Options	0)	 Share Vigor Publis 	r2960_001E	DAA694AI		Dir	ectory	0 Byt	ie Oć		45		Close
Protocol Options	Selec	Ct the	e mec	chani		pr per	ectory ectory	0 Byt	ie Oć	re upgra	45		Close
Protocol Options	Selec TR06 HTTF	 Share Vigot Pubb Pubb Share Vigot Pubb Pubb Share Vigot Pubb Pub Pub Pubb Pub	e mec This is	chani s the CS w	sm fo defau ill aut	or per ult set	ectory ectory formi cting. cate t	o Bys o Bys ng fil	rmwa	re upgra	ade.	× name an	

	username for accessing the router.								
	• Router Password – Enter the password (e.g., admin) of the router for accessing the router.								
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								
	Name MAC Address Model Name Firmware Version Modern Version								
	 ▲ O Root Network(91) ▲ O ALANWEN(3) 								
	Z 😋 2952n_001DAAE061E8 001DAAE061E8 Vigor2952n 3.9.1.1_RC3 No DSL								
	2010 201007FFF3900 00507FFF3900 Vigor2960 1.3.0_Beta undefined								
	▷ ⊙ AriesTest(0)								
	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.								
	The firmware upgrade job will be performed based on the above conditions automatically.								

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)

Maintenance / Device Reboot				
User Group : RootGroup ~				
Networks & Devices Reboot Settings Pr	ofile			
Name	Model Name	Firmware Version	Modem Version	Reboot Setting
Root Network(90)				Empty ~
ALANWEN(3)				As Parent 🗸
AnPhat_VN(8)				As Parent ~
ArlesTest(0)				As Parent 🗸 🗸
Cshih(2)				As Parent $$
FAE(3)				As Parent 🗸 🗸
Marketing_carrie(0)				As Parent $$
OCTOBER(1)				As Parent $$
RD1(3)				As Parent 🗠
SEG1(1)				As Parent $$
ScanAccess(3)				As Parent $$
D TreeDepthTest(0) D				As Parent $~~$
D 🖸 USA(1)				As Parent $$
Cole6666(0)				As Parent ~
▷ ③ cole777777777777777777777777777777777777	7(0)			As Parent ~
mamte(2)				As Parent ~
p 🐼 robintest2(0)				As Parent ~
or rrwerwe(0)				As Parent ~
b Stest(0)				As Parent ~
b Stest6666666(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 Empty As Parent Empty reboot_wizard Default #1 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.

MaIntenance / Device Reboot				
User Group : RootGroup ~				
etworks & Devices Reboot Settings Profile				
Add				
łame	Period(Days)	Time Interval	Action	
eboot_wizard	365	00:00-23:59	🖉 Edit 👘 Delete	
efault	1	00:00-00:00	🖉 Edit 🛛 🕆 Delete	
1	1	Now	🖉 Edit 🛛 🕆 Delete	
I	365	01:05-03:15	🖉 Edit 👘 Delete	
shih_test	1	13:15-17:05	🖉 Edit 👘 Delete	

These parameters are explained 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.

Maintenance / Device Reboot	
User Group : RootGroup ~	
Networks & Devices Reboot Settings Profile	
Name	
Period (days)	1
Reboot Time	Now Scheduled Schedule Profile
Start Time	Select time
End Time	Select time
Specify Start Date	0
Date	Select a date
	c

ltem	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 - 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	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 12 21 20 7 6 19 13 19 18 19 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 state of the set of t								
	<	Jan		× 2	2022	~	>	1	
	Su	Мо	Tu	We	Th	Fr	Sa		
							1	le	
	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	2.5	20	21	20	25		
		51							
chedule Profile	which, Vig	gorACS	offer	s defa				m the drop down list. I e.	
	reset_password_wizard ~								
	reboot	_wizard e_wizard p_wizard	1	ITC					
ancel	Discard c	urrent	settin	gs and	d retur	n to p	reviou	is page.	
ve	Save the	curren	t setti	ngs.					

6.1.5 System Password Reset

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

Maintenance / System Passwor	rd Reset			
Reset Time	Now Scheduled			
Start time	00:00			
End time	23:59			
Start Date	01/07/2022			
Select devices				
Name	Model Name	Firmware Version	Modem Version	
⊿ 🐼 Root Network(2)				
▷ 🕥 111111(0)				
> 22222(0)				
Manual_Carrie(1)				
AP 903_00507FF1	91BC VigorAP 903	1.4.2	No DSL	
				Save

ltem	Description
Reset Time	 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.
	$\begin{array}{c} 03:10 \\ 23 & 00 & 13 \\ 22 & 11 & 12 & 1 \\ 10 & 2 & 2 \\ 21 & 9 & 3 & 15 \\ 20 & 7 & 6 & 5 & 16 \\ 19 & 18 & 17 \\ 19 & 18 & 17 \\ \end{array}$ $\begin{array}{c} \text{ule Profile} \\ \text{o3:10} \\ \end{array}$
	• Date – Click to pop up a calendar to choose a date as the starting date.

		<	Jan		~ 2	022	~	>
	s	Su	Мо	Ти	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					
		I		_				
ct devices	Choo	se the	device	that	you wa	ant to	do dev	vice p
	Save	the cu	rent s	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.

MaIntenance / Schedule Profile					
User Group : RootGroup ~					
+Add					
Name	Start Day	End Day	Start Time	End Time	Action
reset_password_wizard	2017-04-27		07:08	07:13	🖉 Edit 🔋 Delete
reboot_wizard	2017-06-20		08:21	20:11	🖉 Edit 🛛 🗎 Delete
restore_wizard	2016-12-14		05:12	05:17	🖉 Edit 🛛 🗎 Delete
backup_wizard	2016-12-07		03:05	03:25	🖉 Edit 🛛 🗟 Delete
default	2016-10-08	2016-10-09	00:00	00:00	🖉 Edit 🛛 🖹 Delete
test1	2017-04-19	2017-04-11	00:00	00:00	🖉 Edit 🛛 🔒 Delete
test2					🖉 Edit 🛛 🔒 Delete
test3					🖉 Edit 🛛 🗎 Delete
test4					🖉 Edit 🔋 Delete
test5					🖉 Edit 🛛 🗐 Delete
test6					🖉 Edit 🛛 🗟 Delete
test7					🖉 Edit 🛛 🖹 Delete
ttl			00:00	23:59	🖉 Edit 🔋 Delete

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

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. Scheduled – To specify a certain day to perform the job, choose this one and specify start day and end day respectively. 	
Start Day	Use the drop down calendar to specify the day you want to start the operation.	
Check End Day	Click to enable the end day to determine if the job is performed or not. For example, the end day for firmware upgrade is out of date, then the upgrade will not be executed for the selected CPE.	
End Day	Use the drop down calendar to specify the day you want to end the operation.	
Time Type	Now – When CPE meets settings configured in the profile, the job (e.g., upgrade) for the CPE will be performed immediately.	
	Scheduled – 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.

1. Uplo	ad 🕹 Download 🗐 Delete 🕒 New Folder	DrayTek FTP					Search	(
	Filename	J↑ Device Name	↓↑ Property	Ψî	Size	↓↑ Last Modified	↓↑ File Path	
	C SharedFirmware		Directory			07/30/2020 09:16:40	./RootGroup	
	🗅 test555		Directory			06/06/2019 14:22:59	./RootGroup	
	□ tt1		Directory			03/04/2019 14:39:56	./RootGroup	
	C Vigor2925Vac_001DAAF06DF0		Directory			10/08/2019 11:23:27	./RootGroup	
	C 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.bxt		txt file			05/22/2019 14:03:32	./RootGroup	
ו	🗋 docker.txt		txt file		1.98 KB	06/19/2019 09:22:04	./RootGroup	
]	C certificate.cfg		cfg file		5.92 KB	03/04/2019 14:40:01	./RootGroup	
]	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.
	Lupload 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.
	+ New Folder
	Folder Name:
	tfg K Cancel + Add
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.

=	Dray Tek VigorACS 3	Root Network (100142)	Q Q	Pcap	mk_carrie System Administrator	М
(¹)	Maintenance / WCF Batch Activation (For URL Reputation	on)				
	+Add					
	Create Time 41 Create	User	11 Devices Count	↓↑ Action		
		No data a	avaitable			
Z						_
P						
\$						
ŝ						
ß						
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				
A				
	on is the feature which provided to the distrib butor privilege account.	utor only, please login MyVigor		
	e requirement of batch activation, please cont	act your local distributor for		
Username			-	
Password	•••••	\odot		
A Pack to profile list				
↑ Back to profile list				ogin

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.

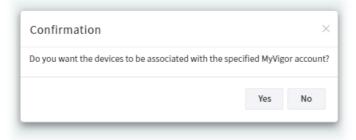
2. Enter the username and password and click **Login.** After authenticated by MyVigor server, the following page will be shown.

	-					
Import WCF batch activation	data					
Upload file	Browse					
	A Download entry sample file					
↑ Back to profile list		නි Upload				
ltem	Description					
Upload file	Click Browse to locate the CSV file import-batch-activation-file.	with name of				
	Maintenance / WCF Batch Activation (For 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, click "Download entry sample file" link to download one file.					
Download entry	Click to download an entry sample	e file (import-batch-activation-file.csv).				
sample file	Open the CSB file and enter the "N device.	MAC address" and "WCF KEY" for each				
Back to profile list	Return to the previous profile list	page.				
Login	Access into next page.					

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

Maintenance	e / WCF Batch Activation (For Cyren)					
Upload Re	esult					
🕹 Export						
ΨŤ	Device Name	↓↑ Device MAC	↓↑ Network	↓↑ License Key	↓↑ ACS Check Status	$\downarrow \uparrow$
~	2865Lac_1449BC0D8F00	1449BC0D8F00	MKT_manual	6F6CD-CF2A6-EE7CE-6C5D2	Check OK	
↑ Back to profil	le list					
-1. Back to bioli	ie itst.				Previous	Next

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.

lyVigo & Expor	or Devices & License Ch	eck							
¢↑	Device Name	$\downarrow \uparrow$	Device MAC	$\downarrow\uparrow$	Network	$\downarrow\uparrow$	License Key	$\downarrow\uparrow$	MyVigor Check Status
~	2865Lac_1449BC0D8F00		1449BC0D8F00		MKT_manual		6F6CD-CF2A6-EE7CE-6C5D2		Check OK
Back to p	profile list								Previous Activa

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

Root Net… V	Dray Tek VigorACS 3	
Maintenance Save OK	×	

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… ∨	Dray	Tek VigorACS 3			
Maintenance / WCF Bat	ch Activation (For Cyren)				
+Add					
Create Time	↓↑ Create User ↓	Devices Count	↓↑ Action		
2021-02-26 06:27:12	root	1	Q View Log 💼 Delete		
ltem	Description				
		Click to create a new batch activation profile.			
+Add	Click to create a new	batch activat	ion profile.		
+Add View Log	Click to create a new Click to view the reco		•		

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

example 2

Device Name	¢	MAC	ψt	License Key Number	ψt	License Date	$\downarrow \uparrow$	Network $\downarrow\uparrow$	Last Update Time $$\downarrow\uparrow$$	Status ↓↑	Result	J↑
2860n+_001DAAD1E290		001DAAD1E290		03F10-D646B-2B0A1-40DA6		2019-02-13~2019-03-1	5	RD8	2019-04-02 11:30:41	Complete	CPE sync license successfully	
2925Ln_001DAADD75B0		001DAADD75B0		671C8-8222F-55F4E-907CB		2019-02-13~2019-03-1	5	RD8	2019-04-02 11:32:40	Fail	Cannot connect to CPE (timeout)	
↑ Back to profile list												

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
	Legacy Report Tasks
I —	
Z	
I 🖉 🖣	Reports
-	
ŝ	
<u> </u>	
I (i)	

6.2.1 Report Tasks

6.2.1.1 Report Tasks

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

=	Dray Tek VigorACS 3		Root Network (100142)	Q	Рсар Ф 14:50:10 7/29/24 System	mk_carrie M
(7)	Report / Report Tasks User Group : RootGroup	~				С
\$1 \$1 \$1	Report Tasks Generated Reports					
-0-	+ Add				Profile N	umber Limit: 1/20
Z	Profile Name	↓↑ Report Type	↓↑ Report Range	J↑ Recurrence	J↑ Action	.↓↑
F	2024-1-42-s-t1-5CPEs	Statistic Report	Device(s)	Once	🖉 Edit 🛛 🖻 Delete	
\$						
<u>رې</u>						
43						
(j)						

These parameters are explained as follows:
--

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.

Click **+Add** to create a new report task. Select **Statistics Report** or **Comprehensive Report**. Then click **Apply.**

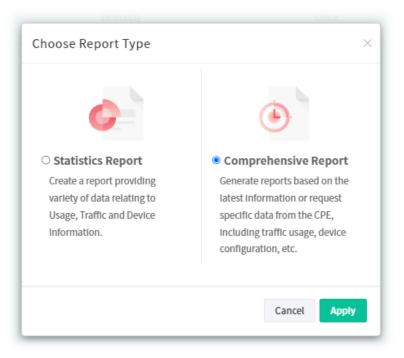
Choose Report Type	×
0	
Statistics Report	Comprehensive Report
Create a report providing	Generate reports based on the
variety of data relating to	latest Information or request
Usage, Traffic and Device	specific data from the CPE,
Information.	Including traffic usage, device configuration, etc.
	Cancel Apply

If **Statistics Report** is selected, the following setting page will appear.

Report / Report Tasks User Group: RootGroup			c
Statistic Report Settings			
General			
Profile Name			
Report Range	Network Device(s)		
Network	Nothing selected ~		
Timeframe	Last 24 hours 🗸		
Send Report by Email			
Recipients and Logo			
Report Recurrence	Every Week v 1st v		
Report file Logo	Please select an image. Browse		
Customized Widgets			
Network Wide	Usage Overvlew	Client Number	
	Uireless Client Overview	Client Traffic	
Device/ Client Ranking	Top Device Ranking by Client Number	Top Client Ranking by Traffic	
	Top Device Ranking by Traffic	Top Device Ranking by Uptime	
			Cancel Save
		a Tuna	

Item Description	em
------------------	----

more entry box(es) for adding more recipients. Recipients and Logo Report Recurrence Once - The report will be made just for one time. Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 timescrift1 Devise(S) Select timescrift1 Devise(S) Report Lewise (Distance (General			
Network Select one or more networks for generating the statistics report. Timeframe Display the report related to the CPE detected within 24 hours, 7 days, 3 days or user defined days. Send Report by Email Switch the toggle to enable/disable this function. If enabled, Recipients (User) – Specify the subject for the email. Recipients (Email) - 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. Recipients and Logo Once – The report will be made just for one time. Every Day/Every Week/Every Month – The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. Only the CPEs under the selected User Group (e.g., RootGroup in this case will be shown in this field. Network the best to be left of the network group to select the device(s) you want to make report. Network to make report. Network the device(s) you want to make report. Select the items related to the left of the network group to select the device(s) you want to make report. Sectorecome Sectorecome	Profile Name	Enter a name for such report task profile.		
Timeframe Display the report related to the CPE detected within 24 hours, 7 days, 3 days or user defined days. Send Report by Email Switch the toggle to enable/disable this function. If enabled, Recipients (User) - Specify the subject for the email. Recipients (Email) - 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. Recipients and Logo Once - The report will be made just for one time. Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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. Network Wide Sectement(1) Display 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. Display the CPEs under the selected User Group (e.g., RootGroup in this case will be Shown in this field.	Report Range	Determine the content range (network or devices) of the report.		
days or user defined days. Send Report by Email Switch the toggle to enable/disable this function. If enabled, Recipients (User) - Specify the subject for the email. Recipients (Email) - 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. Recipients and Logo Once - The report will be made just for one time. Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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. Set determine Note More Note State S	Network	Select one or more networks for generating the statistics report.		
Recipients (User) - Specify the subject for the email. Recipients (Email) - 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. Recipients and Logo Report Recurrence Once - The report will be made just for one time. Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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. Sett device: Set	Timeframe			
Report Recurrence Once - The report will be made just for one time. Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 devices Network Wide Note Network group to select the device(s) you want to make report. Select devices Network to make report. Select devices Network group to select the device(s) you want to make report. Select devices Network Time Network to make report. Select devices Select devices Network group to select the device(s) you want to make report. Select devices Network group to select the device(s) you want to get device (group (get 2000 get 2000	Send Report by Email	 Recipients (User) – Specify the subject for the email. Recipients (Email) - Enter the email address of the recipient. +Add - If there is more than one recipient for adding, click the link to have 		
Every Day/Every Week/Every Month – The report will be made repeatedly. Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 the itemser(11) Performance Wester Network Wide Select the itemser(12) Generation of the network group to select the device(s) you want to make report. Select the select(22) Select the select (Second Second Seco	Recipients and Logo	!		
Set the day, starting date and starting time based on the selection. Report file Logo Click to put a logo on the report. Select the logo file (with the file size less than 100KB). Customized Widgets Network Wide Network Wide Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 devices Network Wide Network 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 devices Network Version Network Version Select devices Network Version Select devices Network Version Select devices Select device	Report Recurrence	Once – The report will be made just for one time.		
than 100KB). Customized Widgets Network Wide Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 devices Image: Model Name		Every Day/Every Week/Every Month – The report will be made repeatedly. Set the day, starting date and starting time based on the selection.		
Network Wide Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 devices Name Name Name Name <td>Report file Logo</td> <td colspan="3"></td>	Report file Logo			
Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report. Report Device(s) If Devices(s) is selected as Report Range, this option will appear. 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 devices Name Firmware Version If @ @style*_1(1) If @ @style*_1(1) If @ @style*_1(1) If @ @style*_1(1)() If @ detected If @ detected If the endevices If the endevices If @ detected If endevices	Customized Widgets	·		
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 devices Name Nordel Name Image: Root Network[11] Image: Root Network[12] Image: Root Network[13] Image: Root Network[13] Image: Root Network[13] Image: Root Network[13] Image: Root Network[14] Image: Ro	Network Wide	Monitoring, and Hotspot Web Portal. Corresponding information will be		
Image: Wigor 2862Vac 3.8.8.1_STD Image: Wigor 2927Lac_14498C023768 Vigor 2927Lac Image: Wigor 2927Lac 4.1.0_RC2_SDWAN	Only the CPEs under the selected User Group (e.g., RootGrowill be shown in this field. Check the box to the left of the network group to select the want to make report.			
	Save	▷		



If **Comprehensive Report** is selected, the following setting page will appear.

Report / Report Tasks User Group: RootGroup	c
Comprehensive Report Settings	
General	
Profile Name	
Report Type	Traffic ~
Report Content	LAN Statistic v
File Type	PDF Word CSV Excel
Report Range	Network Device(s)
Network	Nothing selected ~
Send Report by Email	
Recipients and Logo	
Report Recurrence	Every Week v 1st v
Report file Logo	Please solect an image. Browse
	⚠ The file must be less than 100KB.
	Cancel Save

ltem	Description	
General		
Profile Name	Enter a name for such report task profile.	
Report Type	At present, VigorACS offers several types of report, including traffic, firmware, network, status, information and device configuration.	

	Traffic Firmware Network Status Information Hotspot Web Portal Device Configuration Use the scroll bar to choose the type you want and select an option for that type.	
Report Content	Select the way (statistic or graph) to show the report. The content will vary based on the Report Type. LAN Statistic select an option LAN Statistic WAN Statistic NAT Statistic LAN Graph WAN Graph NAT Graph	
File Type	Choose PDF, Word, CSV, or Excel as the file format for device configuration report.	
Report Range	Determine the content range (network or devices) of the report.	
Network	Select one or more networks for generating the statistics report.	
Send Report by Email	 Switch the toggle to enable/disable this function. If enabled, Recipients (User) – Specify the subject for the email. Recipients (Email) - 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. 	
Recipients and Logo	<u>.</u>	
Report Recurrence	Once – The report will be made just for one time. Every Day/Every Week/Every Month – The report will be made repeatedly. Set the day, starting date and starting time based on the selection.	
Report file Logo	Click to put a logo on the report. Select the logo file (with the file size less than 100KB).	
Save	Save the settings and return to previous page.	

6.2.1.2 Generated Reports

This page displays the report(s) generated by VigorACS server.

=	Dray Tek VigorACS 3	Root Network (100142) V Q		Pcap	
(7)	Report / Report Tasks				С
<u></u>	User Group : RootGroup ~				
	Report Tasks Generated Reports				
Z	Show 20 ~ entries			Search	
I E	Time	↓↑ Report Type	৾৾↑ Action		
<u></u>	2024/01/08 13:53:08 2024-1-42-s-t1-5CF	Es Statistic Report	Contract Con		
	Showing 1 to 1 of 1 entries				≪ 1 ≫
ŝ					
යින					
i					

6.2.2 Legacy Report Tasks (Deprecated)

This page displays the legacy report tasks and is just for reference.

=	Dray Tek VigorACS 3	CRO	oot Network (100142)	v a			Pcap	15:56:		
(7)	Reports / Legacy Report Tasks (Deprecated)									
<u>-</u>	User Group : RootGroup ~									
								Sez	rch Title/Type	Q
	Title	Network/Device	Report Content	Report Delivery	Schedule/Period	Last Implemented	Action			
Z	Device Information Report from 141:8080 Report Task	Root Network	Information	Email	Now	2018-09-12 10:32	/ E	lit 🐵 Dele	e	
P	666	U_2133_100	Device Configuration	Download	-	-	/ E	lit 🐵 Dele	e 🕁 Download	
\$										
{ĵ}										
43										

Click **Edit** to review the detailed settings.

Enable This Task		
Task Title	Device Information Report from 141:80	
Report Content	Information	
	Device Information ~	
Report delivery	Send By Email Download File	
File Type	PDF CSV Excel Word	
Created By	root / Internal	
Run Report	Once Repeat	
	Now ~	

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.

(7)	Provisioning	ur)
<u>F</u>	Global Parameters	~
~°?	CPE Set Parameters	
	CPE Keep Parameters	
Z	Firmware Upgrade	15
I E		
A		

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.

- 1	Dray Tek VigorACS 3	Root Network (100142) V					Pcap 🗘	16:29:41 7/29/24	mk System Adr	carrie
9)	Provisioning / Global Parameters									(
3	User Group : RootGroup ~									
-	Global Profile Network & Devices									
	Profile Edit Mode : All Web UI View XML File Parameter List									
5	🕲 Delete 🕂 Add 🕁 XML Template									
F	Profile Name	Pro	ofile Edit N ode		Always Keep	Revision	Last Modification At	Action		
₽	□ test123456	ХМІ	IL File G	General	Yes	1	2018/09/12 11:29:58 AM	🖉 Edit	С Сору То	€ View Log
} }	U vigor2860	Par	rameter List		Yes	19	2019/05/09 04:15:20 PM	🖉 Edit	🗅 Сору То	€ View Log
3	Ulgor2760	Para	rameter List		No	15	2019/05/09 04:15:20 PM	🖉 Edit	🔾 Сору То	€ View Log
)	- ttt	Para	rameter List		No	0	2019/05/09 02:39:36 PM	🖉 Edit	🗅 Сору То	€ View Log
	□ vigor28606	Para	rameter List		No	1	2019/05/09 04:12:05 PM	🖉 Edit	🛛 Сору То	€ View Log
	12345678913245678912314567891324567891234564897xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	rameter List		No	0	2020/02/27 11:29:32 AM	🖉 Edit	🗅 Сору То	€ View Log
		Web	eb UI View V	Vigor2927Lac	No	0	2023/08/07 10:40:06 AM	🖉 Edit	🗅 Сору То	€ View Log
	xmtSample	XML	IL File G	General	No	1	2023/12/20 01:20:33 PM	🖉 Edit	Сору То	€ 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.						
Delete	Click to remove the selected profile.						
+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. Skeps: 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.						

Action	Сору Т		ministrato	r wants to	e selected profile. apply the provision to	certain user
	£	Copy the pro	ofile to			×
	ħ	Сору То:		þick some us RootGrou SDWAN rd8		
	View Le	og – Click to	review det	tailed info	× Cancel	Apply d profile.
		g / Global Parameters				
		e Network & Devices				
	Profile Int Profile II Profile II Profile II Model Always R Revision Last Moo	ormation 6 ame root_gro Jit Mode Web UI General eep Yes 559			Status Overview	Complete Pailed
	Device ID	Device Name	↓↑ MAC Address	↓↑ Network (ID)	↓↑ Time ↓↑ Result	↓↑ Status
	293 295	2952n_001DAAE061E8 2960_00507FFF3900 3910_001DAA18E740	001DAAE061E8 00507FFF3900 001DAA18E740	ALANWEN (82) ALANWEN (82) ALANWEN (82)	2019/09/27 12:00:46 AM	Complete. Not yet applied. Not yet applied.

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

Provisioning / Global Parameters User Group: RootGroup ~		С
Global Profile Network & Devices		
Add a Profile		
Create Profile by Always Keep Reboot after Provisioning	Choose an action Sampling from an OAline Device Sampling from an XML file Creating a New Parameter List	
 8 Note: • After applying the parameter Provisioning Time 	ters, ACS will check the CPE responses and ask the CPE to reboot if needed. Now Scheduled Schedule Profile	
	Cancel	

ltem	Description
Create Profile by	There are three methods (Sampling from an Online Device, Sampling from

	an XML file, Creating a New Parameter List) to create a profile.						
For Sampling from an Online Device,	 Profile Name - It is available when Sampling from an Online Device / Creating a New Parameter List is specified on "Create Profile by". 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						
	AnPhat_VN						
	V 🚥 FAE						
For Sampling from an X ML file ,	Select XML file - Click Browse to choose a file.						
For Creating a New Parameter List,	Profile Name - Enter a name to create a new profile.						
Always Keep	Some ISPs do not wish CPE client changing the parameters of CPE device, therefore make the profile being kept is required.						
Reboot after Provisioning	Enable it to reboot the CPE after the provisioning is applied by certain CPE.						
Provisioning Time	 Set a time interval for executing the backup work for networks and devices. 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. 03:10 00 13 122 11 12 14 122 11 12 14 12 13 14 15 12 13 14 16 12 19 15 16 19 13 17 16 19 18 17 17 19 18 17 17 20 7 6 5 19 18 17 17 20 7 6 5 19 18 17 2 19 18 17 2 19 17 2 2 10 Select time 5 Start Date – Click to enable the time setting. 5 Start date – Click to pop up a calendar to choose a date as the starting						
	Start date – Click to pop up a calendar to choose 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	22
	23	24	25	26	27	28	29
	30	31					
Schedule Profile	Trigger F	rofile -	Choo	se a tr	igger p	orofile	from
Schedule Profile	Trigger F VigorACS	offers		ılt sch		orofile	
Schedule Profile	VigorACS Now reset	_passwo ot_wizaro re_wizaro up_wizar ult	defau eduled rd_wiza d	Ilt sch Sche	edule p	orofile	
chedule Profile	VigorACS Now reset rebo resto back defai test1 test2	_passwo ot_wizaro re_wizaru up_wizar ult	defau eduled rd_wiza d d d	Sche	edule prof	ille	~

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.

r Group : RootGroup ~		
bal Profile Network & Devices		
ame	Profile id	
Root Network(90)	Empty	~
ALANWEN(3)	root_group_always_keep	~
AnPhat_VN(8)	(As Parent)	~
ArtesTest(0)	(As Parent)	×
Schih(2)	Manoj	~
FAE(3)	(As Parent)	~
Marketing_carrie(0)	(As Parent)	~
OCTOBER(1)	(As Parent)	~
D1(3)	(As Parent)	~
b SEG1(1)	(As Parent)	~
b ScanAccess(3)	(As Parent)	~
> S TreeDepthTest(0)	(As Parent)	¥
> ③ USA(1)	(As Parent)	~
> S cole6666(0)	(As Parent)	~
cole777777777777777777777777777777777777	(As Parent)	~
> 🐼 mamle(2)	Empty	~
p 🐼 robintest2(0)	(As Parent)	×
b 🐼 rrwerwe(0)	(As Parent)	×
b 🐼 test(0)	(As Parent)	~
b 🐼 test6666666(0)	(As Parent)	v
b S wholesaletest(0)	(As Parent)	~
> 🐼 xxxxxxxx(0)	(As Parent)	~
▷ 📀 yyyyy(0)	(As Parent)	~
2762Vac_001DAA653308	(As Parent)	~
2860Vn+_001DAAD83D80	(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.

(i) 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.

Provision	Provisioning / CPE Set Parameters C						
User Gro	User Group v						
+Add	්Import XML ්aXM	IL Template					search Profile Name / Device Q
	File Id / Profile Id	Profile Name / Device Name			Complete	Action	
~	26	CPE Set Parameter Test.xml				🗊 Delete	
305		13.13.13.13	Model: Renew Count: 2	Reboot: 1 Retry: 0	No Set.	View Parameters	€ View Log
467		001DAA5D585A	Model: Renew Count: 0	Reboot: 0 Retry: 0	No Set.	View Parameters	€ View Log
>	28	CPE_Set_Parameter_Examplxxxxxxe.xml				🗊 Delete	
>	1	Henry Test.xml		🗊 Delete			
>	4	test.xml				🗊 Delete	

ltem	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 × Browse Cancel Apply			
VAAL Tommelate				
XML Template	Click to store current global parameter configuration as a file (*.xml).			
File Id / Profile Id	Displays the number of parameter file or the ID number of the profile.			
Profile Name / Device Name	Displays the profile name or the device name.			
Action	Delete – Click to delete the profile.			
	View Parameters – Click to display parameter settings for the selected profile.			
	View Log – Click to review detailed information for the selected profile.			

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

risioning / CPE Set Parameters			
Create an XML File			
名 Note: • After applying the param	neters, ACS will check the CPE responses and ask	he CPE to reboot if needed.	
File Name			
Device MAC or IP	Search By Device Information		
Reboot after Provisioning			
Name(optional)			
Network(optional)			
		Cancel Continue	

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**.

Provisioning / CPE Set Param	eters
Device: 172.16.2.222	Web UI View Parameter List
WAN	Select the parameters to be set
NAT Object Settings QoS	
Firewall VoIP Routine	
↑ Back to Profile List	

Item	Description
Device	Display the name of the device which will be applied with the parameters configured in this page.

Web UI View	Parameters (including WAN, LAN, NAT, Object Settings, QoS, Firewall, System, Routing, Wireless, Applications and etc.) ready for each CPE provision profile can be seen and configured in this page.	
	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 ListReturn 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.

rovisioning / CPE Keep Parameters			
ser Group : RootGroup	~		
Device	Parameters Count	Action	
Root Network(123)	Parameters count	Action	
AutoTest_SD-WAN(2)			
U_2133_100(100)			
VigorSwitch(2)			
A aaa(5)			
Ssue6925(0)			
Jason_test(1)			
2133Vac_001DAA66E020	0	🖉 Edit 🛛 📾 View Log	
2762Vac_001DAA653308	0	🖉 Edit 🛛 🖴 View Log	
2765Vac_1449BC2C42E8	0	🖉 Edit 🛛 🗟 View Log	
2850V_001DAA7D9CC8	0	🖉 Edit 🛛 🔒 View Log	
2865ac_001DAA4ACFB0	0	🖉 Edit 🛛 🗟 View Log	
2865ac_1449BC143DA0	0	🖉 Edit 🛛 🗟 View Log	
2962_1449BC0D2040	0	🖉 Edit 🛛 📾 View Log	
3910_1449BC1CA218	0	🖉 Edit 🛛 🗟 View Log	
3910_1449BC6B9178	0	🖉 Edit 🛛 🗟 View Log	
3912S_1449BC3072A0	0	🖉 Edit 🛛 📾 View Log	
P1280_001DAA4E6C33	0	🖉 Edit 🛛 🗟 View Log	
P1282_1449BC43CD19	0	🖉 Edit 🛛 🗟 View Log	
Q2121x_1449BC506AA4	0	🖉 Edit 🛛 🗎 View Log	

ltem	Description			
Edit	Click to open the configuration page.			
	Device : 3910_001DAA18E740 Parameter List			
	Reboot Reboot After Provisioning Image: Note: Image: Note: Image: Note: Image: Note:			
	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.

ProvIsionIng / Firmware Upgrade User Group : RootGroup ~			
Firmware Upgrade Job List			
TAdd Name ↓↑ Status ↓↑ Model	↓↑ FW Version	↓↑ FW File	↓↑ Schedule ↓↑ Start Date ↓↑ Action
sample Disabled Vigor2700 Series	3.1.1.1_RC6	v2k7v_a_3.1.1.1_RC6.all	Now N/A ∂ Edit © Delete € View Log
Exclude Devices			
+Add /Edit @Delete			
↓↑ MAC Address		¢¢.	
No data ava	ilable		

Item	Description
User Group	Specify a user group. The job list under that group will be displayed on this page.
Firmware Upgrade Job L	ist
+Add	Click to create a new job profile.
Edit	Click to modify, change the selected profile.
Delete	Click to delete the selected profile.
View Log	Click to view the record related to the firmware upgrade of the CPE.
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.

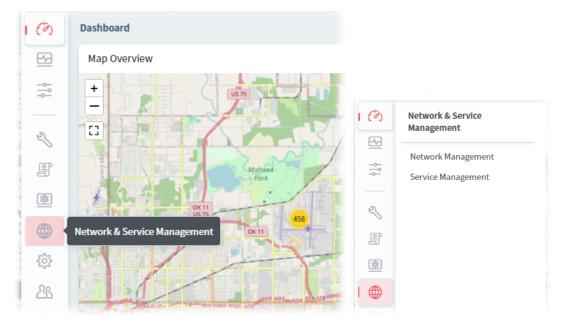
Provisioning / Firmware Upgrade User Group: RootGroup		
Firmware Upgrade Job Settings		
Name		
Status	Disable Enable	
Upgrade Time	Now Scheduled Schedule Pr	Profile
Job Type	Normal Auth Key Check	
Protocol Options	TR069 HTTP	
Device Criteria		
Model 🚱	Vigor167*	▼
Upgrade Type 😧	Target Current	
Device does not match the firmware version	1.2.3RC4 ~	×
Modem Version	No DSL ~	×
Firmware Upgrade & Network selecti	on	
Apply Firmware		
	Firmware Version Modem Version	
 Root Network(123) 		NO ~
AutoTest_SD-WAN(2)		As Parent v
U_2133_100(100)		As Parent v
VigorSwitch(2)		As Parent ~

ltem	Description
Firmware Upgrade Job S	ettings
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
Јоb Туре	 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 devices

	via authentication key issued by DrayTek to ensure the network security.				
Protocol Options	Select the mechanism for performing firmware upgrade.				
	TR069 – This is the default setting.				
	HTTP – VigorACS will authenticate the router/CPE by router name and the password and then perform the firmware upgrade for the CPE.				
	• Router Username – Enter the name (e.g., admin) of the router as the username for accessing the router.				
	• Router Password – Enter the password (e.g., admin) of the router for accessing the router.				
Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.				
	$\begin{array}{c} 03:10 \\ 23 & 00 & 13 \\ 22 & 11 & 2 & 1 \\ 21 & 9 & 2 & 15 \\ 20 & 7 & 6 & 5 & 16 \\ 19 & 18 & 17 \\ 20:10 \end{array}$				
	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				
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 listed 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 in "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 fi the received model r match with the infor type "*" in this filed, comparison conditio ignored.	name, mo mation re the mode	odem ecord em ve	firmware ve ed in VigorA rsion will no	ersion, a CS 3 ser t be reg	nd so ver o ardeo	ftware version r not. lf you d as a
Firmware Upgrade &	Network selection						
Apply Firmware	Click to open a dialog	g.					
	Select a firmware					>	
	Filename	Property ↓↑	Size	Last Modified	↓↑ File Path	J↑	
	⊵	Directory	0 Byte	11/19/2019 17:07:11			
	□ SharedFirmware	Directory	0 Byte	05/08/2019 08:36:52	./RootGro	up	
	□ test555	Directory	0 Byte	06/06/2019 14:22:59	./RootGro	up	
	C #1	Directory	0 Byte	03/04/2019 14:39:56	./RootGro	up	
	Vigor2925Vac_001DAAF06DF0	Directory	0 Byte	10/08/2019 11:23:27	./RootGro	up	
	VigorAP 902_001DAA3D9808	Directory	0 Byte	10/08/2019 13:25:36	./RootGro	up	
	🗅 PublicArea	Directory	0 Byte				
						X Close	
	Available versions fro Select the firmware v	-					ed in this field.
Apply	As Parent - The settin top setting.	ng for the	e seleo	cted networl	k / devic	e is tl	he same as the
	NO - No setting for the selected network / device.						
	YES - Use the firmwa					/ dev	vice.
Cancel	Discard current settings and return to previous page.						

6.4 Network & Service 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 Network Management

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

6.4.1.1 Settings for Root Network

Network & Service Management / Network Managemen	nt	
Search by Device ID/Name/Model/MAC/IP Address C 🚔	Setting Map	
 Root Network(100142) AutoTestNetwork(1) 	+Add New Network	
AutoTest_Dev(9)	General Settings	
AutoTest_SD-WAN(2)		
AutoTest_VPN(1)	Network ID	Username
Hotspot_Web_Portal(2)	2	acs
Router_App_Network(2)	Name	Password
T_2024-07-30_Wholesale_GA_D(0)	Root Network	••••••
T_2024-07-30_Wholesale_GA_E(0)	Location	
T_2024-07-30_Wholesale_GA_OOBE(0)	American	
T_2024-07-30_addNetwork_A(0)		
U_2133_100(100)		Save
▷ ♣ U_2865_5(2)		
▷ 👬 U_2866_5(4)		
▷ ♣ U_2927_5(5)		
VigorSwitch(2)		
aaa(5)		
expireLicense_A(0)		
fullLicense_A(1)		
Issue6925(0)		
Jason_test(1)		
▷ 👬 tttt1(3)		
▷ 👬 tttt4(2) 🔹		
Delete Devices		

ltem	Description
Search by Device ID/Name/Model/MAC/I P Address	Enter the ID, name, model or MAC/IP 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.
Username	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	~
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).**

arch by Device ID/Name/Model/MAC/IP Address	Setting Map A	larm Setting			
Root Network(100142)		This Network 🛛 🚓 Change	Network		
AutoTest_Dev(9)					
Autorest_SO-WAN(2)	General Settings				
AutoTest_VPN(1)	Network ID			Username	
Hotspot_Web_Portal(2)	4424			U_2866_5	
Router_App_Network(2)	Name			Password	
T_2024-07-30_Wholesale_GA_D(0)	U_2866_5				
T_2024-07-30_Wholesale_GA_E(0)	Location				
T_2024-07-30_Wholesale_GA_OOBE(0)					
T_2024-07-30_addNetwork_A(0)					
U_2133_100(100)	Advanced Settings				
U_2865_5(2)					
▷ ♣ U_2866_5(4)	Enable SD-WAN				
U_2000_5(4)					
VigorSwitch(2)	pull puts putties.				
aaa(5)	Bulk Data Settings				
expireLicense_A(0)	Set the category of data to be col	lected for statistical analysis.	You can freely select the data vo	ou want to count, use drag an	d drop to place each category in the corresponding profil
fullLicense_A(1)	specify the report interval at whi				
Issue6925(0)	Profile #1	Enable	Profile #2	Enable	Available / Disabled Bulk Data Categories
issueses(0)	Report Interval (sec)		Report Interval (sec)		
b # tttt1(3)	120	~	300	~	L
▷ ♣ tttt4(2)					
Delete Devices	* Bulk Data Categories		Bulk Data Categories		
Delete Derives	WAN and VPN	Size: 8	Users and Apps	Size: 4	

ltem	Description		
Search by Device ID/Name/Model/MAC/I P Address	Enter the ID, name, model or MAC/IP 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			
Network ID	Display a number which is given by VigorACS randomly for the selected network.		

Name Location Username	Display the name of the parent network. You can modify it if required. Type the location (e.g., HsinChu, New York) for this network.	
Username		
	Display the name of the selected network (e.g., rd8, in this case). Change it if required.	
Password	Display the password of the selected network. Change it if required.	
Advanced Settings		
Enable SD-WAN	Enable or disable the SD-WAN function for current network group.	
Bulk Data Settings		
Profile #	Enable - Click to enable or disable the profile.	
	If you disable bulk data categories, it will affect the SD-WAN operation.	
Report Interval (sec)	Specify the report interval for the profile returning a bulk data to VigorACS server.	
Bulk Data Categories	Set the category of data to be collected for statistical analysis. You can freely select the data you want to count. Use drag and drop to place each category in the corresponding profile, and specify the report interval at which the profile returns a bulk data to VigorACS server.	
Available / Disabled Bulk Data Categories	At present, available categories include <i>VoIP, WAN and VPN, Users and Apps</i> . Each category can be joined to the selected profile or be removed from the selected profile, by using drag-and-drop.	
Reset Bulk Data Profiles to Default	Click to reset to factory default settings of Bulk Data Settings.	
Disable All Bulk Data Profiles	After clicking the link, all data categories on Profile # will be removed. The data report for all CPEs under the selected network group will not be collected for VigorACS. Thus, no data, message can be collected by and displayed on the sub items based on SD-WAN feature under Monitoring menu. However, the SD-WAN functions such as Hub and Spoke, Full Mesh VPN, Route Policy, and VoIP WAN for the selected network group are still active.	
	0 0 Buik Data Categories 0 Buik Data Categories 0 0	

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

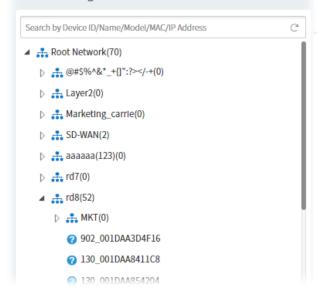
Add Network	
Parent Network	
rd8	
Name	
МКТ	~
Location	
HsInChu	
Username	
YFN	~
Password	
•••••	✓ ●

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



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.

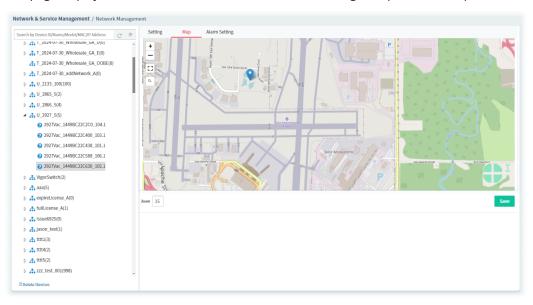
Network & Service Management / Network Manager	nent	
Search by Device ID/Name/Model/MAC/IP Address C 🚔	Setting Map Alarm Setting	
I_2024-01-30_WHOlesale_GA_D(0)		
T_2024-07-30_Wholesale_GA_E(0)	Delete This Device Change Network	
A T_2024-07-30_Wholesale_GA_OOBE(0)		
T_2024-07-30_addNetwork_A(0)	General Settings	
▷ ♣ U_2133_100(100)	Status	Known Device
▷ ♣ U_2865_5(2)	Disable Enable	Known Unknown
▷ 👬 U_2866_5(4)		
▲ 👬 U_2927_5(5)	Device ID 104532	Network ID 4422
2927Vac_1449BC22C2C0_104.1		
2927Vac_1449BC22C400_103.1	Model Name Vigor2927Vac	Device Name 2927Vac_1449BC22C630_102.1
2927Vac_1449BC22C438_101.1		Note 2
2927Vac_1449BC22C588_106.1	Note 1	
2927Vac 1449BC22C630 102.1	Serial number	MAC Address
VigorSwitch(2)		14:49:BC:22:C6:30
aaa(5)		
expireLicense_A(0)		
fullLicense_A(1)	Location	CPE Client IP
> 👬 Issue6925(0)		192.168.103.10
Jason_test(1)	Phone No.	CPE Client Port
▷ ♣ tttt1(3)		8069
▷ ♣ tttt4(2)	Domain Name	CPE Client URI
▷ ♣ tttt5(2)		/cwm/CRN.html
transition transition	Management Protocol	CPE Client User Name
N	CPE default (http) http https	vigor
Delete Devices	Management Port	
	80	CPE Client Password
		0 Luk

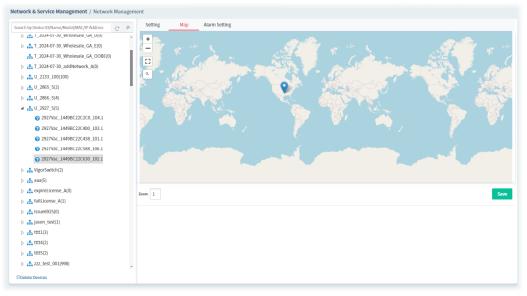
Item	Description
Delete This Device	Click to remove the selected CPE from current group.
Change Network	Click to change the network / group for the selected CPE.

	A concel Apply	
	Move the mouse cursor on the network you want and click Apply.	
General Settings		
Status	Disable – The selected device will be hidden on the tree view.	
	Enable – The selected device can be displayed on the tree view.	
Known Device	Known – The selected CPE is known(😃) to VigorACS 3.	
	Unknown – If the selected CPE is new added device, it will be identified as Unknown (?).	
Device ID / Network ID	Device ID – Display the number of that device which is given by VigorACS 3 randomly.	
	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.	
	Device Name – Display the name of the device for identification. It can be changed if required.	
Note 1 / Note 2	Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network.	
Serial number / MAC	Serial number – Enter a number for identification of the device.	
Address	MAC Address – Display the MAC address of the device.	
Location	Display the position of the device.	
Phone No.	It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device.	
Domain Name	Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE.	
Management Port	Enter a port number which will be used for accessing into web user interface of the CPE.	
Management Protocol	Choose HTTPS or HTTP.	
CPE Client IP / Port / URI	Display the IP address, port number and URI.	
CPE Client User Name / Password	Display the username and password that VigorACS 3 can use to access into the CPE.	
	Edit - Click to change the username and password.	

6.4.1.4 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.

6.4.1.5 Alarm Setting

VigorACS can detect the WAN interface for specific CPE or network group and send alarm message if the selected WAN interface disconnection due to some reasons.

