

DrayTek Training

VigorACS 2 – Features and Benefits

Roy Panetta

Table of Contents

Course Outline	5
1. What is VigorACS 2.....	7
1.1 VigorACS 2 Highlights.....	8
1.2 Video Demonstration.....	8
1.3 Benefits of VigorACS 2	9
1.3.1 Time and Cost Saving Examples for VigorACS 2.....	9
1.4 Supported Devices List.....	10
1.5 Minimum System Requirements	11
2. How does VigorACS 2 Work	12
2.1 Terminology	12
2.2 TR-069 Communication Process	12
2.2.1 Provisioning Session Steps	13
3. VigorACS 2 Features.....	14
3.1 Auto Provisioning.....	14
3.2 Real-Time Monitoring	14
3.3 Device Maintenance	15
3.4 AP Management	16
3.5 VPN Wizard	16
3.6 Alarm & Log Management.....	17
3.7 Reports.....	18
3.8 User Management	19
User Management.....	19
3.9 RWD Design.....	19
4. Getting Started with VigorACS 2.....	20
4.1 Logging into VigorACS 2 web page.	20
4.2 Logging out from VigorACS 2 Web Page	22
4.2 VigorACS 2 Menu Options.....	23
4.2.1 Network Menu	24
4.2.1.1 Dashboard Menu	24
4.2.1.2 Statistics Menu	25
4.2.1.3 Monitoring Menu.....	26
4.2.1.3 Configuration Menu	30
4.2.2 System Menu	31

4.2