Network & Service Management / Network Ma	inagement
Search by Device ID/Name/Model/MAC/IP Adc C 😤	Setting Map Alarm Setting
▷ 👬 I_2024-07-30_Wholesale_GA_D(0)	Alarm setting as parent network
T_2024-07-30_Wholesale_GA_E(0)	
T_2024-07-30_Wholesale_GA_OOBE(0)	
T_2024-07-30_addNetwork_A(0)	WAN Alarm Settings
▷ 🚠 U_2133_100(100)	WAN disconnection alarm Interface
▷ ♣ U_2865_5(2)	
▷ ♣ U_2866_5(4)	Interface:
⊿ 👬 U_2927_5(5)	WAN2
2927Vac_1449BC22C2C0_104.1	WAN3 Save
2927Vac_1449BC22C400_103.1	WAN4
2927Vac_1449BC22C438_101.1	WANS WANG
2927Vac_1449BC22C588_106.1	WATU
2927Vac_1449BC22C630_102.1	
▷ 🚠 VigorSwitch(2)	
D 🚓 aaa(5)	
expireLicense_A(0)	
Image: A fullLicense_A(1)	
▷ 🚠 issue6925(0)	
jason_test(1)	
▷ 👬 tttt1(3)	
▷ 🚠 tttt4(2)	
▷ 🚠 tttt5(2)	
<pre>> # zzz_test_001(998)</pre>	
間 Delete Devices	

These parameters are explained as follows:

ltem	Description
Alarm setting as parent network	Switch the toggle to enable/disable the setting. Enable – If enabled, the alarm setting for specified CPE will be the same as the parent network.
	Disable – If disabled, please specify the WAN interfaces independently for the specified CPE.
	• WAN Alarm Settings – Select WAN interfaces to let VigorACS send an alarm message to the CPE if the selected WAN interface disconnected.

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

6.4.2 Service Management

The System Administrator can import DrayTek WCF license keys and assign them to or cancel the assignment of the keys to the managed user groups.

6.4.2.1 Service Subscription

Open Nework & Service Management >> Service Management. Click the Service Subscription tab.

(%) ==	Network & Service Management	Network & Service Management / Service Management User Group: RootCroup	C
	Network Management	Service Subscription History	
	Service Management		
		Bind with MyVigor Account	
Z		Status Login with MyVigor	
Ø			
-			

Click **Login with MyVigor** to get the following dialog.

	Tak
Dray	Тек
MyVigo	r
Isername	
draytek_rd8	
assword	
	Q
Login	
Login	

Please enter the username and password registered for the MyVigor server.

The following web page will appear.

=	Dray Tek VigorACS 3 Root Network (100142) Q Pcap et al. 13:43:22 BIL5(24) mk_carrie system Administrator	М							
(7)	Network & Service Management / Service Management	С							
<u></u>	User Group CootGroup								
-0	Service Subscription History								
z	Bind with MyVigor Account								
P	Status draytek_rd8 Log out Unbind								
	User Group Device Service Subscription 🛛 🐵								
\$	Manage Subscription								
23	Service Status Purchased Used Nodes								
(i)	URL Reputation - B Card Unsubscribed Total : 0 Node								
0	URL Reputation - A Card Unsubscribed Total : 0 Node								
	URL Reputation - Silver Card Subscribed 1 1 Total : 1 Node								
	Network Device Inventory								
	Select Network (13) Vetwork (13)								
	Network ID 2								
	Device Name 41 Model 41 MAC Address 41 Serial Number 41 License Type 41 Binding Status 41 MyVigor Account 41 Auto Renew?								

ltem	Description				
Bind with MyVig	gor Account				
Status	To bind with MyVigor Account, make sure you already have one set of user account and user password to login MyVigor website. If not, apply one account first.				
	Login with MyVigor – Enter the user name and user password using MyVigor account to login MyVigor website.				
	Relogin MyVigor – This button appears if you have login MyVigor website previously and successfully. Click to access MyVigor again.				
	Log out – Log out MyVigor website but still bind with MyVigor server.				
	Unbind – Unbind from MyVigor website.				
User Group Dev	vice Service Subscription				
0	Click this icon to open the settings dialog.				
~	Settings				
	Auto Apply				
	Auto Renew				
	Cancel Save				
	Auto Apply – Switch the toggle to enable or disable the function. When enabled, the VigorACS server will automatically send a license key to a newly added device for the currently selected user group.				
	Auto Renew - Switch the toggle to enable or disable the function. When enabled, the VigorACS server will renew a license key for the device with a nearly expired key for the currently selected user group.				

Manage Subscription	Bind the selected license keys to specified device. Click to open the following page.	
	Manage Subscription ×	
	3 Select Service Select Device Confirm	
	Select Service	
	Service Purchased Keys Keys Currently Avaliable	
	URL Reputation - B Card 3 3	
	URL Reputation - A Card 8 4	
	URL Reputation - Silver Card 5 2	
	Auto Renew	
	Previous Next	
	Enable Auto Renew to renew the licenses for all specified devices	
	automatically.	
	After selecting the service card (s), click Next .	
	Manage Subscription X	
	1 2 3 Select Service Select Device Confirm	
	Selacted Service URI Reputation - Silver Card Available Keys : 2	
	Select Networks or Devices Name Model Name WAC Address	
	A Cool Network(3)	
	Elvis(0) Network-RD8(0)	
	C 0 2562_1449BC3EECC8 Vigor2962 14:49:BC:3B:ED:C8	
	① 3510_14498C5E9178 Vigo(3910 L4:49:BC:58:91:78 ① 35125_14498C30266F8 Vigo(3912S L4:49:BC:30:C6:F8	
	Provious Next	
	Select the CPE(s) to apply the service card. Then click Next .	

	Manage Subscription
	0-0-0
	Select Service Select Device Confirm
	Confirm
	Selected Service Available Keys Selected Devices Remaining Keys URL Reputation - Silver Card 2 1 1
	Auto Renew Enable
	Previous Apply
	Previous Apply
	Click Apply.
	Manage Subscription
	Enable List
	Drvice Name Model MAC Address Status Message
	2962 1449BC38ECC8 Vigor/2962 1449BC3BECC8 1 Success
	Selected Service Available Keys Success Devices Remaining Keys URL Reputation - Silver Card 2 1 1
	Auto Renew Enable
	✓ Finish
	The page with brief summary will be shown as above. Click Finish to exit this page.
Service	Display the name of the service (e.g., URL Reputation).
Status	Display current status (Unsubscribed or Subscribed) of the service.
Purchased	Display the quantity of the service card purchased.
Used	Display the quantity of the service card used.
Nodes	Display the number of nodes that have used this service card.
Network Device Invento	ŗy
Select Network	To view the status of keys bound of CPE devices under some group, use the drop-down list to select the network you want.
Network ID	Display the index number of the current network, randomly assigned by VigorACS for identification.
Edit	Click the button to activate and enable the Auto Renew, Cancel, and Save buttons for editing.
Device Name	Display the name (composed by model and MAC address) of the device.

Model	Display the model name of the CPE.
MAC Address	Display the MAC address of the model.
Serial Number	Display the serial number of the model.
License Type	Display the license type used by the model.
Binding Status	Display the binding status (expired, or others).
MyVigor Account	Display the name of MyVigor account.
Auto Renew	Switch the toggle to enable / disable the Auto Renew function.
Save	Save the current settings.

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

6.4.2.2 History

This page displays the binding record of CPE and WCF license.

Bi	inding Log	5		Activated a	t Select a date	🗇 ~ Select	a date 📋 License Type	All	∽ Search
Us	ser Group	Network	Device MAC	License Key	Activated Date	Expired Date	License Type	Action	Status Operator
Ro	otGroup	Root Network	00:1D:AA:65:33:08				URL Reputation - B Card	Bind	Device is not exist
Ro	ootGroup	Root Network	00:1D:AA:66:E0:20				URL Reputation - B Card	Bind	Device is not exist
Ro	otGroup	Root Network	14:49:BC:30:72:A0	1656A-80691-7B7E4-39021	2024/01/22	2024/02/21	URL Reputation - Silver Card	Bind	Success
Ro	otGroup	AutoTest_SD-WAN	14:49:BC:34:F5:D0				URL Reputation - A Card	Bind	Device is not exist
Ro	otGroup	AutoTest_SD-WAN	14:49:BC:34:F5:D0				URL Reputation - A Card	Bind	Device is not exist
Ro	otGroup	Root Network	00:1D:AA:4A:CF:B0				URL Reputation - A Card	Bind	Device is not exist root
									Show 10 v entries < 1

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.

(7)	System
000	System Parameter
<u></u>	Language
-0- 0-	External Monitoring Server Access Control
(((1)	Storage Management
	Upload Serial Number
Z	API Keys
P	Certificate
南	Backup Database
	Login Bulletin Adverts Carousel
<u>ية</u>	Logs
<u>}</u>	XMPP Profile Server Support Settings App Server
	License Key Pools

6.5.1 System Parameter

System / System Parameter			C
			Search Q
ID	Name	Value	
88	EnableSecureCookieSessions	false	
87	JbossConfigForStandaloneMode	standalone.xml	
86	ForceWUIRedirectHttps	false	
85	NotifyServerProcessCountPerMinute	-1	
84	EnableClientRecord	true	
83	IsDeleteExpiredClientTrafficByTimestamp	false	
82	O 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	HealtherExposeIp	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
	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
	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
	ABBI COSINC

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
40	True – Enable the function of data collection (StatisticsStep) for RRD traffic.
47	AutoDetectRouteName
4/	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
52	DeleteOldDeviceBySamelP True – If a new CPE with an IP address which is the same as an old device recorded on
52	DeleteOldDeviceBySameIP
52	DeleteOldDeviceBySamelP 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.
	DeleteOldDeviceBySamelP 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.
	DeleteOldDeviceBySamelPTrue - 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.DisablePolling
	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. DisablePolling True – Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration.
54	DeleteOldDeviceBySamelP 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. DisablePolling True - Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration. False - Default value. DisableAlarmMailByClear True - Disable the function of sending alarm e-mail when alarm status is clear. It is the
54	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. DisablePolling True - Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration. False - Default value. DisableAlarmMailByClear True - Disable the function of sending alarm e-mail when alarm status is clear. It is the default setting.
54	DeleteOldDeviceBySamelP 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. DisablePolling True - Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration. False - Default value. DisableAlarmMailByClear True - Disable the function of sending alarm e-mail when alarm status is clear. It is the

	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.
67	EnableAutoChangeWebPort
	True – Enable for changing web port automatically. It is the default setting.
	False – Disable the function.
	DisableSaveInformLog

	True – Disable the function of Save Inform Log.
	False – Default value.
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	HealtherExposelp
	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
	True – Enable the function of displaying graph of web user interface. It is the default value. False – Disable the function.
78	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.
79	EnableAuditorDeletedLog
79	
79	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
79 80	 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
	 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.

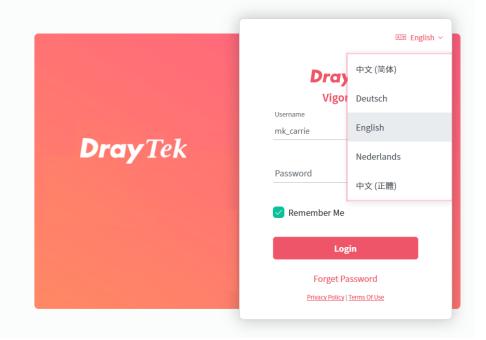
81	PacketCaptureTool
	True – VigorACS will capture the packets automatically and the result will be specified from the drop down list of Capture Packets on the top-right of the screen.
	False – Default value.
82	ClientRecordAliveTimeInDays
	Set the number of days for reserving the record (about client 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.
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
	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, theForceWUIRedirectHttps 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.
	• Size
	Periodic
	Periodic-size
91	MapServiceProvider
	There are two mechanisms to display maps on VigorACS, Google and Leaflet.
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.

93	NetflowSetPortConfig
	The function in "Monitoring>>Flow" requires VigorConnect servers, which are installed in remote networks, to collect NetFlow data from routers in the background.
	When browsing "Monitoring>>Flow" on VigorACS, the corresponding VigorConnect servers will establish connections to VigorACS. Thus, VigorACS can retrieve the relevant data. The idle timeout of the connection is 30 minutes. This parameter defines the allowed port range on the VigorACS server to be used for incoming connections from VigorConnect.
94	ShowRootNetworkGraphicStatistics
	true - If it is enabled, the graphic statistics can be seen on the Dashboard for the Root Network.
	false - Default setting.
95	WebServicesRateLimit
	Set a number that allows the web service API to receive requests from the user. The default is 10. It means 10 requests can be accepted by the VigorACS server within 1 minute.
96	EnableAccessControlByMAC
	If enabled (true), VigorACS permits CPE registration with MAC address listed in System>> Upload Serial Number only.
97	ResendSetParameterByBootstrap
	If enabled (true), VigorACS will resend the corresponding set parameter when the 0 BOOTSTRAP event code is received from CPEs. This allows you to push configuration again when CPE has been factory reset.
98	HeartbeatInterval
	It is the VigorACS server method to determine whether a CPE is online.
	When the value equals 0, VigorACS will poll CPE automatically; when there is no response, VigorACS will consider the CPE offline.
	When the value exceeds 0, and the CPE does not send an Inform within this period, the VigorACS server will consider the CPE offline. That means the VigorACS will not actively check the online and offline status of the CPE.
	Notes:
	The time unit is in second.VigorACS needs to restart after changing the setting.
99	EnableNewFirmwareReleaseNotify
33	If enabled (true), Notification Center will show the notification about new firmware release.
100	MaximumUploadFileSize
100	Set the maximum upload size (unit: MB) for the CPE firmware file.
101	ResetCredentialAfterMovingNetwork
	The parameter can change CPE TR069 Username and Password.
	If enabled (true), TR069 Username and Password of CPE moved to a network with blank Username and Password will be changed to the Username and Password of the higher level network.
102	DisableAlarmSNMPTrapForDeviceLossConnectionByACSReboot
	If enabled (true), VigorACS will suspend alarm messages by SNMP trap so the device loses connection after VigorACS restarts.
103	ResendGlobalParameterByBootstrap
	If enabled (true), VigorACS will resend the corresponding global parameters when the 0 BOOTSTRAP event code is received from CPEs. It allows the configuration to be pushed

	again when the CPE has been factory reset.
Save	Save the current settings.

6.5.2 Language

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



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

Open System >> Language.

Syst	System / Language									
⊥Upload @Delete ⊥ Download						И <	1	/1	>	G
	Filename	¢↑	Size	$\downarrow \uparrow$	Last Modified					$\downarrow\uparrow$
	lang_CN.txt		218722		2024/07/20 05:06:31					
	lang_DE.txt		564595		2024/05/29 05:06:35					
	lang_EN.txt		443410		2024/05/29 05:06:35					
	lang_NL.txt		570735		2024/07/20 05:06:31					
	lang_TW.txt		438027		2024/07/20 05:06:31					

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.

Health Server	System / External Monitoring Server		
Wireless Client Information Server	Enable Server		
	URL	api.iptechview.com	
	Username	acs.drayddns.com	
	Password	••••	
	API	Health_Default_GLOBAL ~	
			Cancel Save
	L		

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.
API	Use the drop down menu to specify the third party's server.
Cancel	Discard current settings and restore the default settings.
Save	Save and activate the current settings.

6.5.3.2 Wireless Client Information Server

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

Health Server	System / External Monitoring Server		С
Health Server Wireless Client Information Server	User Group	RootGroup	
Whetess cheric mormation betwee			
	Enable Server		
	Authentication	NzYCcCGM23NS2sW2rGpWJC6apQLsE48tZkqD86Vac	
	URL	http://www.draytek.co.uk/forms/json.php	
	API	Wireless_Client_Default_GLOBAL ~	
		Saw	

ltem	Description		
Use the drop down list to specify a user group. In which, RootGrou contains all of the users with the role of system administrator in d			
Enable Server	Click the icon to enable / disable the server.		
Authentication	Enter a string for authentication.		
URL	Enter the URL or IP address of the third party's server.		
Dns API Service	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	Block	Device List	
WUI Login			None	Blacklist	Whitelist
CPE Service			None	Blacklist	Whitelist
API WebService			None	Blacklist	Whitelist

These parameters are explained as follows:

Item	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.

						Search IP / Description	C
+ Add 🏦	Delete All						Limit: 3/2
IP ↓↑	Description ↓↑	WUI Login $\downarrow\uparrow$	CPE Service	API WebService	J↑		
1.1.1.1	ttl				🖉 Edit	1 Delete	
111.111.111.111	tt2				🖉 Edit	🛍 Delete	
	tt5				// Edit	🗇 Delete	

ltem	Description
Search IP / Description	Enter an IP or a brief description for searching the profile.
+Add	Click to create a new profile with a blacklist.
Delete All	Click to delete all profiles.
IP	Displays the IP address, IP range, or subnet specified on the profile.
Description	Displays the comment of the profile.
WUI Login,	Displays the type(s) selected for the profile.
CPE Service,	Select the type(s) by checking the box(es).
API WebService	
Edit	Click to modify, change the selected profile.
Delete	Click to remove the selected profile.
Save	Click to save the settings.

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

IP Address For	m		2
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 Enter a name of the blacklist profile.		
Description			
Address Type	Specify the address type to enter the IP address. Single IP Address Range IP Address Subnet IP Address Will Login COPE Service 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 AddressIt 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.

Whitelist Block Device List						
					Search IP / Description	٩
						Limit: 1/256
Description $\downarrow\uparrow$	WUI Login $\downarrow \uparrow$	CPE Service 41	API WebService	¢↑		
192.168.105.141				<i>⊘</i> E	dit 🛍 Delete	
						Save
	Description J↑	Description 1 WUI Login 1+	Description ↓↑ WUI Login ↓↑ CPE Service ↓↑	Description 🕴 WUI Login 4↑ CPE Service 4↑ API WebService	Description 🕴 WUI Login 4↑ CPE Service 4↑ API WebService 4↑	Description J↑ WUI Login J↑ CPE Service J↑ API WebService J↑

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 profile with a whitelist.
Delete All	Click to delete all profiles.
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. Select the type(s) by checking the box(es).
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	v			
Start IP Address	123.12.1.10] ~		
Service Enable	🗹 WUI Login 🗹 CPE Service				
	API WebService				
				× Cancel	🖹 Save
					4

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 Subnet 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.		

6.5.4.4 Block Device List

This page displays information related to device(s) blocked by the VigorACS server.

System / Ac	cess Control					
General Settin	g Blacklist	Whitelist	Block Device List			
Id	Name	Model Na	me	Firmware Version	IP Address	Network
				No data available		

6.5.5 Storage Management

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

em / Storage Management	
rLogs	
All ~	
ete Type 🚱 🔅 Alarm 🗋 Log 📄 Device Syslog	
o Clear	
ation Every Day Every Week Every Month	
iodic(days)	
Jear Now	

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, and Device Syslog) that corresponding log can be deleted through this 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.						
Clear 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.						

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.

ûUploa	d ≟Download Template ≟Expo	rt + Add @Delete	Search		Rows 10 ~	И < 1	$/1 \rightarrow \bowtie$
	Mac Address $\downarrow \uparrow$	Serial Number $\downarrow\uparrow$	Device Name $\downarrow \uparrow$	Network $\downarrow\uparrow$	Model ↓↑	WAN IP ↓↑	LAN IP 🕂 FV
	001DAA9FD698	1234657987					
	001DAAB0BB78	9999999999999999					
	001DAAE5CFA8	6543213212					
	001DAAFEF9D0	777777777777777777777777777777777777777					
	001DAAFEF9F0	888888888					

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.						
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.						
Export	Click to export the current serial number table as a file.						
Add	Click to add a CPE or VigorAP onto this table.						

	+ Add Form ×
	Mac Address Serial Number
	× Cancel 🕅 Save
Delete	Click to delete the selected entry.
Check box	Check the box to specify an entry. Later, the selected one required.

6.5.7 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.

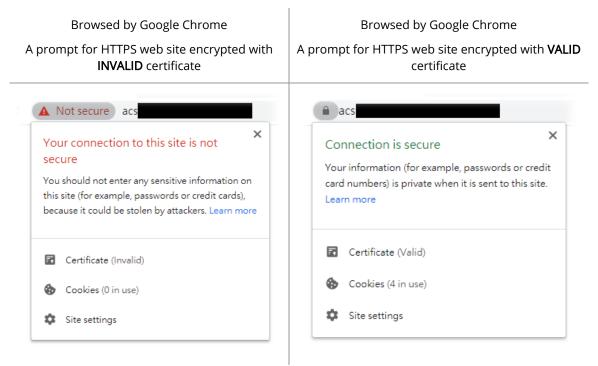
System / Google API Key								
Google Maps API Key 🚱	AlzaSyDnoAWeT6DlzdnkBPnjHGZv44ekxrePCdg							
	Please go to the function management to assign user roles to access the map.	Function Management						
	Or go to the System Parameter page to select another map service.	System Parameter						
Google Analytics API Key 🥑								
		Save						

ltem	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.									
	User / Function Management									
	Role SI	now Unknown Device	Wireless Is Writable	Show About Menu	Show Version Number	Show Maps	Can Reboot Device	Manage Public Area Files		
	Group Administrator									
	Administrator									
	Commissioning									
	Operator									
	Customized Operator									
	View Only Operator									
	Customized View Only Operator									
								Save		
	• System Parameters - There are two mechanisms to display maps of VigorACS, Google and Leaflet. Select the one you need.									
	91 © MapServiceProvider 90 © EnableCommonCpeWul 89 © LogRotationiHandlerType					Leaflet Google Leaflet Ze		~		
Google Analytics API Key	Enter the analy	tics API	key for tr	acking tl	ne data.					
Save	Save and activa	te the c	urrent se	ttings.						

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.



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.

rtificate Certificate with private key	PKCS #12 Let's Encrypt	
1. Create a local Certificate Signing Reques	:(CSR) :	
Generate a CSR		
① Note: Please submit the "certreq.csr" file	to the Certificate Authority then do the next step.	
2. Import Certificate :		
Root CA Certificate (.cer, .crt)		Browse
Intermediate CA Certificate (.cer, .crt)		
	Brows	e Delete
	+Add	
Trusted Certificate (.cer, .crt)		Browse
nusteu ceruncate (.cer, .crt)		
		C arrow
		Save

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 PK	CS #12	Let's Encrypt					
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)							Browse
Root CA Certificate(.cer, .crt)							Browse
Intermediate CA Certificate(.cer, .crt)						Browse	Delete
		+Add					
Trusted Certificate(.cer, .crt)							Browse
							Save

ltem	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.		
When With Root and In	termediate 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.		
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 CA Bundle i	s selected		
CA Bundle (.cer, .crt)	Click the Browse button to select one certificate or obtain the content of the certificate from the clipboard.		

Trusted Certificate (.cer, .crt)Click the Browse button to select one Trusted CA certificate or obtain content of the certificate from the clipboard.			
When One PEM File is selected			
PEM File (.pem)	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	Root CA Certificate
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 類型: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.

System / Certificate		
Certificate Certificate with private key PKCS #12	Let's Encrypt	
Import PKCS #12 file	Browse	I
PKCS #12 Password	¢	
① Note: Please use the "tr069" as the entry name for ye	ur PKCS #12 certificate file.	
	Save	l i

These parameters are explained as follows:

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

6.5.8.4 Let's Encrypt

This page will help to

- create a Private Key & Account from Let's Encrypt .
- create a Certificate signed by Let's Encrypt Account.
- automatically change your keystore file form your Certificate.

System / Certificate	
Certificate Certificate with private key PKCS #12	Let's Encrypt
Register Domain	
Auto Renew	
Challenge Type	HTTP-01 Challenge DNS-01 Challenge
Copy Current Domain to Register Domain	Copy to register domain
Note: Acme Let's Encrypt will do the following things Creating a Private Key & Account from I Creating a Certificate sign by Let's Encr Automatically change your keystore file	et's Encrypt . /pt Account.
 Note: Let's Encrypt provides rate limits to ens 	ure fair usage by as many people as possible. For more information please visit ACME website.
	Generate Save

and

Certificate Certificate with private key PKCS #12	Let's Encrypt			
Register Domain				
Auto Renew	\bigcirc			
Challenge Type	HTTP-01 Challenge DN	4S-01 Challenge		
API			~	
Export Data	Key DuckDNS_T	Value oken aaaaaaa-bbbb	Action	
	+Add			
Note: Acme Let's Encrypt will do the following things: • Creating a Private Key & Account from Let's Encrypt . • Creating a Certificate sign by Let's Encrypt Account. • Automatically change your keystore file form your Certificate.				
 Note: Let's Encrypt provides rate limits to ensure 	e fair usage by as many pe	ople as possible. For more information	n please visit ACME website.	
			Generate Save	

ltem	Description		
Register Domain	Enter the URL for registering the certificate.		
Auto Renew	If enabled, the VigorACS server will periodically detect the validity of the certificate.		
	It will be renewed automatically by VigorACS once the certificate is nearly expired.		
Challenge Type	To validate the domain names, select HTTP-01 Challenge or DNS-01 Challenge as the challenge type used by this certificate. The default setting is HTTP-01 Challenge.		
API	Use the drop down list to select an interface.		
Export Data	The third-party API (with specified key and value) can be exported for other purposes.		
	Key - Enter the string provided by the third-party API.		
	Value - Enter the information (e.g., URL, server ID, token, or number) provided by the third-party API.		
	Delete - Click to remove the selected entry.		
	+Add - Click to have new fields for creating new key and value.		
Generate	Click to generate the Let's Encrypt certificate based on the above configuration.		
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.

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
estBckDaily	Now	 Completed 	2019-03-21 14:17	yrctw	Internal	🖉 Edit 🕆 🕆 Delete
estBckDailyPM	Dally	Completed	2020-11-02 20:00	yrctw	Internal	🖉 Edit 🔺 🗎 Delete
askBckNowExclude	Now	 Completed 	2020-10-29 15:55	yrctw	Internal	🖉 Edit 🔋 Delete
ackup	Now	 Completed 	2020-03-03 09:20	arles	Internal	🖉 Edit 🕆 Delete

These parameters are explained as follows:

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		×	
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 \sim		
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		

ltem	Description		
Task Settings	Enable 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 available when Once is selected as Run Backup.		
	 Starts on xxxxx – It is available when Repeat is selected as Run Backup. Click Edit to open the following web page for modifying the time setting. 		

	Repeat			
	Repeats	Weekly		
	Repeat on	Sun Mon Tue Wed		
	Starts on	02/25/2020		
	Starts time	00:00		
	Summary	Weekly on Sunday		
	le			
		Cancel Done		
Backup Options	Backup Type - Choose an	ontion to perform the backup		
	Backup Type – Choose an option to perform the backup.			
	Backup all tables ~			
	Backup all tables			
	Exclude syslog tables			
	Exclude syslog and log tables			
	Ignore License Tables – VigorACS system performs the database backup by			
	ignoring the tables concerning of backup and license (such as syscd, syssn, dslpmid, dslpmshow and etc.,) to prevent from license error while			
	transferring VigorACS server. The default value is "Enabled".			
	Compress Backup File - The backup file will be compressed.			
	After backup delete log tables – Delete the log tables immediately when			
	VigorACS server finishes t			
Email Notification	 Enable Email Notification – If enabled, VigorACS server will send a notification email about database backup to the recipient. Email Subject – Enter the subject for the email. 			
	• Email From – Enter the email address of the sender/agent/registrar.			
	 Email Content – Enter the content of the email. Email To – Enter the email address of the recipient. 			
	 +Add recipient – Add VigorACS server. 	d more recipients to receive the email from		
Cancel	Discard current modification.			
Save	Save the current settings and exit the page.			

6.5.9.2 Backup Files

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

ackup Tasks	Backup Files Error Logs		
Delete	LDownload		1 < 1 /44 > 1 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
0	backup_ACS_Trunk AutoBuild 13427_ExcludeSyslogAndLogVer_2020-02-08.2000.sql	11.83 MB	02/08/2020 20:00:03

ltem	Description	Description				
Delete	Click to remove the selected filename.	Click to remove the selected filename.				
Download	Click to download the file from the hard disk of Vigo restoration or transferring.	orACS server located for				
	System / Backup Database Backup Tasks Backup Files Error Logs Detet -i-Download					
	Filename	↓↑ Size ↓↑ Last Modified				
	backup_ACS_Trunk AutoBuild 2016_ExcludeSyslogAndLogVer_2020-11-02.2000.sqLzip	1.09 MB 11/02/2020 20:00:04				
	backup_ACS_Trunk AutoBuild 2016_ExcludeSyslogAndLogVer_2020-11-01.2000.sqLzip	1.09 MB 11/01/2020 20:00:02				
	backup_ACS_Trunk AutoBuild 2016_ExcludeSystogAndLogVer_2020-10-31.2000.sqLztp	1.09 MB 10/31/2020 20:00:07				
	backup_ACS_Trunk AutoBuild 2016_ExcludeSyslogAndLogVer_2020-10-30.2000.sqLztp	1.09 MB 10/30/2020 20:00:07				
Filename	Display the name of the backup file.	Display the name of the backup file.				
Size	Display the size of the backup file.	Display the size of the backup file.				
Last Modified	Display the last modified time.	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 Ta	sks Backup Files Error Logs				
			K < 1 /1	> N	C
	Filename	↓↑ Size ↓↑ Last Modified			4
	backup_ACS_Trunk AutoBuild 1024_ExcludeSyslogAndLogVer_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_ExcludeSyslogAndLogVer_2020-07-09.2000_error.log	0 Byte 07/09/2020 20:00:00			
	backup_ACS_Trunk AutoBuild 852_ExcludeSyslogAndLogVer_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.

=	Dray Tek VigorACS 3	Root Network (100142)	✓ Q	Pcap	15:54:08 7/31/24	mk_carrie System Administrator	М
(7)	System / Login Bulletin						
-			Preview General Settings	Bulletin Items	1		
				⊕ EN ~			
Z			Dray Te	ek –			
			VigorACS				
(Dray Tek					
			Username				
<u>ې</u> ا			Password	٢			
23			Remember me				
í			Login				

6.5.10.2 General Settings

Preview General Settings Bulletin Items Image: Setting setti	=	Dray Tek VigorACS 3	Root Network (100142)	✓ Q	Pcap 🏳	15:54:08 7/31/24	mk_carrie System Administrate
Show Carousel Indicators C Shuffle Message C Shuffle Message C Shuffle Message	11↓	System / Login Bulletin	Dray Tek	Enable Login Bulletin		Î	

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.

М

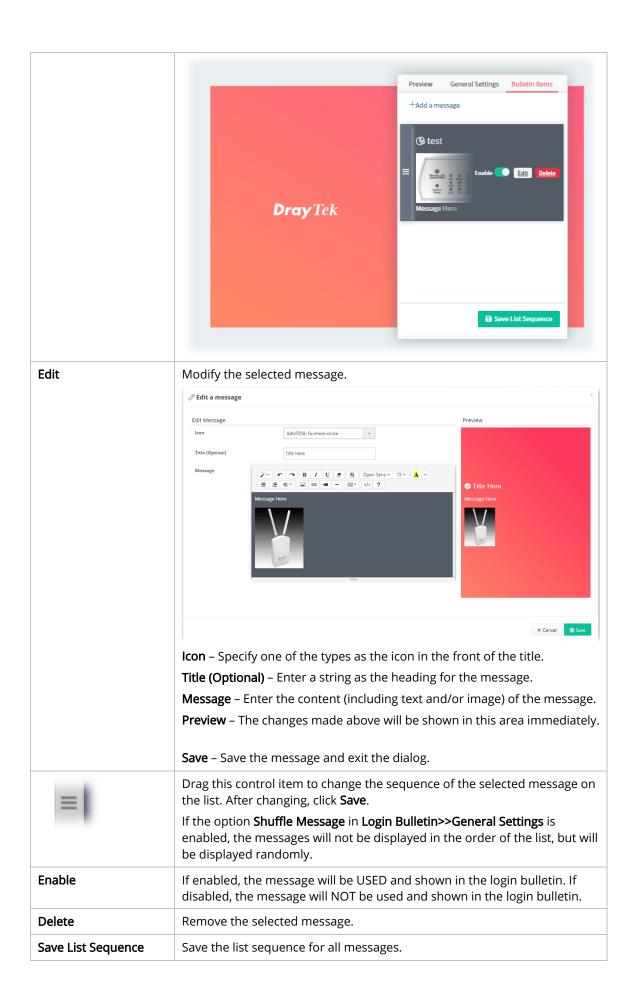
6.5.10.3 Bulletin Items

=	Dray Tek VigorACS 3	Root Network (100142)	✓ Q	Pcap	15:54:08 7/31/24	mk_carrie System Administrator	М
(7)	System / Login Bulletin						
<u></u>			Preview General Settings	Bulletin Items			
			+Add a message				
			A Notice: Option "Shuffle Messag has been enabled. The messages				
Z			following order but in random.				
		Dray Tek					
। 🔅							
쓰							
í							
				ave List Sequence			

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
	Icon  fa-check-sircle v	
	Title (Optinal) Title Here	
	Message Here	● Title Hare Message Here
		X Cancel 🔯 Save
	lcon – Specify one of the types as the icon in the	front of the title.
	Title (Optional) – Enter a string as the heading fo	r the message.
	Message – Enter the content of the message.	
	Preview – The changes made above will be show	n in this area immediately.
	Save – Save the message and exit the dialog. Ref result.	fer to the following setting

These parameters are explained as follows:



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

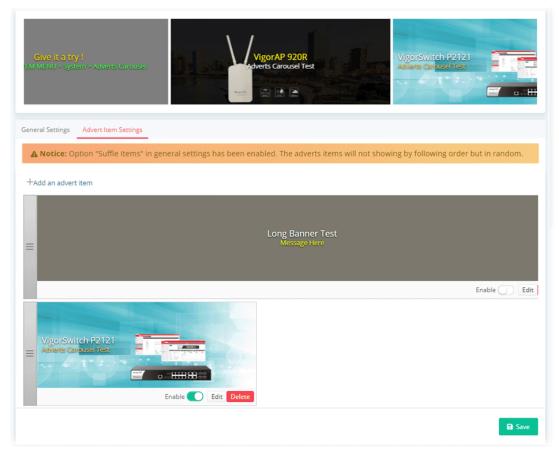
This page determines if displaying the adverts on the login page or not, enabling the auto play carousel function, selecting cycling delay time and using the shuffle items.

System / Adverts Carousel	
Adverts Carousel Preview	~
	Vigor2762 Series Adverts Carousel Test Change it on SYSTEM MENU > System > 1
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:

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

To add an advert item, do the following steps.

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

Add an item Add a		×
Upload Image	Please select an image. Browse	
	الله Upload گ	
①Note:Height will automaticall	y adjust to 180px.	
 Notice: Image width needs to b 	e greater than or equal to height.	
Preview		
	Upload an Advert Image Please upload an image first.	
		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 automatica adjusted to 180 pixel. Image width needs to be greater than or equa 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	
1	د Upload	ĺ
Title (Optinal)	Title Here (Max. 60 characters)	ł
a Title Color		
Message (Optinal)	Message Here (Max. 250 characters)	
Message Color	- #IIIII	
Enable Hyper Link		
Link Address	http://www.draytek.com/	
Text Block Position	0 1 2	
	3 4 5 6 7 8	
Preview		
	Tide Here Wassage Here	
	Cancel 🔯 Save	

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

Preview	Any changes on this setting page will be shown in this field.
	Preview
	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.

Give it a try ! EMMERU > System > Asserts Carousel The second and the second an
General Settings Advert Item Settings
A Notice: Option "Suffle Items" in general settings has been enabled. The adverts items will not showing by following order but in random.
+Add an advert item
E Long Banner Test Message Here
Enable Edit
G Save

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	If enabled, the advert item will be USED and shown in the adverts carousel. If disabled, the advert item will NOT be used and shown in the adverts carousel.		
Edit		ys for the selected image. ✓ Please select an image. Browse	
Delete	Delete the selected advert item.		
Save	Save the current settings.		

6.5.12 Logs

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

System / I	ogs							2020/10/04 to 2020/11/03 ~	search ID / Username / Login IP
ICS System	1 Log Syster	n Log Login	Log Acce	ss Control Lo	g				
		verity / Category							
Critical	Major Mir	nor Warning	Normal	Mainten	ance Reports Provisioning Ne	twork System User Apply Succeeded Apply Failed			
								И	< 1 /6 > N C
ID	User	Authentication	Severity	Interface	Category	Overview	Result	Login IP	Time
3718	յու	Internal	▲ Critical	WUI	User > Group Management	User root has been removed from RootGroup's group	Succeeded	172.16.3.134	2020/11/03 10:21:38 AM
3717	angela	Internal	\Lambda Major	WUI	Provisioning > Global Parameters	(Angela) Profile test_angela has been added.	Succeeded	172.16.3.134	2020/10/30 11:42:57 AM
3716	Kevin	Internal	\Lambda Minor	WUI	Network Management	ALANWEN (82) Network location has been changed.	Succeeded	192.168.105.99	2020/10/28 04:32:54 PM
3715	David	Internal	\Lambda Minor	WUI	Network Management	AP 1060C_001DAA80FED4 (141446) Device has been deleted.	Succeeded	192.168.105.135	2020/10/28 03:39:37 PM
3714	David	Internal	\Lambda Minor	WUI	Network Management	Network has been moved to another parent network.	Succeeded	192.168.105.135	2020/10/28 03:37:47 PM
3713	David	Internal	▲ Critical	WUI	User > User Management	User david has been created.	Succeeded	192.168.105.135	2020/10/28 03:04:44 PM
3712	arles	Internal	\Lambda Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192.168.105.120	2020/10/28 01:16:30 PM
3711	link_chiang	Internal	\Lambda Minor	WUI	Network Management	RD2 (138) Network Information has been updated.	Succeeded	172.16.2.145	2020/10/26 03:21:54 PM
3710	arles	Internal	\Lambda Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192.168.105.2	2020/10/26 03:04:00 PM
3709	arles	Internal	\Lambda Minor	WUI	Network Management	RD8 (53) Network Information has been updated.	Succeeded	192.168.105.2	2020/10/26 03:03:33 PM

ltem	Description			
ACS System Log / System Log / Login Log / Access Control Log / Device Reject Log / Server 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		C
Status	Disconnected	
Enable	\bigcirc	
Server IP/Domain	192.168.105.1	
Server Port (default : 5222)	9090	
Username	admin	
Password	•••••	Φ.
		Save

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**.

System / Delete Logs Actions		
Category filter: ACS Users Vigor Devices Network Clients	2021/01/26 to 2021/02/25 ~	search ID / operator / keyword c 🔍
	ы <	1 /1 → № C ⊗
ID 31 Category 31 Log Table 31 Operator 31 Authentication: Login IP 31 Deleted Object	↓↑ Overview	J↑ Time J↑
\wedge		
دا No data available		

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.

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.
	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.

6.5.16 App Server

To use the push notification function, the App Server must be ena	bled first.
---	-------------

System / App Server		C
Enable App Server App API Key		
	Send App Notification Test	
 O Note: An API key is required. Server' to get the ansatz 	ed to use the push notification functions. Please log in MyVigor and then click 'App PI Key.	
		Save

These parameters are explained as follows:

Item	Description
Enable App Server	Switch the toggle to enable/disable the function.
Арр АРІ Кеу	Enter the API key assigned by MyVigor server.
Send App Notification Test	Click to send a notification to the CPE.
Save	Save the settings.

6.5.17 License Key Pools

The System Administrator can import DrayTek WCF license keys and assign them to or cancel the assignment of the keys to the managed user groups.

From the following page, click **Login with MyVigor**.

(7)	System / License Key Pools	С
<u></u>	Bind to User Group	
4°°	Bind with MyVigor Account	
Z	Status Login with MyVigor	
		_
\$		

Later, a login page appears.

Dray	Tek
MyVigo	
Username draytek_rd8	
Password	۵
Login	

Please enter the username and password registered for the MyVigor server.

6.5.17.1 Bind to User Group

In this page, the System Administrator can assign the available license key(s) to the managed user groups.

Dray	YTek VigorACS :	3	Root Ne	etwork (100142) 🛛 🗸	a)	10: 8/	17:27 m 16/24 System Ad	Iministrator
Syster	m / License Key Pool	5						
Bind to	to User Group Key I	List						
Bir	ind with MyVigor A	Account						
Sta	atus	draytek_rd8	Log out Unbind					
Ava	vailable Keys							
	Total Keys	URL Reputation B Card	URL Reputation A Card	URL Reputation Silver Card				
			Acaiu	Silver Card				
	8 / 26	4 / 11	1/5	3 / 10				
Bir	8 / 26 ind Keys to User G	4 / 11			Nodes		Search User Grou	p Q
	ind Keys to User G	4 / 11	1/5	3/10	Nodes		Search User Grou	p Q. ∕∕ Edit
(user Group / Licer	4 / 11	1/5	3/10	Nodes		Search User Grou	
6	User Group / Licer	4 / 11	1/5	3/10	Nodes		Search User Grou	∕∕ Edit
6	Ind Keys to User G User Group / Licer (+) RootGroup (+) AutoTest	4 / 11 Group	1/5	3/10	Nodes		Search User Grou	 ✓ Edit ✓ Edit
	Ind Keys to User Goup/Llcer ① ③ ④ AutoTest ④ ●	4 / 11 Group	1/5	3/10	Nodes		Search User Grou	 ✓ Edit ✓ Edit ✓ Edit
	User Group / Licer ① RootGroup ① RootGroup ① AutoTest ① fullLicense_A ① expireLicense_A ① tttt1 ① tttt4	4 / 11 Group	1/5	3/10	Nodes		Search User Grou	 Edit Edit Edit Edit Edit Edit Edit Edit
	Ind Keys to User Goup/Llcer ① ③ ④ AutoTest ④ ●	4 / 11 Group	1/5	3/10	Nodes		Search User Grou	 Edit Edit Edit Edit Edit Edit

These parameters are explained as follows:

ltem	Description
Bind with MyVigor Accou	Int
Status	To bind with MyVigor Account, make sure you already have one set of user account and user password to login MyVigor website. If not, apply one account first.
	Login with MyVigor – Enter the user name and user password using MyVigor account to login MyVigor website.

	Relogin MyVigor – This button appears if you have login MyVigor website previously and successfully. Click to access MyVigor again.
	Log out – Log out MyVigor website but still bind with MyVigor server.
	Unbind – Unbind from MyVigor website.
Available Keys	
Total Keys x/y	Display current status (Unsubscribed or Subscribed) of all service (B, A, silver card).
	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation B card	Display current status (Unsubscribed or Subscribed) of the service (B card).
x/y	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation A card	Display current status (Unsubscribed or Subscribed) of the service (A card).
x/y	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation Silver Card x/y	Display current status (Unsubscribed or Subscribed) of the service silver card).
	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
Bind Keys to User Group	
User Group / License Type	Displays the name of the user group and the license type used.
Number of Keys	Display the quantity of the service card purchased.
Used Keys	Display the quantity of the service card used.
Nodes	Display the number of nodes that have used this service card.
Edit	Click to bind another key used for the selected user group.

To bind a key or keys to an existed user group,

1. Click **Edit** of a selected user group to open the following dialog.

Group Name	RootGroup	
Action	Assign New Keys	Cancel Assigned Keys
License Type	Remaining Keys In Pool	Add Keys To Current User Group
URL Reputation - B Card	4	0
URL Reputation - A Card	1	0
URL Reputation - Silver Card	3	0

2. Use the drop-down menu to specify the number of key(s) for binding with the user group. Then click **Next**.

Group Name	RootGroup		
Action	Assign New Keys	Cancel Assigned Keys	
License Type	Remaining Keys In Pool	Add Keys To Current User Gr	oup
URL Reputation - B Card	4	0	
URL Reputation - A Card	1	1	\$
URL Reputation - Silver Card	3	0	

3. A summary of the key additions will be displayed in the dialog. Click **Apply**.

Edit Key			
Confirm Key Assignment			
License Type	Added Keys	Remaining Keys After Key Assignment	
URL Reputation - A Card	1	0	
		Cancel Previous	Apply

Now the available keys will be changed as follows:

d to User Group Key	List				
ind with MyVigor	Account				
tatus	draytek_rd8	Log out Unbind			
valiable Keys					
Total Keys	URL Reputation B Card	URL Reputation A Card	URL Reputation Silver Card		
7 / 26	4 / 11	0 / 5	3/10		
ind Keys to User (Group				Search User Group
User Group / Lice	ense Type	Number Of Keys	Used Keys	Nodes	
① RootGroup					/ E
AutoTest					/ E

6.5.17.2 Key List

This page displays the binding record of CPE and WCF license. In addition, the system administrator can import more license keys to VigorACS server.

Moreover, the "Sync License" button is used to ensure consistency in the number of license keys between the MyVigor server and the VigorACS server. Click "Sync License" whenever you want to avoid inconsistent license keys.

Ŧ	Dray Tek VigorACS 3		Root Network (100142)	✓ Q	Pcap	11:13:32 mk_carrie 8/16/24 System Administrator
(7)	System / License Key Pools					
<u></u>	Bind to User Group Key List	_				
	Avaliable Keys					
Z	Total Keys 7 / 26	B Card	Reputation URL Reputation A Card Silver Card 0 / 5 3 / 10			
Ĩ	.,	.,	-,			
			Lio	ense Type All ~ Valio	dity All	✓ Search Q.
\$	Key List			Last Update Time : 2024-08-16 10:4	11:43 Sync License	Import License Key
<u>4</u> 2	License Key	Activated Date	Expire Date	License Type	Validity	User Group
(j)	8A219-****-**-BD88C			URL Reputation - B Card	Available	
	B7B56-*****-***-7CE0B			URL Reputation - B Card	Available	
	88F52-*****-F7349			URL Reputation - B Card	Available	
	F1A40-****-*-74CEE			URL Reputation - B Card	Available	
	EAC8D-*****-26346			URL Reputation - Silver Card	Available	
	0352B-*****-FB154			URL Reputation - Silver Card	Available	
	F70E3-*****-****26204			URL Reputation - Silver Card	Available	
	3867F-****-*-15EFB			URL Reputation - A Card	Available	RootGroup
	1656A-*****-39021	2024-01-22	2024-02-21	URL Reputation - Silver Card	Expired	RootGroup

To import the license key to VigorACS,

1. Click the **Import License Key** button.

Туре	All	✓ Validity	All	~	Search Q		
	Last Update Time : 2024-0	8-16 10:41:43	Sync License		Import Licer	nse Key	
I	License Type		Validity		User Group		
l	URL Reputation - B Card		Available				

A dialog will be shown as follows:

Import Li	cense Key		×
立 Upload	Jownload Template	Search	Q
License Key	Serla	l Number	
	No data ava	ilable	
	S	ihow 10 ~ entries	€ ₩
		Cancel	

2. Click the **Upload** link to open another dialog for selecting a license key. Then, click **Browse** to locate the license key file. Next, click **Apply**.

License Key		Serial Number			
	No dat	a available			
		Shi	10	v ontrioc	
	1 Select Import Lic	ense Key F	ile	×	
	upload_license_key.csv		Browse		
					Ŀ
		Car	ncel	Apply	
-					

3. The license key(s) under the profile will be shown on the screen. Click **Import**.

🗘 Upload 🛛 🕁 Download Template	
	Search C
License Key	Serial Number
C5B0F-7ABCA-84CB4-ABC64	2204V0226375
59043-38804-2AB07-5A8EF	2204V0226376
	Show 10 v entries < 1

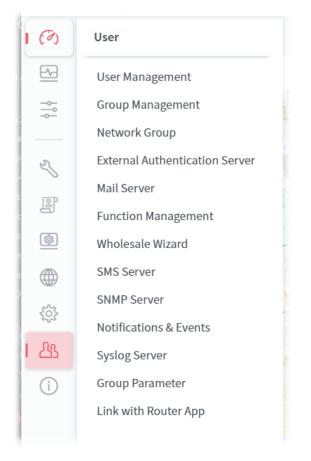
4. Later, the status of the license key(s) will be shown as "License imports success". Click **Finish** to apply the license to VigorACS and exit the dialog.

License Key	Status
C5B0F-7ABCA-84CB4-ABC64	License imports success.
59043-38804-2AB07-5A8EF	License imports success.
	Show 10 v entries 44 1

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.

	User Management	settings					Search	(Q
ihowing	g 1 to 10 of 133 entries				Show	10 v entries 📢	1 2 3 4 5 … 14	H
	Username 4	↑ Authentication ↓	Role	$\downarrow\uparrow$ Status $\downarrow\uparrow$	Email Notification 41	SMS Notification $\downarrow\uparrow$	Email	¥
	root	Internal	System Administrator	Active	Enabled	Disabled	tim_yang@draytek.com	
	tim_radius	External - AutoTest	Group Administrator	Active	Enabled	Disabled	tim_yang@draytek.com	
	kc_radius	External - RootGroup,f…	System Administrator	Active	Disabled	Disabled		
	auto_test	Internal	System Administrator	Active	Disabled	Disabled	auto_test@draytek.com	
	AutoTestGroup_GA	Internal	Group Administrator	Active	Disabled	Disabled	AutoTestGroup_GA@test.com	
	aries	Internal	System Administrator	Active	Disabled	Disabled	aries_chen@draytek.com	
	fullLicense_A	Internal	Group Administrator	Active	Disabled	Disabled	fullLicense_A@test.email	
	expireLicense_A	Internal	Group Administrator	Active	Disabled	Disabled	expireLicense_A@test.email	
	tim_yang	Internal	Group Administrator	Active	Disabled	Disabled		
	eric_lai	External - tttt1,tttt4,ttt…	System Administrator	Active	Disabled	Disabled	eric_lai@draytek.com	

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 ~
	Enable Auto Logout
	 Note: When select multiple users includes "View Only Operator", "Auto Logout" will not apply to "View Only Operator", only to other users.
	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.

ser / User Management		C
Add User Profile		
Enable		
Username	carrieni 🗸	
Password	• • • • • •	
Role	weak System Administrator	
 ▲ Note: • This account will be added to all 	Luser group If the role is a system administrator.	
Enable WUI Login		
Enable API Service		
Disable Auto Logout		
Enable OOBE feature		
OOBE pages to display	Read the Agreements, Set new passi \vee	
Email Notification		
Email	carrie_n(@draytek.com	
SMS Notification		
Telephone	carrie_ni 🗸	
	Cancel Crea	te

Item	Description					
Enable	Click to enable the user profile.					
Username	Enter a name for the new user.					
Password	Enter the password for the user.					
Role	Choose the role for the selected user . Different role represents different authority that the user group will have. The great the authority is, the more functions the user can have.					
	Operator ~					
	System Administrator Group Administrator					
	Administrator					
	Commissioning					
	Operator					
	View Only Operator Auditor					
	Auditor					
	 System Administrator – Have the highest authority. If it is selected, the corresponding settings configured in this page will be added to all user groups listed below. 					
	 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 WUI Login	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the web user interface of VigorACS.
Enable API Service	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the API service.
	Confirm API Password - Enter the password for access the API service.
Disable Auto Logout	Switch the toggle to enable / disable the function.
	If enabled, 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 user interface of VigorACS and allowed to view the OOBE page(s).
	OOBE pages to display - If the OOBE feature is enabled, select the page(s) to display on the screen.
Email Notification	Switch the toggle 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 Notification	Switch the toggle 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.
Chatbot Notification	Switch the toggle to enable / disable the function.
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications and information related to VigorACS.
	If enabled, this user account can check general information of VigorACS server through specific mobile phone device and/or PC.
APP Notification	Only the login user has the right to enable the function of APP Notification. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of DrayTek APP Notification, go to the APP Notification setting page.
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications, and information related to VigorACS.
Two-factor authentication	Only the login user has the right to enable the function of 2FA authentication. The System Administrator of VigorACS is allowed to disable
	this feature only. To enable/disable the function of 2FA authentication, go to the Two-factor authentication setting page.

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.

To edit an existing user account, select the one (e.g., mk_carrie) and click it.

ser /	User Management										С
⊢Add	🗊 Delete 🛛 🔗 User Batch	Settings							Search		Q
howir	ng 111 to 120 of 123 entries					Show	10 $ \!$	•	··· 9 10 11	12 13	₩
	Username 4	↑ Authentication	$\downarrow\uparrow$	Role ↓↑	Status↓↑	Email Notification	SMS Notification	Email			$\downarrow \uparrow$
	zzz_test_094	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_095	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_096	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_097	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_098	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_099	Internal		Group Administrator	Active	Disabled	Disabled				
	zzz_test_100	Internal		Group Administrator	Active	Disabled	Disabled				
	mk_carrie	Internal		System Administrator	Active	Disabled	Disabled				
	T_2022-12-12_addUser_8	Internal		Group Administrator	Active	Enabled	Enabled			-	
	T_2022-12-12_addUser_I	D Internal		View Only Operator	Active	Disabled	Disabled				

The following shows the Edit User Profile page.

User / User Management		C
Edit User Profile		
Enable		
Authentication	Internal	
Username	mk_carrie	
Password	•	
Confirm Password	•	
Role	System Administrator ~	
 A Note: This account will be added to a second second	b all user group if the role is a system administrator.	
Enable WUI Login		
Enable API Service	\bigcirc	
Disable Auto Logout		
Enable OOBE feature 🔞		
Email Notification		
Email	nn20200331@gmail.com	
SMS Notification	\bigcirc	
T.I		Cancel Save

These parameters are explained as follows:

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

Enable	Click to enable the user profile.					
Username	Enter a name for the new user.					
Password	Enter the password for the user.					
Confirm Password	Enter the password again.					
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". 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.					
Enable WUI Login	Switch the toggle to enable / disable the function. If enabled, this user account is allowed to access the web user interface of VigorACS.					
Enable API Service	Switch the toggle to enable / disable the function.					
	If enabled, this user account is allowed to access the API service.					
Disable Auto La sout	Confirm API Password - Enter the password for access the API service.					
Disable Auto Logout	Switch the toggle to enable / disable the function. If enabled, 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 user interface of VigorACS and allowed to view the OOBE page(s).					
	OOBE pages to display - If the OOBE feature is enabled, select the page(s) to display on the screen.					
Email Notification	Switch the toggle 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 Notification	 Switch the toggle 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.
Chatbot Notification	Switch the toggle to enable / disable the function. When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications and information related to VigorACS. If enabled, this user account can check general information of VigorACS server through specific mobile phone device and/or PC.
APP Notification	Only the login user has the right to enable the function of APP Notification. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of DrayTek APP Notification, go to the APP Notification setting page. When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications, and information related to VigorACS.
Two-factor authentication	Only the login user has the right to enable the function of 2FA authentication. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of 2FA authentication, go to the Two-factor authentication setting page.
Description	Enter a brief description for the user.
Cancel	Discard current modification.
Create	Save the current settings and exit the page.

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.

User / Gr	roup Managem	ent					С
Setting	Managem	ent					
+Add						S	earch Q
	Group ID [↓] ↑	Group Name	Max Nodes ↓↑	Used Nodes ↑	Enable Expire Date $\downarrow \uparrow$ Expire Date $\downarrow \uparrow$	Enable Global Mail Server	$\downarrow\uparrow$ Enable Global SNMP Server $\downarrow\uparrow$
	4239	tttt7	200000	0	Disabled	Disabled	Disabled
	4240	tttt8	200000	0	Disabled	Disabled	Disabled
	4067	zzz_test_001	1000	499	Disabled	Disabled	Disabled
	4068	zzz_test_002	1000	500	Disabled	Disabled	Disabled
	4069	zzz_test_003	1000	499	Disabled	Disabled	Disabled
	4070	zzz_test_004	1000	500	Disabled	Disabled	Disabled
	4071	zzz_test_005	1000	500	Disabled	Disabled	Disabled
	4072	zzz_test_006	1000	500	Disabled	Disabled	Disabled
	4073	zzz_test_007	1000	499.5	Disabled	Disabled	Disabled
	4074	zzz_test_008	1000	500	Disabled	Disabled	Disabled
	4075	zzz_test_009	1000	500	Disabled	Disabled	Disabled
				N1891	國人 信息日 辨别的时候时	U+/ 2U	

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		C
Setting Management		
Add Group		
Group name	Marketing 🗸	
Nodes	4	
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	
	22 23 24 23 20 27 28 29 30 31	

These parameters are explained as follows:

Item	Description
Group Name	Enter the name (e.g., Marketing) that can represent the user group.
Nodes	Display the number of license nodes for this group. Change the number by using the scroll box.
Enable CPE Notify Mail/SMS/SNMP	If it is enabled, this group will be allowed to use CPE's notify server / mail server / SNMP server.
Enable Global Mail Server	If it is enabled, this group will be allowed to use global mail server.
Enable Global SNMP Server	If it is enabled, this group will be allowed to use global SNMP server.
Enable Expire Date	Click to enable / disable the expire date setting. If enabled, set the expire date. 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 Management	С
Setting Management	
User Group : RootGroup ~	
Users root O auto_test O aries O tim_yang O tttt5_2fa O Kevin O cole5 O 20240612 O mk_carrie Kc_radius O tttt1 O	

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.
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.

lame	User Group	
S Root Network(100142)	RootGroup	~
AutoTestNetwork(1)	AutoTest	~
AutoTest_Dev(9)	AutoTest_Dev	~
AutoTest_SD-WAN(2)	(As Parent)	~
AutoTest_VPN(1)	AutoTest_VPN	~
V Web_Portal(2)	Hotspot_Web_Portal	~
Router_App_Network(2)	Router_App_Group	~
> ST_2024-08-01_Wholesale_GA_D(0)	T_2024-08-01_Wholesale_GA_D	~
> ST_2024-08-01_Wholesale_GA_E(0)	T_2024-08-01_Wholesale_GA_E	~
> X T 2024-08-01 Wholesale GA OOBE(0)	T 2024-08-01 Wholesale GA OOBE	~
T_2024-08-01_addNetwork_A(0)	T_2024-08-01_addGroup_E	~
> ST_2024-08-01_addNetwork_B(0)	(As Parent)	~
▷ 🔇 U_2133_100(100)	(As Parent)	~
▷ 🔇 U_2865_5(2)	AutoTest	~
▷ 🔇 U_2866_5(4)	AutoTest	~
▷ 🔇 U_2927_5(5)	AutoTest	~
VigorSwitch(2)	(As Parent)	~
▷ 🐼 aaa(5)	(As Parent)	~
expireLicense_A(0)	expireLicense_A	~
IullLicense_A(1)	fullLicense_A	~

These parameters are explained as follows:

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

6.6.4 External Authentication Server

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

Enable Choose User Role at Registration View Only Operator Server IP Address IT2.16.1.86 Authentication Server Type Active Directory / LDAP Destination Port 389 Use SSL O Note: 10 Type Ind Type Simple Mode Anonymous Regular DN Regular Password Totle Name 2 Motion Line Common Name Base Distinguished Name Additional Filter		
Server IP Address 172.16.1.86 Authentication Server Type Active Directory / LDAP Destination Port 389 Use SSL 0 Onote: • For security consideration, it is strongly recommended to use LDAP or TACACS+ instead of RADIUS if the external authentication server is on the Internet. Blind Type Simple Mode Anonymous Regular Regular DN 0 Regular Password 0 + Add		
Authentication Server Type Active Directory / LDAP Destination Port 389 Use SSL Image: Construction of the external authentication server is on the Internet. Bind Type Simple Mode Regular DN Image: Construction of the external of		
Destination Port 389 Use SSL 0 ONOTE: • for socurity consideration, it is strongly recommended to use LDAP or TACACS+ instead of RADIUS if the external authentication server is on the Internet. Bind Type Simple Mode Anonymous Regular Regular DN 0 Regular Password •		
Use SSL Use SSL Use SSL Use SSL Action Server is on the Internet. Bind Type Simple Mode Anonymous Regular Regular DN Regular Password Action A		
O Note: • For security consideration, it is strongly recommended to use LDAP or TACACS+ instead of RADIUS if the external authentication server is on the Internet. Bind Type Simple Mode Anonymous Regular Regular DN Regular Password + Add		
For security consideration, it is strongly recommended to use LDAP or TACACS+ instead of RADIUS if the external authentication server is on the Internet. Bind Type Simple Mode Anonymous Regular Regular DN Regular Password Add		
Regular Password $ riangleta$		
+ Add		
Id Profile Name Common Name Base Distinguished Name Additional Filter		Profile Number Limit: 1/5
•••• 0	Group Distinguished Name	Action
1	Group Distinguished Name	5 Clear

Item	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	 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			C
User Group : All User Group v			
Profile Name	LD_1] ~	
Common Name Identifier	UID]	
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

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.	

These parameters are explained as follows:

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 I						Profile Number Limit: 2
d	Profile Name	Common Name	Base Distinguished Name	Additional Filter	Group Distinguished Name	Action
	Idap	uid	ou=People,dc=ms,dc=draytek,dc=com			🗊 Delete
t .	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.

User / Mail Server User Group: All User Group ~		С
Send Test Email		
Enable Server		
Authentication Method	No Authentication Basic OAuth2	
Security	None SSL TLS	
Host	ms.draytek.com	
Port	465	
Sender Email	tim_yang@draytek.com	
Username	tim_yang	
Password	••••••	
Subject	VigorACS Alarm Level	
	Network Name ③ Device Name ③ Model Name ③ MAC Address ③ Device IP ④	
	Alarm Message 🛞 User Name 🛞	
つ Reset To Default	s	ave
-		

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	Switch the toggle to enable /disable the SMTP server.			
Authentication Method Select the authentication method to authenticate the mail server. No Authentication Basic OAuth2				
When No Authentication	is selected as the Authentication Method			
Security Choose None / SSL / TLS for the security of the mail transferr				
Host	Enter the IP address of the SMTP server.			
Port	Type the port number of the SMTP server.			
Sender Email Enter the e-mail address which will be used to send a notification e the recipients under the selected user group or all user groups.				
Subject	At present, there are several objects to be selected for the subject of the email.			

When Basic is selected a	s the Authentication Method			
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.			
Sender Email	Enter the e-mail address which will be used to send a notification e-mail to the recipients under the selected user group or all user groups.			
Username	Enter the user name for authentication.			
Password	Enter the password for authentication.			
Subject	At present, there are several objects to be selected for the subject of the email.			
When OAuth2 is selected	d as the Authentication Method			
OAuth2 API	There are three options to select. Google Microsoft Others 			
When Google is	Host – Enter the IP address of the SMTP server.			
selected as the OAuth2 API	Port – Enter the port number of the SMTP server.			
	 Sender Email – Enter the e-mail address which will be used to send a notification e-mail to the recipients under the selected user group or all user groups. Client ID – Enter the ID number which can identify a single APP to Google's OAuth servers. Please obtain the number created by https://console.developers.google.com/projectcreate. 			
	Client Secret – Enter the secret information which can identify a single APP to Google's OAuth servers. Please obtain the secret created by https://console.developers.google.com/projectcreate.			
	Authorize URL – Enter https://accounts.google.com/o/oauth2/auth in this field.			
	Token URL – Enter https://oauth2.googleapis.com/token in this field.			
	Redirect URI – Enter VigorACS server URL with callback path (e.g., https://acs.example.com/ACSServer/oauth2/callback).			
	Authentication Code – Click the Get Authentication Code icon to open the API service login page. The page will ask for agreement. Click Continue. Later, if the credentials are correct, the authentication code will be provided.			
	Copy the authentication code and paste it into the Authentication Code entry box.			
	Click the Exchange authorization code for tokens button to get tokens.			
	Refresh Token and Access Token - If the authentication code is correct, you will get the Refresh Token and Access Token from the system.			
	Subject - At present, there are several objects to be selected for the subject of the email.			
When Microsoft is	Host – Enter the IP address of the SMTP server.			
selected as the OAuth2	Port – Enter the port number of the SMTP server.			
API	Sender Email – Enter the e-mail address which will be used to send a notification e-mail to the recipients under the selected user group or all			

	user groups. Tenant ID – Enter the tenant (Directory) ID obtained while registered to the
	server (e.g., Microsoft Azure) providing OAuth2 authentication.
	Client ID - Enter the application (client) ID obtained while registered to the server (e.g., Microsoft Azure) providing OAuth2 authentication.
	Client Secret – Enter the secret obtained from the remote client.
	Authorize URL – Enter https://accounts.google.com/o/oauth2/auth in this field.
	Token URL – Enter https://oauth2.googleapis.com/token in this field.
	Redirect URI – Enter VigorACS server URL with callback path (e.g., https://acs.example.com/ACSServer/oauth2/callback).
	Authentication Code – Click the Get Authentication Code icon to open the API service login page. The page will ask for agreement. Click Continue. Later, if the credentials are correct, the authentication code will be provided.
	Copy the authentication code and paste it into the Authentication Code entry box.
	Click the Exchange authorization code for tokens button to get tokens.
	Refresh Token and Access Token - If the authentication code is correct, you will get the Refresh Token and Access Token from the system.
	Subject - At present, there are several objects to be selected for the subject of the email.
When Others is	Host – Enter the IP address of the SMTP server.
selected as the OAuth2 API	Port – Enter the port number of the SMTP server.
	Sender Email – Enter the e-mail address which will be used to send a notification e-mail to the recipients under the selected user group or all user groups.
	Client ID - Enter the ID number obtained from the remote client.
	Client Secret – Enter the secret obtained from the remote client.
	Authorize URL – Enter https://accounts.google.com/o/oauth2/auth in this field.
	Token URL – Enter https://oauth2.googleapis.com/token in this field.
	Redirect URI – Enter VigorACS server URL with callback path (e.g., https://acs.example.com/ACSServer/oauth2/callback).
	Authentication Code – Click the Get Authentication Code icon to open the API service login page. The page will ask for agreement. Click Continue. Later, if the credentials are correct, the authentication code will be provided.
	Copy the authentication code and paste it into the Authentication Code entry box.
	Exchange authorization code for tokens – Click the Exchange authorization code for tokens button to get tokens.
	Refresh Token and Access Token - If the authentication code is correct, you will get the Refresh Token and Access Token from the system.
	Subject - At present, there are several objects to be selected for the subject of the email.
Reset To Default	Click to reset the mail server to default settings.

Click **Save** to save the change.

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.

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				

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	Create user group	Create network	Summary	Finished		
Step 1- Create user						
Username *	Carrie003					
Password *	•••••	۵				
Telephone	5972727					
Email	carrie@draytek.com					
Role	System Administrator	~				
Enable Auto Logout						
Enable OOBE feature 🔞						
OOBE pages to display	Read the Agreements, Set new passwo	rd, Verify 🗠				
				_		
				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 Auto Logout	Switch the toggle to enable / disable the function of auto logout.
Enable OOBE feature	Switch the toggle to enable / disable the function of OOBE feature. OOBE pages to display - Select the pages to display on the screen.
Status	Choose Active to make this 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.

User / Wholesale Wizard					
1 Create user	2 Create user group	3 Create network	G	5 Finished	
Step 2- Create user group					
Select group:	Existing group New group				
New group					
Group Name *	DrayTek_Marketing				
Nodes	-1 (-1: No Limit Nodes)				
Global Mail Server					
Enable Expire Date					
Expire Date	2025/08/01				
				Previous Next	

These parameters are explained as follows:

Item	Description			
Select group	Determine the group source by choosing Existing group or New group .			
Existing group	It is available when Existing group is selected as Select group . User group – Use the drop down list to choose the group you want.			
New group	It is available when New group is selected as Select group . Group Name – Type the name (e.g., Marketing) that can represent the user group. Nodes – Set the number of Nodes for such group. The default number "-1" means there is no limit of the number.			
	 Global Mail Server –Switch the toggle to enable /disable the global mail server. Enable Expire Data – Switch the toggle 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.

User	/ Wholesale Wizard				
	L Creato usor	Create user group	3 Create network	3 Summary	5 Finished
	Step 3- Create network				
	Select network:	Existing network New network			
	New network				
	Parent Network	Root Network	٩		
	Network Name *	CARRIE003			
	Username	cardtest			
	Password	••••••)		
	Location	HsInChu			
					Previous Next

These parameters are explained as follows:

Item	Description		
Select network	Determine the group source by choosing Existing network or New network.		
Existing network	It is available when Existing network is selected as Select network . Network – Use the drop down list to choose the network you want.		
New network	 It is available when New network is selected as Select network. Parent Network - Choose one of the existing networks as the Parent Network. Network Name - 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.

User / Wholesale Wizard				
Create user	Create user group Crea	3 te network	4 Summary	5 Finished
Step 4- Summary				
User				
Username		Role		
Carrie003		Group Administrator		
Status		Mail Notify		
Active		Enable		
SMS Notify		Telephone		
Enable		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.

User / SMS Server		С
User Group : RootGroup ~		
Enable SMS Server		
SMS API	SMS_VigorRouter_GW ~	
Connection URL	http://192.168.106.144	
Username	11111111	
Password	••••••	
	Send SMS Test	
		Save

ltem	Description	
User Group	Specify a user group to apply the SMS server settings.	
Enable SMS Server	Switch the toggle to enable /disable the SMS server.	
SMS API	Use the drop down list to choose an ISP for sending SMS.	
Connection URL	Enter the CPE's URL (WAN or LAN IP, e.g., 192.168.1.1).	
User Name	Type the user name for authentication.	
Password	Type the password for authentication.	
From Telephone	Type the phone number of the sender.	
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 / SNMP	Server		
User Group :	All User Group ~		
Enable SNN	/P server	\bigcirc	
SNMP serve	er address		
Port		0	
Community	y		
SNMP versi	on	version1	~
SNMP API		SNMP_2_GLOBAL	~
Alarm Leve	l	Critical	Major
		Minor	🗹 Warning
		Normal	
L			

ltem	Description	
User Group	Specify a user group to apply the SNMP server settings.	
Enable SNMP Server	Switch the toggle 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.	
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.	

6.6.10 Notifications & Events

This menu is available only when the role of the user account accessing to VigorACS server is **System Administrator** or **Group Administrator**.

6.6.10.1 Recipients

Define the ways (email, SMS, or chatbot) that the recipient will get the alarm messages.

User / Notifications & Events			C
User Group : AutoTest	v		
Recipients Severity Definition	n		
Notified User Role :	System Administrator V		
Recipient Settings			
Severity	Email Notification	SMS Notification	Chatbot Notification
Critical			
Major			
Minor			
Warning			
Normal			
			Save

ltem	Description
Notified User Role	Select a user role. Each role can be configured with different notifications and alarm levels.
Email Notification SMS Notification Chatbot Notification	While encountering events with alarm degrees in critical, major, minor, warning, and normal, the recipient will receive the alarms from the VigorACS server via email, SMS, or chatbot.
Save	Click to save the configuration.

6.6.10.2 Severity Definition

Define the alarm levels for various events under each user group.

User / Notifications & Events User Group: RootGroup ~	С
Search Events Q	
Router Events	
Events	severity
WAN Lost Connection	Minor ~
VPN Lost Connection	Warning ~
Cellular Data Usage	Normal ~
Device Network & Maintenance Events	
Events	Severity
Device Lost Connection	Major ~
Firmware Recovered	Minor ~
New Firmware Release	Warning ~
	Save

Click **Save** to save the configuration.

6.6.11 Syslog Server

Except for DrayTek SysLog server, VigorACS syslog can be stored at specified host.

User / Syslog Server		C	2
User Group : All User Group ~			
Enable Syslog server			
Host			
Port	0		
Token		۵	
SysLog API	Syslog_OVHcloud ~		
		Save	

ltem	Description	
Enable Syslog server	Switch the toggle to enable/disable the Syslog server.	
Host	Enter the IP address of the host where ACS logs will be sent.	
Port	Enter the port number for the host.	
Token	Enter the content of the token obtained from OVH website.	
SysLog API	Select the API required to store the Syslog records. At present, only	

	OVHcloud is available for use.
Save	Click to save the configuration.

6.6.12 Group Parameter

Differing from the settings configured on the page of System >> System Parameter which will influence all user accounts and the whole system settings (e.g., CPE configuration, HTTPS connection, security), the parameters listed on this page can be configured for different user groups separately.

Open **User** >> **Group Parameter** to get the following web page:

User / Group Parameter		С
User Group : AutoTest ~	Search	Q
Name		Value
Automatically detects Router name		default (false)
5 Reset to default		Save

6.6.13 Link with Router App

The engineer sent by an ISP will be able to conveniently carry out the hardware installation and software configuration using the router app on a mobile device. Once the installation is complete, VigorACS will automatically manage the router/modem/access point remotely.

6.6.13.1 Settings

Configure the general settings related to VigorACS.

User / Link with Router App User Group: RootGroup ~	C
Settings Status Checking Profile Monitoring Hel	pDesk
General Setup	
Enabled Access from Router App	\bigcirc
Authorized User 🕜	Nothing selected ~
Profile Name	VigorACS
URL	Your ACS Domain
Port	443
Onboard Information	
Enabled	\bigcirc
Onboard Information List	
つ Reset to default	Save

ltem	Description	
General Setup		
Enable Access from	Switch the toggle to enable/disable the function.	
Router App	To complete the router installation by connecting VigorACS using the Vigor router APP, this feature must be enabled.	
Authorized User	Only the users profiles(with Enabled API Service) listed here are allowed to connect VigorACS using the Vigor router APP.	
Profile Name	Display the name of VigorACS server.	
URL / Port	URL – Enter the URL representing VigorACS server. Port – Enter a port value. The default is 443 (for ACS server).	
QR Code	The QR Code is generated according to the profile name, URL and port value defined above.	
Onboard Information		
Enabled	Switch the toggle to enable/disable the function. The onboard information will be shown on the mobile APP if enabled.	
Onboard Information List	A table lists all onboard information.	
Steps before Provisionir	·	
Validate Site Configuration before Provisioning	Switch the toggle to enable/disable the function. Enabled – Write the parameters to the CPE device via the mobile phone. Disabled – The behavior of set parameter is the same as present.	
Site Configuration	Determine which site (AP, router, switch) settings will be configured in the installation process. Ste Configured The Type options are Text and Dropdown. Default is Text. If Dropdown is selected, click the Edit Option List to define available option name(s). Then use the drop-down list to select one from the option list.	

	enable the entry of the site configuration.
	Regex Validation – The default value is empty if the Type is set as Text.
	Action – Click Delete to remove the selected entry.
Reset to default	Click to return to default settings.
Save	Click to save the configuration.

6.6.13.2 Status Checking Profile

The system administrator can customize the status checking profile including the parameters to be monitored and displayed on the status page.

Up to five profiles can be created.

User / Link with Router	Арр			C
User Group : RootGroup	p ~			
Settings Status Chee	cking Profile Monitoring HelpDesk			
+ Add				Profile Number Limit: 0/5
Profile Name	↓↑ Comments	↓↑ Hardware Installation Hint Images	Action	
		No data available		
		No data available		

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

User / Link with Router App User Group: RootGroup	C
User Group : RootGroup Settings Status Checking Profile Monitoring Help[ek -
General Setup	an
Profile Name	
Comments	
Hardware Installation Hint Images	Nothing selected ~
Parameter Group	
් Import XML	
+ Add Parameter Group Max: 5 Groups	
	Cancel Save

ltem	Description
General Setup	
Profile Name	Define the name that will be shown on the Name field of Site Configuration (Steps before Provisioning on User>>Link with Router App>>Settings).
Comments	Enter a brief description for identifying the profile.
Hardware Installation Hint Images	Specify the interface (DSL, Ethernet, SIM \$ LTE) to use during the router APP installation.

Parameter Group		
Import XML	Import an existing XML file and upload it to VigorACS.	
+Add Parameter	Up to five parameter groups can be created.	
Group	Group Name – Define a new name for a parameter group.	
	Delete Group – Remove the selected parameter group.	
	+Add Parameter – Up to 15 parameters can be added to a parameter group.	
	• Index – Displays the index number of the parameter entry.	
	• Name – Enter the item name that will be shown on the router APP.	
	 Parameter – Enter the TR-069 parameter name to be monitored by VigorACS. Refer to System >> System Parameter for detailed parameter name. 	
	• Status Colour – Switch the toggle to enable/disable the conditional control status color. If enabled, configure the following settings.	
	 Priority – Set the priority for the specified condition and value. 	
	 Condition – Select Equals to (=), Less Than (<), Greater Than (>) as a comparison condition. 	
	 Value – A value corresponding to the parameter specified above will be shown in this field. Please note the value type (String or Integer) should match the parameter's type. 	
	 Colour – Currently, there are three colors to choose from: red, green, or orange. 	
	+Add – Create a new entry for setting color.	
	Delete – Remove the selected entry.	
Cancel	Discard current settings and return to previous page.	
Save	Click to save the configuration.	

6.6.13.3 Monitoring

This page displays the information of CPEs monitored by VigorACS.

User / Link with Router App User Group: RootGroup	C
Settings Status Checking Profile Monitoring HelpDesk	
Last 24 Hours Last 30 Days Custom Start: 2024-07-31 End: 2024-08-01	
Search Device Name/ MAC/ IP Address Q K < 1 /1 >	C Export
Install Status 4 Install Started 4 Install Completed 4 MAC Address 4 Router Name 4 Device Status 4 Action	
No data available	

ltem	Description
Install Status	Information Submitted – It means VigorACS receives the install command.

	Installation Completed – It means VigorACS receives the logout API command.
Install Started	Display the time that VigorACS receives the install API command.
Install Completed	Display the time that VigorACS receives the logout API command.
MAC Address	Display the MAC address of the CPE monitored by VigorACS.
Router Name	Display the device name of the CPE monitored by VigorACS.
Device Status	Display the online/offline status of the CPE monitored by VigorACS.
Action	Go to Dashboard – A link is available to access to the dashboard of the device.
	View Status – A link is available to display the parameter information configured at the Status Checking Profile.
	View Information – A link is available to access onboard information, site information, and other details for the CPE.

6.6.13.4 HelpDesk

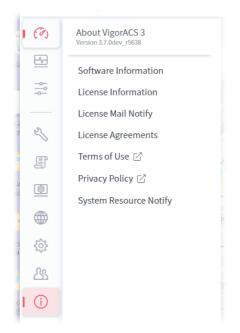
Some ISP engineers may not be able to use the mobile APP to connect to VigorACS at the installation site. In this case, they can use HelpDesk to assist with the installation.

User / Link with Router App		С
User Group ·		
Settings Status Checking Profile Monitoring Help	Desk	
Device Information		
MAC Address		
Configuration for Installation		
Site Type	Nothing selected ~	
Location		
	 8 Note: Enter either address or the latitude and longitude coordinates with the following format. Latitude;Longitude Example 24.868162980491277;121.006106339836 No. 26, Fuxing Rd, Hukou Township, Hsinchu County, 30352, Taiwan 	
	Si	ive

ltem	Description	
Device Information		
MAC Address Enter the MAC address of the CPE device.		
Configuration for Installation		
Site TypeSelect one of the Status Checking Profiles.		
Location Enter either address or the latitude and longitude coordinates of the device with the following format:		

Latitude; Longitude (e.g., 24.868162980491277;121.006106339836)	
Save	Click to save the configuration.

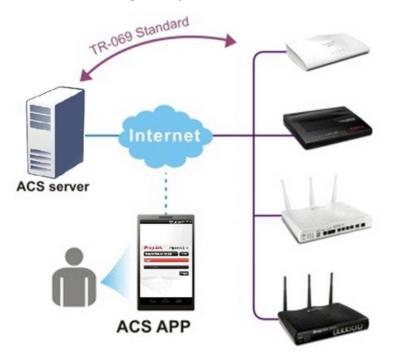
6.7 About VigorACS



(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 login 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 Software Information

System Information	Release Notes	Others
ACS Version	3.7.0dev_r5638	
Java Version	17.0.11	
MarlaDB Version	10.6.5	
InfluxDB Version	1.8.3	
Operation System	Linux	

This page displays relational information for software installed for VigorACS 3.

6.7.2 License Information

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

About / License Informa	tion	C
Host ID	ACS3200200003	
License ID	0002aa90	
License Type	Normal	
License Period	Start Date 	Expire Date (Today) -O 8/5/24
Licensed Node Usage	Used: 50142.5 / Max: 200000	
Activate License	Activate License	

Click **Activate License** to update the status of licenses on the MyVigor server. After that, all users will be logged out, and the system administrator will need to log in to MyVigor to update the license. The updated license information will then be displayed on the page above.

6.7.3 License Mail Notify

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

6.7.3.1 Sync License Info Failed

VigorACS will delete the license record from the system if it cannot get the license information three times. At this time, you will need to log in to MyVigor and activate the license manually.

VigorACS server will send a notification e-mail when failing to get the license. Please set the content of the notification e-mail in this page.

(7)	About / License Mail Notify		C
	Sync License Info Failed	License Expired License Capacity	
م الله الله (About failure to sync license info ACS will delete the license record on the system if ACS cannot get the license info or 3 times. At this time, you will need to login to MyVigor and activate the license manually.	
⊕ ॐ <u>८</u> ⊾		▲ Configure Mail Server You can enable this feature to receive a notification mail. Please go to User > Mail Server to configure the email server setting for All_UserGroup.	
	Subject	ACS cannot get the license info from M	
	Content	Normal e Sans Serif e I	
	Recipients	+ Add Recipient 1/10	ave

ltem	Description	
Enable	Switch the toggle to enable /disable the mail notification function. You can enable this feature to receive a notification mail. Please go to User >> Mail Server to configure the email server setting for all user groups.	
Subject	Enter the subject of the mail.	
Content	Enter the actual text for informing the recipient.	
Recipients	Enter the e-mail address of the one to receive the mail.	
+Add Recipient	Click to enter a new e-mail address.	
Delete	Click to remove the selected e-mail address.	
Save	Save the current settings.	

6.7.3.2 License Expired

VigorACS server will send a notification e-mail when the VigorACS license expires soon. Please set the content of the notification e-mail in this page.

(7)	About / License Mail Notify		C
	Sync License Info Failed	License Expired License Capacity	
	Enable		
\$ @] @		▲ Configure Mail Server You can enable this feature to receive a notification mail. Please go to User > Mail Server to configure the email server setting for All_UserGroup.	
(ل) ل	Subject	Service License Expires Soon	
بې لا ا	Content	Normal ÷ Sans Serif ÷ B I <u>U</u> <u>A</u> <u>M</u> <u>E</u> = = % <u>A</u> ACS license is going to expire at [DATE]. Please contact your provider to renew the license. <u>A</u> <th></th>	
	Recipients	+ Add Recipient 1/10 Recipient Invalid email format	
			Save

ltem	Description	
Enable	Switch the toggle to enable /disable the mail notification function. You can enable this feature to receive a notification mail. Please go to User >> Mail Server to configure the email server setting for all user groups.	
Subject	Enter the subject of the mail.	
Content	Enter the actual text for informing the recipient.	
Recipients	Enter the e-mail address of the one to receive the mail.	
+Add Recipient	Click to enter a new e-mail address.	
Delete	Click to remove the selected e-mail address.	
Save	Save the current settings.	

6.7.3.3 License Capacity

In general, the system administrator will purchase licenses for future node assignments.

This page is used to set the threshold for node usage. When the licensed node usage reaches the percentage set here, the VigorACS system will send a notification e-mail to the recipient, informing the administrator that the license capacity is about to be used up, which can facilitate the system administrator to proceed with the next step (such as purchasing new licenses to expand CPE management).

(7)	About / License Mail Notify		C
₽ 	Sync License Info Failed License E	xpired License Capacity	
~ iij @		▲ Configure Mail Server You can enable this feature to receive a notification mail. Please go to User > Mail Server to configure the email server setting for Al_UserGroup.	
(ب چې	Subject	Service Node usage exceeds [PERCENT.	
23	Capacity (%)	80	
	Content	Normal • Sans Serif • B I U A (A) (A)	
	Recipients	+ Add Recipient 1/10 Recipient Invalid email format	
		Sa	ve

ltem	Description	
Enable	Switch the toggle to enable /disable the mail notification function. You can enable this feature to receive a notification mail. Please go to User >> Mail Server to configure the email server setting for all user groups.	
Subject	Enter the subject of the mail.	
Capacity	Specify the percentage of the current node. For example, the default is 8 That means if there are 2000 nodes in total, once 1600 nodes are used, VigorACS will notify the listed recipients.	
Content	Enter the actual text for informing the recipient.	
Recipients Enter the e-mail address of the one to receive the mail.		
+Add Recipient Click to enter a new e-mail address.		
Delete Click to remove the selected e-mail address.		
Save	Save the current settings.	

6.7.4 License Agreements

About / License Agreements			
			C Search Keyword
Package Name ↑↓	License Type ↑↓	Author ↑↓	Website Modified Source Codes
Ant	Apache License, Version 2.0		8 Link 🗹
Apache POI	Apache License, Version 2.0		🖉 Link 🖾
Axis	Apache License, Version 2.0		8 Link 🖻
Castor	Apache License, Version 2.0		🖉 Link 🗹
Commons FileUpload	Apache License, Version 2.0		8 Link 🗹
Dashboard	Apache License, Version 2.0	Google Inc.	8 Link 🖾
EasySSL	Apache License, Version 2.0	olamy	🖉 Link 🗹
Jakarta common tool	Apache License, Version 2.0		🖉 Link 🗹
jCasbin	Apache License, Version 2.0		🖉 Link 🖾
JDBC Adapter	Apache License, Version 2.0		🖉 Link 🖾
JSTUN	Apache License, Version 2.0		S Link 🖾

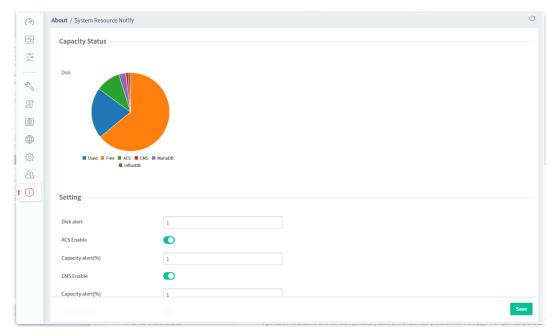
This page displays relational license information required by VigorACS 3.

6.7.5 System Resource Notify

VigorACS server can regularly <u>inspect hardware usage</u> under the directories of EMS, ACS & Maria database & influx database every day if this function is enabled. When the hard disk (file size) reaches the upper limit percentage, the VigorACS server will send a notification mail to a specified person. With this feature,

- Users can enable the notification settings for EMS, ACS & Maria database & influx database separately.
- Users can understand the percentage of the hard disk capacity occupied by each file through the pie chart on this page.

Only the users with the authority of the System Admin/Auditor can view this page. Only the user with the authority of the System Admin can modify/edit this page.



These parameters are explained as follows:

ltem	Description
Disk alert	Set the upper limit percentage (by default, 1) of the total hard disk space. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
ACS Enable	Switch the toggle to enable/disable the function of checking ACS database.
Capacity alert(%)	Set the upper limit percentage (by default, 1) of the disk space for the ACS database. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
EMS Enable	Switch the toggle to enable/disable the function of checking the EMS database.
Capacity alert(%)	Set the upper limit percentage (by default, 1) of the disk space for the EMS database. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
InfluxDB Enable	Switch the toggle to enable/disable the function of checking Influx Database.

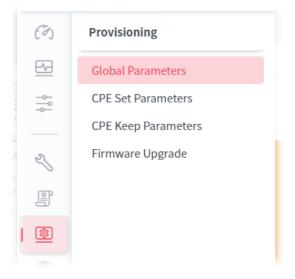
Capacity alert(%)	Set the upper limit percentage (by default, 1) of the disk space for the Influx database. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
MariaDB Enable	Switch the toggle to enable/disable the function of checking Maria Database.
Capacity alert(%)	Set the upper limit percentage (by default, 1) of the disk space for the Maria database. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
Recipient	Up to 10 mail addresses can be listed. +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.

Applications

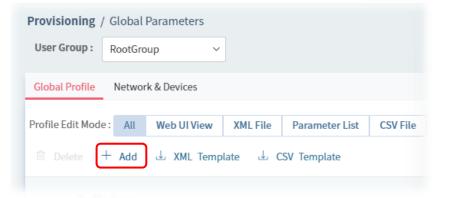
A.1 How to Create a Provision Profile with Global Parameters?

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

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



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



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

Provisioning / Global Parameters	
User Group : RootGroup ~	
Global Profile Network & Devices	
Add a Profile	
Create Profile by	Creating a New Parameter List ~
Profile Name	
Always Keep	0
Reboot after Provisioning	0
និ Note: After applying the parameters, ACS wil	I check the CPE responses and ask the CPE to reboot if needed.
Provisioning Time	Now Scheduled Schedule Profile
	Cancel Add

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

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
888888	Parameter List		No	3	2018/11/28 04:43:07 PM	
angela test	Parameter List		No	1	2018/11/12 02:48:25 PM	🖉 Edit 🗈 Delete 斗 Copy To 🛛 🔒 View Log
tt	Parameter List		Yes	0	2018/11/08 02:38:05 PM	🖉 Edit 🗇 Delete 🍳 Copy To 🗣 View Log
Global_parameter_Example_Parameter_List	Parameter List		No	0	2018/11/08 03:13:55 PM	🖉 Edit 🗇 Delete 🎱 Copy To 🗣 View Log
66667	Parameter List		No	2	2019/05/31 08:47:36 AM	
Marketing	Parameter List		Yes	0	2020/11/03 02:18:29 PM	🖉 Edit 🐵 Delete 斗 Copy To 🛛 🕯 View Log

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

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

(7)	Provisioning
<u></u>	Global Parameters
	CPE Set Parameters
	CPE Keep Parameters
Z	Firmware Upgrade
<u></u>	

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

ning / Clobal Parameters oup: RootGroup ~								С
Yrofile Network & Devices								
itt Mode: Alt Web UI View XML File Parameter List CSV File_ ere + Add J XML Template J CSV Template								
Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action		
vlgor2860	Parameter List		Yes	19	2019/05/09 04:15:20 PM	🖉 Edit	🛾 Сору То	🗟 View
Vigor2760	Parameter List		No	15	2019/05/09 04:15:20 PM	🖉 Edit	🗅 Сору То	🖨 View
ttt	Parameter List		No	0	2019/05/09 02:39:36 PM	🖉 Edit	🗅 Сору То	🔒 View
vigor28606	Parameter List		No	1	2019/05/09 04:12:05 PM	🖉 Edit	🗅 Сору То	🔒 View
12345678913245678912314567891324567891234564897xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Parameter List		No	0	2020/02/27 11:29:32 AM	🖉 Edit	🗅 Сору То	🔒 View
Marketing	Parameter List		Yes	0	2024/08/05 11:31:46 AM	🖉 Edit	🗅 Сору То	🖨 View

3. Click the **Add** 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	~

() 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 ID/Name/Model/MAC/IP Address	C Setting Map		
A 👬 Root Network(277)	+Add New Network		
ALANWEN(3)			
Alvaco(1)	General Settings		
AnPhat_VN(8)			
Angela(5)	Network ID	Username	
ArlesTest(0)	2	acs	
CARRIE(0)	Name	Password	
CARRIE003(0)	Root Network		0
Cshih(2)	Location		
DraytekChina(0)	Koldingweg 19-1, Groningen, Nederland		
FAE(3)			
GetterNetwork(1)			Save
⊳ 🚓 IK1(1)			
Marketing_carrie(0)			
Novanet(0)			
OCTOBER(1)			

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

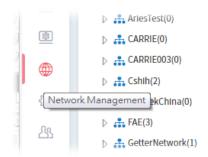
Parent Network	
Root Network	
Name	
Marketing_carrie	
Location	
HS	
User Name	
carrie	
Password	

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

etwork Management	
Search by Device ID/Name/Model/MAC/IP Addre	Setting Map
Root Network(240)	+Add New Network
Þ 📥 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	Setting Map
 2865Lax 1449BC0C5920 2865ac_001DAA000000 	Delete This Device 🤹 Change Network
2865ac_001DAA41DF18 2865ac 001DAA41DF78	General Settings
2866ac_001DAA41DFC0	Status Disable Enable
 2912n_001DAA8E14B0 2922n_001DAA8CAC84 	Device ID
2925Ln_001DAADD75B0	141436 Model Name
2925ac_001DAA512820	Vigor2865ac
 2926Vac_001DAA5DCAD0 2927Lac_1449BC023720 	Note 1
2927Lac_1449BC023740	Serial number
2927Lac_1449BC023768	

3. Click Change Network.

Network Management	
Search by Device ID/Name/Model/MAC/IP Address	C' Setting Map
2865Lax_1449BC0C5920	Delete This Divice 4 Change Network
2865ac_001DAA000000	m Delete TRIS DIVICE and Change Network
2865ac_001DAA41DF18	Conoral Sottings
2865ac_001DAA41DF78	General Settings
2866ac_001DAA41DFC0	Status Disable Enable
2912n_001DAA8E14B0	
2922n_001DAA8CAC84	Device ID
2925Ln_001DAADD75B0	141436
2925ac 001DAA512820	Model Name
2926Vac_001DAA5DCAD0	Vigor2865ac
2927Lac_1449BC023720	Note 1
2927Lac_1449BC023740	
2927Lac 1449BC023768	Serial number
2327LaC_1443BC023708	

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

Name	
2865ac_001DAA000000	
Add to network	
	Q
🔺 👬 Root Network	
ALANWEN	
👬 Alvaco	
🚓 AnPhat_VN	
👬 Angela	
🕂 ArlesTest	
🚓 CARRIE	
🚠 Cshih	
🚓 DraytekChina	
👬 FAE	
👂 👬 GetterNetwork	
📫 IK1	
👬 Marketing_carrie	
🚓 Novanet	
🚓 OCTOBER	
RD1	
👬 RD2	
🚓 RD3	
• ppc	
	× Cancel + Apply

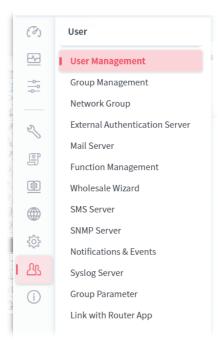
Sel	(100%)		Deratic us of each					pleted.		
Ge		 Suc 	ceed: 1	•	Proce	0		Waiting: 0	Failed: 0	
	Device Name	Ψî	Model	Ψî	Retry	↓ ↑	Progress	Status		$\downarrow\uparrow$
Sta	2865ac_001DAA(000000	Vigor286	5ac	0		≈100%		ffline. Settings will hen device is online	
Den 14					— HI	de De	alls			
Мо					×	Close				
	gor zaosac								2003	Nac_ool

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

arch by Device ID/Name/Model/MAC/IP Address	C Setting Map	
Root Network(277)	🗊 Delete This Device 🛛 🚓 Change Network	
ALANWEN(3)		
Alvaco(1)	General Settings	
AnPhat_VN(8)	Ť	
Angela(5)	Status DIsable Enable	
ArlesTest(0)		
 CARRIE(1) 	Device ID 141436	
2865ac_001DAA000000	Model Name	
CARRIE003(0)	Vigor2865ac	
Cshih(2)	Note 1	
	Note 1	

A.5 How to Add a User?

1. Open User>>User Management.



2. Click +Add.

User / Use	er Management					C
+Add	Delete 🔗 User Batch Setting	s				Search Q
Showing 1 t	to 10 of 133 entries				Show 10 v entries 44 1	2 3 4 5 … 14 🅪
U	Username	↓↑ Authentication	↓↑ Role	↓↑ Status ↓↑ Email Notifie	cation $\downarrow\uparrow$ SMS Notification $\downarrow\uparrow$ Email	↓↑
	root	Internal	System Administrator	Active Enabled	Disabled tim_yang@dr.	aytek.com

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

User / User Management		C	;
Add User Profile			
Enable			
Username	CNIII] 🗸	
Password	••••••] 🗸	
Role	Operator ~		
Enable Auto Logout			
Enable OOBE feature			
OOBE pages to display	Read the Agreements, Set new passi $\stackrel{\scriptstyle\scriptstyle{\vee}}{}$		
Email Notification			
Email	carrie@draytek.com]~	
SMS Notification			
Telephone			
Description			
		Cancel Create	
			e.

4. Click **Create**.

lser / l	Jser Management						C
+Add	Delete 🔗 User Batch Settings					Search	Q
Showing	131 to 134 of 134 entries				s	Show 10 ~ entries 44 1 10 11 12 1	13 14 🕨
	Username	$\downarrow\uparrow$ Authentication	↓↑ Role ↓1	↑ Status ↓↑ Email Notification	$\downarrow\uparrow$ SMS Notification	↓↑ Email	J↑
	T_2024-08-04_Wholesale_GA_E	Internal	Group Administrator	Active Enabled	Enabled	T_2024-08-04_Wholesale_GA_E@test.email	
	T_2024-08-04_Wholesale_GA_D	Internal	Group Administrator	Active Disabled	Disabled	T_2024-08-04_Wholesale_GA_D@test.email	
	T_2024-08-04_Wholesale_GA_OOBE	Internal	Group Administrator	Active Enabled	Enabled	T_2024-08-04_Wholesale_GA_OOBE@test.email	
	CNIII	Internal	Operator	Activo Enabled	Disabled	carrie@draytek.com	

A.6 How to Add a Group?

1. Open User>>Group Management.

(7)	User
<u></u>	User Management
	Group Management
	Network Group
2	External Authentication Server
(FI)	Mail Server
Ĩ	Function Management
\$	Wholesale Wizard
	SMS Server
	SNMP Server
255	Notifications & Events
යී	Syslog Server
i	Group Parameter
	Link with Router App

2. Click +Add.

User / Grou	Jser / Group Management								
Setting	Managemer	nt UI Customization							
+Add									
	Group ID	↓↑ Group Name	$\downarrow\uparrow$	Max Nodes ↓↑	Used Nodes				
	4239	tttt7		200000	0				
	4240	tttt8		200000	0				

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

User / Group Management		C
Setting Management UI Customiz	zation	
Add Group		
Group name	yfnts 🗸	
Nodes	-1 (-1: No Limit Nodes)	
Enable CPE Notify Mail/SMS/SNMP		
Enable Global Mail Server		
Enable Global SNMP Server		
Enable Expire Date		
Expire Date	2024/08/31	
		Cancel Save

- Group Name Enter a new name of the user group.
- Nodes Define number of node.
- Enable CPE Notify Mail/SMS/SNMP Server Switch the toggle to enable /disable global mail server.
- Enable Global Mail Server Switch the toggle to enable /disable global mail server.
- Enable Global SNMP Server Switch the toggle 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.

	5063	Router_App_Group	No Lir	nit Nodes	2	Disabled		Disabled	Disabled	
	5395	AutoTest_Dev	No Lir	nit Nodes	7	Disabled		Disabled	Disabled	
	6611	yfnts	No Lir	nit Nodes	0	Enabled	2024/08/31	Disabled	Enabled	
Nodes In	Nodes Information									
Current N	lodes In Used	Configured Max Nodes	Purchased License	Nodes						(\uparrow)
50142.5		500263	200000							

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.

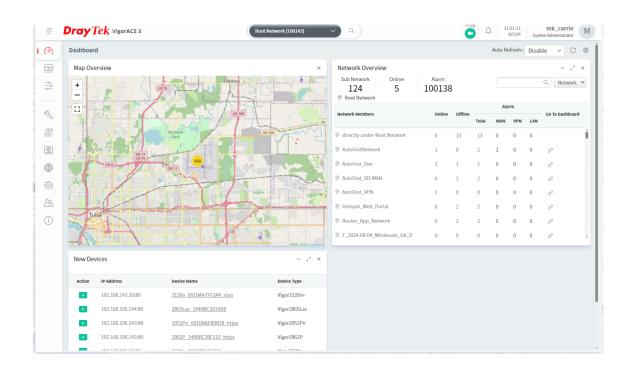
Use the drop-down menu on the top of the left side to select a network group.

Root Network(267)		
	Model	
器 RD3(14)	>	
윪 RD5(9)	>	
몲 RD6(3)		
몲 RD7(15)		
윮 RD8(58)		
몲 RD8-1(1)		

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



7.1 Dashboard for the Root Network



7.2 Monitoring

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

1 (7)	Monitoring
I 🗠	Alarm
	Logs
	Devices
2	Cellular Data Usage
	Floor Plan
\$	

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.

a)	/Tek vig	gorACS 3		Root Net	twork (100143)	✓ Q			Cap 	mk_carr System Administrat	
onito	oring / Alarr	n						2024/07/06 to	5 2024/08/05 V Search 1	No. / Device Name /	(MAC Q
Alarm	Hi	story									
	ete 🕀 Delet	te All 🕁 Dor	wnload						K < 1	/1 > ▷	C
	NO.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Type	Ack Time	Ack User
	38517749	Not Ack	2024/08/05 05:19:53	Q2121x_1449BC506AA4	Root Network	14:49:BC:50:6A:A4	\land Major	Device Loss Connection	Device Lost Connection		
	38517748	Not Ack	2024/08/05 05:19:53	P1282_1449BC43CD19	Root Network	14:49:BC:43:CD:19	\land Major	Device Loss Connection	Device Lost Connection		
	38517747	Not Ack	2024/08/05 05:19:53	P1280_001DAA4E6C33	Root Network	00:1D:AA:4E:6C:33	\land Major	Device Loss Connection	Device Lost Connection		
	38517746	Not Ack	2024/08/05 05:19:53	3912S_1449BC3072A0	Root Network	14:49:BC:30:72:A0	🔥 Major	Device Loss Connection	Device Lost Connection		
	38517745	Not Ack	2024/08/05 05:19:53	3910_1449BC6B9178	Root Network	14:49:BC:6B:91:78	\land Major	Device Loss Connection	Device Lost Connection		
	38517744	Not Ack	2024/08/05 05:19:53	3910_1449BC1CA218	Root Network	14:49:BC:1C:A2:18	\land Major	Device Loss Connection	Device Lost Connection		
	38517743	Not Ack	2024/08/05 05:19:53	2962_1449BC0D2040	Root Network	14:49:BC:0D:20:40	\land Major	Device Loss Connection	Device Lost Connection		
	38517742	Not Ack	2024/08/05 05:19:53	2865ac_1449BC143DA0	Root Network	14:49:BC:14:3D:A0	\land Major	Device Loss Connection	Device Lost Connection		
	38517740	Not Ack	2024/08/05 05:19:53	2865ac_001DAA4ACFB0	Root Network	00:1D:AA:4A:CF:B0	\land Major	Device Loss Connection	Device Lost Connection		
	38517737	Not Ack	2024/08/05 05:19:53	2850V_001DAA7D9CC8	Root Network	00:1D:AA:7D:9C:C8	\land Major	Device Loss Connection	Device Lost Connection		
	38517735	Not Ack	2024/08/05 05:19:53	2765Vac_1449BC2C42E8	Root Network	14:49:BC:2C:42:E8	\land Major	Device Loss Connection	Device Lost Connection		
	38517733	Not Ack	2024/08/05 05:19:53	2762Vac_001DAA653308	Root Network	00:1D:AA:65:33:08	\land Major	Device Loss Connection	Device Lost Connection		
	38517732	Not Ack	2024/08/05 05:19:53	2133Vac 001DAA66E020	Root Network	00:1D:AA:66:E0:20	▲ Maior	Device Loss Connection	Device Lost Connection		

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.
Network Name	Displays the name of the network that the monitored device belongs to.
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.

PE AI	ttions De	vice Reboot Reboot By CPE Reset Syst	tem Password Set Pa	rameter nie nanster bet	ting Profile Device SysLog	CPE Notify Device Register Dev	rice Operate	
Dele	te 🗎 De	lete All 🞍 Download						KI < 1 /12 > N C
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
	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
2	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

Item	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.

Ionitoring / Devices									Auto	Refresh: Disable ~
Search Device Name / IP / MA	IC .	Model Vigor16	7, Vigor2120n+, \	/igor213: ~	Status	AII	~	SSID All		~
								Rows 10	~ N <	1 /10015 > ▷ ◎
Download									General	Wireless
Device $\downarrow\uparrow$	IP Address	MAC Address	Model 4	Network $\downarrow \uparrow$	Status∕↑	Up Time Ut	F/W Version $\downarrow \uparrow$	Last Inform Time $-\downarrow\uparrow$	Current Client	Current Traffic
2927Lac 1449BC023768	192.168.106.140:80	14:49:BC:02:37:68	Vigor2927Lac	AutoTestNetwork	Online	0 days 08:28:50	4.4.2.3 🥥	2024/08/05 11:46:45	0 (Local Wireless: 0)	638.74 KB († 60.63 KB ↓ 57
2120n 001DAA7FF2A4 stun	192.168.106.143:80	00:1D:AA:7F:F2:A4	Vigor2120n+	AutoTest_Dev	Online	54 days 22:51:03	3.8.10 🥥	2024/08/05 11:55:05	0 (Local Wireless: 0)	52.49 KB (↑ 36.13 KB ↓ 16.3
2865Lac 1449BC3D7A08	192.168.106.144:80	14:49:BC:3D:7A:08	Vigor2865Lac	AutoTest_Dev	Offline	0 days 00:00:00	4.4.5_STD 🥝	2024/07/11 16:42:09	0 (Local Wireless: 0)	0 Byte († 0 Byte \downarrow 0 Byte)
2952Pn 001DAAF8D818 https	192.168.106.143:80	00:1D:AA:F8:D8:18	Vigor2952Pn	AutoTest_Dev	Offline	0 days 00:00:00	3.9.7.2 🧭	2023/09/25 10:41:51	0 (Local Wireless: 0)	0 Byte († 0 Byte \downarrow 0 Byte)
2962P 1449BC39F110 https	192.168.106.143:80	14:49:BC:39:F1:10	Vigor2962P	AutoTest_Dev	Online	59 days 22:20:48	4.3.2.6 🥑	2024/08/05 11:50:33	1 (Local Wireless: 0)	1.03 MB (↑ 111.50 KB ↓ 938
3220n 001DAA554758	192.168.105.22:80	00:1D:AA:55:47:58	Vigor3220n	AutoTest_Dev	Offline	0 days 00:00:00	3.9.7.4 🥑	2023/07/06 15:02:44	0 (Local Wireless: 0)	0 Byte († 0 Byte \downarrow 0 Byte)
AP 810 001DAA7C2B50	192.168.106.150:80	00:1D:AA:7C:2B:50	VigorAP 810	AutoTest_Dev	Offline	0 days 00:00:00	1.3.4 🕗	2023/09/12 06:03:00	0 (Local Wireless: 0)	
AP 902 001DAA3F150E stun	192.168.106.143:80	00:1D:AA:3F:15:0E	VigorAP 902	AutoTest_Dev	Offline	0 days 00:00:00	1.3.4 🥑	2024/04/16 02:53:44	0 (Local Wireless: 0)	
AP 903 1449BC5D8AFC	192.168.106.151:80	14:49:BC:5D:8A:FC	VigorAP 903	AutoTest_Dev	Offline	0 days 00:00:00	1.4.13 🥑	2024/06/02 11:22:46	0 (Local Wireless: 0)	-
AP 960C 1449BC427DB6	192.168.105.52:80	14:49:BC:42:7D:B6	VigorAP 960C	AutoTest Dev	Offline	0 days 00:00:00	1.4.3_RC2 🥑	2022/01/21 13:28:37	0 (Local Wireless: 0)	

ltem	Description
search Device Name / IP / MAC	Enter the condition for VigorACS to search and display relational information.
Model	This area lists all of the devices that monitored by VigorACS.
	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 Da	ata Usage							С		
LTE Data Usage Overview					Quota Settings					
Data Used 0 Byte	Data Cycle 11/02 - 11/08	Status: NORMAL		0% of 1500MB	Data Usage Alarm					
1 Byte	11/02 - 11/08			 Total 	Data Quota	1500 MB ~				
					Trigger Alarm When Usage Reached	51 % of Quota (765.00 MB)				
					Alarm Serverity Level	Critical ~				
0 Byte					Data Usage Cycle	Weekly Monthly Custom				
0.0,00			1-03		Weekly Reset Day	Monday ~				
Device		Total	Download	Upload						
2866L_1449BC02F990		0 Byte								
2927LVac_1449BC02F9A8	8	0 Byte					Cancel	Save		
2865Lax_1449BC0C5920		0 Byte								
2862Ln_001DAA625DE0		0 Byte								
2925L_001DAA5B0D98		0 Byte								
2860Ln_001DAA5B1CE0		0 Byte								

These parameters are explained as follows:

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.

ray Tek VigorACS 3	Root Network (100143) V	Pcap Pcap Pcap p 12:02:07 mk_carrie System Administrator
Monitoring / Floor Plan		
+ Add		55
Profile Name	↓↑ Devices	J↑ Action
20240605	1	🖉 Edit 🛛 🗓 Delete
test	0	🖉 Edit 👘 Delete

 Item
 Description

 +Add
 Creates a new profile.

 Click to change to browse view.
 It displays all of the floor plan profiles with the map used.

 It displays all of the floor plan profiles with the map used.
 It displays all of the floor plan profiles with the map used.

 Vou 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 Delete Map Profile Edit Map & Plan
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.

ofile Name masseting_carrie		loot Network 🗸 🗸	Dray Tek VigorACS 3	Capture Packets 👻	carrie System Administrator
	Edt Dimenson ▲ Add Dexice	Ionitoring / Floor Plan			
		Profile Name	marketing_carrie		
		Edit Dimension			
	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.

nitoring / Floor Plan			
Profile Name	marketing_carrie		
Edit Dimension + Add Device	ce		
g and drop a virtual AP or an un-	assigned AP to the floor plan.		
		Un-assigned APs	٢
		Un-assigned APs Device Name	Model
		Device Name	VigorAP 8
		Device Name	VigorAP (VigorAP
		Device Name A 810_001DAA7D6514 A P 1000C_001DAA04F084	VigorAP VigorAP VigorAP
		Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38	VigorAP (VigorAP VigorAP VigorAP VigorAP
		Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7	VigorAP (VigorAP) VigorAP) VigorAP (VigorAP)
		Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7 ▲ AP 800_001DAA2A5870	VigorAP 8 VigorAP 1

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.

nitoring / Floor Plan			
Profile Name	marketing_carrie		
Edit Dimension Add Device			
ig and drop a virtual AP or an un-a	ssigned AP to the floor plan.		
		asigned APs Device Name	Model
		▲ 810_001DAA7D6514	VigorAP 81
		AP 1000C_001DAA04F084	VigorAP 10 VigorAP 10
		AP 710_00507FF138F7	VigorAP 71
		AP 800_001DAA2A5B70	VigorAP 80
		AP 903_00507FF17ECA	VigorAP 90
+		AP 903_00507FF19216	VigorAP 90
0			

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 Y System Administrator	С
Monitoring / Floor Plan				
Profile Name	marketing_carrie			
Edit Dimension + Add Device				
			<pre></pre>	×

- **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		
Profile Name	↓↑ Devices	J↑ Action
bedroom	2	🖉 Edit 🛛 🗊 Delete
jpg	0	🖉 Edit 🛛 🗇 Delete
marketing_carrie	1	🖉 Edit 🝈 Delete

7.3 Configuration

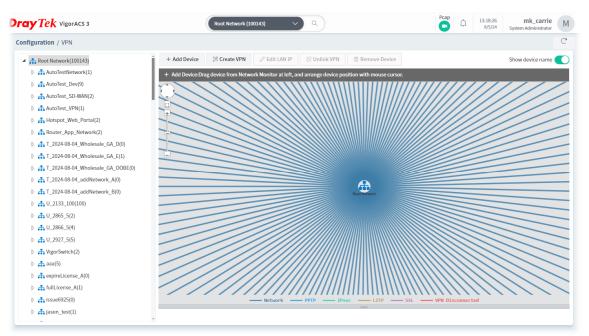
Configuration menu will vary for root network, group network and specified CPE.

(7)	Configuration	
<u></u>	VPN Wizard	~
	AP Profile	
-		

7.3.1 VPN Wizard

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.

file Name	Action			
fault Profile	✓ Edit II Delete II Duplic	rate O Copy To		
<	⊘ Edit			
st	✓ Edit			
st2				
	🖉 Edit 🗎 Delete 🏼 Duplic	cate Copy To		
df	🖉 Edit 🐵 Delete 斗 Duplic	cate 🛛 Copy To		
_Carrie	🖉 Edit 🐵 Delete 🚨 Duplic	cate 🚨 Copy To		
endy test	🖉 Edit 🐵 Delete 🖓 Duplic	cate Copy To		
P_test	🖉 Edit 🕆 Delete 🔍 Duplic	cate 🖾 Copy To		
ame	Model Name	Last Provisioned	Status	AP Profile
	Model Name	Last Provisioned	Status	AP Profile Empty
	Model Name VigorAP 810	Last Provisioned	Status -	
Root Network		Last Provisioned	Status -	Empty
-	VigorAP 810	Last Provisioned - -	Status - -	Empty V (As Parent) V
Root Network 2860ac_00507F00000e 2860ac_00507F00000e	VigorAP 810 VigorAP 810	Last Provisioned - - -	Status - - -	Empty (As Parent) (As Parent)
Root Network 2860ac_00507F00000e 2860ac_00507F00000f Arr Liu_oubuliF100406	VigorAP 810 VigorAP 810 VigorAP 140	Last Provisioned	Status - - - -	Empty ~ (As Parent) ~ (As Parent) ~ (As Parent) ~
Root Network 2860ac_00507F00000e 2860ac_00507F00000F wer Lau_obs07F700000F AP 902_001DAA3D4F16	VigorAP 810 VigorAP 810 Figurar 110 VigorAP 902	Last Provisioned	Status - - - - - -	Empty(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).

	+ Change Network ×
	Select a Network
	 An facto Network Antal Set Network<!--</th-->
	Cancel Copy for
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.

Dray Tek VigorACS 3	Root Network (100143)	v Q	Pcap	13:21:48 mk_carrie 8/5/24 System Administrator
Configuration / AP Profile				
Add a Profile				
Profile Type:	DrayOS 4 AP DrayOS 5 AP			
Profile Name:	AP_Carrie			
AP Login Username:	admin			
AP Login Password:	······ •			
↑ Back to profile list				Save

ltem	Description					
Profile Type	Recognize and confirm your AP belongs to DrayOS 4 or DrayOS 5 and select the correct version.					
	DrayOS 4 AP – Repres	sentative models such as AP903, AP802, AP912C, etc.				
	DrayOS 5 AP – Repres	sentative models such as AP1062C.				
Profile Name	Enter a name of the p	profile.				
AP Login Username	Enter a username for	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 Add New Profile	display the new profile on the AP profile list.				
	Test	🖉 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To				
	Test2	🖉 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To				
	ttt	🖋 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To				
	redf	🖉 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To				
	AP_Carrie	🖋 Edit 🂼 Delete 🛅 Duplicate 🛅 Copy To				

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:

ray Tek VigorACS 3	Roc	ot Network (100143) V Q	Pcap Pcap 13:27:35 mk_carrie System Administrator
Configuration / AP Profile			
General Setup	Operation Mode:	Access Point Range Extender Mesh Root Mesh Node	
SSID Settings	2.4G General Setup		^
Roaming		B	
Load Balance	2.4G Wireless LAN		
	802.11 Mode	Mixed(11b+11g+11n) ~	
LAN	2.4G Channel	Channel_11,2462MHz ~	
Airtime Fairness	Channel Width	Auto_20/40_MHz ~	
Mobile Device Management	Extension Channel	Channel_7,2442MHz ~	
Application			
	Antenna	2T2R ~	
MM Configuration	TX Power	100% ~	
System	MAC Clone		
Profile Setting	MAC Address		
	Band Steering		
	5G capability Check Time (sec.)	15	
↑ Back to profile list			

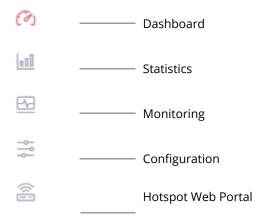
These parameters are explained as follows:

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.

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

Chapter 8 Network Group Menu

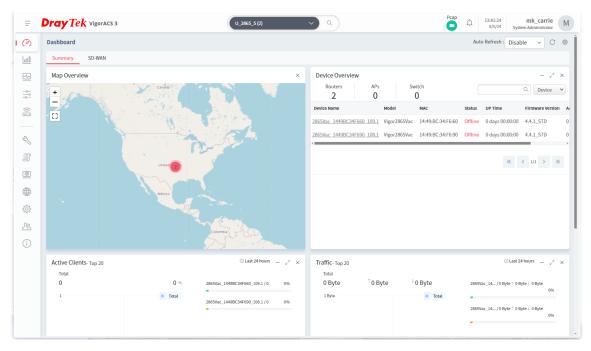
The menu items related to the network group:



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.

U_2865_5 (2)		<u>^ </u>	
Root Network (100143)			×
Network Model			C ~
Root Network > U_2865_5			
器 U_2865_5 (2)	>	⊌_2865Vac_1449BC34F660_109.1	
器 U_2866_5 (4)	>	₽ 2865Vac_1449BC34F690_108.1	
器 U_2927_5 (5)	>		
器 VigorSwitch (2)	>		
器 aaa (5)	>		
	>		
윪 fullLicense_A (1)	>		



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

8.2 Statistics for Network Group

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

Statistics						С
Last 24 Hours Last 7 Days Last	30 Days Custom Start: 2020/03/08	End: 2020/03/09				Export
Usage Overview (_)		- 2 ×	Wireless Clients Overview $\{j\}$			- 2 ×
Total Number of Clients	Wireless Clients Wir 1 (50%) 1 (ed Clients 50%)				
Total amount of Traffic 270.79 MB	Download Up 254.05 MB (93.8%) 16	.75 MB (6.2%)	Band	SSID		05
Max. Number of Concurrent Client 2	Avg. Number of Hourly C 1	lient 🛛	100.0% 2.4G 5 G	100.0%	Android IC	
Clients	OV	— ₂² ×	Traffic			- 2 ×
2	22:00 00:00 02:00 04:00 06:00	08:00 10:00 12:00 14:00	190,73 MB 143,05 MB 95,37 MB 47,68 MB 0 Byre 16:00 18:00 20	200 0000 0200 040	○ Wired ○ Wireles	An
Device Ranking (,)		≡Client • - 🗸 ×	Client Ranking (,)			Traffic • - 🗸 ×
J↑ Device	J↑ MAC	↓↑ Client ↓↑	ليث Host Name	.↓↑ MAC	4↑ Traffic	41
1 2865ac_001DAA000000	001 DAA000000	1	1 MKHL	406C8F525BFF	269.83 MB (99.6%)	
2 2926Vac_001DAA7033E0	001 DAA7033E0	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.

-		
(7)	Monitoring	
1 600	Alarm	80
I 🗠	Logs	
	Devices	W
	Clients	0
	Cellular Data Usage	0 58
	Floor Plan	
Z	Rogue AP Detection	
P	WAN (SD-WAN)	
- (2)	VPN (SD-WAN)	
	VoIP (SD-WAN)	
	Data Usage (SD-WAN)	
ξĝ3		
<u> </u>		
(j)		

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.

Monito	oring / Alarr	n						2024/07/06 to	2024/08/05 ~	Search No. / Device M	lame / MAC
Alarm	n 🕜 Hi	story									
	ete 🛱 Delet	e All Jov	wnload						ы <	1 /1 >	ØC
	No.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Type	Ack Tir	ne Ack Usi
	38617870	Not Ack	2024/08/05 05:33:10	AP 903_1449BC5D8AFC	AutoTest_Dev	14:49:BC:5D:8A:FC	\Lambda Critical	Device Loss Connection	Device Lost Cor	nection	
	38517763	Not Ack	2024/08/05 05:20:19	AP 960C_1449BC427DB6	AutoTest_Dev	14:49:BC:42:7D:B6	\Lambda Critical	Device Loss Connection	Device Lost Cor	nection	
	38517741	Not Ack	2024/08/05 05:19:53	AP 902_001DAA3F150E_stun	AutoTest_Dev	00:1D:AA:3F:15:0E	A Critical	Device Loss Connection	Device Lost Cor	nection	
	38517739	Not Ack	2024/08/05 05:19:53	AP 810_001DAA7C2B50	AutoTest_Dev	00:1D:AA:7C:2B:50	\Lambda Critical	Device Loss Connection	Device Lost Cor	nection	
	38517738	Not Ack	2024/08/05 05:19:53	3220n_001DAA554758	AutoTest_Dev	00:1D:AA:55:47:58	\Lambda Critical	Device Loss Connection	Device Lost Cor	nection	
	38517736	Not Ack	2024/08/05 05:19:53	2952Pn_001DAAF8D818_https	AutoTest_Dev	00:1D:AA:F8:D8:18	\Lambda Critical	Device Loss Connection	Device Lost Cor	nection	
	38517734	Not Ack	2024/08/05 05:19:53	2865Lac_1449BC3D7A08	AutoTest_Dev	14:49:BC:3D:7A:08	\land Critical	Device Loss Connection	Device Lost Cor	nection	

These parameters are ex	xplained 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.
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.

	oring / Logs									2021/01/31 to	2021/03/02 〜	search ID / Devi	ce Name / De	vic (
All CP	E Actions Device	Reboot Reboot By CPE I	Reset System Password	Set Parameter	File Transfer	Setting Profile	Device SysLog	CPE Notify	Device Register	Device Operate				
	iete 🛛 🖻 Delete All	Download									м <	$1 \hspace{0.5cm} /1 \hspace{0.5cm} \rightarrow \hspace{0.5cm}$	ЫС	6
	ID	Device Name		Device ID	MAC Address		Device IP		Action	Action ID	Time			
	3997642	2925Ln_001DAADD75B0		136121	001DAADD7	580	192.168.105.2	8	Inform		2021/02/17	08:35:11 AM		
	3997641	2952Pn_001DAAF8D818		141468	001DAAF8D8	318	192.168.105.5	2	Inform		2021/02/17	08:35:04 AM		
	3997640	2133Vac_001DAA66E020		141455	001DAA66E0	120	192.168.105.5	9	Inform		2021/02/17	08:35:02 AM		
	3997630	2133Vac_001DAA66E020		141455	001DAA66E0	120	192.168.105.5	9	Inform		2021/02/02	09:18:12 AM		
	3997629	2133Vac_001DAA66E020		141455	001DAA66E0	20	192.168.105.5	9	Inform		2021/02/02	06:53:48 AM		
	3997628	2133Vac_001DAA66E020		141455	001DAA66E0	120	192.168.105.5	9	Inform		2021/02/02	03:07:36 AM		
-														

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

Ŧ	Dray Tek VigorACS 3			AutoTes	t_Dev (9)	``	v a			Pcap	13:49:19 8/5/24 Syste	mk_carrie	М
(7)	Monitoring / Devices										Auto Refresh:	Disable 🗸	С
000	Search Device Name / IP / MA	C	Model Vigor2120)n+, Vigor2865La	c, Vigoı ~	Status	All	~	SSID All		~		
									Ro	ows 10 ~ M	< 1 /1	> D	۲
	Download									Genera	ι	Wireless	
	Device Ut	IP Address	MAC Address	Model 41	Network 4	Statusi↑	Up Time 41	F/W Version 🕂	Last Inform Time 🛛 🕸	Current Client	Current Traffic		$\downarrow\uparrow$
	2120n 001DAA7FF2A4 stun	192.168.106.143:80	00:1D:AA:7F:F2:A4	Vigor2120n+	AutoTest_Dev	Online	55 days 00:41:41	3.8.10 🥥	2024/08/05 13:39:59	0 (Local Wireless: 0)	12.65 KB († 9.	84 KB ↓ 2.82 KI	B)
2	2865Lac 1449BC3D7A08	192.168.106.144:80	14:49:BC:3D:7A:08	Vigor2865Lac	AutoTest_Dev	Offline	0 days 00:00:00	4.4.5_STD 🥝	2024/07/11 16:42:09	0 (Local Wireless: 0)	0 Byte († 0 Byt	te↓0 Byte)	
P	2952Pn 001DAAF8D818 https	192.168.106.143:80	00:1D:AA:F8:D8:18	Vigor2952Pn	AutoTest_Dev	Offline	0 days 00:00:00	3.9.7.2 🥑	2023/09/25 10:41:51	0 (Local Wireless: 0)	0 Byte († 0 Byt	te↓0Byte)	
	2962P 1449BC39F110 https	192.168.106.143:80	14:49:BC:39:F1:10	Vigor2962P	AutoTest_Dev	Online	60 days 00:11:16	4.3.2.6 🥑	2024/08/05 13:35:49	0 (Local Wireless: 0)	1.01 MB († 95.	87 KB ↓ 937.20) KB)
\$	3220n 001DAA554758	192.168.105.22:80	00:1D:AA:55:47:58	Vigor3220n	AutoTest_Dev	Offline	0 days 00:00:00	3.9.7.4 🥑	2023/07/06 15:02:44	0 (Local Wireless: 0)	0 Byte († 0 Byt	te↓0 Byte)	
	AP 810 001DAA7C2B50	192.168.106.150:80	00:1D:AA:7C:2B:50	VigorAP 810	AutoTest_Dev	Offline	0 days 00:00:00	1.3.4 🥝	2023/09/12 06:03:00	0 (Local Wireless: 0)			
-	AP 902_001DAA3F150E_stun	192.168.106.143:80	00:1D:AA:3F:15:0E	VigorAP 902	AutoTest_Dev	Offline	0 days 00:00:00	1.3.4 🧭	2024/04/16 02:53:44	0 (Local Wireless: 0)			
£\$}	AP 903 1449BC5D8AFC	192.168.106.151:80	14:49:BC:5D:8A:FC	VigorAP 903	AutoTest_Dev	Offline	0 days 00:00:00	1.4.13 🥥	2024/06/02 11:22:46	0 (Local Wireless: 0)			
23	AP 960C 1449BC427DB6	192.168.105.52:80	14:49:BC:42:7D:B6	VigorAP 960C	AutoTest_Dev	Offline	0 days 00:00:00	1.4.3_RC2 🥑	2022/01/21 13:28:37	0 (Local Wireless: 0)			
i													

These parameters are explained as follows:
--

ltem	Description
search Device Name / IP / MAC	Enter the condition for VigorACS to search and display relational information.
Model	This area lists all of the devices that monitored by VigorACS. 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
Download	group. 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.

Ξ	DrayTek VigorACS 3 AutoTest_Dev (9) 🗸 🖓 🖓 🖓 🖓 🖓 🖓 AutoTest_Dev (9)
(7)	Monitoring / Clients
000	Last 24 Hours Last 7 Days Last 30 Days Custom Start 2024-08-05 End: 2024-08-05
ı 🖾	Search Hostname / MAC / IP Type: All ~ SSID: All ~
	Rows → 10 < 1 /1 > 10 (2 @
	Hostname 47 MAC Address 47 IPAddress 47 Connected Device 47 Connected Device 47 Connected Device MAC 47 OS/7 Type 47 SSID47 ConnectionTime 47 Traffic 47
Z	00:1D:AA:7F:F2:A5 192.168.143.10 2962P_1449BC39F110_https 14:49:BC:39:F1:10 WIRED 54d 12h 53m 26s 43.87MB(† 23.77MB ↓ 20.10MB)
Ø	Total Number of Clients: 1
園	

These parameters are explained as follows:

ltem	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 WIRED WIRELESS_2.4g	Wired – This page displays information for the device without wireless feature.
WIRELESS_52 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.

✓ Hostname	MAC Add	dress	IP Address	
Connected Device	Connect	ed Device MAC	🗹 OS	
🗹 Туре	SSID		ConnectionTime	
Traffic				
Select devices				
Name	Model Name	Firmware Version		
🖌 📃 🕜 rd8(48)				
🛛 🕐 810_001DAA7D6514	VigorAP 810	1.2.5		
902_001DAA3D4F16	VigorAP 902	1.2.3.1		
130_001DAA83A094	Vigor130	a		
130_001DAA8411C8	Vigor130	r70663_beta		
130_001DAA854204	Vigor130	r72469_beta		
	Vigor130	a		
@ 2120n+_001DAA0FE010	Vigor2120n+	3.8.9.2		
2130Vn_001D000000E	Vigor2130Vn	v1.5.4.2		
2132FVn_001DAAE486C8	Vigor2132FVn	3.7.9.1_CBizz_1		
2133Vac_001DAA66E020	Vigor2133Vac	3.9.0_RC2		
2620Ln_001DAA926F58	Vigor2620Ln	3.8.10_RC1		
2710n_00507F9A3648	Vigor2710n	3.6.8.6		
@ 2830V_00507F708028	Vigor2830V	3.8.8.2_sb_246302		
28301_001DAAA09418	Vigor28301	3.6.8.7_db_RC3		
2860n+_001DAAD1E290	Vigor2860n+	3.8.9.3_STD		
				× Cancel +

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.

Dray Tek VigorAC	S 3		AutoTest	t_Dev (9)	✓ Q	Pca	Ģ	13:54:16 8/5/24	mk_carrie System Administrator	
Monitoring / Cellular Da	ta Usage									С
LTE Data Usage Overvi	ew				Quota Settings					
Data Used 0 Byte	Data Cycle 08/04 - 08/10	Status: WAR	ING	0% of 0M	B Data Usage Alarm	\bigcirc				
1 Byte					Data Quota	0 MB ~				
					Trigger Alarm When Usage Reached	0 % of Qu	ota (0 Byte)			
					Data Usage Cycle	Weekly Monthly	Custom			
0 Byte					Weekly Reset Day	Sunday			~	
Device		Total	Download	Upload					Cancel	iave
2865Lac_1449BC3D7A08		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 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.			
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.

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	Capturo Packots ~ Capturo Packots ~ Capturo Packots ~
(4)	Monitoring / Floor Plan			
000	+ Add			
<u>5</u>	Profile Name	J↑ D	Devices	J↑ Action
	test	0)	🖉 Edit 🔞 Delete
â	test2	0)	🖉 Edit 🔞 Delete
2				

ltem	Description
+Add	Creates a new profile.
	Dray Tek vigorAcs 3 Q 2017.5169 Q A LISEZS Mic.carrie M
	Monitoring / Floor Plan
	Profile Name 🗸
	Upload Map Floor_MAP.png
	Cancel Centinue
88	Click to change to browse view.
	It displays all of the floor plan profiles with the map used.

	Monitoring / Floor Plan			
	bedroom 🗣 jpg	Q tte	٥	₽Add
				K < 1 /1
	You can click Add on this page to existed profile, click the icon on Then click Edit Map & Plan to pe Profile to remove the selected fl marketing	the right-top to di rform the modific	splay a drop c	lown menu.
	De	elete Map Profile dit Map & Plan		
Profile Name	Displays the name of the floor p	lan profile.		
Device	Displays the number of AP devic	es placed on the p	plan profile.	
Action	Edit - Click to modify the profile. Delete - Click to remove the sele			

To create a new profile:

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

Dray Tek VigorACS 3		U_2927_5 (5)	✓ Q	Pcap Â	13:57:25 8/5/24	mk_carrie M
Monitoring / Floor Plan						
Profile Name	test_Carrie	~				
Upload Map	Floor_MAP.png	Browse				
					C	ancel Continue

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

Monitoring / Floor Plan		
Profile Name	test_Carrie	
Edit Dimension + Add Device		
		+
	c	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.

Profile Name	marketing_carrie				
Edit Dimension + Add Device	ce				
ag and drop a virtual AP or an un-	assigned AP to the floor plan.				
			* -	Un-assigned APs Un-assigned APs Device Name A 810_001DAA7D6514 A AP 1000C_001DAA575038 A AP 110_00507F13877 A AP 800_001DAA2A5870 A AP 903_00507F17ECA A AP 903_00507F17ECA A AP 903_00507F17E16 A AP 910_001DAA755D8C	Model VigorAP 81 VigorAP 10 VigorAP 10 VigorAP 71 VigorAP 80 VigorAP 90 VigorAP 90 VigorAP 91

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.

rofile Name	marketing_carrie			
Edit Dimension Add Device				
g and drop a virtual AP or an un-assigned	d AP to the floor plan.			
			00	, •
		ų.	Jn-assigned APs	
		Ĩ	Device Name	Model
		Ľ	Device Name	VigorAP 810
		L	Device Name 810_001DAA7D6514 AP 1000C_001DAA04F084	VigorAP 810 VigorAP 100
		L	Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38	VigorAP 81 VigorAP 10 VigorAP 10
		Ē	Device Name & 810_001DAA7D6514 & AP 1000C_001DAA04F084 & AP 1000C_001DAA575D38 & AP 710_00507FF138F7	VigorAP 81 VigorAP 10 VigorAP 10 VigorAP 71
			Device Name & 810_001DAA7D6514 A P 1000C_001DAA04F084 A P 1000C_001DAA575D38 A P 710_00507FF138F7 A P 800_001DAA25870	VigorAP 81 VigorAP 10 VigorAP 10 VigorAP 71 VigorAP 80
		•	Device Name & 810_001DAA706514 & A P 1000C_001DAA04F084 & A P 1000C_001DAA575D38 & A P 100,00507F138F7 & A P 800_001DAA2A5670 & A P 903_00507F17ECA	VigorAP 810 VigorAP 100 VigorAP 100 VigorAP 100 VigorAP 710 VigorAP 800 VigorAP 900
			Device Name & 810_001DAA7D6514 A P 1000C_001DAA04F084 A P 1000C_001DAA575D38 A P 710_00507FF138F7 A P 800_001DAA25870	

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 + Add Device		
		×

- **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.

	E
↓↑ Devices	↓↑ Action
2	🖉 Edit 👘 Delete
0	🖉 Edit 👘 Delete
1	🖉 Edit 🖷 Delete
	2

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.

ay Tek VigorACS 3				C	8/5/24	System Administrator	
onitoring / Rogue AP Detection							
Last 24 Hours Last 7 Days Last 30 Days Custom	Start: 2024-08-04 End	d: 2024-08-05					
Scan Now Periodic Scan	Daily Weekly	Start Time 1:00	~				Save
Rogue AP Known AP							
-Hark as Known Delete Delete All					М < 1	$/1 \rightarrow \bowtie$	C
BSSID $\downarrow\uparrow$ SSID $\downarrow\uparrow$ Band	↓↑ Channel	↓↑ Security	↓↑ Detector	↓↑ Signal	↓↑ Last Detected		4
		No data avai	lable				

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.

	Periodic Scan	Daily Weekly Start Time 10:00	_	
Scan Now	_	Daily Weekly Start Time 10:00	Y	Sav
Rogue AP Kn + Add 🖉 Edi	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	

ltem	Description	Description						
Add	Click to crea	ate a new entry for er	ntering informat	ion for access point.				
Edit	Change the settings for a selected access point.							
	then. After clickin	·		be available for clicking will be allowed to be				
	Scan Now	Periodic Scan 🔵	Daily Weekly	Start Time 10:00 🔻				
	Rogue AP + Add Ø	Known AP Edit 💼 Delete 🐵 Delete All						
		BSSID	Channel	Security				
	•	00:1d:aa:00:00:02	Any	Any				
		22:33:11:22:33:33	Any 👻	Any 👻				
				WEP WPA2/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA2/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x				
Delete	Remove the	e selected access poir	nt from the list.					
Delete All	Remove all	of the access points f	rom the list.					
BSSID	Display the	MAC address of the o	detected access	point.				
Channel		channel used by the box of the selected ac	-	lick Edit .				
Security	Display the lt can be ch	security mode used b anged.	by the access po	pint.				

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.

SD-WAN is not enabled
SD-WAN is not enabled in this network. No new SD-WAN data will be saved. Do you want to enable it?
No 🗸 Yes
- 48 A

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	Network 🛛 🚓 Change Network				
General Settings					
Network ID			Username		
254			fae		
Name			Password		
FAE		~	•••	¢	
ocation					
Bulk Data Settings et the category of data to be collected hich the profile returns a bulk data to				category in the corresponding profile, and specify the report interval	
Profile #1	Enable 🔵	Profile #2	Enable	Available / Disabled Bulk Data Categories	
Report Interval (sec)		Report Interval (sec)		[
120	~	300	~		
Bulk Data Categories		Buik Data Categories			
\equiv WAN and VPN	Size: 8	\equiv Users and Apps	Size: 4		
			1		
≡ VoIP	Size: 1		•		

8.4 Configuration Menu for Network Group,

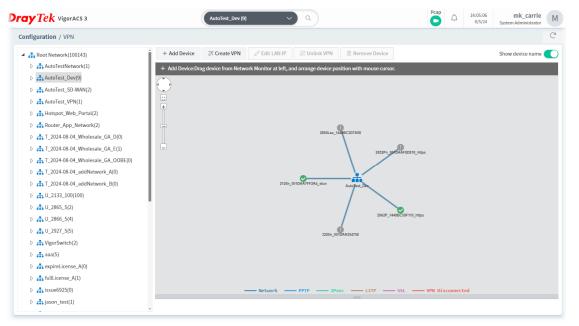
Configuration settings will vary for root network, group network and specified CPE. This section introduces the menu item used for the network group with SD-WAN feature.

k (7)	Configuration	
00	VPN Wizard	
I 🗠	AP Profile	
_ ≏ ≂	Load Balance	
·	Route Policy	
	Link Health Check	
	Interface Settings	
Z		

8.4.1 VPN Wizard

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

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



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

8.4.2 AP Profile

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

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

~
~
~
~
~
)

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).							
	Root Network DrayTek VigorAcS3 Capture Packets ~ System Administrator + Change Network ×							
	Select a Network							
	Select a Network							
	 A Root Network A 1111 A ALANVEN A Akaco A Akaco A desterNetwork A IKI Marketing carrie A Novanet A OCTOBER A RD1 A RD2 A RD3 							

	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.

8.4.2.1 Add an AP Profile

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

Configuration / AP Profile			
Add a Profile			
Profile Type:	DrayOS 4 AP DrayOS 5 AP		
Profile Name:			
Profile Name:	AP_Carrie	~	
AP Login Username:	admin	~	
AP Login Password:	·····	~	
A LOBITIONOLO.		~	
↑ Back to profile list			
The Back to profile list			

ltem	Description							
Profile Type	Recognize and confirm your AP belongs to DrayOS 4 or DrayOS 5 and select the correct version.							
	DrayOS 4 AP - Re	epresentative models such as AP903, AP802, AP912C, etc.						
	DrayOS 5 AP – Re	epresentative models such as AP1062C.						
Profile Name	Enter a name of	Enter a name of the profile.						
AP Login Username	Enter a usernam	Enter a username for login the access point.						
AP Login Password	Enter a password	Enter a password for login the access point.						
Back to profile list	Return to previou	Return to previous page, AP profile list.						
Save	Save the settings	and display the new profile on the AP profile list.						
	Test	🖉 Edit 💼 Delete 🖸 Duplicate 🖸 Copy To						
	Test2	🖋 Edit 💼 Delete 🖸 Duplicate 🖸 Copy To						
	ttt	🖋 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To						
	redf	🖋 Edit 💼 Delete 🛄 Duplicate 🛄 Copy To						
	AP_Carrie	🖋 Edit 💼 Delete 🛅 Duplicate 🛅 Copy To						

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:

General Setup	Operation Mode:	Access Point Range Extender Mesh Root Mesh Node
SSID Settings		
Roaming	2.4G General Setup	^
Load Balance	2.4G Wireless LAN	
Load Balance	802.11 Mode	$M_{ ext{Mixed(11b+11g+11n)}}$ \sim $oldsymbol{B}$
LAN	2.4G Channel	Channel_11,2462MHz ~
Airtime Fairness	Channel Width	Auto 20/40 MHz
Mobile Device Management		
	Extension Channel	Channel_7,2442MHz v
Application	Antenna	2T2R 🗸
WMM Configuration	TX Power	100% ~
System	MAC Clone	
Profile Setting	MAC Address	
4	Band Steering	
	5G capability Check Time (sec.)	15

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.

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	ow High	
Download Bandwidth Weight	ow High	
Low Latency Weight	cow High	
Low Jitter Weight	ow High	
Less Packet Loss Weight	ow High	
lear	Save and Apply to CPEs	I

Item	Description
Load Balance Mode	IP Based - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.
	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 Weights	There are four weight types for choosing to meet your request.
	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

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

(rd8	~				Dray Tek VigorACS 3		Capture Packets ~	carrie System Administrator	С
	Configuration / Route P	olicy								C
	+ Add New Route Policy									
	App Service Profile	In Use O	Remaining 32	dmum 32	① Note App service	rofiles are currently managed by VigorACS, unused profiles will t	be removed automatically.			
	# UT Status	↓↑ Comme	int	Ų	Source	3↑ Destination	.↓↑ Interface		J↑ Action	
						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.

×

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.

App Service Profile Create a new profile From an existing profile Selected App Service FTP ③ DNS ③ Wikipedia ③	
Source Any Destination App Services App Service Profile Create a new profile Selected App Service FTP © DNS © Wikipedia ©	
Destination App Services App Service Profile Create a new profile Selected App Service FTP ② DNS ③ Wikipedia ③	
App Service Profile Create a new profile From an existing profile Selected App Service FTP DNS Wikipedia 	
Selected App Service FTP 🛞 DNS 🛞 Wikipedia 🛞	~ ~
Send via Interface WAN 1	-
	~
Note If you want to send via VPN (to the Hub), please dial VPN Hub and Spoke connection fir Go to SD-WAN VPN Settings + Advanced Mode	t.

These parameters for Basic Mode are explained as follows:

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 				
	Note that, when a route policy is set with App services, it will be applied to the router at the same time. Open Configuration>>Routing>>Load Balance / Policy Route. The routing rule with APP service will be highlighed and marked as "Managed By SD-WAN". It means the policy was created by ACS SD-WAN, and can be edited or deleted by ACS SD-WAN only.				

	← Configuration	2865ac_001DAA00	00000 /	Configuration	/ Routing				C
	Load Balance/Policy Route								
	Static Route IPv4		Index	Enable	Comment	Protocol	Interface	Src IP	Dest IP
	Static Route IPv6		1	Enable		Any	WAN1	Range	Any
	BGP	Managed By SD-WAN	2	Enable		Any	WAN1	Any	APP Service
			3	Disable		Any	WAN1	Any	Any
a b b b b c b c b c c c c c c c c c c								<u> </u>	
Send via Interface	WAN#/LAN#	#/DMZ/IP	P Rc	outed S	ubnet - Sel	ect an in	terface	from th	e list. The
Send via Interface	WAN#/LAN #						terface	from th	e list. The
	traffic will be	e sent to	the	e desig	nated inter	face.		from th	e list. Th
Send via Interface +Advanced Mode		e sent to	the	e desig	nated inter	face.		from th	e list. Th
	traffic will be	e sent to	the	e desig	nated inter	face.		from th	e list. The
	traffic will be	e sent to	the	e desig	nated inter	face.		from th	e list. The
	traffic will be Click to ope	e sent to n the con	the	e designuration	nated inter	face. more o	ptions.	from th	e list. The
+Advanced Mode	traffic will be	e sent to n the con	the	e designuration	nated inter	face. more o	ptions.	from th	ie list. Th

2. Click Save and set to CPEs.

0%	Please wait for a w	hile.		
~	Succeed: 0	Processing: 0	Waiting: 0	🔴 Failed: 0

3. A route policy has been set successfully.

rd8		~					Dray	ek VigorACS 3		Et Capture Packets ×	System Adminis	carrie strator
Configu	uration / Rout	e Policy										
+ Add	d New Route Policy	In Us		Remaining	Maximum	① Note						
App Ser	rvice Profile	0		32	32		iles are currently man	aged by VigorACS, unused profiles will be ren	noved automatically.			
# -11	Status	4t	Comment				↓↑ Source	↓↑ Destination	4† Interface		J† Action	
1	Enabled		Marketing_	Carrie			Any	Any	WAN1		🖉 Edit 🏦) Delete

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 vi Go to SD-WAN VPN Se	a VPN (to the Hub), please dial VPN Hub and Spo ttings	ke connection first.

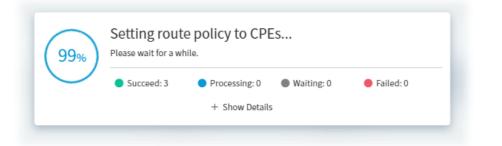
2. Click **+Advanced Mode** to get the following page.

Send via Gateway	Default Gateway	Specific Gat	teway
Packet Forwarding to WAN/LAN	Force NAT F	orce Routing	
via			
Failover	\bigcirc		
Failback	\bigcirc		
	— Basio	Mode	

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	Force NAT - The source IP address will not be used to connect to the remote destination. Network Address Translation (NAT) will be used, where a common IP address will be used.
	Force Routing - The source IP address will be preserved when connecting to the remote destination.
Failover	Click the icon to enable / disable the failover function.

	Failover							
		✓ Failover to D	efault 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.							
	Failover to Specify Gateway - Enter an IP address.							
	Failback - Click the icon to enable / disable the failback function.							
Basic Mode	Click to return to configuration	on page with les	s options.					
Save and set to CPEs	Save the above configuration	and set to CPE	devices.					

4. Click Save and set to CPEs.



5. A route policy has been set successfully.

18	~			Dray Tel	VigorACS 3	Capture Packe	carrie System Administrator
onfiguration / Route	e Policy						
+ Add New Route Policy	(
pp Service Profile	In Use O	Remaining 32	Maximum 32	Note App service profiles are currently managed	by VigorACS, unused profiles will be removed at	romatically.	
J↑ Status	↓↑ Commen	t		41 Source	↓↑ Destination	↓↑ Interface	41 Action
1 Enabled	Marketin	g Carrie		Any	Any	WAN1	🖉 Edit 📋 Delete

8.4.5 Link Health Check

This page enables the system administrator to set up various profiles for quality monitoring. This allows the VigorACS server to conduct quality monitoring on the WAN interface of each CPE using different profiles.

Configuration / Link Health Check +Add Profile Name Profile Name / Link Health Check # Profile Name Detection Method Primary Target Secondary Target Interval Action 1 Default Ping Detect 8.8.8 8.8.4 10 Image: View	ray	Tek VigorACS 3		U_2927_5 (5)	✓ Q		4:24:34 mk_carrie 8/5/24 System Administrator	
# Profile Name Detection Method Primary Target Secondary Target Interval Action	Confi	iguration / Link Health C	Check					C
	+Ad	dd					Profile Number Limit	t: 1/2
1 Default Ping Detect 8.8.8.8 8.8.4.4 10 € View	#	Profile Name	Detection Method	Primary Target	Secondary Target	Interval	Action	
	1	Default	Ping Detect	8.8.8	8.8.4.4	10	€ View	

Click **+Add** to create a new link health check profile.

dd		
rofile Name		
etection Mode	Ping Detect HTTP Detect ✓	
arget Type	IP Address	
rimary Target		
econdary Target (Optional)	IPv4 format (EX:123.12.1.1)	
iterval (sec)	0	

ltem	Description
Profile Name	Enter the profile name.
Detection Mode	Select Ping Detect or HTTP Detect.
Target Type	Display the target type of this profile.
Primary Target	Enter the IP address to be monitored by VigorACS.
Secondary Target (Optional)	Enter the secondary IP address to be monitored by VigorACS. If the IP address is the same as the Primary Target, only that specific IP address will be monitored.
Interval(sec)	Set the interval for monitoring the interface.
Save	Click to save the changes in this page.

8.4.6 Interface Settings

This page enables the system administrator to set interface settings (WAN) for quality monitoring. This allows the VigorACS server to conduct quality monitoring on the WAN interface of each CPE using different profiles.

8.4.6.1 Performance Probe

The default performance probe includes profiles of the Wired WAN and Wireless WAN.

	(- <u></u>		U +	8/5/24 System Administrator
Faabla	14	Link Health Check	¢	Action
t	Profile	$_{\downarrow\uparrow}$ $~$ Detection Method $~$	↓↑ Target	↓↑
Disabled	Default	Ping Detect	8.8.8.8, 8.8.4.4	🖉 Edit
Disabled	Default	Ping Detect	8.8.8.8, 8.8.4.4	🖉 Edit
				Apply to CPEs
	Disabled	Enable 41 41 Profile CREMMO Default	Enable 47 Link Health check 47 Profile 47 Detection Method CCCMP Default Ping Detect	Enable Link Health check Image: Profile Image: Im

Click **Apply to CPEs** to apply the configuration in this page to all the CPEs managed by VigorACS server.

Click **Edit** of the selected profile (Wired WAN Performance or Wireless WAN Performance) to make modifications.

Configuration / Interface Settings				C
Wired WAN Performance Probe				
Enable Wired WAN Performance Probe				
Link Health Check Profile	Default (8.8.8.8, 8.8.4.4)	~		
Link Health Check Detail	Edit Detection Method :	Ping Detect		
	Primary :	8.8.8.8		
	Secondary :	8.8.4.4		
				Cancel Save

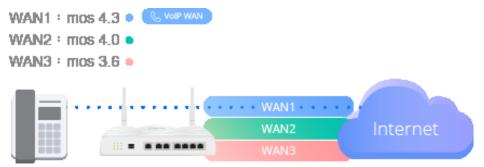
These parameters are explained as follows:

Item	Description
Enable Wired WAN Performance Probe	Switch the toggle to enable or disable this profile.
Link Health Check Profile	Use the drop-down list to specify a link health check profile.
Link Health Check Detail	Display the detailed information of the link health check.

Click **Save** to save the settings and return to previous page.

8.4.6.2 VoIP 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.

Configuration / Interface Settings	C
Performance Probe VolP WAN	
Enable VoIP WAN	
Change VoIP WAN when current WAN MOS score is less than	3.5 ~
And another WAN is better by	0.3 ~
Clear	Save and Apply to CPEs

These parameters are explained as follows:

ltem	Description
Enable VoIP WAN	Switch the toggle 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 3.0(bad) to 4.0 (excellent).
And anther WAN is better by	Specify a MOS number as the ending point. The rating for MOS is from 0.1(bad) to 0.9 (excellent).
Clear	Click to return to factory default setting.
Save and Apply to CPEs	Click to save the settings and apply to all of the CPE devices managed by VigorACS server.

(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.



8.5 Hotspot Web Portal for SD-WAN Network Group

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

(7)	Hotspot Web Portal
000	Profile
<u></u>	Quota Management
	Network & Device
	PIN Generator
	Analytics
Z	
0	

8.5.1 Profile

Profile is used to create or modify Hotspot Web Portal profiles. Up to 20 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

ray Te	k VigorACS 3		U_2927_5 (5)	~ Q	Pcap		57:19 /5/24 Sys	mk_ca	
Hotspot We	b Portal / Profile : RootGroup ~								(
+Add							Pro	ofile Numbe	er Limit: 5/.
id ↓†	Profile Name	↓↑ Enable	J↑ Hotspot Server Mode J↑	LogIn Method	↓↑ Applied Interfaces ↓↑	Action			
2	105.169	Disabled	ACS3 as Hotspot Server	Google	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	🖉 Edit	🗊 Delete	Сору	€ View Lo
6	copy_root_ltest	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1,2) WLAN 2.4G (1,2) WLAN 5G (1,2)	🖉 Edit	🗊 Delete	Сору	View Le
7	wwwwwwww	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1,2) WLAN 2.4G (1,2) WLAN 5G (1,2)	🖉 Edit	🗊 Delete	С Сору	🔒 View Lo
8		Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	🖉 Edit	🗊 Delete	СОру	View Le
18	d	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	🖉 Edit	🗊 Delete	() com	A Mourt

Item	Description
+Add	Click to create a new hotspot web portal profile.
Index	Displays the index number of the profile.
Profile Name	Displays the name of the profile.
Enable	Displays if this profile is enabled or disabled.
Hotspot Sever Mode	 Displays the hotspot server mode. 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.

		opied to another hot be copied. Then clie	
Copy Profile			
New Profile Name	Please enter a	a profile name	
Copy Item	🗹 Configurati	ion	
	_		
	Locales		
		Cancel Apply	
View Log – Click to	review detailed ir	Cancel Apply	
View Log – Click to Hotspet Web Partal / Hotspot Profile	review detailed ir		
Hotspot Web Portal / Hotspot Profile User Group : RootGroup *	review detailed ir		
Hotspot Web Portal / Hotspot Profile	review detailed ir		
Hotspot Web Pertal / Hotspot Profile User Group : RootGroup •	review detailed ir		
Hotspot Web Portal / Hotspot Profile User Group : RootGroup • T Back To Profile List Profile Information Profile ID 9		nformation for the s	
Hotspot Web Portal / Hotspot Profile User Group : RootGroup	arrie	nformation for the s	
Hotspot Web Portal / Hotspot Profile User Group : RoolGroup		nformation for the s	elected profile.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup	arrie uist for test	nformation for the s	elected profile.
Hotspot Web Portal / Hotspot Profile User Group : RootGroup •	arrie ust for test is Hotspot Login	nformation for the se	elected profile.

To create a new hotspot web portal profile:

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

+ Create New Profil	le		
New Profile Name	NYF_Carrie		
		Cancel	Create

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

	Web Portal / Profile up: RootGroup	~							С
+Add								Profil	e Number Limit: 3/20
Index ↓↑	Profile Name 41	Enable $\downarrow\uparrow$	Hotspot Server Mode	↓↑ Login Method	↓↑ Applied Interfaces	↓↑ Action			
1	NYF_Carrie	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	🖉 Edit	Delete	Сору	
2	dsadas	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	🖉 Edit	Delete	Сору	View Log
3	NYF_carrie	Disabled	ACS3 as Hotspot Server	Click Through	LAN (1)	🖉 Edit	🗄 Delete	C Copy	Ciew Log

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

Hotspot Web Portal / Hotspot Profile User Group : RootGroup •	c
1 Profile Se	tup Splash Page Customication Whitelet Setup (Optional)
Basic Settings	
Enable Profile	
Profile Name	NYF_Carrie
Comments	just for test
Hotspot Server Mode	ACS3 as Hotspot Server ACS3 as Hotspot Server
Applied Interfaces	The 3rd Party Hotspot Server
Subnet	C LAN1 O LAN2 O LAN3 O LAN4 O LAN5 O LAN6 O LAN7 O LAN8
WLAN 2.4G	SSID1 SSID2 SSID3 SSID4
WLAN 5G	□ \$5ID1 □ \$5ID2 □ \$5ID3 □ \$5ID4
External RADIUS Server	
External RADIUS Server	No External RADIUS Server Dedit
RADIUS MAC Authentication	
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	
	ß Example:https://Your VigorACS Server/ACSServer/HotsposPortal/home
Redirection URL	Http:// v portal.draytek.com
HTTPS Redirection ()	
Captive Portal Detection 🕑	
Landing Page Method	Fixed URL *
Landing Page URL	http://draytolc.fovcd.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

ltem	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	Displays the IP address of the external RADIUS Server.
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 1812
	Secret D
	Retry 2
	Secondary Server Server IPv4 format (EX : 123.12.1.1)
	Destination Port 1812
	Secret $ riangle and a constraint of the second sec$
	Retry 2
	Cancel Confirm
RADIUS MAC	If the RADIUS server supports authentication by MAC address, enable
Authentication	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
	 requested. Bulletin Message - Show a message on Bulletin.
Londing Dags UD	
Landing Page URL	It is available when Fixed URL is selected as Landing Page Method .
	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.

Layout	Components	Login Method	
Background Layout	Color Image		
Background 1 Color 🔗	#4a4972	C	
Background 2 Color 🔗	#FFFFF	5	
Login Method Background Color 🔗	#4a4972	5	Welcome! Please log in to enjoy Wi- FL
Login Method Opacity 🔗	97		Connect
Browser Tab Title	Draytek Hotspot		
Enable Browser Tab Icon	0		
Enable Logo			
SplashPage Logo 🔗	DrayTek Red Image Upload	1	
Splash Page Logo 🔗	DrayTek Red Image Upload	1	

These parameters are explained as follows:

ltem	Description
	Layout
Background	Select either Color or Image as the login page background scheme.

Layout		
Background 1 / 2 Color	0	of the login window (up and down layer) from enter the RGB value (with the format of HEX).
Login Method Background Color	Select the background color list, or enter the RGB value (v	of the login panel from the predefined color with the format of HEX).
Login Method Opacity	Adjust the opacity (1-100) of	the login panel.
Browser Tab Title	Enter the text to be shown a	s the webpage title in the browser.
Enable Browser Tab Icon	Click to enable / disable the	browser tab icon for VigorACS WUI.
Browser Tab Icon	DrayTek - It is default setting	<u>,</u>
	Image Upload - Select an ima will be used as the browser t	age by using Browse and upload to VigorACS. It ab icon for VigorACS WUI.
Enable Logo	Click to enable / disable the	logo display on the login window.
Splash Page Logo	DrayTek Red - It is default se	tting.
	Image Upload - Select an ima will be used as the logo disp	age by using Browse and upload to VigorACS. It lay on the login window.
	Components	
Layout	Components Login Method	
	Welcome Message	Dray Tek
	Terms & Conditions Marketing Language Option	
Welcome Message 🔗	Welcomel Please log in to enjoy	English (UK) Welcome! Please log in to enjoy Wi-
		FL.
Terms & Conditions Text 🔗 🛛 🌑	I have read and accept the Terms and Conditions.	Lannet
Content Ø	ir information on the data Draviek collects	
an	d how it is used please see the Draytek vacy Policy.	
	User must tick to get the Internet access	
		I
		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 Would like to receive emails about the latest events, products, and services from you.
		Reject Accept
Splash Page Components	Defines the content of the sp login page.	plash page. Select the one(s) to show on the

	Welcome Message	
	 Terms & Conditions 	
	 Marketing 	
	 Language Option 	
Welcome Message	Enter the text to be displayed a	as the welcome message.
Terms & Conditions Text	lf it is enabled, it will be shown Connect / Submit button on th	on the second page after clicking the e login page.
	Enter the text which will be sho Conditions.	own after the checkbox for Terms and
Content	lf it is enabled, it will be shown Connect / Submit button on th	on the second page after clicking the e login page.
	Enter the text to be displayed i	n the Terms and Conditions window.
Marketing Text	Connect / Submit button on th	on the second page after clicking the e login page. own after the checkbox for marketing
Marketing Content	Connect / Submit button on th	on the second page after clicking the e login page. n the Terms and Conditions window.
Language	Use the drop down menu to se	elect a language.
	Browse - Select a properties fil	e from your host.
	Upload - Click to upload a lang	uage file.
	Download - Click to download	-
	Login Method	
Layout	Components Login Method	
	ear-gradient(to right, #ef5568 5	
	c toma	Dray Tek
Enable Hint Message 🔗 🛛 🚺		05-04-010
<u>_</u> 0	ick to Get Internet Access	t≑ English (UK) Welcome! Please log in to enjoy Wi-
		FL.
		Click to Get Internet Access
		Connect
	#edfd08 \$	
	HEX	
		Cancel Previous Continue
Connect	It is available when Click Throu	gh is selected as Landing Page Method.
		he color of the connect button from the he RGB value (entered with the format of
		e text to be displayed on the connect in be set from the predefined color list or

	Connect Button Color 🔗 e linear-gradient(to right, #ef5568 09
	Connect Button Text 🔗 Connect 5
	Enable Hint Message 🔗
	Click to Get Internet Access
Facebook	It is available when Facebook is selected as Landing Page Method.
	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	Pr	ofile Number Limit: 10
	Leave Info Type Text (Max: 170 characters)	Required	
	General Info 🔹 information		0
	Email		Û
	E Checkbox • Agree		
	Submit Button Color 🔗 🛑 ##13100	5	
	Submit Button Text 🔗	5	
	Enable Hint Message		
	 +Add - Click to add general information, e panel which will be shown on the login pa Submit Button Color - Select the color of t predefined color list, or using the RGB val HEX). Submit Button Text - Enter the text to be a submit form text to be a submit form text text. 	nel as entry b he submit bu ue (entered w displayed on	box or check box. Itton from the vith the format of the submit button.
	The color of the text can be set from the p RGB value (entered with the format of HE		lor list or using the
Enable Hint	Click to enable / disable the hint message		
Message	If enabled, enter a sentence as a hint mes	sage.	
Cancel	Click to Discard current modification.		
Previous	Click to return to the previous page.		
Continue	Click to get into the next page.		

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

RootGroup •					
	Profile 5	Setup S	2 Splash Page Customization (Optional)	3 Whitelist Setup (Optional)	

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

		1 Profile Setup	2 Splash Page Customization (Optional)	3 Whitelist Setup (Optional)	
ype: All	NAT Rules Destination Domain Desti	nation IP Destination Port Source	P Search		+ Add 🛛 🕄 Clear All
Index	Туре	Enable	Content		Action
1	NAT Rules NAT Rules Destination Domain Destination IP Destination Port	\bigcirc		*	Cancel Previous Save

These parameters are explained as follows:

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	~					Dray Tek	VigorACS 3		🔳 Ca	pture Pack	ets Y	System Adm	carrie inistrator	C
lotspot Web l	Portal / Hotspot Pro	ofile												
User Group :	RootGroup	٣												
+Add														
Profile ID	Profile Name	$\downarrow\uparrow$	Enable	$\downarrow \uparrow$	Login Method		41	Applied Interfaces	ψî	Action				
9	NYF_Carrie		Enabled		Click Through			LAN (1) WLAN 2.4G (1) WLAN 5G (1)		🖉 Edit	🗊 Delete	🗅 Сору	l 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.

ray	Tek Vig	prACS 3	U_2921	r_5 (5)	Q	Pcap	14:59:29 mk_carr 8/5/24 System Administrat	
Hotspo	t Web Portal	/ Quota Management	t					С
User G	roup : Root	Group ~						
+Add							Profile Number L	Limit: 2,
	Index 41	Profile Name	↓↑ Expired Time After 1 st Login	$\downarrow\uparrow$ Idle Timeout	↓↑ Bandwidth Limit	↓↑	Session Limit	4
	1	Default	0d 6h 0m	Disabled	Unlimited		Unlimited	
	2	tt_root	6d 6h 6m	Disabled	Unlimited		Unlimited	

These parameters are explained as follows:

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 Manageme	ent	С
User Group : RootGroup		
Add Quota Policy Profile		
Profile Name	0P_1 ~	
Account Validity		
Expired Time After 1 st Login	0 ~ days 6 minutes	
Enable Idle Timeout		
Idle Timeout	0	
Device Control		
Devices Allowed	Unlimited Vaccount	
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 Sa	ive

These parameters are explained as follows:

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 Limit	Click to enable the function of bandwidth 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.

ray Tek VigorACS 3	U_2927_5 (5) V	٩	Pcap	Ċ	15:01:57 8/5/24	mk_carrie System Administrator	Μ
Hotspot Web Portal / Network & Device				Sea	rch Device Nan	ne / Model / MAC	С
Name	Model Name	Hotspot Profile					
⊿ 👬 U_2927_5		As Parent	~				
2927Vac_1449BC22C2C0_104.1	Vigor2927Vac	As Parent	~				
2927Vac_1449BC22C400_103.1	Vigor2927Vac	As Parent	~				
2927Vac_1449BC22C438_101.1	Vigor2927Vac	As Parent	~				
2927Vac_1449BC22C588_106.1	Vigor2927Vac	As Parent	~				
2927Vac_1449BC22C630_102.1	Vigor2927Vac	As Parent	~				

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 PIN Generator

The system administrator can generate multiple PIN codes for various uses. Before generating PIN codes, please make sure a **USB** has been inserted onto your Vigor device.

8.5.4.1 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.

otspot Web Portal / PIN G	enerator										(
cspot web Fortat / Three	increator .																		
ser Group : RootGroup	~																		
IN Generator PIN Status																			
Generate new PIN									Profile	Number Limit:	:0/€								
how 10 ~ entries									Search										
		Create Time ↓↑											Hotspot Profile/ Quota Management			Quantity			
Id ↓↑ Profile Name	↓↑ Create Time		1 Quota	J↑ Expl	red Time after 1 st Login†	Generated 41	Used 4	t Unused ↓↑	Action										
				No data availab	le														
										-44	¢								

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.
+Generate new PIN	Click to generate a new PIN profile.
Delete Expired Profiles automatically	If enabled, the expired profile will be automatically removed at 12:00 AM every night.
	Switch the toggle to enable or disable this function.

Click **Generate new PIN** to create a new profile.

U_2927_5 (5)	~ Q			
+ Generate new PIN				\times
PIN Generator Profile				- Í
Profile Name			×	
PIN Digits	6	~		
Quantity	1	~		
PIN Validity	1 Day	~		
Bind PIN Code to Router	Nothing selected	~		ł
Hotspot Profile	105.169	~		
Quota Management Policy	Default			
Expired Time after 1 st Login	0d 6h 0m			
Device(s) Allowed per PIN	Unlimited			
Speed Limit	Unlimited (Unload) Unlimited (Download)			
		Cancel	Apply	/

ltem	Description						
PIN Generator Profile							
Profile Name	Enter a name for the profile.						
PIN Digits	Specify the length (6/7/8/9) of PIN code.						
Quantity	Set the quantity (1~20) of the PIN code.						
PIN Validity	Set the period of time that the PIN will be kept in the database.						
Bind PIN Code to Router	Select a router (under the selected network group).						
Hotspot Profile	 Select a hotspot profile. If there is no profile to be selected, please open Hotspot Web Portal>>Profile to create a new profile. In which, "ACS3 as Hotspot Server" must be selected as the Hotspot Server Mode. Quota Management Policy - Displays the name of the management policy. Expired Time after 1st Login - Displays the expired time. Device(s) Allowed per PIN - At present, no limitation. Speed Limit - At present, no limitation. 						
Print PIN Code							
Show Quota Policy	Select this item to display the quota policy on the voucher.						
Show PIN Expire Date	Select this item to display the expiration date (according to the date on PIN Validity) of the PIN on the voucher.						

Router Name	Select this item to display the router's name selected on the Bind PIN Code to Router on the voucher.					
Router Note	Select this item to show the brief description for the selected device (also displayed on router's note 1, Network & Service Management>>Network Management) on the voucher.					
Voucher Title	Set the title (up to 30 characters) of the voucher.					
Custom Message	Set a message (up to 50 characters) displayed on the voucher.					
Apply	Click it to generate a PIN code as a voucher.					

Click **Apply** to save the settings. A new profile (in this case, PIN_Carrie) will be shown on the web page.

Hotspo	Iotspot Web Portal / PIN Generator											
User G	roup : RootGroup	~										
PIN Ge	PIN Generator PIN Status											
+Gen	+Generate new PIN Profile Number Limit: 1/600											
Show	10 v entries										Search	
				Hotspot Profile/ Quota Management			QuantIty					
ıd ↓↑	Profile Name 41 C	↓↑ Create Time ↓	Hotspot Profile	↓↑ Quota		Expired Time after 1 st ↓ Login ↑	Generated $\downarrow\uparrow$	Used ↓↑	Unused	¢↑	Action	
1	PIN_Carrie	2024/08/19 09:27:48	105.169	Default		0d 6h 0m	1	0	1		🖨 Print Unused PIN 🛛 📋 Delete	
< Delet	e Expired Profiles auto	matically								_	≪ 1 ≫	

ltem	Description						
Print Unused PIN	Open a page to display the unused PIN number. Print Unused PIN - Google Chrome aboutblank WiFi PASS PIN Code : 458560 Expired Time: 0d 6h 0m Device Allowed: Unlimited Speed Limit: Unlimited (Upload) Unlimited (Download) Session Limit: Unlimited PIN Expired Date: 2024/08/20 09:27:48 Enjoy your WiFi Network						
Delete Delete Expired Profiles automatically	Remove the selected PIN profile. s If enabled, the expired profile will be automatically removed at 12:00 AM every night. Switch the toggle to enable or disable this function.						

8.5.4.2 PIN Status

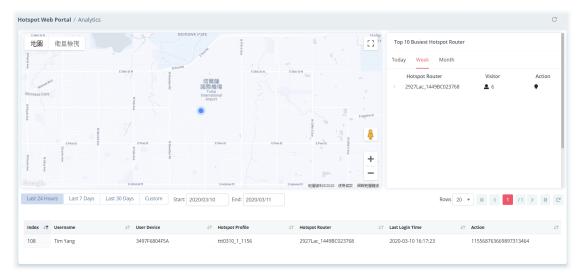
This page displays the PIN codes generated by PIN Generator.

Hotspot Web Portal / PIN Generator					С
User Group : RootGroup ~					
PIN Generator PIN Status					
Status	ALL Used Unused				
Generator Profile	Show All ~				
Hotspot Router	Search Device MAC or Device Name				
Client Device	Search Client MAC				
Show 10 ~ entries				Search	
# PIN Code ¹ Status 4 Generator Profile	utra Profile	↓↑ Create Time	$\downarrow\uparrow$ PIN Expire Date	$\downarrow \uparrow \text{Hotspot Router} \qquad \downarrow \uparrow$	Action
458560 UNUSED PIN_Carrie	Default	2024/08/19 09:27:48	2024/08/20 09:27:48	2927_1449BC13E640	🗊 Revoke
					€ 1 →

ltem	Description					
Status	All – Select to show all the PIN codes on this page.					
	Unused - Select to show unused PIN codes on this page.					
	Used - Select to show used PIN codes on this page.					
Generator Profile	Use the drop down menu to display all the profiles or the selected profile.					
Hotspot Router	Enter the MAC address or the name of the device (hotspot router) to display the PIN status related to the device.					
Client Device	Enter the MAC address of the client to display the PIN status related to the client device.					
Action	Revoke – Remove the selected entry.					

8.5.5 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.

RDS	~	Dray Te
Root Network(241)		Q X
	Model	
80 ·····		AP 910C_001DAA7F5D8C
융 RD6(2)		AP 912C_001DAA72E14A
윩 RD7(15)		AP 918RPD_001DAA3F580C
		AP 920R_001 DAA632C78
器 RD999(3)		BX 2000ac_001DAAD7EC88
옮 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
łł	Load Balance (SD-WAN)				
((())	Route Policy (SD-WAN)				
	VOIP WAN (SD-WAN)				
Z					
12	Device Provisioning				
\$	Name	Model Name	Last Provisioned	Status	AP Profile
	A D 1000C 001DAA04E05C				Y

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 💌
A VigorAP900	VigorAP 900		(As Parent) Root Network-UK-Copy-edit Marketing_carrie
			Refresh Sa

(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.

This page is left blank.



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., Vigor2927 series).

Root	Network (100143)			×						
Netw				c ~						
Netw	Model			0 -						
< F	Root Network > AutoTestNetwor	k								
윪 Au		>								
읆 Au	utoTest_Dev (9)	>								
=	Dray Tek VigorACS 3	2927Lac_144	9BC023768 🗸	٩			Pcap	15:49:29 8/5/24	mk_carrie System Administrator	
10	2927Lac_1449BC023768			D	evice Status: 🥑 Online	Alarms: 2 Activ	ve Clients: 0	Auto Refre	esh: Disable 🗸	C
600	Port Status			WAN Ove	rview				③ Last 24 hou	n-
	ACT WAAG LTE Dray			1.19 MB 976.56 KB 732.42 KB 488.28 KB 244.14 KB	/			M	• Total	
	Device Information				00 18:00 20:00 22:00 ↑4.47 MB ↓25.66 MB)	0 00:00 02:00	04:00 06:00	08:00 10:0		00 %
2	Device Name	2927Lac_1449BC023768		_	(↑4.47 MB ↓25.66 MB)					00 %
R	IP Address	http://192.168.106.140:80			(↑0 Byte ↓0 Byte)			an a	Ĩ	0 %
a	Network Name	AutoTestNetwork		•	(↑0 Byte ↓0 Byte)					0%
_	Model	Vigor2927Lac 🤡		•	(↑0Byte ↓0Byte)					0%
	Firmware Version	4.4.2.3 🤡		•	OByte ↓OByte)					0%
ξĝ}	MAC Address	14:49:BC:02:37:68		•						0%
쓰	Up Time	0 day 12:19:31		4	(↑0 Byte ↓0 Byte)					0 %
í			∽ show more ③ Last 24 hours		Line/Mode	↓† IP		Uptime	↓↑ Active Mode	↓↑
	System Resource		Case 24 Hours	WAN1	Ethernet / Static IP	192.168.106	140	0d 12h 18m	Always On	
	CPU	4 % Memory	81 %	WAN2	Ethernet / DHCP Client			0d 00h 00m	Always On	
	100% 75% 50% 25%	100% 75% 50% 25%		WAN3 WAN4	Wireless_2.4G / Wireless_5G /			0d 00h 00m 0d 00h 00m	Always On Always On	
	0% 16:00 20:00 00:00 04:00 08:00	12:00 16:00 20:00 00:00 04:00 08:	00 12:00	LTE	LTE / DHCP Client			0d 00h 00m	Always On	
	Connectivity and Alarte			WAN6	USB / DHCP Client			0d 00h 00m	Always On	

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.

Dray Tek VigorACS 3		2927Lac_1449BC023	1768	v	Pcap Â	15:50:35 mk_ca 8/5/24 System Administ	
Statistics							С
Last 24 Hours Last 7 Days	Last 30 Days Custom Start: 2	024-06-23 End: 2024-08	3-05			Export	e Ø
Usage Overview			- 2 ×	Wireless Clients Overview		-	2 ×
Total Number of Clients	Wireless Clients 0 (0%)	Wired Clients 1 (100%)					
Total amount of Traffic 130.17 MB	Download 124.87 MB (95.9%)	^{Upload} 5.30 MB (4.1%)		Band	SSID	os	
Max. Number of Concurrent Clier	nts Avg. Number 1	of Daily Client 🕑		■ 2.4G ■ 5G	No Data	Android iOS Wind	ows
Clients			- 2 ×	Traffic		-	2 ×
		OWired OWireless O2.4G	○5G			OWired OWireless O2.4G €	○ 5G
2				5.72 MB			
				4.77 MB			
				3.81 MB 2.86 MB			
1		A A		1.91 MB			
				976.56 KB			
0				0 Byte			
07-01	07-08 07-16	07-24 08-01		07-01	07-08 07-16	07-24 08-01	

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, Vigor2135 series is used as an example).

(7)	Monitoring	
000	Alarm	
	Logs	
494		
E.		

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.

Tek vig	orACS 3		2135Vac	_1449BC03B060	~ a			Pcap	16:02:49 8/5/24	mk_ca System Adminis	
ring / Alarn	ı						2024/07/06	to 2024/08/05 🗸	Search N	o. / Device Nan	ne/MAC 🤇
• His	tory										
te 🖶 Delet	eAll ⊥Dow	nload						И	< 1	/1 >	Ø C
No.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Type		Ack Time	Ack Use
38517757	Not Ack	2024/08/05 05:20:19	2135Vac_1449BC03B060	aaa	14:49:BC:03:B0:60	\Lambda Major	Device Loss Connection	Device Lost	Connection		
	ring / Alarm 1 His te Belete No.	No. Ack Status	ring / Alarm History © Delete All Lownload No. Ack Status Time	ring / Alarm ● History ● Delete All →Download No. AckStatus Time Device Name	ring / Alarm History Biblete All Download No. Ack Status Time Device Name Network Name	ring / Alarm History Biblete All J.Download No. Ack Status Time Device Name Network Name MAC Address	ring / Alarm History Belete All JOwnload No. Ack Status Time Device Name Network Name MAC Address	I EK Vigor ACS 3 2135Vac_14498C038060 Q A ring / Alarm 2024/07/06 Image: Bill Alarm Accord and Alarm Accor	I Ck Vigor ACS 3 2135Vac_1449BC038860 Q Q ring / Alarm 2024/07/06 to 2024/08/05 ~ Image: Mistory 2024/07/06 to 2024/08/05 Image: Mistory 1 Image: Mistory 1	Pick VigorACS 3 215V/2 C49blutsbool C E 8/5/2 ring / Alarm 2024/07/06 to 2024/08/05 Search N Image: Search N Image: Search N Image: Search N Image:	I Col: I Col: <thi col:<="" th=""> I Col: I Col:</thi>

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.
Network Name	Displays the name of the network that the managed device belongs to.
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.

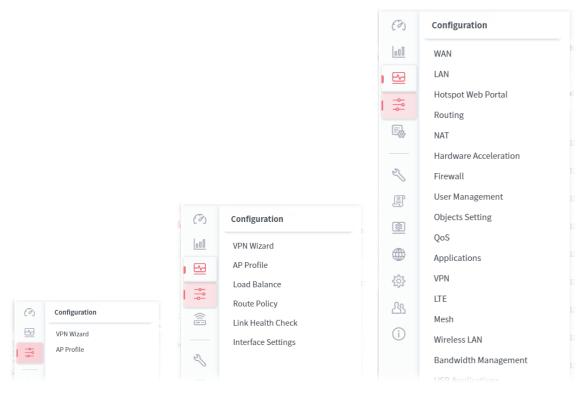
PE Actio	ons Device Re	boot Reboot By CPE	Reset System Password	Set Parameter	File Transfer Setting Profi	e Device SysLog CPE No	tify Device Register	Device Operate
Delete	Delete All	Download						N < 1 /2 > N C @
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
	2968439	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Set Parameter Values	13923	2020/03/06 05:18:11 PM
	2968051	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Set Parameter Values	13788	2020/02/24 05:25:40 PM
	2968049	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Set Parameter Values	13786	2020/02/24 02:42:06 PM
	2968041	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Set Parameter Values	13783	2020/02/24 02:37:23 PM
	2968040	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	42	2020/02/24 02:37:21 PM
0	2968039	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	41	2020/02/24 02:37:20 PM
	2968038	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	40	2020/02/24 02:37:19 PM
	2968037	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	39	2020/02/24 02:37:18 PM
	2968035	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	38	2020/02/24 02:37:16 PM
	2968033	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	37	2020/02/24 02:37:15 PM
	2968031	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	Add Object	36	2020/02/24 02:37:13 PM
	2968029	2865ac_001DAA41DF78	141326	001DAA41DF	78 192.168.105.67	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 / 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 the log as an XLS file.

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.



Root Network

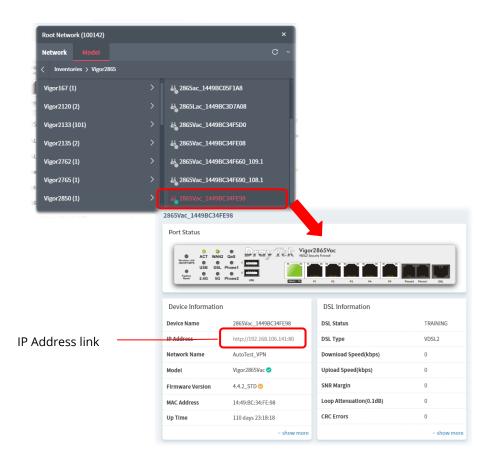
Group Network

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 Vigor2865 (series) as an example.

(7)	Configuration	
000	WAN	b
. 🗠	LAN	
- **	Hotspot Web Portal	d
- ≃	Routing	
E.	NAT	
	Hardware Acceleration	
Z	Firewall	
P	User Management	
-	Objects Setting	
2	QoS	
	Applications	
2022	VPN	
23	LTE	
	Mesh	
(j)	Wireless LAN	
	Bandwidth Management	

(i) 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 A	Access
--------------------	--------

Internet Access	2927Lac	_1449BC	023768 / Configu	ation / WAN						C
Connection Detection	Alarm	Index	Display Name	Physical Mod	Access Mode	status	Bandwidth(Kbps) DownLink/UpLink	Ping Latency	Ping Jitter	Ping Pkt Loss
Multi-VLAN	Enable	WAN1		Ethernet	Static or Dynamic IP	Enable	9/7	8.8 ms	2.9 ms	0%
WAN IPv6	Disable	WAN2		Ethernet	Static or Dynamic IP	Disable	0/0	0 ms	0 ms	0%
WAN Budget	Disable	WAN3				Disable	0/0	0 ms	0 ms	0%
-										0%
·			4G Connection							0%
DHCP Client Option IPv6	Enable	WAN6		USB	3G/4G USB Modem(DHCP mode)	Enable	0/0	0 ms	0 ms	0%
	Load	Balance	Setup							
	Mode				P Based ~					
	Line S	peed			Auto Detect ~					
	Weigh	t Type			Bandwidth-Based ~					
		lata								
			cy, jitter, and packe				page.			
										🔯 Save
	_									_
	Connection Detection Multi-VLAN	Connection Detection Aur Multi-VLAN Enable WAN IP-y6 Disable Disable DHCP Client Option IP-y6 Enable DHCP Client Option IP-y6 Enable DHCP Client Option IP-y6 Load Mode	Connection Detection Multi-VLAN WAI IPVG WAN IPVG WAN Budget DIREP Client Option IPvd DIREP Client Option IPv6 DIREP Client Option IPv6 Load Balance Mode Line Speed Weight Type	Connection Detection Mutri VI.AN Mutri VI.AN WAN IN-K WAN IN-K WAN Budget UPP Client Option IP-4 Disable LTE 4G Connection DIRCP Client Option IP-6 Line Speed Weight Type Node	Connection Detection Atam index Display Name Physical Node Muts VLAN WAN NoC Usable WAN2 Disable WAN2 Disable WAN2 Disable WAN3 Wireless 324 Disable WAN4 Wireless 35 Dis2Die WAN4 Usable USB Dis2Die Usable USB Dis2Die Usable WAN5 USB Dis2Die Usable USB Load Balance Setup Mode I Une Speed Weight Type I	Connection Detection Atom index Display Name Physical Mode Access Mode Multi VLAN Enable WAN IA Ethernet Static or Dynamic IP WAN Rodget Disable WAN 2 Ethernet Static or Dynamic IP Disable WAN 3 Wireless 2.4.6 None Disable WAN 3 Wireless 5.6 None Disable UTE 4.6 Connection USB 36/46 USB Modem(DHCP mode) DHCP Client Option IPv6 Enable WANS USB 36/46 USB Modem(DHCP mode) DHCP Client Option IPv6 Enable WANS USB 36/46 USB Modem(DHCP mode) DHCP Client Option IPv6 Enable WANS USB 36/46 USB Modem(DHCP mode) DHCP Client Option IPv6 Enable WANS USB 36/46 USB Modem(DHCP mode) Une Speed Auto Detect ✓ ✓ Weight Type Bandwidth-Based ✓ IP Resed ✓ ✓	Atam index Display Name Physical Mode Access Hode Status Mathi Yu AN Enable WAN IL Ethernet Status or Dynamic IP Enable Disable WAN Rodget Disable WAN 2 Ethernet Status or Dynamic IP Disable Disable Disable WAN 2 Ethernet Status or Dynamic IP Disable Disable Disable WAN 2 Ethernet Status or Dynamic IP Disable Disable WAN 2 Wireless 2.46 None Disable Disable WAN 2 Use 3.26/4G USE Modem(DHCP mode) Enable DIPCP Client Option IPv6 Enable USB 36/4G USB Modem(DHCP mode) Enable DIPCP Client Option IPv6 Enable WANS USB 36/4G USB Modem(DHCP mode) Enable Line Speed Auto Detect ✓ ✓ Weight Type Bandwidth-Based ✓	Alarm index Disglay Name Physical Mode Access Mode Status Bandwidth/UpUpuk Multi VLAN Enable WAN I Ethernet Status or Dynamic IP Enable 9/7 Multi VLAN Disable WAN I Ethernet Status or Dynamic IP Disable 0/0 WAN IN-6 Disable WAN2 Ethernet Status or Dynamic IP Disable 0/0 WAN Badget Disable WAN2 Ethernet Status or Dynamic IP Disable 0/0 Disable WAN2 Ethernet Status or Dynamic IP Disable 0/0 Disable WAN2 Wireless 2.4G None Disable 0/0 DHCP Client Option IPA Enable UTE 4G Connection USB 3G/4G USB Modem(DHCP mode) Enable 0/0 DHCP Client Option IPA6 Mode VER Auto Detect v V V Weight Type Bandwidth-Based V Bandwidth-Based v V	Kate Display Name Physical Mode Access Mode Status Bandwidth/bips/pi DownLink/upLink Ping Latinov Multis VA N Enable WAN I Ethernet Statu or Dynamic IP Enable 0/0 0 ms WAN Budget Disable WAN 3 Wireless 2.4G None Disable 0/0 0 ms Disable WAN Budget Disable WAN 4 Wireless 2.4G None Disable 0/0 0 ms Disable WAN 4 Wireless 2.4G None Disable 0/0 0 ms Disable WAN 4 Wireless 2.6G None Disable 0/0 0 ms Disable UTE 4G Connection USB 3G/4G USB Modem(DHCP mode) Enable 0/0 0 ms DIPCP Client Option IP/4 Enable UTE 4G Connection USB 3G/4G USB Modem(DHCP mode) Enable 0/0 0 ms DIPCP Client Option IP/4 Enable UTE 4G Connection USB 3G/4G USB Modem(DHCP mode) Enable 0/0 0 ms ULCD Etect	Aum Nor Physical Mode Access Mode Status Bandwidth(bt/pip DownLink/upLink Ping Latency Ping Here Maile WAN Enable WAN Mode Enable 9/7 8.8 ms 2.9 ms WAN Mode Disable WAN 2 Ethernet Static or Dynamic IP Disable 0/0 0 ms 0 ms 0 ms WAN Mode Disable WAN2 Wireless 2.4 G None Disable 0/0 0 ms 0 ms

These parameters are explained as follows:

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.

027Lac_1449BC023768 / Configu	ration / WAN	(
General Setup		
Alarm	Show an alarm message when this WAN Interface disconnects. Alarm option will follow WAN Alarm Setting in Network management. If you change Alarm option on Configuration > WAN, you need to set WAN Alarm again for all enabled WAN interfaces on this CPE.	
Enable		
Display Name		
Physical Mode	Ethernet	
Enable Load Balance		
Active Mode	Always On Failover	
Physical Type(Ethernet)	Auto negotiation V	
Service VLAN Tag Insertion	\bigcirc	
nternet Access		
Access Mode	None PPPoE Static or Dynamic IP	
	PPTP/L2TP	
МТО		
		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 (DSL model only)	Specify the physical mode (Auto, VDSL or ADSL) for the router manually.	
DSL Modem Code (DSL model only)	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.		
Fallover	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.		
	Interne Access		
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.		
	Static IP MTU - Set a number as the Max Transmit Unit for packet. Modem Settings (for ADSL only)		
Multi-PVC channel			
	Modem Settings (for ADSL only) The selections displayed here are determined by the setting page of Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be		
VPI/VCI	Modem Settings (for ADSL only) The selections displayed here are determined by the setting page of Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be chosen.		
Multi-PVC channel VPI/VCI Encapsulating Type Protocol	Modem Settings (for ADSL only) The selections displayed here are determined by the setting page of Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be chosen. Enter the value provided by ISP.		

	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.		
	MTU		
Static IP MTU	It means Max Transmit Unit for packet. The default is 1500.		
Path MTU Discovery	Click to enable the path MTU discovery function for this WAN interface.		
	Path MTU Discovery		
Path MTU to	Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, a 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.		
	πι		
Change the TTL value	Enable/disable the function of changing the TTL value.		
	Keep WAN Connection		
Enable PING to keep alive	Some ISPs will drop connections if there is no traffic within certain periods of time.		
	Switch the toggle to enable/disable this function.		
PING to the IP	If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.		
PING Interval	Enter the interval for the system to execute the PING operation.		
	RIP Protocol		
Enable RIP	Click to enable the RIP function.		
	Bridge Mode		
Enable Bridge Mode	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.		

Enable Full Bridge Mode	Click to make the router work as a bridge modem which is able to forward incoming packets with VLAN tags.		
Bridge Subnet	Make a bridge between the selected LAN subnet and such WAN interface.		
	WAN IP Network Settings		
Connection Type	Static or Dynamic IP (available when Static or Dynamic IP is selected as the Connection Mode)		
	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.		
	• Gateway IP Address – Enter gateway IP address.		
Primary DNS Server / Secondary DNS Server	Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future.		
	WAN IP Alias (Multi-NAT)		
Index	Display the index number of the WAN IP alias.		
Enable	Click to enable the selected WAN IP alias.		
Aux. WAN IP	Display the IP address of the WAN IP alias.		
Cancel	Discard current modification.		
Save	Save the current settings.		

9.4.1.2 Connection Detection

This page displays physical mode and access mode for each WAN interface.

anneellen Debettoon Index Physical Mode uiti VLAN WAN1 Ethernet WAN2 Ethernet WAN3 Wirreless 2.4G AN Budget WAN4 Wirreless 5G	Access Mode Static or Dynamic IP Static or Dynamic IP
WIP6 WAN2 Ethernet WAN3 Wireless 2.4G	
N IPv6 WAN3 Wireless 2.4G	Static or Dynamic IP
WAN3 Wireless 2.4G	
Budget WAN4 Wireless 5G	None
	None
P Client Option IPv4 LTE USB	3G/4G USB Modem(DHCP mode)
P Client Option IPv6 WANG USB	3G/4G USB Modem(DHCP mode)

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.

2927Lac_1449BC023768 / Configuration / W	/AN	C
WAN Connection Detection		
Index	1	
Mode	ARP Detect ~	
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 or Always 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-loss status for each WAN interface, you have to specify the IP transmitting data 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.		

9.4.1.3 Multi-VLAN

This page allows you to configure multiple permanent virtual circuits (PVCs).

Disable Disable Disable Disable
Disable
Dirable
Disable

To modify the setting, move the mouse cursor to any entry and click to open the setting page.

927Lac_1449BC023768 / Configuration /	NAN	C
Enable Channel 7		
WAN Type	Ethernet(WAN1) ~	
General Settings		
VLAN Tag	0	
Service Tag Value	Disable	
Priority	0 ~	
 Note: Tag value must be set between 1- Only one channel can be untagge 	4095 and unique for each channel. d (equal to 0) at a time.	
Open Port-based Bridge Connection for this		
Channel		
 Note: P1 is reserved for NAT use,and can If the port be configured for bridg 	not be configured for bridge mode. e mode, the setting of the port in LAN >> VLAN Configuration will not work.	
		Cancel Save

ltem	Description	
Enable Channel #	Click to enable or disable the channel.	
	General Settings	
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 for this channel	 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.			
(For DSL model only)	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				
Connection Detection	Index	Index Physical Mode Connection Type			
Multi-PVC/VLAN	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 / Configu	ration / WAN		
Basic			
Connection Type	Offline	*	
	Offline		
	PPP TSPC AICCU DHCPv6 Client Static IPv6 6in4 Static Tunnel		Cancel Save
	6rd		

Offline

When Offline is selected, the IPv6 connection will be disabled.

PPP

2865Lac_1449BC0D8F00 / Configuration / WAN		
Basic		
Connection Type	ppp ~	
RIPng Protocol	•	
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_1449BC0D8F00 / Configuration / WAN	
Basic	
Dasic	
Connection Type	NCCU ~
AICCU	
Always On	D
Username	
Password	•
Tunnel Broker	tic.sixos.net
Tunnel ID	
Subnet Prefix	/ 0
WAN Connection Detection	
Mode	Ping Detect ~
Ping1P/Hostname	
T⊤L(1-255,0:Auto)	0
	Cancel Sawe

DHCPv6 Client

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Connection Type	DHCPv6 Client ~
IAID	0
DUID	000300011449bc0d8f01
Authentication Protocol	None v
RIPng Protocol	0
Enable Bridge Mode	0
Enable Firewall	Ø
Bridge Subnet	LANI v
WAN Connection Detection	
Mode	Ping Detect 🗸
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

Static IPv6

5Lac_1449BC0D8F00 / Configuratio	n / WAN		
Basic			
onnection Type	Static IPv6	~	
Static IPv6			
Current IPv6 Address Table			
Index IPv6 Address	Pre	rfix Length Action	
1		+ Add	
1		1 700	
IPv6 Gateway Address	==		
RIPng Protocol	\bigcirc		
Enable Bridge Mode			
Enable Firewall	\bigcirc		
Bridge Subnet	LAN1	~	
VAN Connection Detection			
An connection petection			
Mode	Ping Detect	~	
Ping IP/Hostname			
TTL(1-255.0:Auto)	0		
11L11-200.0:AUT01	1.0		Canc
			Ca

6in4 Static Tunnel

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Durit	
Connection Type	6in4 Static Tunnel 🗸
Remote Endpoint IPv4 Address	IPv4 format (EX: 123.12.1.1)
6in4 IPv6 Address	/ 64
LAN Routed Prefix	/ 64
Tunnel TTL	255
Turinet FL	233
WAN Connection Detection	
Mode	Ping Detect V
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

6rd

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Connection Type	6rd v
6rd	
Mode	Static_6rd ~
IPv4 Border Relay	IPv4 format (5X: 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.
	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.

	Gene	ral Setup Status										
ection 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 Obje
VC/VLAN	WAN1	false	0	MB	false	Monthly	1	00:00	1	0	1	
V6	WAN2	false	0	MB	false	Monthly	1	00:00	1	0	1	
	WAN3	false	0	MB	false	Monthly	1	00:00	1	0	1	
	WAN4	false	0	MB	false	Monthly	1	00:00	1	0	1	
Client Option IPv6	LTE	false	0	ΜВ	false	Monthly	1	00:00	1	0	1	
	WAN6	false	0	MB	false	Monthly	1	00:00	1	0	1	
											_	
		lote: • 1. The budget traf	ffic informatio	n provided h	ere is for reference only, p	lease consult :	our ISP for the actu	al traffic usage and d	harpes.			
					sed, the monitored WAN to							

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.

	_	
Enable		
Quota Limit	0 M ~	
Shutdown WAN Interface		
Notification Object	v	
Cycle Mode	Monthly Custom	
Enable	Use Cycle In hours Use Cycle In days 🗸	
User Defined Cycle Days	1 ~	
User Defined Current Day	1 ~	
User Defined Reset Hours	00:00 ~	
	and Date of the router is configured. be 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_1449BC0D8	2865Lac_1449BC0D8F00 / Configuration / WAN Set to Factory Default					
Internet Access	Enable	Interface	Option	Туре	Data		
	false		0	ASCII			
Connection Detection							
Multi-PVC/VLAN	③ Note: 1 Option 1.7	2, 3, 4, 5, 8, 13, 20, 23, 25, 26 are reserved.					
WAN IPv6				ocol" if you configure option 11 in			
WAN Budget							
DHCP Client Option IPv6							

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 Default	C
Index	1			
Enable				
Interface	WAN1 ~	×		
Option Number	0			
Туре	ASCII Hex Address 🗸			
Data				
🚔 Clear			Cancel Sa	ve

Item	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

9.4.2.1 General Setup

This page provides you the general settings for LAN.

2865_1449BC080090 / Configuration / LAN				C
Index	Status	DHCP	IP Address	
LAN1	Enable	Enable	192.168.1.1	
LAN2	DIsable	Enable	192.168.2.1	
LAN3	DIsable	Enable	192.168.3.1	
LAN4	DIsable	Enable	192.168.4.1	
LAN5	DIsable	Enable	192.168.5.1	
LANG	DIsable	Enable	192.168.6.1	
LAN7	DIsable	Enable	192.168.7.1	
LAN8	DIsable	Enable	192.168.8.1	
DMZ Port	DIsable	Enable	192.168.254.1	
Force router to use "DNS server IP address"	Dtsable	~		
			Si	ave

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.
	1

9.4.2.2 IP Routed Subnet

2865Lac_001DAA1F8090		Dray Tek VigorACS 3	Carrie Capture Packets Carrie System Administrator
General Setup	2865Lac_001DAA1FB090 / Configuratio	n / LAN	Q
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 IPv6	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	Save the current settings.

9.4.2.3 VLAN

VLAN Enable				
Permit untagged device	e in P1 to access router			
Name	Subnet	VLAN Tag Enable	VLAN Tag ID	VLAN Tag Priority
VLAN0	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 🗸

ltem	Description		
	VLAN Configuration		
VLAN Enable	Click to enable / disable the VLAN configuration.		
Permit untagged device P1 to access router	Click to enable / disable the function. 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					
🖻 Delete All					
Index	IP Address	MAC Address	Comment	Action	
1	192.168.1.11	B0-6E-BF-C9-96-DE		🖉 Edit 💼 Delete	
2				+ Add	
ARP Table					
+Add to Bind List					
TAdd to Bind List	IP Address	MAC Address		Host ID	
1	192.168.1.11	B0-6E-BF-C		R1000683	
1	192.100.1.11	B0-6E-BF-C	3-30-DF	KT000683	

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.

false				
		0	ASCII	
Note: I Those options are re	eserved by OS which are not allowed to conf	Igure In this page: Option 1, 2, 3, 4, 5, 6, 8, 11, 13, 20, 23	8-25 and 26	
2.Option 23 could be	configured from DNS server field of LAN >> (
• 3.0puoli 11, 25, 26 to	ulu be configured from DAN >> General Seco	p >> LAN [A] IPV0 Setup >> Difterv0 Setver >> 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.

865Lac_1449BC0D8F00 / Configuration / LAN		Set to Factory Defaul
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
Option Number	server. Enter a DHCP option number (e.g., 100).
Data	Enter the data for this DHCP option based on the data type selected.
Next Server IPAddress/SIAddr	Enter the DHCP next server IP address. It is available for DHCP Server Option IPv4 only.
Cancel	Discard current modification.

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

9.4.2.6 InterLAN Routing

Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1									
LAN 2									
LAN 3									
LAN 4	0		0						
LAN 5	0	0	0	0					
LAN 6	0		0	0	0	8			
LAN 7	0		0	0	0	0			
LAN 8			0	0	0	0	0		
DMZ Port	0	0	0			0	0		8

ltem	Description
LAN1 to DMZ Port	Check the box(es) to let the 2 intersecting LANs can communicate with each other.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.7 LAN IPv6

This page allows to configure IPv6 settings for each LAN.

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.

Deale Cotur					
Basic Setup					
LAN Name		LAN1			
Enable					
WAN Primary Interface		WAN1	~		
Static IPv6					
ULA Config		Off	~		
ULA Config Address					
		Prefix Length: 64			
IPv6 Address Table	Index	IPv6 Address	Prefix Length	Action	
	1	FE80::B9A1:14C0:2AB4:900B	64	🗇 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			
secondary bits					
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
	6
Enable	If enabled, RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

Selected WAN	Additional WANs selected to carry IPv6 traffic.			
Cancel	Discard current modification.			
Save	Save the current settings.			

9.4.2.8 Port Mirror

The LAN Port Mirror function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis.

Bind IP to MAC			
Enable			
MirrorPort	Port3		*
Mirrored Tx Port	Port1	Port2	
	Port3	Port4	
	DMZ	WAN1	
	VAN2		
Mirrored Rx Port	Port1	Port2	
	Port3	Port4	
	DMZ	WAN1	
	2 WAN2		

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.

Enable LAN 802.1X							
Authentication Type	Externa	I RADIUS			r		
802.1X Ports	🗆 P1	🗆 P2	🗆 P3	🗆 P4			
	🗆 P5						
ß Note: 802.1X enabled LAN ports of you need an 802.1X-capable					authenticate multiple devices through a	LAN port	
							Cancel S

Item	Description
Enable LAN 802.1x	Check the box to enable LAN 802.1x function.
Authentication Type	External RADIUS - An external RADIUS server is to be used for 802.1X authentication. 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 w other DNS server on LAN, please make sure t		tek.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.dr	aytek.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				
				c	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 login 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 Server)	 This setting is available when Receive PIN via Mail is selected as the login method. 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</u> <u>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.

Login Method	2 Background	2.1 Login Page Setup	3.2 Login Page Setup	4 Whitelist Setting	S More Options	
Step 2 - Background		Color Background	Image Background			
Drag Tick	2. Logo Ir	ir Tab Title nage & Logo Background Color Aethods Background Color				
Browser Table Title		Draytek Hotspot				
Logo Image		Default Draytek Logo V				
Logo Background Color		Vigor Red	•			
Login Method Background Color		Vigor Grey	v			
					Cancel Previous Save and	Next

Item	Description
Choose Login	Select either Color Background or Image Background as the login page

Background	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	2 Background	3.1 Login Page Setup	3.2 Login Page Setup	4 Whitelist Setting	S More Options	
Step 3.1 - Login Page Set	qu					
Configure Login Method and D	etails					
R						
Welcome Message		Welcomel Please	log in to enjoy Wi-Fi.			
Privacy Policy & Terms and Co Terms and Conditions	nditions	Default				
		🗹 User must tick to ge	r the internet arress			
Description		By clicking the button t Terms and Conditions.				
		Default	le.			
Content		Internal Content	External Content			
		(Max 1360 characters)				
Data Collection for Marketin	ng	\bigcirc	li			
		User must tick to ge				
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 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 (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	Enter the text to be displayed on the Facebook login button.

Description	
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

Login Method	Background	31 Login Page Setup	3.2 Login Page Setup	Whitelist Setting	
	Background		Login Page Setup	whitelist setting	More Options
Step 3.2 - Login Page Setup					
onfigure Login Method and Details					
	7				
	Back Button				
< Back					
PIN Code will be sent over via SMS.	PIN Code Mess	age			
	D.C. HO.	5			
+ 886 enter your mobile number	Default Country	, Enter Mobile Number Do	escription		
Send PIN	Send Button De	scription and Color			
	Send Succeede	d Message			
Enter PIN Submit	Enter PIN and S	ubmit Button			
End Fin			_		
Back Button Description		Back			
		Default	- Ab		
		Default	h		
PIN Code Message			//		
PIN Code Message		PIN code will be sent ov	//		
PIN Code Message		PIN code will be sent or	// ver via SMS.		
PIN Code Message			# ver via SMS.		
-		PIN code will be sent ov Default	Æ		
PIN Code Message Default Country Code		PIN code will be sent or	/er via SMS.		
-		PIN code will be sent ov Default			

The parameters are explained as follows:

ltem	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.

Login Method Step 4 - Whitelist Setting	2 Background	23 Login Page Setup	32 Login Page Setup	4 Whitelist Setting	5 More Options
NAT Rules Dest Domain Always allow outbound conn	Dest IP Dest Port	Source IP NAT >> Port Redirection NAT >> Open Ports NAT >> DMZ	1		
					Cancel Previous Save and Next

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

Login Method	Background	Login Page Setup	Login	Page Setup Wi	hitelist Setting M	ore Options
Step 5 - More Options						
Quota 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
	a settings, please go to Hotspot W	feb Portal ≫ <u>Quota Manag</u>	<u>ement</u>			
To modify the quote	a settings, please go to Hotspot W	feb Portal >> <u>Quota Manag</u>	<u>emens</u>			
To modify the quote Veb Portal Options HTTPS Redirection Note: When an unauthent	a settings, please go to Hotspor W stated client opening a HTTPS pa to redirect only HTTP pages. HT	ge, redirect will work but o	ertificate errors may	be shown. nd also no certificate errors.		
To modify the quote Veb Portal Options HTTPS Redirection Note: When an unauthent	ticated client opening a HTTPS pa	ge, redirect will work but o	ertificate errors may	be shown. nd also no certificate errors.		
To modify the quot Arrow and the second se	ticated client opening a HTTPS pa nto redirect only HTTP pages. HT inticated client to automatically p available when using Social Login	ge, redirect will work but o 1P5 browsing will timeout v 0 00 up the Web Portal page	ertificate errors may without redirection a when connects to V	nd also no certificate errors. h-fi.	bulls in Captive Portal Detection.	
To modify the quot Veb Portal Options HTTPS Redirection Note: Otsable this function Captive Portal Detection Note: Trigger the unauther	ticated client opening a HTTPS pa nto redirect only HTTP pages. HT inticated client to automatically p available when using Social Login	ge, redirect will work but o 1P5 browsing will timeout v 0 00 up the Web Portal page	ertificate errors may without redirection a when connects to V	nd also no certificate errors. h-fi.	built in Captive Portal Detection.	

ltem	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	Facebool	c.	Google	
	PIncode	Click		RADIUS	
					Apply
				Auto Refresh (per	
See Table Avtive User - 0 Online Users / 0 All Users Index 하 Status 하 Profile 하 User	· ↓↑ Login Method	47 IP 47 MAC 47 Er	nail ↓↑ Phone N		min): off ~
Avtive User > 0 Online Users / 0 All Users		نث اله باث MAC باث Er مُنْهُمُ	nail 🖓 Phone N		min): off ~

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.

Justication Include database Enable database Enable database recovery Image: Include database recove	55ac_001DAA41DF78 / Configuration	/ Hotspot Web Portal	Ø
Enable automatic database recovery Enable automatic database every I I I Nours I I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Iser Info Database Setup		
Backup database every 1 nour 0 min Enable sending user information to syslog File Path No USB Disk Detected Database Usage NiA Clear User Info Notification Notification Notification Notification Notification Notification Notific	Enable database		
min Enable sending user information to syslog File Path No USB Disk Detected Database Usage N/A Clear User Info Notification and Action when Storage Exceeded Notification Notification Don't send notification Action Stop recording user information Advanced options Database Encryption On the ensistic and the process. Once enable Database Encryption, roater will create a new encrypted Ontabase encryption is a irreversible process. Once enable Database Encryption, roater will create a new encrypted Action on table to change back to non-encrypted	Enable automatic database recovery		
syslog File Path No USB Disk Detected Database Usage N/A Clear User Info Clear	Backup database every		
File Path No USB Disk Detected Database Usage N/A Clear User Info otification and Action when Storage Exceeded Notification Don't send notification Action Don't send notification Action Stop recording user information dvanced options	Enable sending user information to		
Database Usage N/A Database Usage N/A Iotification and Action when Storage Exceeded Notification Don't send notification Action Don't send notification dvanced options Database Encryption ① I Note: • Database Encrypting is a irreversible process. Once enable Database Encryption, router will create a new encrypted database, which will not content the data from the non-encrypted database, and not able to change back to non-encrypted.	syslog		
Clear User Info Intification and Action when Storage Exceeded Notification Don't send notification Action Stop recording user information dvanced options	File Path	No USB Disk Detected	
Notification and Action when Storage Exceeded Notification Don't send notification Action Stop recording user information dvanced options	Database Usage	N/A	
Action Stop recording user information Action Control of a Note: Control of a Note:	Notification and Action when Storage E		
dvanced options Database Encryption	Notification	Don't send notification	
Database Encryption O ß Note: • Database encrypting is a irreversible process. Once enable Database Encryption, router will create a new encrypted database, which will not contert the data from the non-encrypted database, and not able to change back to non-encrypted.	Action	Stop recording user information	
6 Note: Database encrypting is a irreversible process. Once enable Database Encryption, router will create a new encrypted database, which will not content the data from the non-encrypted database, and not able to change back to non-encrypted. 	dvanced options		
 Database encrypting is a irreversible process. Once enable Database Encryption, router will create a new encrypted database, which will not content the data from the non-encrypted database, and not able to change back to non-encrypted. 	Database Encryption	D	
	 Database encrypting is a irreve database, which will not conter 	nt the data from the non-encrypted database, and not able to change back to non-encrypted.	

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.

able Bandwidth Limit					
able Session Limit	D				
a Policy Profile					
Add 📋 Delete			Profile Num	iber Limit: 20	0
Index Name Ex	pired Time After First Login	Device Allowed Per Account	Reconnection Time Restriction	Bandwidth	h

ltem	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.

+Add 🗊 Delete Profile Number Lin						
	Index	Name	Expired Time After First Login	Device Allowed Per Account	Reconnection Time Restriction	Bandy
	1	Default	0d 6h 0m	Unlimited	Unlimited	Unlim
2	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 / He	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	\odot	
Idle Timeout	0	
Device Control		
Devices Allowed per account	Unlimited •	
Enable Reconnection Time Restriction	\odot	
Time Restriction	Set Time Set period	
	0 • hours 0 • mins	
	Block the same user from reconnecting for the set period	
Bandwidth and Session Limit		
Enable Bandwidth Limit	\odot	
Download Limit	0 Kbps 🔻	
	Cancel	ave

Item	Description					
Index	Display the index number of the profile.					
Profile Name	Enter a name for a new profile.					
	Account Validity					
Expired Time After 1st Login	Sets the days, hours, and minutes. After the login has expired, Vigor router will block the client from accessing the network/Internet.					

Enable Idle Timeout	If enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.				
Idle Timeout	Enter a time value (unit: minutes).				
	Device Control				
Devices Allowed per account	Select the maximum number of devices that can be connected to the network using the same account.				
Enable Reconnection Time Restriction	Click to enable / disable the function.				
Time Restriction	Blocks the account from being used to connect devices to the network in one of two ways:				
	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.

Profile Setup			/ Cor	nfigurat	ion / H	lotspot Web Port	al			
Users Information	PIN Status		enerator < T	/0 >	D					
Quota Management 7IN Generator	PIN P	rofile	Status	Batch	Name	Valid Through	Quota Policy	Activated On	Expiry Time	Action
						No data av	ailable			

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 P	PIN Generator	
Profile		•
Batch Nam	ne	
PIN code le	ength	•
PIN Validit	ty Days	0 *
PIN Validit	ty Hours	0 *
		The period of time the PIN will be kept in the database.
Quantity		0
Quota Mar	nagement Policy	•

Item	Description
Profile	Use the drop down menu to specify an index number (from 1 to 4).
Batch Name	Enter a string as a batch name.
PIN code length	Specify the length of PIN code.
PIN Validity Days	Set the days for the period of validity.
PIN Validity Hours	Set the hours for the period of validity.
Quantity	Set the quantity of the PIN code.
Quota Management Policy	Use the drop down list to choose policy profile.
Generate	Click to generate a PIN code as a voucher.

9.4.4 Routing

9.4.4.1 Load Balance/Policy Route

This page lists the configured policies coming from Vigor CPE.

							System Administrator
2865ac_0	01DAA0000	00 / Configuration / Routing	1				Ø
Delet	e						
	Index	Enable	Comment	Protocol	Interface	Src IP	Dest IP
۲	1	Disable	cnn	Any	WAN1	Any	Domain Name
0	2	Enable	SIP	Any	VoIP_WAN	Any	VoIP
0	з	Disable		Any	WAN1	Any	Any
L							

Item	Description
Delete	Click to remove the selected routing policy.
Index	Displays the index number of the routing policy.
Enable	Displays the status (enable / disable) of the routing policy.
Comment	Displays the description for the routing policy.
Protocol	Displays the protocol used for this policy.

Interface	Displays the interface to send packets to once the policy is matched.
Src IP	Displays the mode for the source IP.
Dest IP	Displays the mode for the destination IP.

To configure the policy, move the mouse cursor to any entry and click to open the setting page.

2865Lac_1449BC0D8F00 / Configuration / Routi	ng	C
Index	1	
Enable	\bigcirc	
Comment		
Criteria		
Protocol	Any ~	
Source IP	Any ~	
Destination IP	Any ~	
Destination Port	Any ~	
Send via if Criteria Matched		
Interface	WAN1 ~	
Gateway IP	Default Gateway ~	
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
5	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

To configure the profile, move the mouse cursor to any entry and click to open the setting page.

865ac_001DAA000000 / Configurat	on / Routing	Ç
Static Route IPv4		
Index	2	
Enable	\bigcirc	
Destination IP Address	0.0.0	
Subnet Mask	0.0.0	
Gateway IP Address	0.0.0	
Network Interface	LAN1 •	
🗓 Clear		Cancel Save

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	Dtsable
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 / Ro	uting	S
Static Route IPv6		
Index	1	
Enable	0	
Destination IPv6 Address		
Prefix Len	0	
Gateway IPv6 Address		
Network Interface	LAN1 v	
🗓 Clear		Cancel Save

Item	Description
Index	Displays the index number of the static route policy.
Enable	Click to enable or disable the static route policy.
Destination IPv6 Address / Prefix Len	Enter the IP address with the prefix length for this entry.
Gateway IPv6 Address	Enter the gateway address for this entry.
Network Interface	Specify an interface for this static route.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.4.4 BGP

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

2865ac_001DAA000000 ~			DrayTek VigorAC	5 3		Capture Packets 👻	carrie System Administrator
Load Balance/Policy Route	2865ac_001DAA000000 / Cor	figuration / Rout	ing				Q
Static Route IPv4	Basic Settings						
Static Route IPv6	Enable Local BGP	(D				
BCP	Local AS Number		(1~4294967295)				
	Hold Time		180				
	Connect Retry Time		120				
	Router ID		192.168.1.1				
	+ 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 Addres	5		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.		

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:

Item	Description	
Basic SettingsIndex - 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	ling	Q
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.	
CancelDiscard current modification and return to previous page.		
SaveSave 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_001DAA000000 ~				Dray	Tek Vige	orACS 3			Capture Pad	kets × Sy	stem Ádmir	carrie nistrator	C
Port Redirection	2865ac_0	01DAA00	0000 / Configuration /	NAT								:	S
DMZ Host										÷,) Set to Fac	tory Default	t -
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	e e
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	0
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 (IX:123.12.1.1)
Private Port	0
ි Note: In "Range" Mode the End IP will be calcul	ated 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	Capture Packets 👻	carrie System Administrator
Port Redirection	2865ac_001DAA000000	/ Configuration / NAT		S
	Index	Profile Name		
Open Ports	1	WAN1		
Port Triggering	2	WAN2		
ALG	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.

5ac_001DAA4	11DF78 / Configuration	1 / NAT				
AT DMZ Host						
Interface		WAN1				
Index	WAN Type	Mode	Enable	Private IP	WAN IP	
1	0	None	false	0.0.0.0		
						Cancel Sav

2. Click the index number of the profile to open the settings page.

/ Configuration / NAT		Ø
NAT DMZ Host Setup		
Interface	WAN1	
Mode	Private IP 💌	
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							Ø
DMZ Host									ら Set to Factory Defa	ault
Open Ports	Index	Enable Open Ports	Comment	WAN Interface	WAN IP	Local IP Address	Source IP	Open Ports Factory Defau	lt Source IP Typ	e
Port Triggering	1	false		WAN1	WAN1_IP_Alias[1]	0.0.0.0	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		
	1		
Enable	\bigcirc		
Comment			
WAN Interface	WAN1	×	
Source IP	Any IP	Object IP Group	
Local IP Address	0.0.0.0		
pen Port List			
Index Proto	col	Start Port	End Port
		0	0
2			
2			
		0	0
4		0	0
4 5		0 0 0	0 0 0
3 4 5 6 7		0 0 0	0 0 0
4 5 6 7		0 0 0 0	0 0 0 0
4 5 6		0 0 0	0 0 0

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 / Configura	tion / NAT						Ø
									Set to Factory Def	ault
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.

	\bigcirc
rvice	User Defined ~
omment	
ource IP	Any IP Object IP Group
iggering Protocol	~
iggering Port	
coming Protocol	· ·
coming Port	
 Note: The legal format of Triggering Port and 123 123,456 	Incoming Port should like this:
123,456,789 123-456,789 123-456,777-789	

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 / C	onfiguration / NAT				Set to Factory Default	C
Port Redirection	ALG (Application Lay	yer Gateway)					
DMZ Host	Enable	0					
Open Ports	Enable	0					
Port Triggering							
ALG	Index	Enable	Protocol	Listen Port	TCP	UDP	
	1	false	SIP	5060	true	true	
	2	false	RTSP	554	true	true	
							_

To configure the ALG profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA41DF78 / Config	uration / NAT	R
Enable		
Protocol	SIP	
Listen Port	5060	
тср		
UDP		
		Cancel Save

Item	Description
Enable	Click to enable / disable the ALG profile.
Protocol	Displays the type (SIP, RTSP) of ALG.
Listen Port	Enter a port number for SIP or RTSP protocol.
TCP/UDP	Click to enable/disable the TCP/UDP. If enabled, it will make correspond protocol message packet from TCP/UDP transmit and receive via NAT.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.6 Hardware Acceleration

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself.

← 2865ac_001DAA000000 / Configuration	n / Hardware Acceleration	C
Acceleration	Disable Enable	
NAT		
Protocol	TCP 🗌 UDP	
IPsec		
Protocol	TCP 🗌 UDP	
		Cancel Save

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.

Filter Setup		
Data Filter		
Data Filter Set Start	Set#2 *	
nbound Policy		
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		
 Bote: Packets are filtered by firewall function 1. Data Filter Sets and Rules. 2. Block routing connections initiated 3. Default Rule. 		

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	Click to enable / disable the function.
Firewall	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
ion 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
Codepage	Selecting the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed.
Window Size	Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535.
Session Timeout	Sets the timeout sessions are allowed to idle before they are removed from the system.
Save	Save the current settings.

9.4.7.3 Filter Rules

This page displays the filter rule profile and allows to create new filter rule profile(s).

+Add	d 🖄 Delete			
	Set	Comments	Next Filter Set	
	1		None	
0	2	Default Data Filter	None	

These parameters are explained as follows:

Item	Description	
+Add	Click to add a new filter rule set.	
Delete	Click to remove the selected filter rule.	
Set	Displays the number of filter set.	
Comments	Displays the comment of the filter rule.	
Next Filter Set	Displays the name of next filter set. None means no filter set is specified for current filter set.	

To configure the filter rule set profile, move the mouse cursor to any entry and click to open the setting page. Or, click **+Add** to create a new filter rule profile.

	c		1				
Com	ments		Default Data Filter				
Next	Filter Set		None	~			
Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action
1		xNetBios -> DNS	LAN/RT/DMZ/VPN->WAN	Any	Any	TCP/UDP	Block Immediately
2		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
3							

These parameters are explained as follows:

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

65Lac_1449BC0D8F00 / Configuration	/ Firewall	C
DoS Defense		
DoS Defense	\bigcirc	
	White/Black List Option	
DoS defense Log	Enable ~	
Flood Defense		
SYN Flood Defense	\bigcirc	
SYN Flood Threshold (pkts/sec)	2000	
Session Time-Out (sec.)	10	
UDP Flood Defense		
UDP Flood Threshold (pkts/sec)	5000	
Session Time-Out (sec.) ICMP Flood Defense		
ICMP Flood Detense	250	
Session Time-Out (sec.)	10	
Port Scan Detection		
		Cancel 🕋 Clear All Save

ltem	Description
	DoS Defense
DoS Defense Click to enable / disable the DoS Defense.	
White/Black List Options	Click to set white or black list.

	2005.cc_100920001790 / Configuration / Trevail C Proof y Windue free Leg Nore Legitorroule E
	Norm Norm Norm 1 6464 2 6464 3 6464 4 6464 3 6464 3 6464 3 6464 3 6464 3 6464 3 6464 3 6464 3 6464 3 6464 4 6464 5 6464 6 6464 6 6464 6 6464 6 6464 6 6464 6 6464 6 6464 7 6464 6 6464 6 6464 6 6464 7 6464 7 6464 7 6464 7 6464 7 6464 7 6464 <td< th=""></td<>
	9 0.00 10 0.00 11 0.00 12 0.00 13 0.00 14 0.00 15 0.00 14 0.00
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.

65Lac_1449BC0D8F00 / Configuration / Firewall			Set to Factory Default
Index	1		
Profile Name			
Instant Message	AIM Login	Aliww	Ares
Select All Clear All	🔲 BaiduHi	E Facebook/Instagram	Fetion
	🗌 GaduGadu Protocol	CQ ICQ	□ iSpQ
	🗆 КС	LINE	LinkedIn
	Paltalk	PocoCall	Qnext
	Signal	Slack	Snapchat
	Telegram	Tencent QQ	
	WebIM URLs	□ WhatsApp	UWhatsApp Call
VoIP	RC Voice	Skype/Teams	TeamSpeak
Select All Clear All	TelTel	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	□ НТТР
	IBM Informix	IRM DR2	
			Cancel Sav

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_0	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	0	1		false	Pass	false	Pass
Web Content Filter	Adn	ninistration Message		- <center> The requires</center>			
DNS Filter				p>Please contact your syste	em		
Diagnose			admin	istrator for further information	n.		
							り 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.

2865ac_001DAA41DF78	/ Configuration / Fire	wall Set to Fac	tory Default	Ø
URL Content Filter Pro	ofile			
Index		1		
Profile Name				
Priority		Either: URL Access Control First		
Log		Block		
URL Access Control				
URL Access Control	I	\bigcirc		
Prevent web access	s from IP address	D		
Action		Pass Block		
Index	Keyword Object	Action		
1	None	▼ + Add		
Index	Keyword Group	Action		
1	None	▼ +Add		
Exception List				
		Ca	ncel Save	
em		escription		

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 Table	Index - Displays the index number of keyword object profile.		
	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	It 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, Upload	Click to enable or disable cookie function.		
	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.		
Save	Save the current settings and return to previous page.		

9.4.7.7 Web Content Filter

Users can also be prevented from browsing certain types of websites by using the Web Content Filter. This filter classifies website domain names into different categories, which can be selectively blocked.

General Setup	2865ac_001DAA41DF78 / Configu	2865ac_001DAA41DF78 / Configuration / Firewall Set to Factory Default 3			
Default Rule		Web Content Filter License Not Activated			
Filter Rules	+Add 🗇 Delete	+Add Delete			
DoS Defense	Index	Profile Name	Log	Action	Black/White List:Action
APP Enforcement	0 1	Default	Block	Block	Block
URL Content Filter					
Web Content Filter					
DNS Filter	Cache	L1+L2 Cache	Ψ.		
Diagnose	Administration Message	 <body-<center> requested Web page SCL54 SCL54 SCL54 SCL54 SCL54 SCL54 SCL54 Legend: </body-<center>	It's crategorized with ocked by %RNAME% p; %DIP% - Destination		
					り Default Message Save

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	The message to be displayed in the browser when access to a website has

Message	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	Ø
Web Content Filter Profil	e				
Index	2				
Profile Name					
Syslog	Block	•			
Action	Pass Block				
White/Black List					
Black/White List	\bigcirc				
Action	Pass Block				
Index	Keyword Object	Acti	ion		
1	None	• +	Add		
Index	Keyword Group	Act	ion		
1	None	• +	Add		
Category Selection		 Criminal Activity 			
				Cancel Save	

ltem	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 Table	 Index - Displays the index number of keyword object profile. 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 / Configuration / Firewall Set to Factory Defau				Set to Factory Default 🛛 🔿
General Setup	+ Add 🗎 Delete				
Default Rule	Index	Profile Name	DNS Syslog	DNS WCF	DNS UCF
Filter Rules	□ 1		Block	None	None
DoS Defense					
APP Enforcement	DNS Filter Local Setting				
URL Content Filter	DNS Filter	\bigcirc			
Web Content Filter	Syslog	None	~		
DNS Filter	WCF	None	~		
Diagnose					
	UCF	None	~		
	Administration Message	Web page brocked by %RNAM	brbrpr-The requested %5/PM-6-br-to %URL% with %CL%-br-has been %0NS Filter,-p-Please administrator for 6 who		
					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	The message to be displayed in the browser when access to a website has			

Message	been blocked. A custom message can be entered with HTML formatting in the text box.
Default Message	Click to reset the administration message to the factory default.
Save	Save the current settings.

To create a new DNS profile, click **+Add** to open the following page.

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 Diagnos	e					
Default Rule							
Filter Rules	Mode		UDP	~			
DoS Defense	Direction		From LAN	~			
APP Enforcement	IP Ver		IPv4	~			
URL Content Filter	LAN IP		192.168.1.12				
Web Content Filter	LAN Port		0				
DNS Filter	LAN MAC		00:00:00:00:00:00				
Diagnose	WAN IP		0.0.0.0				
	WAN Port		0				
						_	
					Analyze Reset Sav	e	
	① Note:						
	Please set	"Mode" and save first before mod					
						_	
	Packet & Payload	1					
	Index	Enable	Direction	Payload Type	Payload Data	TCP Flag	
	1	Enable	AtoB	CUSTOMIZE			
	2	Disable	AtoB	CUSTOMIZE			
	① Note:This is firew	all live test which need setup WAI	N and plug cable In.				

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.

2865ac_001DAA41DF78 / Configura	ation / Firewall Diagnose		Q
Packet & Payload			
Packet	1		
Enable	Enable Disable	~	
Direction	AtoB BtoA	~	
Payload Type		*	
			Cancel Save
Note: • This is firewall live test which nee			

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 Schup User Profile User Group	Mode Selection	Rule-Based User-Based	
	Authentication page Web Authentication	нттр нттру	
	Display IP Enable O Display IP address on the dialog, box pops up at	Logn Page Greeting	
	Landing page	+body stats=1>-script language="javascript">	
		window.location="http://www.draytek.com"t>=/body>	
			Cancel Save

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.
Save	Save the current settings.

9.4.8.2 User Profile

This page allows you to create up to 200 user profiles for use with User Management.

In 1	Enable This Account	User Name	Password	Idle Theorem						
1				Idle Ilmeout	Max User Login	External Server Authentication	Log	Pop Browser Tracking Window	Authentication:Web	A
	true	admin		0	0	None	None	false	true	t
2	true	Dial-In User		0	0	None	None	false	true	f
	true	999		10	0	None	None	true	true	ti
4	false			10	0	None	None	true	true	t

To configure the user management profile, move the mouse cursor to any entry and click to open the setting page.

	2865Lac_1449BC0D8F00 / Configuration / User	Management	C
General Setup User Profile	General Settings		
User Group	Index	1	
	Enable This Account		
	Username	admin	
	Password	٥	
	Log	None	
	External Server Authentication	None ~	
	Login Settings		
	Idle Timeout	0	
	Max User Login	0	
	Authentication:Web	C	
	Authentication:Alert Tool		
	Authentication:Telnet	0	
	Landing Page	\bigcirc	
	Auto Logout(minutes)	0	
		Cancel	e

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 Server Authentication	The router will authenticate dial-in users using either a built-in (None) or external service (LDAP, Radius or TACACS+).
	Login Settings
Idle Timeout	If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will need to re-authenticate before Internet access is once again allowed.
Max User Login	Enter the maximum number of concurrent logins allowed for this profile.
Authentication:Web	Click to enable or disable the function. If enabled, user will need to authenticate by entering a username and password when attempting to access an external website for the first time. The user will be redirected to the external website after a successful authentication.
Authentication:Alert Tool	Click to enable or disable the function. If enabled, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed.
Authentication:Telnet	Click to enable or disable the function. 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 Tracking	Click to enable or disable the function.
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 Services
Internal RADIUS	Click to enable or disable the function.
Local 802.1x	Click to enable or disable the function.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.8.3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in **Firewall>>General Setup**.

General Setup	2865ac_001DAA151EB	8 / Configuration / UserManag	ement	C
User Profile	Index	Name	Selected User Objects	
	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	S
User Group		
Name		
Selected User Objects		
會 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.

	2865ac_001D4	2865ac_001DAA151EB8 / Configuration / 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: Exclamation mark (I) on Information column means that Invert Selection is enabled. 									

To configure the IP object profile, move the mouse cursor to any entry and click to open the setting page.

55ac_001DAA000000 / Configura	ation / Objects Setting		Set to Factory Default
Index	1		
Name	RD Department		
Interface	Апу	V	
Address Type	Range Address	\checkmark	
Start IP Address	192.168.1.9		
End IP Address	192.168.1.9		
Invert Selection			
			Cancel

These parameters are explained as follows:

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.

đ	2865ac_001D	AA151EB8 / Configura	ation / Objects Setting		
	Index	Name	Interface	Selected IP Objects	
	1		Any		
	2		Any		
	3		Any		
	4		Any		
	5		Any		
	6		Any		
	7		Any		
Service Object	8		Any		
	9		Any		
cation Object	10		Any		
	11		Any		
try Object	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	n / Objects Setting		S
Index	1		
Name			
Interface	Any		
Selected IP Objects			
		Ca	incel Save

These parameters are explained as follows:

Item	Description
Index	Displays the index number of the IP object profile.
Name	Enter the name of the IP object profile.
Interface	Select WAN, LAN or Any to filter IP objects.
Selected IP Objects	Use the drop down menu to select the IP object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.3 IPv6 Object

Up to 64 IPv6 Objects can be created.

2865ac_001D	AA151EB8 / Configu	ration / Objects Setting			
Index	Name	Address Type	Information	Match Type	Prefix Le
1		Subnet Address			0
2		Subnet Address	11 11		0
3		Subnet Address	:		0
4		Subnet Address			0
5		Subnet Address			0
6		Subnet Address	:		0
7		Subnet Address	:		0
8		Subnet Address	:	-	0
9		Subnet Address	:	-	0
10		Subnet Address	:		0
11		Subnet Address	:		0
12		Subnet Address	:		0
13		Subnet Address			0
14		Subnet Address	:		0
15		Subnet Address	:		0
16		Subnet Address	:		0

To configure the IPv6 object profile, move the mouse cursor to any entry and click to open the setting page.

5ac_001DAA000000 / Configuration / Obj	ects Setting	Set to Factory Default
ıdex	1	
lame		
ddress Type	Subnet Address V	
tart IP Address	::	
refix Length	0	
vert Selection		
		Cancel

ltem	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.

IP Object	2865ac_0010	AA151EB8 / Configuration	/ Objects Setting	Q
IP Group	Index	Name	Selected IPv6 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			
	13			
	14			
	16			
	10			

To configure the IPv6 group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration / Objects Setting			
Index	1		
Name			
Selected IPv6 Objects			
	Cancel	Save	
	Carcei	Save	

ltem		escription	
------	--	------------	--

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.

IP Object	2865ac_001	DAA151EB8 / C	onfiguration / Ob	ojects Setting			S
	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	1 A A A A A A A A A A A A A A A A A A A	0	
	5		Any	0		0	
	6		Any	0	=	0	
	7		Any	0	-	0	
	8		Any	0		0	
Mail Service Object	9		Any	0		0	
Notification Object	10		Any	0	=	0	
String Object	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 / Configuration /	Objects Setting	S
Index	1	
Name		
Protocol	Any 👻	
	Any ICMP IGMP TCP UDP TCP/UDP ICM/V6 Other	Cancel Save

Item	Description
Index	Displays the index number of the service type object profile.
Name	Enter the name of the service type object profile.
Protocol	Choose a protocol to which this profile applies.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

Multiple Service Type Objects can be placed into a Service Type Group.

IP Object	2865ac_001DAA1	51EB8 / Configuration / Objects Setting		C
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	11			
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 / Objects Setting		
Index	1	
Name		
Selected Service Type Objects		
	Cancel	Save

These parameters are explained as follows:

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 /	Configuration / Objects Setting		
	Index	Name	Contents	
	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
al Service Object	9			
stification Object	10			
ring Object	11			
suntry Object	12			
	13			
	14			
	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			S
Index	1		
Name			
Contents			
			Cancel Save

These parameters are explained as follows:

Item	Description			
Index	Displays the index number of the keyword object profile.			
Name	Enter the name of the keyword object profile.			
Contents	Enter the keywords to be matched. Up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered.			
Cancel	Discard current modification and return to previous page.			
Save	Save the current settings and return to previous page.			

9.4.9.8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

Object	2865ac_001DA	A151EB8 / Configuration	/ Objects Setting	
	Index	Name	Selected Keyword 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 keyword group profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA151EB8 / Configuration / Objects Setting			C2
Index	1		
Name			
Selected Keyword Objects			
			Cancel Save

These parameters are explained as follows:

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 / Co	onfiguration / Objects Setting	Ç
IP Group	Index	Profile Name	
IPv6 Object	1		
IPv6 Group	2		
Service Type Object	3		
	4		
Keyword Object	5		
	6		
	7		
SMS Service Object	8		
Mail Service Object	0		
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	bcts Setting	Set to Factory Default	C
File Extension Object Setup			
Index	1		
Profile Name			
Categories			
Index	Categary Name		
1	Image		
2	Video		
3	Audio		
4	Java		
5	ActiveX		
6	Compression		
7	Execution		
8	P2P		
9	Document		
🗊 Clear		Cancel Sa	ve

These parameters are explained as follows:

Item	Description	
Index	Displays the index number of the file extension object profile.	
Profile Name	Enter the name of the file extension object profile.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.10 SMS Service Object

Up to 10 SMS Service Objects can be set up for use.

← Configuration	2865ac_001DAA	000000 / Configuration / Objects Setti	ing	Set to Factory Default	C
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)		
	5		kotsms.com.tw (TW)		
Service Type Group	6		kotsms.com.tw (TW)		
Keyword Object	7		kotsms.com.tw (TW)		
Keyword Group	8		kotsms.com.tw (TW)		
File Extension Object	9	Custom 1			
	10	Custom 2			
Mail Service Object					

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 / Obje	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		
 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.		
會 Clear		Cancel	Save

These parameters are explained as follows:

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	ts Setting	Set to Factory Default	C
Index	9		
Profile Name	Custom 1		
Service Provider			
Exact URL			
	/// Please contact with your SMS provide to get the exact URL String eg builkms voms.net.5567(pap)(submission/send _sms/1/2.0? username=###txtUser###gbassword=###txtPwd####Kmission=###txtDest###&message=###txtHsg	<i>368</i>	
Server Response			
Username			
Password	Φ		
Quota	10		
Sending Interval	3		
 Note: Only one message can be sent during the If the "Sending Interval" was set to 0, there 	Sending Interval" turne. will be no limitation.		
f Clear		Cancel Sav	/e

Item	Description	
Index	Displays the index number of the SMS service object profile.	
Profile Name	Displays the name of the SMS service object profile.	
Service Provider	Enter an identifier for the service provider. Maximum length is 23 characters.	
Exact URL	Enter the URL for the SMS service.	
Username	Enter a name to log in to the service.	
Password	Enter a password to log in to the service.	
Quota	Set the remaining number of text messages allowed to be sent.	
Sending Interval	Set the minimum amount of time, in seconds, to wait between sending SMS messages.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.11 Mail Service Object

Up to 10 Mail Service Objects can be set up for use.

IP Object	2865ac_001DAA00000	0 / Configuration / Objects Setting				ß
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	Set to Factory Defa	ult				

To configure the mail service object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Object	cts 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 "Seen If the "Sending Interval" was set to 0, there 	ding interval" time. will be no limitation.			
億 Clear			Cancel	Save

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_001DAA	000000 / Configuration / Obje	cts Setting	
	Index	Profile Name	Settings	
	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	Set to Factor	y 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 Se	tting		Ø
Index	1		
Profile Name			
Frome Name			
WAN	Disconnected		
	Reconnected		
	Disconnected		
	Reconnected		
Temperature Alert	OutofRange		
WAN Budget	LimitReached		
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		
	Telnet Login		
	SSH Login		
	TR069 Login		
	FTP Login		
🔋 Clear	C		
			Cancel Save

Item	Description
Index	Displays the index number of the notification object profile.
Profile Name	Enter the name of the mail service object profile.

Check boxes	Select the states to be monitored.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.13 String Object

Set string profiles which will be applied in route policy.

← Configuration	2865ac_001D4	A000000 / Configuration / Objects Setting	Set to Factory Default	G
IP Object	Index	String		
	1	Floor_1		
	2	Floor_2		
IPv6 Object	3	server1.draytek.com		
IPv6 Group	4	Draytek Hotspot		
Service Type Object	5	Floor_3		
	Index String 1 Rior_1 2 Rior_2 3 server1/arytek.com 4 Draytek Hotspot			
	7			
Keyword Object		portal.draytek.com		
Keyword Group				
File Extension Object				
SMS Service Object				
Mail Service Object	1 For.1 2 For.2 3 serverLdraytek.com 4 Draytek.fotspot 5 For.3 6 ortaldraytek.com 7			
Notification Object		Draytek Hotspot		
		nır		
	20			

To configure the string object profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Object	s Setting	Cancel Save
Index	1	
String	(Max.253 chars.)	
	<i>I</i> E	
🗓 Clear		Cancel Save

Item	Description
Index	Displays the index number of the string object profile.
String	Enter a string.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.14 Country Object

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

ject	2865ac_001DAA	0000000 / Configuration / Objects Se	tting		
	Index	Name		Selected Objects	
	1				
	2				
ervice Type Object	3				
ervice Type Group	4				
eyword Object	5				
	6				
	7				
	8				
	9				
	10				
	11				
, tring Object	12				
	14				
	15				
	16				
	17				
	18				
	19				
	20				
	21				
	Set to Factor	y 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	tting	2
Index	1	
Name		
Selected Country Objects		
 Note: The maximum number of Selected Count 	y is 16.	
🛱 Clear		Cancel 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	2865ac_001DAA000000 / Configuration / QoS							С		
	Index	Status	Direction	Inbound Bandwidth	Outbound Bandwidth	Class 1 Ratio	Class 2 Ratio	Class 3 Ratio	Others Ratio	Enable UDP Bandwidth Control	
OoS Class	1	false	BOTH	0	0	25	25	25	25	false	
	2	false	BOTH	100000	100000	25	25	25	25	false	
QoS Service Type	3	false	BOTH	100000	100000	25	25	25	25	false	
VolP Prioritization	4	false	BOTH	100000	100000	25	25	25	25	false	
Tag Outbound Traffic	5	false	BOTH	100000	100000	25	25	25	25	false	
	6	false	BOTH	100000	100000	25	25	25	25	false	

To configure the QoS WAN profile, move the mouse cursor to any entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / Qo	05		Ŕ
Interface Settings			
WAN	2		
QoS Policy	\bigcirc		
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	\odot		
UDP Bandwidth Ratio (%)	25		
Prioritize Outbound TCP ACK	\bigcirc		
			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_001DAA000000 / Configuration / QoS			
QoS Class	Index	Enable Tag Packet AS	Tag Packet AS	
QoS Service Type	1	false	Default	
VoIP Prioritization	2	faise	Default	
Tag Outbound Traffic	3	faise	Default	

To configure the QoS class profile, move the mouse cursor to any entry and click to open the following page.

1 false	Anu									
	000	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0		
2 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 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 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 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. Subnet - The rule covers a range of IP address specified in subnet notation. Local Start IP Address - Enter an IP address as the starting point. Subnet - The rule covers a range of IP address as the starting point. 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 as the starting point. Subnet - The rule covers a range of IP address as the starting point. Remote Start IP - Enter an IP address as the starting point. Remote Start IP - Enter an IP address as the starting point. Remote Mask - Enter an IP address as the starting point. Remote 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. 					
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_001DAA000000 / Configuration / QoS						
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.

65ac_001DAA000000 / Configuration / QoS	
Index	1
Name	
Service Type	TCP •
Port Type	Single Range 🗸
Port Number Start	0
Port Number End	0

These parameters are explained as follows:

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
	 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 / Configura	tion / Qo5						g
QoS Class	Enable the First Priority for VolF	SIP/RTP						
QoS Service Type	SIP UDP Port	5060						
NoIP Prioritization								
Tag Outbound Traffic								Cancel Save
	VoIP QoS Status							
	VoIP Staus LAN IP VoIP Staus Pe	er IP VoIP Staus Interface	VolP Staus Delayms	VoIP Staus Delay Draw	VoIP Staus Jitterms	VoIP Staus Jitter Draw	VoIP Staus Packet Lossms	VolP Staus Loss Drav
					No c	lata available		
							•	

These parameters are explained as follows:

Item	Description
Enable the First Priority for VolP 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					
QoS Class	Enable Tag Packet AS	Tag Packet AS				
QoS Service Type	false	Default				
VoIP Prioritization	false	Default				
	false	Default				

To configure the tag outbound traffic profile, move the mouse cursor to any entry and click to open the following page.

2865ac_001DAA000000 / Configuration / QoS		
Class	1	
Enable		
Add DSCP or Precedence Value	Default	*

These parameters are explained as follows:

Item	Description
Class	Display the index number of the class.
Enable	Click to enable or disable the profile.
Add DSCP or Precedence Value	Use the drop-down list to choose the value for applying the DSCP or precedence value for each class.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11 Applications

9.4.11.1 Dynamic DNS

The Vigor router supports a wide range of DDNS providers, such as DynDNS, No-IP.com, DtDNS, and ChangeIP. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.

← Configuration	2865a	2865ac_001DAA000000 / Configuration / Applications						Set to	Factory Defau	lt C					
Dynamic DNS														View Log Ford	e Update
LAN DNS / DNS Forwarding															
DNS Security	Dyı	namic DNS Se	tup												
Schedule	Enab	le													
External RADIUS	Auto	-Update interval		14400											
Internal RADIUS															
External TACACS+															Save
Active Directory /LDAP															
UPnP	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 API
IGMP	1	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
IGMP	2	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
Wake on LAN	3	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
SMS / Mail Alert Service	4	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
	5	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
Bonjour	6	false	dyn.com_(www.dyn.com)	Dynamic					false	false		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 / A	Applications			C
Enable Account				
WAN Interface	WAN1 First	~		
Service Provider	dyn.com (www.dyn.com)	~		
Service Type	Dynamic	~		
Host Name				
Domain Name		~		
Login Name				
Password		٢		
Wildcards	\bigcirc			
Backup MX	\bigcirc			
Mail Extender				
Determine WAN IP	WAN IP	~		
前 Clear				Cancel Save

ltem	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		/ Configuration / Applications							
LAN DNS / DNS Forwarding	Index	Enable	Profile Name	Domain Name	DNS Server IP Address	Set To Factory Default			
ONS 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	tion / App	lications			
Enable					
Profile					
Domain Name					
DNS Server IP Address					
CNAME(Alias Domain Name)					
	Index	CNAME		Action	
	1			+ Add	
IP Address List					
	Index	IP Address	Same Subnet Reply	Action	
	1		\bigcirc	+ Add	
fi Clear					Cancel Save

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.
CNAME	Enter a domain name alias for the domain name.
+Add	After entering the CNAME, Click to save the setting and create a new entry.
	IP Address List
Index	Displays the index number of the IP address.
IP Address	The IP address entered here will be used for mapping with the domain name specified above.
Same Subnet Reply	Click to enable or disable the function. 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	2865ac_00	2865ac_001DAA000000 / Configuration / Applications					C	
Dynamic DNS	General Se	etup						
LAN DNS / DNS Forwarding	Index	Interface	Enable		Primary DNS	Secondary D	NS Bogus DNS Reply	
	1	WAN1	false		0.0.0.0	0.0.00	Pass	
Schedule	2	WAN2	false		0.0.0.0	0.0.0.0	Pass	
External RADIUS	3	WAN3	false		0.0.0.0	0.0.0.0	Pass	
Internal RADIUS	4	WAN4	false		0.0.0.0	0.0.0.0	Pass	
	5	WAN5 WAN6	false false		0.0.0.0	0.0.0.0	Pass Pass	
	•	WARD	Idise		0.0.0.0	0.0.0.0	Pd55	
	Domain Di	iagnosis						
IGMP	Domain							
Wake on LAN	Domain T	VDe		IPv4 IPv6				
SMS / Mail Alert Service								
Bonjour	Interface			WAN1	Ý			
High Availability	DNS Serv	er						
Local 802.1X General Setup								_
								Dlagnose
	Domain Name	e		IP Addres	is	Interface	Verify Result	

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.

2865ac_001DAA000000 / Configuration / Appl	cations	C
General Setup		
Enable	0	
Interface	WANI	
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.

Dynamic DNS	2865ac_001	DAA000000 / Confi	iguration / Applications		Set to Factory Default	0
	Index	Enable	Comment	Time	Frequency	
	1	false		00:00 00:00	Sun.	0
ternal RADIUS ternal RADIUS	2	false		00:00 00:00	Sun.	e
ternal TACACS+ tive Directory /LDAP	3	false		00:00 00:00	Sun.	0
	4	false		00:00 00:00	Sun.	e
	5	false		00:00 00:00	Sun.	9
	6	false		00:00 00:00	Sun.	0
igh Availability ocal 802.1X General Setup	7	false		00:00 00:00	Sun.	0
	8	false		00:00 00:00	Sun.	0
	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	false		00:00 00:00	Sun.	0
	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 Comment Comment Start Date (yyyy-mm-dd) 2000 - 1 - 1 - 2 Start Time (hh:mm) 0 - 2 0 - 2 Duration Time (hh:mm) 0 - 2 0 - 2 End Time (hh:mm) End Time (hh:mm	55ac_001DAA000000 / Configuration	/ Applications			
Comment Start Date (yyyy-mm-dd) 2000 · - 1 · · 1 · Start Time (hh:mm) 0 · : 0 · Duration Time (hh:mm) 0 : 0 · End Time (hh:mm) 0 : 0 · Action Force On · · · How Often Weekdays · · Weekdays S Sun I Mon I Tue I M					
Start Date (yyyy-mm-dd) 2000 v · 1 v · 1 v Start Time (hh:mm) 0 v : 0 v Duration Time (hh:mm) 0 v : 0 v 0 v : 0 v 0 v End Time (hh:mm) 0 · 2 · 0 v Action Force On v How Often Weekdays Weekdays Sun v Mon 2 Tue v Wed 2 Tue v Wed 2 Tue v Wed 2 Tuu v Fri Sat	Enable				
Start Time (hh:mm) 0 : : <tr< td=""><td>Comment</td><td></td><td></td><td></td><td></td></tr<>	Comment				
Duration Time (hh:mm) End Time (hh:mm) 0 : 0 Action Force On Weekdays Weekdays Sun Tue Weekdays Sun Tue Weekdays Sun Tue Weekdays Sun Tue Sat	Start Date (yyyy-mm-dd)	2000 ~ - 1 ~	- 1 ~		
End Time (hh:mm) 0 : 0 Action Force On How Often Veekdays Sun Image: Compare the second s	Start Time (hh:mm)	0 ~ : 0 ~			
Action Force On ~ How Often Weekdays ~ Weekdays Sun I Mon I Tue I Weekdays I Tue I Weekdays Sat	Duration Time (hh:mm)	0 ~ : 0 ~			
How Often Weekdays Weekdays Sun Mon Tue Weekdays Tue Weekdays Tue Weekdays Tue Fin Sat	End Time (hh:mm)	0 : 0			
Weekdays Sun Mon Tue Wed Tue Wed Thu Fri Sat Note: Comment can only contain A-Z a-z 0-9,.[]()^\$!-`	Action	Force On	~		
Image: Tue Image: Wed Image: Thu Fri Image: Sat Image: Onote: Comment can only contain A-Z a-z 0-9,	How Often	Weekdays	~		
 Thu Fri Sat Note: Comment can only contain A-Z a-z 0-9,(}()^\$!-^` 	Veekdays	🗆 Sun	Mon		
□ Sat ① Note: Comment can only contain A-Z a-z 0-9, . { } () ^ \$! - `		🗹 Tue	🗹 Wed		
O Note: Comment can only contain A-Z a-z 0-9 , . { } () ^ ! ~ `		🗹 Thu	Fri		
Comment can only contain A-Z a-z 0-9 , . { } () ^ \$! - `		Sat			
Comment can only contain A-Z a-z 0-9 , . { } () ^ \$! - `	① Note:				
Clear Canc	Comment can only contain A-Z a-z 0	-9,.{}()^\$!~`			
Clear Canc					
) Clear				

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.
Save	Save the current settings and return to previous page.

9.4.11.5 External RADIUS

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

Dynamic DNS	2865ac_001DAA000000 / Configuration / Applica	ations	ø
LAN DNS / DNS Forwarding	Primary Server		
DNS Security	Enable		
Schedule	Enable Accounting	\odot	
External RADRUS	Comments		
Internal RADIUS			
External TACACS+	Primary Server		
Active Directory /LDAP	Secret	Φ	
UPnP	Authentication Port	1812	
IGMP	Retry	2	
Wake on LAN			
SMS / Mail Alert Service	Secondary Server Secondary Server		
Bonjour	-		
High Availability	Secret	•	
Local 802.1X General Setup	Authentication Port	1812	
	Retry	2	
	🔁 Clear		Save

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					
LAN DNS / DNS Forwarding	General Setup					
DNS Security						
	Enable					
	Authen	tication Port	1812			
		tication Method				
	Authen	tication Method	PAP Only	¥		
	Support	t 802.1X Method	\bigcirc			
UPnP	Authen	tication List				
IGMP	Synchro	onize Internal RADIUS user li	st to			
	Local 80	02.1X user list.	•			
SMS / Mail Alert Service						
						Save
High Availability	RADIUS Client	t Access List				
	Index	Client Access Enable	Client Access Shared Secret	Client Access IP Address	Client Access IP Mask	Client Access IPv6 Address
	1	false		0.0.0.0	0.0.0.0	
	2	false		0.0.0.0	0.0.0.0	
	3	false		0.0.0.0	0.0.0.0	
	4	false		0.0.0.0	0.0.0.0	:
	5	false		0.0.0.0	0.0.0.0	
	6	false		0.0.0.0	0.0.0.0	
	7	false		0.0.0.0	0.0.0.0	
	n 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 Method	 Click to enable or disable the Support 802.1X Method function. EAP_TTLS/PAP EAP_TTLS/MSCHAP EAP_TTLS/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	Displays the text string that is known to both the router's RADIUS server		

Secret	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	$\mathbf{\bullet}$
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		
LAN DNS / DNS Forwarding	Enable	0	
DNS Security	Server IP Address	0.0.0	
Schedule	Destination Port	49	
External RADIUS			
Internal RADIUS	Shared Secret	0	
External TACACS+ Active Directory /LDAP	🖹 Clear		
UPnP			

ltem	Description
Enable	Click to enable / disable the external TACACS+ server settings.

Server IP Address	Enter the IP address of the TACACS+ server.
Destination Port	Enter a port number used by the TACACS+ server. Port 49 is most common.
Shared Secret	Enter a text string. It is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters.
Clear	Clear all modifications on this page.
Save	Save the current settings.

9.4.11.8 Active Directory/LDAP

Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

Dynamic DNS		/ Configuration / Applications						
LAN DNS / DNS Forwarding	General Setup	, ,						
DNS Security	Enable							
Schedule								
External RADIUS	Bind Typ	ie .		Simple Mode +				
Internal RADIUS	Server A	ddress		IPv4 format (EX : 123.12.1.1)				
External TACACS+	Destinat	tion Port		389				
Active Directory /LDAP	Use SSL			0				
UPnP				<u></u>				
IGMP							Save	
Wake on LAN	Active Directo	ry / LDAP Profiles						- I
SMS / Mail Alert Service								
Bonjour	Index	Name	Common Name Ident	ifier Distinguishe	d Name Adv	litional 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.

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 / Applie	2865ac_001DAA000000 / Configuration / Applications		
Dynamic DNS	WAN Interface	Default WAN ~		
LAN DNS / DNS Forwarding	Enable UPnP Service	0		
DNS Security		0		
Schedule	Enable Connection Control Service			
External RADIUS	Enable Connection Status Service	0		
Internal RADIUS	(i) Note:			
External TACACS+	 To allow NAT pass-through to a UPnP 	enabled client the connection control service must also be enabled.		
Active Directory /LDAP				
UPnP	1 Clear	Sa	ve	
IGMP				

These parameters are explained as follows:

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 / Configuration / Appli	865ac_001DAA000000 / Configuration / Applications C						C
Dynamic DNS	IGMP Proxy	O						
LAN DNS / DNS Forwarding	Interface	WAN1		~				
DNS Security								
Schedule	IGMP version	Auto		~				
External RADIUS	General Query Interval (seconds)	125						
Internal RADIUS	Add PPP header	\bigcirc						
External TACACS+	Encapsulate IGMP in PPPoE							
Active Directory /LDAP								
UPnP	Enable IGMP syslog	\bigcirc						
IGMP	IGMP Snooping	\bigcirc						
Wake on LAN								
SMS / Mail Alert Service								Save
Bonjour	Working group							
High Availability								
Local 802.1X General Setup	Index Group ID		P1	P2	P3	P4	P5	P6
				\wedge				
			Ν	io data avallable				

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 IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1-PX	Displays the LAN ports that have IGMP hosts joined to this multicast group.

9.4.11.11 Wake on LAN

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

← Configuration	2865ac_001DAA000000 / Configuration / App	lications
Dynamic DNS	Wake by	MAC Address
LAN DNS / DNS Forwarding	Wate by	INHC RULIESS
DNS Security	IP Address	
Schedule	MAC Address	
External RADIUS		
Internal RADIUS		Wake Up
External TACACS+		
Active Directory /LDAP	Result	
UPnP		
IGMP	() Note:	
Wake on LAN	 Wake on LAN integrates with <u>BInd IP to</u> 	o MAC function; only bound PCs can wake up through IP.

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 Address	Enter any one of the MAC address of the bound PCs.
Result	Displays the result of WOL execution.
Wake Up	Click to wake up the selected device.

9.4.11.12 SMS/Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

← Configuration	2865ac_	001DAA000000 / Co	nfiguration / Applications				
Dynamic DNS	SMS A	lert					Set to Factory Defa
LAN DNS / DNS Forwarding	Index	SMS Enable	SMS Provider	SMS Recipient Number	SMS Notify Profile	SMS Schedule1	SMS Schedule2
DNS Security	1	false	1-Local number		1-		
Schedule	2	false	1-Local number		1-		
External RADIUS	3	false	1-Local number		1-		
	4	false	1-Local number		1-		
nternal RADIUS	5	false	1-Local number		1-		
	6	false	1-Local number		1-		
Active Directory /LDAP	7	false	1-Local number		1-		
UPnP	8	false	1-Local number		1-		
	9	false	1-Local number		1-		
IGMP	10	false	1-Local number		1-		
SMS / Mall Alert Service Bonjour	① No Mail Al	All the SMS Alert pro	files share the same "Sending	g Interval" setting if they use the s	ame SMS Provider.		Set to Factory Def
High Availability							
Local 802.1X General Setup	Index	Mail Enable	Mail Service	Mail Address	Mail Notify Profile	Mail Schedule1	Mail Schedule2
	1	false	1-Mail_Notify		1-		
	2	false	1-Mail_Notify		1-		
	3	false	1-Mail_Notify		1-		
	4	false	1-Mail_Notify		1-		
	5	false	1-Mail_Notify		1-		
	6	false	1-Mail_Notify		1-		
	7	false	1-Mall_Notify		1-		
	8	false	1-Mail_Notify		1-		
	9	false	1-Mail_Notify		1-		

These parameters are explained as follows:

Item	Description
SMS Alert	It allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.
Mail Alert	It allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

To configure the SMS alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

2865ac_001DAA000000 / Configuration / Appli	cations		C
Enable			
SMS Provider	1 ~		
Recipient Number			
Notify Profile	1 ~		
Schedule 1			
Schedule 2			
		Car	ncel 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 / Applications		
Enable		
Mail Service	1 ~	
Mail Address		
Notify Profile	1 ~	
Schedule 1		
Schedule 2		
	Cancel Sa	ave

These parameters are explained as follows:

Item	Description
Enable	Click to enable or disable the mail alert profile.
Mail Service	Use the drop down list to choose mail service object.
Mail Address	Enter the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile.
Schedule 1 / 2	Enter the schedule number (0~15) that the notification will be sent out.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.13 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.

Dynamic DNS	Soot - configuration	/ Applications		
LAN DNS / DNS Forwarding	Enable Bonjour Service			
DNS Security	HTTP Server	D		
Schedule				
External RADIUS	Telnet Server	\bigcirc		
Internal RADIUS	FTP Server	\odot		
External TACACS+	SSH Server	\bigcirc		
Active Directory /LDAP	LPR Printer Server	\bigcirc		
UPnP				
IGMP				
Wake on LAN				
SMS / Mail Alert Service				
Banjour				

Item	Description
Enable Bonjour Service	Click to enable or disable the Bonjour 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 / App	lications	Set to Factory Default 🛛 🕑
Dynamic DNS			
LAN DNS / DNS Forwarding	Enable High Availability	\bigcirc	
DNS Security	Redundancy Method	Active-Standby ~	
Schedule	General Setup		
External RADIUS	Course 10		
Internal RADIUS	Group ID	1	
External TACACS+	Priority ID	10	
Active Directory /LDAP	Authentication Key	draytek	
UPnP	Protocol	IPv4 ~	
IGMP	Management Interface	LAN1 ~	
Wake on LAN	Update DDNS	0	
SMS / Mail Alert Service	Syslog	0	
Bonjour	SYSIOE		
High Availability	Config Sync		
Local 802.1X General Setup	Enable Config Sync (Max. Sync to 10 routers)	\odot	
	Day	0 ~	
	Hour	0 ~	
	Minute	15 ~	
	WAN Settings		
		5	Save

Item	Description
Enable High Availability	Click to enable or disable the HA function.
Redundancy Method	Select the redundancy method (Hot-Standby or Active-Standby) for high availability.
	General Setup
Group ID	Enter a value (1~255). Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group.
Priority ID	Enter a value (1~30). Different routers must be configured with different IDs.
Authentication Key	Enter an authentication key up to 31 characters long.
Protocol	Select the IP protocol (IPv4 or IPv6) to be used for DARP.
Management Interface	Select the interface to be used for DARP negotiation between routers.
Update DDNS	Click to enable or disable the function.

	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.

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 / Application	5	C	
LAN DNS / DNS Forwarding	Enable			
DNS Security	EAP_TTLS/PAP	\bigcirc		
Schedule	EAP_TTLS/MSCHAP	\bigcirc		
External RADIUS	EAP_TTLS/MSCHAPv2	\odot		
Internal RADIUS				
External TACACS+	EAP_PEAP/MSCHAPv2			
Active Directory /LDAP	Authentication List			
UPnP	Sync User Profile Setting to Internal Radius	\bigcirc		
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.

/ Configuratio	n / VPN	ø
 A Root Network(70) A @#\$W^&_+()^:><!---(0)</li--> A Marketing_carrie(0) A Marketing_carrie(0) A SD-WAN(2) A aeaea(123)(1) A rd7(2) A rd8(42) A ap910(0) A rd8-1(0) A rd8-1(0) A rd8-2(0) A 810_001DAA7D6514 902_001DAA3D4F16 A 130_001DAA8411C8 A 130_001DAA8D3FA0 	Add Device Crease VPN Cdd: LAN 8 United VPN Remove Device Show device name Add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device position with mouse cursor. add Device from Network Monitor at left, and arrange device positio	
	PPTP IPSec L2TP SSL VPN Disconnected	

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.
Create VPN Add Device Create VPN Edit LAY PPTP Wizard PPTP Wizard SSL Wizard SSL Wizard SSL Wizard Customized 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 RX 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	Configuration / VPN Set to Factory Defaul							Default	C	
VPN Wizard	Alarm Enable	Index	Enable	Always On	Default Route	Name	Remote Network	Remote Network Mask		Statu	5
	disable	1	true	true	false	I_720_000	192.168.124.1	255.255.255.0		Onlin	e
LAN to LAN	disable	2	false	false	false	???	0.0.0.0	255.255.255.0		Offlin	e
Remote Dial-In User											
Remote Access Control									N <	1/1	> 14
VPN Matcher	Pass packets from LA	Pass packets from LAN in Routing mode to VPN									
OpenVPN	Pass Packets to WAN when VPN disconnects										
											Save
											0.110

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 C	
VPN Wizard LAN to LAN	Common Settings			
Remote Dial-In User	Index	1		
Remote Access Control	Enable this profile			
VPN Matcher	Enable ACS Alarm	\bigcirc		
OpenVPN	Profile Name	I_720_000		
	Call Direction	Both Dial-Out Dial-In GRE Tunnel		
	Dial-Out Through	WAN1 First ~		
	Always on			
	Idle Timeout	-1		
	Quality Monitoring/Keep Alive			
	Netbios Naming Packet	Pass Block		
	Multicast via VPN	Pass Block		
	(i) (for some IGMP,IP-Camera,DHCP Relaye	tc.)		
	Dial-Out Settings			
	VPN Server Type	IPSec_Tunnel ~		
	IPsec Tunnel Type	IKEV1 ~		
	Server IP/Host Name	192.168.105.120		
	🖻 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

	authenticating with remote VPN server. The length of the ID is limited to 47 characters.
Phase 2 Key Lifetime Phase 2 Network ID	For security reason, the lifetime of key should be defined. The default value is 3600 seconds. In Aggressive mode, Local ID is on behalf of the IP address while identity
Phase 1 Key Lifetime	For security reason, the lifetime of key should be defined. The default value is 28800 seconds.
	IKE Advanced Settings
Authentication	
Proposal	Select All, SHA256, SHA1 or None.
Proposal Encryption	Select an proposal encryption mode.
	 ESP(High) AH(Medium)
Security Protocol	Select the dial-out protocol.
	IKE Phase 2 Settings
Authentication	
Proposal	Select SHA256 or SHA1.
Proposal ECDH Group	Select an proposal ECDH group (e.g., G14).
Proposal Encryption	Select an proposal encryption mode.
Local ID	Enter a string.
Pre-Shared Key	It is available when PSK is selected as Authentication. Enter the PSK.
Authentication	Select PSK (IKE Pre-shared key) or X509 (X.509 digital signature).
	Aggressive Mode
	Main Mode
WOUC	since more exchanges are done in a secure channel to set up the IPsec session.
Mode	IKE Phase 1 Settings Select IKE phase 1 mode. Main mode is more secure than Aggressive mode
	Up to four schedule profiles can be specified.
Dial-Out Schedule Profile	Connect and disconnect according to schedule profiles.
Server IP/Host Name	Enter an IP address or DNS host name of remote VPN host.
IPsec Tunnel Type	Select IKEv1 or IKEv2.
VPN Server	Select the VPN protocol to be used.
	Dial-Out Settings
	• Block – This is default setting. Click this button to let multicast packets be blocked by the router.
	 Pass – Click this button to let multicast packets pass through the router.
Multicast via VPN	Specifies whether to allow multicast packets to traverse through the VPN tunnel.
	transmission of Netbios Naming Packet inside the tunnel.

Enable Perfect	Click to enable or disable	e the f	unction.							
Forward Secret	If enabled, the IKE Phase complexity in phase 2.	1 key	will be reuse	d to avoid the com	putation					
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 Settings									
Local Network IP / Mask	Display the local network modify the settings if req			CP / IP configuratio	n. You can					
Remote Network IP / Mask	Add a static route to dire Address/Remote Networ				etwork IP					
More Remote Subnet	Add a static route to direct all traffic destined to <i>more</i> 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	the m	hask address	Click +Add to save	the settings					
	and create a new entry.	the fi			the settings					
Mode	If the remote network on	-		dress for the local ı	network,					
	select NAT; otherwise, se Routing 	elect R	outing.							
	 NAT 									
RIP via VPN	Specifies the direction of	Routi	ing Informatic	on Protocol (RIP) pa	ckets.					
Translate Local	It is available when Routi									
Network	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 type				Specific IP)					
	for you to choose.									
	For Translate Whole Sub		I AN whose IF	P addresses are to	he					
	translated.									
	Translated IP - Spece	-								
	 More Local Subnet 	- Add	more subnet	S.						
	More Local Subnet	Index	Translated To	Local Network	Action					
		1		LAN1 -	+ Add					
	For Translate Specific IP,									
	• Virtual IP Mapping virtual IP address.	- Spec	cify the local IF	Paddress and the r	mapping					
	Virtual IP Mapping	Index	Local IP	Virtual IP	Action					
		1			+ Add					
Change Default Route	Click to enable or disable	this o	option .							

to this VPN	Select this option to direct all traffic that is not LAN-bound to this VPN tunnel.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.12.3 Remote Dial-In User

The system administrator can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

← Configuration	2865ac_001DAA000000 / Configura	2865ac_001DAA000000 / Configuration / VPN					
VPN Wizard	Index	Enable	Username	Status			
LAN to LAN	1	Disable	222	Disable			
Remote Dial-In User					₩ < 1/1	> 14	
Remote Access Control							
VPN Matcher							
OpenVPN							

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 / VPN				Set to Factory Default	C
VPN Wizard	Remote Dial In User					
LAN to LAN	User account and Authentication					
	User account and Authentication					
Remote Access Control	Index	1				
VPN Matcher	Enable	\bigcirc				
OpenVPN	Idle Timeout	300				
	Username	???				
	Password					
	Mobile One-Time Passwords(mOTP)	\bigcirc				
	Note: Username can not contain characters "\" OpenVPN tunnel does not support mOTP					
	Allowed Dial-In Type					
	рртр	\bigcirc				
	IPsec Tunnel					
		KEv1/IKEv2	IKEv2 EAP	IPsec XAuth		
	L2TP					
	L2TP with IPsec Policy	None	~			
	CCI Tunnol					_
	i Clear				Cancel Sa	/e

Item Description	
User account and Authentication	
Index	Displays the index number of the user account profile.
Enable	Click to enable or disable the user account profile.
Idle Timeout	Set the allowed idle time before the router disconnects the VPN connection.
Username	Set a username used for PPTP, L2TP or SSL Tunnel dial-in type
Password	Set a password used for PPTP, L2TP or SSL Tunnel dial-in type

Mobile One-Time Passwords (mOTP)	Click to enable or disable one-time passwords (Mobile-OTP).		
rasswords (morr)	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 Packet	It is available when Specify Remote Node is disabled. 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	It is available when Specify Remote Node is disabled.		
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.		
	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 authent 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 / Configuration / VPN	C
VPN Wizard	Remote Access Control Setup	
LAN to LAN	PPTP VPN Service Enable	
Remote Dial-In User Remote Access Control	IPSec VPN Service Enable	
VPN Matcher	L2TP VPN Service Enable	
OpenVPN	SSL VPN Service Enable	
	OpenVPN Service Enable	
	 O Note: To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured 	
	I	Save

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.

← Configuration	2865ac_001DAA000000 / Configuration / VPN		C
VPN Wizard	VPN Matcher		
LAN to LAN Remote Dial-In User	Enable		
Remote Access Control	Server Ip	vpn-matcher.draytek.com	
VPN Matcher	Server Port	31503	
OpenVPN	Router List Key	\$	
	Note: • You can get your Router List Key on VPN Ma STUN Server	tcher Dashboard . Detect	
	Group Device List	GetLbs	
	Index 4 ⁺ Description	41 MAC 41 Remote Network 41 Model 41 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 ServerDetect - Click to check if the NAT used by Vigor router is core 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 / Configuration / VPN	с
VPN Wizard	OpenVPN Server Setup Client Config	
LAN to LAN		
Remote Dial-In User	General Setup	
Remote Access Control	Enable UDP	0
VPN Matcher	UDP Port	1194
OpenVPN	Enable TCP	0
	TCP Port	1194
	Cipher Algorithm	AES128 ~
	HMAC Algorithm	SHAL ~
	Certificate Authentication	0
	Certificates Setup	
	Certificate Source	Uploading certificates to Router \sim
	Trust CA	default v
	Server Certificate	None ~
	Note: OpenVPN on Vigor Router only support TU	N device Interface currently. So please setup corresponding configurations on the client side.
		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 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.

← Configuration	2865Lac_1449BC0D8F00 / Configuration / VPN		C
VPN Wizard	OpenVPN Server Setup Client Config		
LAN to LAN			
Remote Dial-In User	Client Config		
Remote Access Control	Remote Server	IP Domain VPN Matcher	
VPN Matcher	Transport Protocol	×	
OpenVPN	Auto Dial-Out	Enable Disable	
	Set VPN as Default Gateway	Enable Disable	
	File Name	ovpn	
	Client cert	.ct	
	Client key	Jacy	
		Export	
	Rote: Please make sure the Client cert and the Client Please make sure that WAN can be used as Op	nt key are located in the same folder with .ovpn file. DenVPH server.	

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.

← Configuration	2865ac_001DAA000000 / Co	865ac_001DAA000000 / Configuration / Mesh				
Mesh Setup Add Mesh Node Mesh Status	General Setup Mesh Enable					
	Role Mesh Group Name Log Level Mesh Group		Mesh Root YigorMesh Dasic	×		
	Index	MAC Address 001DAA000000		Modal Vigor 2865	Device Name DrayTek	
	つ Reset Mesh Group					Cancel Save

These parameters are explained as follows:

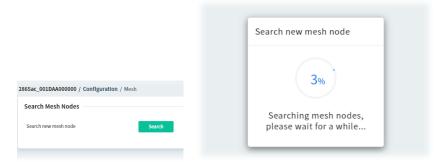
ltem	Description
	General Setup
Mesh Enable	Click to enable or disable the mesh network function.
Role	Displays the role of the router. For Vigor router, it is always Mesh Root.
Mesh Group Name	Displays the name of the current mesh group.
Log Level	Choose Basic or Detailed .
	Mesh Group
Index, MAC Address, 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				
Mesh Setup	Search Mesh Nodes				
Add Mesh Node	Search new mesh node Search				
Mesh Status					

1. Click **Search**. The system will search new mesh node around.



2. Available mesh nodes will be listed on this page.

← Configuration	2865a	c_001DA	A000000 / Con	figuration / Me	esh
Mesh Setup	Sea	rch Me	sh Nodes —		
Add Mesh Node	Sea	rch new r	nesh node		Search
Mesh Status					
	Add	Index	MAC Address	Model	Device Name
		1	00507FF191BC	VigorAP 903	VigorAP903
		2	1449BC426E1E	VigorAP 960C	VigorAP960C
	-				

3. Select the device(s) you want to group under this mesh group and click **+Add**.

← Configuration	2865ac	Sac_001DAA000000 / Configuration / Mesh							
Mesh Setup	Sea	Search Mesh Nodes							
	Sear	ch new n	nesh node		Search				
Mesh Status									
	Add	Index	MAC Address	Model	Device Name				
		1	00507FF191BC	VigorAP 903	VigorAP903				
		2	1449BC426E1E	VigorAP 960C	VigorAP960C				

4. Wait for a moment.



5. Open **Configuration>>Mesh Setup**. The new mesh node will be added.

Mesh Group				
Index	MAC Address	Model	Device Name	
1	001DAA000000	Vigor 2865	DrayTek	
2	00507FF191BC	Unknown	VigorAP903	
්ට Reset Mesh Group			Ca	ncel Save

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.

← Configuration	2865ac_001	2865ac_001DAA000000 / Configuration / Mesh							
Mesh Setup	 Online(system) 	Online(sync ready) Online Online Online							
Add Mesh Node	Index	Status	Device Name	MAC Address (Model)	Нор	Up Link	Up Time	Clients	Disconnect
Mesh Status	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	
	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.

← Configuration	2865ac_001DAA000000 / Configuration / Win	reless LAN		C
2.4G 5G	General Setup			
General SSID Security Access Control WPS	Index Wireless LAN Enable Mode Channel	0 Mtxed(11b+11g+11n) Channel 6, 2437MHz		
Bandwidth Management				
Airtime Fairness				
Advanced Setting				Cancel Save
Band Steering	Index	Schedule	s	SID
AP Discovery	1	0		
Station List	2 3	0		
Station List - Advance	4	0		
Station List - Neighbor Roaming Station Control	 Isolate Member: Prevent the clients a Isolate VPN: Block the wireless clients Only the action "Force Down" in the S 	ed while Wireless 2.4G WAN mode is in use. ssociated with this SSID from accessing each old is from accessing the VPN network and prevent Schedule Profile will be applied to WLAN, other r / Hot-Standby method and it's the Secondary Rc	vireless traffic being sent to VPN connections. Actions will be ignored.	

Item	Description				
	General Setup				
Index	Displays the index number of the WLAN profile.				
Wireless LAN Enable	Click to enable or disable the wireless LAN function.				
Mode	Select the 802.11 mode allowed on the band.				
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting " Auto ".				
Cancel	Discard current modification.				
Save	Save the current settings.				
Index	Displays the index number of the WLAN profile.				
Schedule	Displays the number of the schedule profile.				

To configure the schedule profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

865ac_001DAA000000 / Configu	ration / Wireless LAN		
WirelessLAN_General_SchS	SID		
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.

9.4.14.2 SSID

Set Service Set Identification (SSID), which shows up as the AP identifier.

2.4G 5G	2865ac_001DAA000000 / Configuration / Wireless LAN							
	Index	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN		
	1	true	false	2865_MKHenry	false	false		
	2	false	false	DrayTek_Guest	false	false		
	3	false	false		false	false		
	4	false	false		false	false		
	Note:							
Bandwidth Management								
Airtime Fairness	Isolate VPN	Block the wireless clients	i from accessing the VPN netw	ork and prevent wireless traffic being sent t	o VPN connections.			

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	ration / 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
Isolate 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.

9.4.14.3 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_001	DAA000000 / Configura	ation / Wireless LAN			C
2.4G 5G	Index	Mode	WPA Encryption Mode	WEP Encryption Mode	WEP Key Index	
240 50	1	WPA2/PSK	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1	
	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						
Bandwidth Management						
Airtime Fairness						

To configure security settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

865ac_001DAA000000 / Configu	ration / Wireless LAN	
General Setup		
Index	1	
Mode	WEP/802.1x_Only ~	
WEP		
WEP Encryption Mode		
WEP Key Index	1	
WEP Key	۰	
Note:	ess LAN(2.4GHz) 802.1X Setting.	
r leuse comigure die <u>mier</u>	on na far fan	
		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.				

9.4.14.4 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 / Configuration	Ion / Wirele	ss LAN								C
2.4 6 56	General Setup										
General SSD Security Access Control WPS	SSID 1 Enable SSID 1 Policy SSID 2 Policy SSID 2 Policy		White_List			~					
Bandwidth Management Airtime Fairness Advanced Setting Band Steering AP Discovery Station List	SSID 3 Enable SSID 3 Policy SSID 4 Enable SSID 4 Policy		White_List			~					
Station List - Advance Station List - Neighbor Roaming Station Control	Clear MAC Address Filter List	Index MAC	Address	Attribute	SSID 1	SSID 2	SSID 3	SSID 4	Action	Can	cel Save
		Index MAC	Address						+ Add		

Item	Description
	General Setup
SSID 1 Enable ~ SSID 4 Enable	Click to enable or disable the MAC filter.
SSID 1 Policy ~ SSID 4 Policy	White List - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list.
	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.

9.4.14.5 WPS

It provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.

← Configuration	2865ac_001DAA000000 / Configuration / Wirele	s LAN
2.4G 5G	Enable WPS	
General	WPS Status	Configured
	WPS SSID	DrayTek
	WPS Authentication Mode	WPAZ/PSK
Access Control		
Bandwidth Management		Cancel S

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.					

9.4.14.6 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	2865ac_001DAA0	00000 / Configuration / Wireless LAN				
2.46 56	Index	SSID	Enable	LimitType	UploadLimit	DownloadLimit
240 30	1	DrayTek	false	Auto_Adjustment	30000	30000
	2	DrayTek_Guest	false	Auto_Adjustment	30000	30000
	3		false	Auto_Adjustment	30000	30000
	4		false	Auto_Adjustment	30000	30000
WPS						
Advanced 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	Click 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 limitation of the wireless client.	
	• 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.	

9.4.14.7 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

← Configuration	2865ac_001DAA000000 / Configuration / Wireless LAN	C	
2.4G 5G	Enable Airtime Fairness		
General	Triggering Client Number 2		
SSID	(2 - 64, Default: 2)		
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	Artime:		
Bandwidth Management	 Aritime is the time where a wireless station occupies the wireless channel. Aritime Fairness function tries to assign similar airtime to 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 		
Airtime Fairness	Suitable environment : (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is		
Advanced Setting	wireless connection. Triggering Client Number: Airtime Fairness function is applied only when active station number achieves this number.		
Band Steering			
AP Discovery			
Station List		Cancel Save	

These parameters are explained as follows:

Item	Description	
Enable Airtime Fairness	Click to enable or disable the airtime fairness.	
Triggering Client Number	Airtime Fairness function is applied only when there are at least this many active wireless stations.	
Cancel	Discard current modification.	
Save	Save the current settings.	

9.4.14.8 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 / Configuration / Wireless LAN		
2.46 56	Operation Mode	Mixed_Mode ~	
	Channel Bandwidth	20/40 ~	
	Guard Interval	auto	
Security	Aggregation MSDU(A-MSDU)		
	Long Preamble	\bigcirc	
WPS Bandwidth Management	TX Burst	0	
Airtime Fairness	Antenna	2T2R ~	
	Tx Power	100%	
Band Steering	WMM Capable	100% · · · · · · · · · · · · · · · · · ·	
AP Discovery		0	
Station List	APSD Capable		
Station List - Advance	Rate Adaptation Algorithm	New	
Station List - Neighbor	Fragment Length	2346	
Roaming Station Control	RTS Threshold	(256 - 2346 bytes)	
	RTS Inresnola	2347	
	Country Code	(1 - 2347 bytes)	(Reference)
			c

Item	Description	
Operation Mode	Mixed_Mode - The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless	

	transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected.
	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	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.
Country Code	Vigor router broadcasts country codes according to the 802.11d standard. Click Reference to get detailed information.
Isolate 2.4GHx and	Click to enable or disable the function.
5GHz bands	If enabled, the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.
Cancel	Discard current modification.

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

9.4.14.9 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	2865ac_001DAA000000 / Configuration / Wireless LAN		C
2.4G 5G	Enable Band Steering		
General	5G Capability Check Timer	15	
SSID		(1 - 60 seconds, Default: 15)	
Security			
Access Control	 Note: Please setup at least one pair of 2.4GH. 	z 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		ss LAN, such as 5GHz to prevent from network congestion.	
Airtime Fairness	Band steering would actively block the client 5G capability" would cause the c	: client's attempts to associate with 2.4GHz Wireless LAN. So the setting of "Check time for WLAN lelay of 2.4G WLAN connection.	
Advanced Setting			
Band Steering			Cancel
AP Discovery			Califer

These parameters are explained as follows:

Item	Description	
Enable Band Steering	Click to enable to disable the Band Steering function.	
5G Capability Check Timer	Set a check time value. 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.	

9.4.14.10 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%	WPA1P5KWPA2P5K
SSID	2	Vigor2927 PQC Tang Test	16:49:BC:42:37:D8	9	1096	WPA2P5K
Security	3	staffs_5F	02:50:7F:C1:7F:1F	1	096	WPA1P5KWPA2P5K
Access Control	4	RD8_GW_24G_s1	00:1D:AA:5B:A0:C8	13	83%	WPA1P5KWPA2P5K
WPS	5	DrayTek04F06C	00:1D:AA:57:5D:38	11	096	WPA1PSKWPA2PSK
	б	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	71%	WPA1PSKWPA2PSK
Airtime Fairness	8	FAE-Wendy-2925-BS	00:1D:AA:F0:6D:F0	11	0%	WPA2PSK
Advanced Setting	9	DrayTek04F06C	00:1D:AA:04:F0:6C	11	7196	WPA1PSKWPA2PSK
Band Steering	10		12:1D:AA:04:F0:6C	11	7196	WPA2P5K
	11	DrayTek-E48E80	00:1D:AA:E4:8E:80	11	096	WPA2P5K
AP Discovery	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
	19	RD8 tim 2865 24g	02:1D:AA:41:DF:78	9	34%	WPA1PSKWPA2PSK

9.4.14.11 Station List

Station List provides an overview of all currently connected wireless clients and their status.

← Configuration	2865ac_001DAA000000 / Configuration / Wireless	s LAN		C
2.4G 5G	Station List			
General	Status Codes : • C: Connected, No encryption.			
SSID	E: Connected, WEP.			
Security	P: Connected, WPA. A: Connected, WPA2.			
Access Control	B: Blocked by Access Control.			
WPS	N: Connecting.			
Bandwidth Management	F: Fall to pass WPA/PSK authentication.			
Airtime Fairness	Add to Access Control :			
Advanced Setting				
Band Steering	MAC			
AP Discovery	SSID	(1-4)		
Station List			_	
Station List - Advance			Add	
Station List - Neighbor	Note: After a station connects to the router successfully, it			
Roaming				

These parameters are explained as follows:

Item	Description	
Station List	Displays wireless stations connected to the Vigor router.	
Add to Access Control	MAC - Enter the MAC address.	
	SSID - Specify the number of SSID.	
Add	Click to add a new entry to Access Control.	

9.4.14.12 Station List - Advance

Displays wireless stations connected to the Vigor router with more detailed information.

← Configuration	2865ac_001DAA000000 / Configuration / Wireless LAN									
2.4G 5G	Index	MAC Address	AID	RSSI	Rate	BW	PSM	WMM	PhMd	MCS
General										
SSID					No data available					
Security										
Access Control	Add to Access Control :									
WPS	MAC									
Bandwidth Management	SSID		(1-4)							
Airtime Fairness										
Advanced Setting								Add		
Band Steering	Note: • After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.									
AP Discovery										
Station List										
Station List - Advance										
Station List - Neighbor										
Roaming										
Station Control										

9.4.14.13 Station List - Neighbor

This page displays the nearby wireless stations connected to other access points that are detected by the Vigor router.

← Configuration	2865ac_001DAA00	00000 / Configuration / Wirele	ess LAN						C
2.4G 5G	Index	MAC Address	Vendor	RSSI	Approx Distance		SSID	Visit Time	
General	Add to Access	Control :							
SSID									
Security	MAC		00:1D:AA:00:00:00		<i>(</i>				
Access Control	SSID		1		·				
WPS									
Bandwidth Management	Note:					Add			
Airtime Fairness		stance is calculated by actual signal s	trength of device detected. Inaccuracy						
Advanced Setting									
Band Steering	3. Trademark	s and brand names are the propertie	is of their respective owners.						
AP Discovery									
Station List									
Station List - Advance									
Station List - Neighbor									
Parming									

These parameters are explained as follows:

Item	Description	
Station List	Displays wireless stations connected to the Vigor router.	
Add to Access Control	MAC - Enter the MAC address. SSID - Specify the number of SSID.	
Add	Click to add a new entry to Access Control.	

9.4.14.14 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 / Wireless LAN		
2.4G 5G	Roaming Type	Minimum_RSSI ~	
General	Minimum RSSI	-66	
SSID		60% (Default: -66 dBm)	
Security	Adjacent AP RSSI over	5	
Access Control		(Default: 5 dbm)	
WPS	AP-assisted Client Roaming Note: When AP detects that a station may ne	ed to roam, AP disconnects the station	
Bandwidth Management	 This feature helps those stations with tasticky to the original AP and with bad p 	bad roaming ability. Avoid the situation that a station is already close to the other AP but still	
Airtime Fairness	Please notice that RSSI Requirement m		
Advanced Setting	Minimum RSSI with Adjacent AP RSSI ove Disconnect clients with had signal to e	r X ncourage roaming only when they can have better signal through another DrayTek AP.	
Band Steering	All APs must be DrayTek APs which sup	port 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			
Roaming			
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.

9.4.14.15 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_001DAA00	00000 / Configuration / Wireless LAN				C
2.4G 5G	Index	SSID	Enable	Connect Time	Reconnect Time	
240 30	1	DrayTek	false	0 days:1 hours:0 min	1 days:0 hours:0 min	
General	2	DrayTek_Guest	false	0 days:1 hours:0 min	1 days:0 hours:0 min	
SSID	3		false	0 days:1 hours:0 min	1 days:0 hours:0 min	
Security	4		false	0 days:1 hours:0 min	1 days:0 hours:0 mIn	
Access Control						
WPS						
Bandwidth Management						
Airtime Fairness						
Advanced Setting						
Band Steering						
AP Discovery						
Station List						
Station List - Advance						
Station List - Neighbor						
Roaming						
Station Control						

To configure the station control settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

Index	1	
SSID	DrayTek	
Enable	0	
Connect Time	0 1 > 0 ~ days hours minutes	
Reconnect Time	1 o o days hours minutes	
Display All Station Control List Hotspot Web Portal		
Note: Once the feature is enabled,	the connection time quota will apply to each wireless client (identified by MAC address).	
		Cancel Save

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.	

9.4.15 Bandwidth Management

9.4.15.1 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 / Band	width Management	C
Sessions Limit	IPv4		
Bandwidth Limit	Enable		
APP QoS	Enable		
	Default Max Sessions	100	
	Limitation List	Index Start IP End IP Max Sessions	
		1 0.0.0.0 0.0.0.0 0	
		🗎 Clear All	
	IPv6		
	Enable		
	Default Max Sessions	100	
	Limitation List	Index Start IP End IP Max Sessions	
		1 0	
		10 Clear All	
	Administration Message		
	A designation Management		
	Administration Message (Max 255 characters)	You have reached the maximum number of permitted internet sessions sp-Please close one services are internet sets of the laboration to the second set of t	
		or more applications to allow further Internet access.cp=Contact your system administrator for turbute information.	
		う Reset to default	
		Car	ncel 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.

9.4.15.2 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 / Configuration / Band	2865ac_01DAA000000 / Configuration / Bandwidth Management C		
Sessions Limit	IPv4			
Bandwidth Limit				
APP QoS	Enable			
	IP Routed Subnet	\bigcirc		
	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 Each		
		1 None 0 0 Eac		
		di Clear All		
	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 Ead		
		會 Clear All		
			_	
		Cancel	Save	

ltem	Description			
	IPv4 / IPv6			
Enable	Click to enable or disable the bandwidth limit function. IP Routed Subnet - It is available for IPv4 only.			
Default TX Limit Per User	Set default upstream speed limit for each LAN client.			
Default RX Limit Per User	Set default downstream speed limit for each LAN client.			
Limitation List	Displays specific limitation entries. To add a new profile, click the last index number to open the setting page IPV4 Bandwidth Limitation List Add Entry By IP Range IP Object IP Group None IP Object Each or Shared TX Limit RX Limit Clear After finishing the settings, click Save. A new profile will be added and			

	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	on list.			
Allow user to use more bandwidth than the assigned	Click to enable or disable this f If enabled, it lets the router au downstream limits based on a	tomatically		upstream a	nd
Smart Bandwidth Limit	Click to enable or disable this f If enabled, it restricts the banc limitation list when the networ	width of L			
Apply the below limit to users not in	Enter the number of sessions Smart Bandwidth Limit activat		client is allo	wed to hav	e before
TX Limit	Upstream speed limit for each	LAN client	. Unit can b	e either Kbp	os or Mbp
RX Limit	Downstream speed limit for ea Mbps.	ach LAN cli	ent. Unit ca	n be either	Kbps or
	Time Schedule				
Schedule 1 ~ 4	Specify up to 4 time schedule of management.	entries to a	apply the ba	ndwidth lim	nit
Cancel	Discard current modification.				
Save	Save the current settings.				

9.4.15.3 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
Sessions Limit	APP QoS	
Bandwidth Limit		
APP QoS	Enable	
Traceable		
Untraceable		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
Sessions Limit	Index	Type Name	
Bandwidth Limit	1	Instant Message	
APP QoS	2	VoIP	
	3	Protocol	
Traceable	4	Tunneling	
Untraceable	5	Stream	
	6	Remote Control	
	7	Web HD	
	8	Game	
	9	Apple Services	
	10	Google Services	
	11	Amazon Services	
	12	E-Life	
	Note: Please remember to adjust inboun This will help QoS to work more eff	JOurbound bandwidth of your network in "Quality of Service". oberli.	

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 / Configuration	Bandwidth Man	agement		C
Sessions Limit Bandwidth Limit APP QoS Traccable	Index Type Name Select All Clear All	1 Instant M	tessage	Apply to att	
Untraceable	App Name	Enable	Version	Action	
	Facebook/Instagram	Ο		QoS Class 1 (High) ~	
	LINE	\bigcirc	5.23.0.2134	QoS Class 1 (High) ~	
	Linkedin	\bigcirc		QoS Class 1 (High) ~	
	Signal	\bigcirc	1.26.2	QoS Class 1 (High) \checkmark	
	Slack	\bigcirc	4.0.0	QoS Class 1 (High) ~	
	Snapchat	\bigcirc	10.79.5.0	QoS Class 1 (High) \checkmark	
	Telegram	\bigcirc	1.7.10	QoS Class 1 (High) ~	
	WhatsApp	\bigcirc	0.3.2848	QoS Class 1 (High) ~	
				Cancel	Save

These parameters are explained as follows:

Item	Description
Enable	Click to enable or disable the bandwidth limit function.
Action	Select a QoS class to be applied to the application.
Cancel	Discard current modification.
Save	Save the current settings.

Untraceable

Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

← Configuration	2865ac_001DAA000000 / Configuration /	Bandwidth Management	C
Sessions Limit Bandwidth Limit	Action	QoS Class 1 (High) ~	
	Index	Type Name	
APP QoS	1	Instant Message	
Traceable	2	VoIP	
Untraceable	3	P2P	
	4	Protocol	
	5	Tunneling	
	6	Stream	
	7	Remote Control	
	8	Web HD	
	Note: Please remember to adjust hibourd The will help QoS to work more effe	(Outbound bandwidth of your network in "Quality of Servico". Sent.	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 / Configuration	Ion / Bandwidth Management		
	Index	1		
Bandwidth Limit	Type Name	Instant Message		
APP QoS				
Traceable	Select All Clear All			
	App Name	Enable	Version	
	AIM Login	\bigcirc	8	
	AliWW	\bigcirc	2008	
	Ares	\bigcirc	2.0.9	
	BalduHI	\bigcirc	37378	
	Fetion	\bigcirc	2010	
	GaduGadu Protocol	\bigcirc		
	ICQ	\bigcirc	7	
	1SpQ	\bigcirc	8.0.60	
	кс	\bigcirc	2008	
	Paltalk	\bigcirc	9	
	PocoCall	\bigcirc	2007	
	Qnext	\bigcirc	3.0.1	
	Tencent QQ	\bigcirc	2012/2009 beta3	
				Cancel Save

These parameters are explained as follows:

ltem	Description
Enable	Click to enable or disable the bandwidth limit function.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.16 USB Applications

9.4.16.1 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 A	Application	C
General Settings	Simultaneous FTP Connections	5	
User Management	Default Charset	English	
Disk Status	SMB File Sharing Service	0	
Modem Status	Access Mode	LAN Only LAN And WAN	
Printer Status Sensor Status	Workgroup Name	WORKGROUP	
	Host Name	Vigor	
	Printer Server		
	limit client connections to 1 to improve per	I by Router FTP server. If your FTP client has a multi-connection mechanism, such as FIIeZIIIa, you should formance. The host name. The workgroup name can have up to 15 characters and the host name can have up to 15	ve

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.

9.4.16.2 User Management

This page allows you to set up profiles for FTP/SMB users.

← Configuration	2865ac_001DAA00	00000 / Configuration / USB	Application			Set to Factory Default	C
General Settings	Index	Username	FTP/SMB User	Home Folder	File Access Rule	Directory Access Rule	
	1		false				
User Management							_
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.

65ac_001DAA000000 / Configurat	tion / USB Application	Set to Factory Default	C
🗥 No USB disk Connected ! Please	Insert the disk.		
Index	1		
FTP/SMB User	\bigcirc		
Username	(Max. 11 characters allowed)		
Password	(Max. 11 characters allowed) $\hfill \Phi$		
Confirm Password	Φ		
Home Folder			
Create New Home Folder			
	+ Create		
Note: The folder name can only co	ntain the following characters: A-Z a-z 0-9 \$ % ' $@$ – ` ! () and space.		
Access Rule			
File	Read		
	Write		
Directory	List		
	Create		
D Clear		Cancel	Save

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.

9.4.16.3 Disk Status

This page displays the status information for the USB disk connecting to Vigor router.

← Configuration	2865ac_001DAA000000 / Configuration / USB	Application			C
General Settings	Connection Status	No Disk Connected			
User Management		Disconnect USB Disk			
Disk Status	Write Protect Status	NULL			
Modem Status	Disk Capacity	0 MB			
Printer Status	Free Capacity	0 MB			
Sensor Status		0 HD			
	 Single file size can be up to 4GB, which is 	aximum capacity is 500GB. If there are more then one pa			
	USB Disk Users Connected				
	Index Service	IP Address (Port)	Username	Drop	
	1				

These parameters are explained as follows:

Item	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.

9.4.16.4 Modem Status

General Settings		/ Configuration / USB Application			C
User Management	Index	Connection Status	Manufacturer	Model	
Temperature Sensor	2	No Modem Connected			
Disk Status					
Modem Status					
Printer Status					
Sensor Status					

Click the index number to open the following for viewing detailed information for parameter settings.

/ Configuration / USB Appli	cation	
Index	2	
Connection Status		
Manufacturer		
Model		
Revision		
Serial Number		
IMSI		
Signal Quality (CINR)		
RSSI Signal		
Hardware		
SIMPIN	۵	
Link Speed		

9.4.16.5 Printer Status

This page displays current status for the USB printer connecting to Vigor router managed by VigorACS 3.

← Configuration 2	865ac_001DAA000000 / C	onfiguration / USB Ap	oplication			C
General Settings	Connection Status		No Printer Connected			
User Management	Manufacturer		No Printer			
Disk Status	Model		No Printer			
Modern Status Printer Status	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	

9.4.16.6 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	oplication	C
General Settings	Connection Status	Thermometer Connected	
User Management	Manufacturer	RDing	
Disk Status	Product	TEMPerIFV3.4	
Modern Status		TENCET AT	
Printer Status Sensor Status			
Sensor Status			

9.4.17 System

9.4.17.1 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.

← Configuration	2865ac_001DAA000000 / Configuration / Syste	m	C
Maintenance	Configuration Backup		
Time Settings			
Admin Account	Backup Config	Backup	
Admin Local User	Restore Config	Last Config Local File Shared Folder	
SNMP Settings		Restore Now	
Management	Download Config	Download	
TR069 Settings			
SysLog Settings			
Mail Alert	Firmware Upgrade		
Internal Service User List			
Panel Control	Model Name	Vigor2865ac	
	Modem Firmware Version	(null)_STD	
	Firmware Version	4.2.2_RC1_STD	
	Choose a Firmware File From	Local File Shared Folder	
		Browse	
		Upgrade Now	
		Sav	e

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.

9.4.17.2 Time Settings

This page allows you to configure settings related to the system date and time.

← Configuration	2865ac_001DAA000000 / Configuration / Syste	em
Maintenance	Current System Time	2020-11-09T07:43:37
Time Settings	Local Time Zone	+00:00
Admin Account	Time Setup	Use_Browser_Time Use_Internet_Time
Admin Local User	NTP Server	pool.ntp.org
SNMP Settings	Priority	Auto
Management TR069 Settings	Time Zone	(GMT) Greenwich Mean Time : Dublin ~
SysLog Settings	Daylight Savings	Ο
Mail Alert	Daylight Saving Type	Default By Date By Weekday
Internal Service User List	Start	Yearly on March last Sun
Panel 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.		

9.4.17.3 Admin Account

This page allows you to set or change the administrator password.

← Configuration	2865ac_001DAA000000 / Configuration / System	m	C
Maintenance	Admin Account		
Time Settings	Admin Password	•	
Admin Account	() Note:		
Admin Local User	Password can contain only a-z A-Z 0-9 ,;:	."♥*+= ?@#^!()\$%&	
SNMP Settings	Enable 'admin' account login to Web UI from the		
Management	Internet		
TR069 Settings	Use only advanced authentication method for	\bigcirc	
SysLog Settings	Admin "WAN" login		
Mail Alert Internal Service User List	User Account		
Panel Control	Enable User Account		
	User Password	· ·	
	 Note: Password can contain a 2A 20.9.; :-*-*+=[2@#+]() Password can't be all asterisks(*). For example, ** or **** is lifegal, but *123** or **45* is OK. 		
	Login Greetings		
	Login Page Logo	Default	
	Enable Login Greetings	\bigcirc	
			Cancel Save

Item	Description
	Admin Account

Admin Password	Enter the new password.
Enable admin account	Click to enable or disable the function.
login to	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	Click to enable or disable the function.
authentication	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.

9.4.17.4 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	O / Configuration / System			
Maintenance	Local User	(D		
Time Settings		hentication method for Admin(\mathbb{D}		
Admin Account	"WAN" login				
Admin Local User	Local User List				
SNMP Settings					
Management	Index	Username	Password	Action	
TR069 Settings	1			+ Add	
SysLog Settings					
Mail Alert	Administrator LDA	IP Setting			
Internal Service User List	Enable LDAP/AD login f	or Admin users (
Panel Control	Note: If Local Use	er is enabled, you will need to	select 'admin' group when log into W	Veb UI.	

Item	Description			
Local User	Click to enable or disable the local user setting.			
Use only advanced authentication method for Admin "WAN" login	Advanced authentication method can offer a more secure network connection. Select to require mOTP or 2-step authentication when logging in from the WAN.			
Local User List	Index - Displays the index number of local user profile.			
	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.			
	Password			
	Confirm Passavord Confirm Passavord Cancel Snow			
	Note: * Mox.15 characters for Usermanne and Plassword Index - Displays the index number of the profile.			
	 Note: * More 15 characters for Usermanne and Paceword Index - Displays the index number of the profile. Username - Enter the name of the user profile. 			
	Note: * Mox.15 characters for Usermanne and Plassword Index - Displays the index number of the profile.			
	 Note: the list observations and Plasmont Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step 			
	 Note: • Mac.L5 characters for Usermanne and Paceword 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. 			
	 Note: • Note: 5 characters for Unservice and Pleased 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 			
	 Note: • Note: 5 character for the browned and Present 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	 Note: - Kort & Construction of Present 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. 			

9.4.17.5 SNMP Settings

This page allows you to configure settings for SNMP and SNMPv3 services.

← Configuration	2865ac_001DAA000000 / Configuration / System	em C	3
Maintenance	Enable SNMP Agent	O	
Time Settings	Enable SNMPV1 Agent		
Admin Account	Enable SNMPV2C Agent		
Admin Local User	Get Community	public	
SNMP Settings	Set Community	private	
Management	Secontinuity	private	
TR069 Settings	Trap Community	public	
SysLog Settings	Trap Timeout	10	
Mail Alert	Manager Host IP (IPv4)		
Internal Service User List	Manager Host IF (IF V4)		
Panel Control	Index 1: IP	0.0.0.0	
	Index 1: Subnet Mask	· ·	
	Index 2: IP	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 /	Click to enable or disable the SNMP function.
Enable SNMPV2C Agent	
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.

9.4.17.6 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	2865ac_001DAA000000 / Configuration / Syst	lem	C
Maintenance	Router Name	DrayTek	
Time Settings	Default:Disable Auto-Logout		
Admin Account	Enable Validation Code in Internet/LAN Access	0)	
Admin Local User		9	
SNMP Settings	Note: IE8 and below version does NOT support D	irayOS CAPTCHA auth code.	
Management			
TR069 Settings	Internet Access Control		
SysLog Settings	Allow management from the Internet	0	
Mail Alert	Domain name allowed		
Internal Service User List		FTP Server	
Panel Control		V HTTP Server	
		Enforce HTTPS Access	
		Z HTTPS Server	
		Telnet Server	
		Z TR069 Server	
		SSH Server	
		SNMP Server	
	Disable PING from the Internet		
	LAN Access Control		
		Sec	re

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 InternetClick to enable or disable the function.If enabled, it allows system administrators to login from the Internet 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 the	Click to enable or disable the function.		
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.		
Enable brute force login protection	Click to enable or disable the function. If enabled, any client trying to access into Internet via Vigor router will be asked for passing through user authentication.		

	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	Click to enable or disable the function.		
device	If enabled, the router will function as a slave device.		
Save	Save the current settings.		

9.4.17.7 TR069 Settings

CPE device supports the TR-069 standard for remote management by VigorACS.

	2865ac_001DAA000000 / Configuration / Sy	stem	
Maintenance	Primary		
Time Settings	Tr069 Enable		
Admin Account	ACS Server On	Internet	
dmin Local User	URL	http://192.168.105.120/ACSServer/services/ACSServ	
NMP Settings anagement		Acquire URL from DHCP option 43	
	Username	43 rd8	
SysLog Settings Mail Alert	Password	\$	
	Client Settings		
anel Control	Protocol	Http Https	
	Client URL	http://192.168.105.123:8069/cwm/CRN.html	
	Port	8069	
	Username	vigor	
	Password	Φ	
	Periodic Inform Settings		
	Enable Periodic Inform		

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.	

9.4.17.8 SysLog Settings

SysLog function is provided for users to monitor router.

← Configuration	2865ac_001DAA000000 / Configuration / System C		
Maintenance	Enable	•	
Time Settings	Syslog Save to	✓ Syslog Server □ USB Disk	
Admin Account	Maximum Syslog folder space	1 GB 🗸	
Admin Local User	Keep logging when Syslog folder is full (Overwrite	\bigcirc	
SNMP Settings	oldest logs)		
Management	Router Name	DrayTek	
TR069 Settings	Server IP Address		
SysLog Settings	Destination Port		
Mail Alert		514	
Internal Service User List	Mall Syslog	\odot	
Panel Control	Collect Syslog About	✓ Firewall Log	
		VPN Log	
		User Access Log / Hotspot User Information	
		VAN Log	
		Router/DSL Information	
		VILAN Log	
	Hote: • USB Syslog space is available from 256-10 • Mall Syslog cannot be activated uniters US • Mall Syslog Reature will send the Syslog will	B Disk is ticked for "Syslog Save to".	
		Save	

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.		

9.4.17.9 Mail Alert

This page allows to configure settings for Mail alert.

← Configuration	2865ac_001DAA000000 / Configuration / Syste	m	
Maintenance	Enable	0	
		Send A Test E-Mall	
	Interface	Any ~	
Admin Local User	SMTP Server		
SNMP Settings	SMTP Port	25	
lanagement	Mail To		
rR069 Settings	Sender Address		
SysLog Settings			
	Connection Security	Planintext ~	
	Note: • StartTLS : Accept using plain text if StartTL	S connection falled.	
	Force StartTLS : Stop if StartTLS connectio	h falled.	
	Authentication		
	Username		
	User Password	•	
	Enable E-Mail Alert	DoS Attack APPE	
		VPN Log DAPPE Signature	
		DebugLog	

ltem	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.		

9.4.17.10 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.

← Configuration	2865ac_001DAA000000 / Configuration / System					
Maintenance	Internal Servic	Internal Service User List				
Time Settings	Username	Ν	lothing selected ~			
Admin Account	Internal Services R	ADIUS				
Admin Local User						
SNMP Settings	Internal Services L	ocal8021 X				
Management						
TR069 Settings				Apply		
SysLog Settings	Note: • 1. Only the	user profiles which is enabled in User I	Management >> User Profile will be listed here.			
Mail Alert	• 2. If you en			change its authentication methods via <u>User Management >> User Profile.</u>		
Internal Service User List						
Panel Control						
	Index	Username	Internal Services RADIUS	Internal Services Local8021 X		
	3	marketing	false	false		
	4	test_1	false	false		

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.

9.4.17.11 Panel Control

This page allows you to customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

← Configuration	2865ac_001DAA00000 / Configuration / System C						
Maintenance	LED						
Time Settings		_					
Admin Account	Enable LED						
Admin Local User	Enable Sleep Mode	\bigcirc					
SNMP Settings	Turn off LED after (Minutes)	1					
Management	Button						
TR069 Settings	button						
SysLog Settings	Wireless						
Mail Alert	Factory Reset						
Internal Service User List	Note:						
Panel Control	Enable the Sleep Mode will make the fund	tions of "Wireless Button" and "Fa	ctory Reset Button" on the front panel as below:		_		
	LED Status		LED On	LED Off			
	Wireless Button		Ireless On/Off/WPS				
	Factory Reset Button	Press till the	nd: Turn LED off Immediately* ACT light flashing: Reset router	Turn LED On*			
	*Still functional even the buttons are disa	bled.					
	USB						
	Index	Enable	Status				
	1		No Device				
	2		No Device				
					Cancel Sa	ve	

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.

9.4.18 Switch

9.4.18.1 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

		/ Configuratio	n / Switch							
tatus	Switch Status	Switch Hierarchy								
Profile	Status									
Vert And Log										
atabase Setup	Group	Switch Name	IP Address	MAC Address	Model	System Up Time	Port In Use	Clients	Firmware Version	
roup					No data available					
laintenance										
	New Switch List									
	+Add Device									
	Index	Switch Name	IP A	ddress	MAC Address		Model	ş	irmware Version	
	0 1	G2280	• 1	92.168.1.10	00:1D:AA:22:80	:AA	G2280	1	2.5.1_RC5	
	2	P2500	• 1	92.168.1.12	00:1D:AA:4C:18	:83	P2500	2	2.6.0_RC1	
		torSwitch model and firmwa G2260 V3.48, P1280 2.2.1, G		G2280 2.2.1, P2121 2.3.2, G	2121 2.4.3, P1092 1.04.05, C	51080 1.04.05., G1085 i	2.4.3, P1085 2.4.3			
	IP •	Sear	ch							

ltem	Description									
Status	Displays the switch which is managed by Viogr router.									
	Group - Displays the name link of the group. You can click the link to modify the group settings if required.									
	Switch Name - Displays the name link of VigorSwitch. You can click the name link to access into the switch profile.									
	IP Address - Di									
	MAC Address		-		٦.					
	Model - Displa			-						
	System Up Tim powered up.	-	-		this Vigorwi	tch is				
	Port in Use - D	isplays how	manv devices o	connected to \	/igorSwitch.					
	Clients - Displa		-		-					
	Firmware Vers	-	-	-		currer				
	used.				0					
New Switch List	The one under	New Switch	List is allowed	to be manage	ed under cui	rrent				
	used group.									
	+Add Device -		-	itch to be man	aged by Vig	or				
	router and be	snown unde	r Status.							
	Switch Status	Switch Hierarchy								
	Status									
	Group	Switch Name	IP Address	MAC Address Mod	el Sys	tem Up Time				
				N	o data available					
	New Switch List									
	+Add Device									
	Index	Switch Name	IP Address		MAC Address					
	2 1	G2280	• 192.16	8.1.10	00:1D:AA:22:80:AA					
	. 2	P2500	• 192.16	8.1.12	00:1D:AA:4C:18:83					
	2 1	G2280 P2500	• 192.16 • 192.16 witch List and	8.1.10 8.1.12 click +Add Dev	00:1D:AA:22:80:AA 00:1D:AA:4C:18:83 Vice. Then, th	ne				
	Switch Status	Switch Hierarchy	1 3							
	Status	Sincernationality								
				MAC Address	Model					
	6 m m	Considerable Billions of	ID Adduces	MAC Address	Model					
	Group	Switch Name	IP Address	00-1d-aa-22-80-aa	62280	Sy				
	Group Default	Switch Name	IP Address 192.168.1.10 	00-1d-aa-22-80-aa	G2280	Sy:				
	Default			00-1d-aa-22-80-aa	G2280					
				00-1d-aa-22-80-aa	G2280					
	Default New Switch List +Add Device	62280	• 192.168.1.10			0::				
	Default New Switch List		● 192.168.1.10 192.168.1.10	00-1d-aa-22-80-aa	G2280 MAC Addret	0::				

	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.

Status	/ Configuration / Switch	ß
Profile	Switch Status Switch Hierarchy	
Alert And Log	PI	
Database Setup Group	Vigor/switch G2280 1 192.1643.100 ©2280	
Maintenance	P2	
	P3	
	P4	
	PS	

9.4.18.2 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	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	itch List					
	+Add D	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				
DeleteClick to remove the selected entry from the profile list.					
Check box	Click to select the device.				
Index	Displays the index number of the switch profile.				
Name	Displays the name of the switch profile.				
Group	Displays the group name of VigorSwitch(es).				
IP Address	Displays the IP address of VigorSwitch.				

MAC Address	Displays the MAC address of VigorSwitch.					
Model	Displays the model name of VigorSwitch.					
	New Switch List					
+Add Device	Make the selected VigorSwitch to be managed by Vigor router and be shown under Profile List.					
Index	Displays the index number of the switch device.					
Switch Name	Displays the name of the switch.					
IP Address	Displays the IP address of VigorSwitch.					
MAC Address	Displays the MAC address of VigorSwitch.					
Model	Displays the model name of VigorSwitch.					
Firmware Version	Displays the firmware version that VigorSwitch current used.					

To edit profile for the selected switch:

1. Selecting one device from the Profile List. Click on the entry to open the following page.

witch 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	•••••	٩	
IP Address	DHCP 192.168.1.10		
Set General to Factory Default			

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

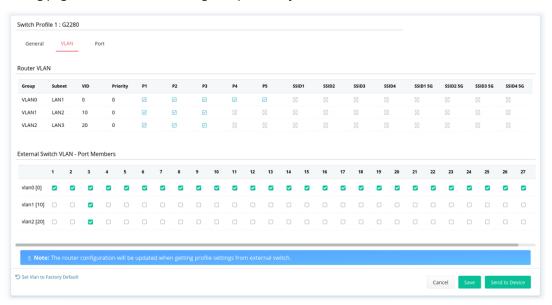
	router, then such field is unavailable.
Login Password	Displays the original login password for the VigorSwitch.
IP Address	Display the dynamic IP address (of the connected switch) assigned by Vigor router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.
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:

	General VLAN Port																											
Router VL/	Router VLAN																											
Group	Sub	net	vi	>	P	riority	P	1		P2	P3		P4	P	5	SSID1		SSID2	551	D3	SSID4		SSID1 5G	SSI	2 5G	SSID3 50	i s	1D4 5G
														No d	lata avai	lable												
External S	witch	VLAN	- Por	t Men	nbers																							
	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
														No d	lata avai	lable												
§ Not	e: The	e route	er col	nfigur	ation	will b	e upd	ated v	vhen	getting	profile	settin	gs from	extern	al swite	:h.												
つ Set Vian to																												

Setting page with LAN>>VLAN configured previously:



General VLAN Port	-			
ort Description	Port Control	Schedule	Ingress Rate (Kbps)	Engress Rate (Kbps)
	Enable Port	•	0	0
	Enable Port	· 0 , 0	•	0
	Enable Port	• 0 , 0	•	0
Uplink	Enable Port	• 0 , 0	0	0
	Enable Port	• 0 , 0	•	0
	Disable Port	• 0 , 0	•	0
	By Schedule	• 0 , 0	•	0
	Enable Port	• 0 , 0	•	0
	Enable Port	• 0 , 0	•	0
	Enable Port	• 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.

9.4.18.3 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.

← Configuration			0000 / Configuration / Switch											
Status	Enab	Enable Alert and Log												
Profile														
	Alert	Levels and	Action											
Switch and Port Setup	Index	Enable	Level Name	Color	Create Log	Send Notification	Object 1	Object 2	Object 3	Object 4				
	1	<	No Alert	No Color	No Log	No Notification								
Database Setup	2		Minor Alert		Enable	No Notification								
	3	✓	Moderate Alert	000			sms 1-Local nu $ imes $	sms 1-Local nu $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	sms 1-Local nu $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	sms 1-Local nu				
Maintenance	4		Major Alert	000			sms 1-Local nu 👻	sms 1-Local nu $ imes $	sms 1-Local nu 🗸	sms 1-Local nu				
	5			000			sms 1-Local nu $ imes $	sms 1-Local nu $ \sim $	sms 1-Local nu 🗸	sms 1-Local nu				
	6			000			sms 1-Local nu ${\scriptstyle \lor}$	sms 1-Local nu $ \sim $	sms 1-Local nu $ \sim $	sms 1-Local nu				
	7			0 00			sms 1-Local nu $ \smallsetminus $	sms 1-Local nu $ \sim $	sms 1-Local nu $ \sim $	sms 1-Local nu				
	8			⊘ ○○			sms 1-Local nu $ imes $	sms 1-Local nu $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	sms 1-Local nu $ imes $	sms 1-Local nu				
										_				
	් Set	to Factory Defa	ult											

ltem	Description										
Enable Alert and Log	Click to enable or disable the function.										
	Enable Alert and Log										
	Index Enable Level Name	Color Create Log	Send Notification	Object 1	Object 2	Object 3	Object 4				
	1 No Alert	No Color No Log	No Notification								
	2 Minor Alert	🧼 🛛 🖾 Enable	No Notification								
	3 Moderate Alert			sms 1-??? •	sms 1-??? •	sms 1-???	• sms 1-??? •				
	4 🖸 Major Alert			sms 1-??? *	sms 1-??? •	sms 1-???	• sms 1-??? •				
	Alert Levels and Action	I									
Index	Displays the index num	Displays the index number of alert profile.									
Enable	Check it to enable this	Check it to enable this feature.									
Level Name	names for index 1 to in	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 ea color and unable to be		llert. Ho	wever,	the colo	or of in	dex 1 is No				
Create Log	Check the box to creat page. Note that No Log default.										
Send Notification	If it is checked, Vigor ro phone number via SMS	-	em will s	end not	tificatio	n to sp	ecified				
Object 1 ~ 4	Select the SMS object v objects can be selected	-		/IS from	Nigor I	router.	Up to 4				
Save	Save the current settin										

Switch and Port Setup

This page defines enabling switch alert and/or port alert for each switch.

Status	 / Configuration / Switch								
	Index	Switch Name		IP Address		lodel	Switch Alert		Port Alert
	1	G2280		192.168.1.10		52280	Enable		Enable
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
1	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻	1-No Alert
2	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻	1-No Alert
Set to Factory Default				

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	/ Configura	/ Configuration / Switch										
Profile	Select Columns to Filter Logs				~							
Alert And Log	Level											
Alert Setup Switch and Port Setup	Туре	Switch Alert	Port Alert									
Aleri Logs	Switch		*									
Database Setup	Time Period	Last 24 Hours	ast 7 Days									
Group												
Maintenance					Apply							
	Alert Logs											
	OLogs					N < 1 /0	> 11					
	Index 👌 Level Name	Ut Time Ut	Туре	41 Switch	.↓↑ Port	4† Incident	ψŢ					
			No da	sta available								

These parameters are explained as follows:

ltem	Description
Select Columns toLevel – The alert can be divided into several levels, Minor Alert, IFilter LogsAlert and Major Alert. Check the one(s) you want to check in Alert	
	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.

9.4.18.4 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 / Swit	2865ac_001DAA000000 / Configuration / Switch	
Status Profile	Enable Database to Record alert logs and traffic history	٥	
Alert And Log	File Path	No USB Disk Detected	
	Database Usage	N/A	
Group	Notification	Send notification \sim	
Maintenance	Email Notification Object	1-Mail_Notify ~	
	SMS Notification Object	1-Local number v	
	Action	Stop recording user Information \vee	
		Stop recording user information Backup and clean up all user info, and start a new	w record
			S
	· · · · · · · · · · · · · · · · · · ·		

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.

9.4.18.5 Group

Different switches can be classified into different group(s). There are ten switch groups available for configuration.

← Configuration	2865ac_0	865ac_001DAA000000 / Configuration / Switch C		C
	Index	Group Name	Member Switch	
Status	1	Default		
Profile	2			
Alert And Log	3			
	4			
Database Setup	5			
Group	6			
Maintenance	7			
	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 / Swi	ch	C
Index	1	
Profile Name	Default	
Enable Group Password	0	
Group Password	۵	
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.

9.4.18.6 Maintenance

This page is able to execute configuration backup, restore, reboot or reset the VigorSwitch devices remotely.

← Configuration	2865ac_001DAA000000 / Configuration / S	witch			C
Status	Action Type	Config Backup	~		
Profile Alert And Log	Select Device				
Database Setup	Switch Name	MAC	IP	Download Config	
Group Malittenance	G2280	00-1d-aa-22-80-aa	192.168.1.10	۵	
					Save

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 Name	Displays the name of the switch.	
MAC	Displays the MAC address of the switch.	
IP	Displays the IP address of the switch.	
Download Config	Click to download the configuration file and store on the host.	
Save	Save the current settings.	

9.5 Advanced

(7)	Advanced	
000	Parameter Tree	
	Exclude Parameters	
-0-	Common UI Status	
~~	Test Inform	
5.		

9.5.1 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.

Dray Tek VigorACS 3	2927Lac_1449BC023768 V Q	Pcap	mk_carrie M
2927Lac_1449BC023768 / Advanced / Parameter Tree			C
Name		Value	DataType
▲ 📀 InternetGatewayDevice.			
LANDeviceNumberOfEntries		9	
WANDeviceNumberOfEntries		6	
DeviceInfo.			
ManagementServer.			
> 🐼 Time.			
Average State S			
ANDEvice.			
WANDevice.			
▷ 🐼 X_00507F_InternetAcc.			
▷ 🐼 X_00507F_LAN.			
X_00507F_LoadBalancePolicyNumberOfEntries		3	
X_00507F_LoadBalancePolicy.			
▷ 🐼 X_00507F_NAT.			
▷			
▷ 🐼 X_00507F_Bandwidth.			
X_00507F_Applications.			
▷ 🛇 X_00507F_VPN.			
▷ S X_00507F_WirelessLAN.			
			⊠ 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.	

9.5.2 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.

Dray Tek VigorACS 3	2927Lac_1449BC023768 ∨ Q	Pcap	
2927Lac_1449BC023768 / Advanced / Exclude Parameters			C
Delete All			
Parameter			
InternetGatewayDevice.X_00507F_Status.CPUTemperature			
$InternetGatewayDevice. X_00507 F_Status. MonitoringDevicesStatistics. ClientStatus Status S$	iG2.Client.		
InternetGatewayDevice.ManagementServer.AliasBasedAddressing			
InternetGatewayDevice.ManagementServer.InstanceWildcardsSupported			
InternetGatewayDevice.X_00507F_VPN.ConnStatusNumberOfEntries			
InternetGatewayDevice.X_00507F_MaxNumberOfLoadBalancePolicy			
InternetGatewayDevice.X_00507F_InternetAcc.MultiPVCs.General.{x}.WAN.{y}.			
$InternetGatewayDevice. X_00507F_InternetAcc. WAN. \{x\}. InternetPhysicalType$			
InternetGatewayDevice.X_00507F_InternetAcc.WAN.{x}.MTU			
InternetGatewayDevice.X_00507F_LTE.LTEStatus.ModemICCID1			
InternetGatewayDevice.X_00507F_LTE.LTEStatus.ModemICCID2			
InternetGatewayDevice.X_00507F_Operation_Mode_AP			
InternetGatewayDevice.X_00507F_VPN.ConnStatus.{x}.Phs2NetworkId			
InternetGatewayDevice.X_00507F_WirelessLAN.General.LongPreamble			
InternetGatewayDevice.X_00507F_WirelessLAN_AP.General.ModeList			
InternetGatewayDevice.X_00507F_WirelessLAN_5G.General.TxBurst			
InternetGatewayDevice.X_00507F_WirelessLAN_5G_AP.General.ModeList			
InternetGatewayDevice.X_00507F_USBApplication.DeviceStatus.Modem.{x}.S	SignalStrength		
InternetGatewayDevice.X_00507F_WirelessLAN.General.SSID.{x}.RateCtrl			
InternetGatewayDevice.X_00507F_WirelessLAN.General.SSID.{x}.Upload			
InternetGatewayDevice.X_00507F_WirelessLAN.General.SSID.{x}.Download			
InternetGatewayDevice.X_00507F_WirelessLAN_5G.General.SSID.{x}.RateCtrl			
InternetGatewayDevice.X_00507F_WirelessLAN_5G.General.SSID.{x}.Upload			
InternetGatewayDevice.X_00507F_WirelessLAN_5G.General.SSID.{x}.Downloa	ad		
$InternetGatewayDevice. WANDevice. \{x\}. WANCommonInterfaceConfig. WANInfNetWorkEnd Config. WANINforWorkEnd Config. WANINforWorkEnd Config. Config$	Name		

Item	Description
Delete All	Click to remove all parameters listed in this page.

9.5.3 Common UI Status

This page allows the user to check if the UI file has been uploaded to VigorACS. If not, the VigorACS server can send a command to the CPE to prompt the upload of the UI file to VigorACS.

Dray Tek VigorACS 3	2927Lac_1449BC023768 V	٩	Pcap	16:33:14 8/5/24	mk_carrie System Administrator	М
2927Lac_1449BC023768 / Advanced /	Common UI Status					C
Device Name	2927Lac_1449BC023768					
Model Name	Vigor2927Lac					
Firmware	4.4.2.3					
TR069 Support Status	Firmware Version is not supported					
	Upload Common UI File					

These parameters are explained as follows:

ltem	Description
Upload Common Ul File	Click to request the selected CPE to upload the UI file to VigorACS. Once completed, the corresponding settings will be displayed on this page.

9.5.4 Test Inform

To test the bidirectional connection between the selected CPE and the VigorACS server, click on **Scan Test**.

Later the test result will be shown below.

Dray Tek VigorACS 3	2927Lac_1449BC023768	✓ Q	Pcap	¢	16:38:06 8/5/24	mk_carrie System Administrator	М
2927Lac_1449BC023768 / Advanced / Test Inform							C
	Device Name	2927Lac_1449BC023768					
	Model Name	Vigor2927Lac					
	FIrmware	4.4.2.3					
		Start Test					
	1 2						

Dray Tek VigorACS 3	2927Lac_1449BC023768	✓ Q	Pcap 🗘	16:56:01 8/5/24	mk_carrie System Administrator	М
2927Lac_1449BC023768 / Advanced / Test In	form					C
	Device Name	2927Lac_1449BC023768				
	Model Name	Vigor2927Lac				
	FIrmware	4.4.2.3				
		Start Test				
	[16:53:53] (INFO) Step 1 ≫ [16:53:55] (INFO) ACS GET http://192.168.106.140.8069) [16:53:55] (INFO) Step 2 ≫ [16:53:55] (INFO) CPF Response HTTP/1.1 200 OK [16:53:54] (INFO) CPF Response HTTP/1.1 200 OK [16:53:54] (INFO) CPF Response HTTP/1.1 200 OK [16:53:54] (INFO) CPF Response HTTP/1.1 200 OK [16:53:56] (INFO) - InternetGatewayDevice. DeviceInfo.b [16:53:55] (INFO) - InternetGateway	tewayDevice.DeviceInfo. Ianufacturere DrayTek IanufacturereOU = 14499C IodelName = Vigor2927Lac escription = DrayTek Nigor Nouter orducClass = Vigor2927Lac erialNumber = 1449EC023768 ardwardeVersion = 4 OftwardeVersion = 4 OftwardeVersion = A OftwardeVersion = A.0.3 DefemFirmwardeVersion = No DSL pecVersion = 1.0 rovisioningCode = pTime = 4238 UI = 14498C				
	316:53:56 [INFO] - InternetGatewayDevice.DeviceInfoX 516:53:56 [INFO] - InternetGatewayDevice.DeviceInfoX 516:53:56 [INFO] - InternetGatewayDevice.DeviceInfoX 516:53:56 [INFO] - InternetGatewayDevice.DeviceInfoX 516:53:56 [INFO] - InternetGatewayDevice.DeviceInfoX	_00507F_ManagementPassword = uthKey = 7a23bb887f2e4ac4a147c92005ee0cee _00507F_ManagementTeInetTimeout = 300 _00507F_ManagementSSHTimeout = 180				

This page is left blank.

Chapter 10 DrayTek Chatbot

DrayTek chatbot server offers a platform for the user account to check general information of the VigorACS server through the web-based browser.

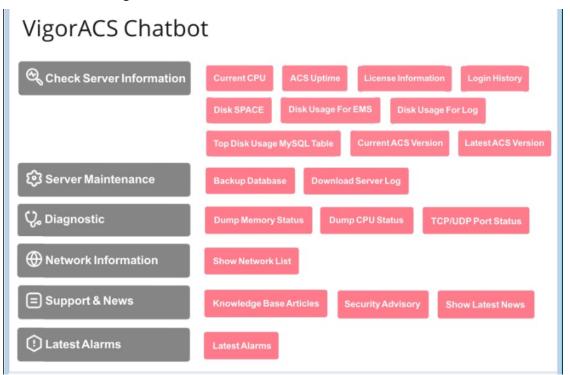
10.1 Installation

DrayTek Chatbot will be installed in accompany by VigorACS software, refer to the section **2.1.3 Installation for VigorACS 3** for detailed information.

10.2 Overview

Login DrayTek Chatbot by entering the URL "https://(domain name or IP address):18443" on a web browser. Note that the port number defined for Chatbot is 18443.

Later, enter the user-defined user name and the password used for login VigorACS server. If not, use the default username/password (root/admin123) to login DrayTek Chatbot.



The main screen of VigorACS Chatbot will be shown as follows:

Menu Items	Submenu
Check Server Information	 Click the category to display the following submenu for viewing the server information. Current CPU ACS Uptime License Information

	Login History
	Disk SPACE
	 Disk Usage For EMS
	 Disk Usage For Log
	 Top Disk Usage MySQL Table
	Current ACS Version
	Latest ACS Version
Server Maintenance	Click this item to display the history/log of Previous server maintenance. Backup Database
	 Download Server Log
Diagnostic	Click this item to display the result of the diagnostic.
	Dump Memory Status
	Dump CPU Status
	TCP/UDP Port Status
Network Information	Click this item to display information on the current network list.
	Show Network List
Support & News	Click this item to get the news related to the VigorACS server.
	Knowledge Base Articles
	Security Advisory
	Show Latest News
Latest Alarms	This item will list the latest alarms related to VigorACS and/or CPE devices.
	Latest Alarms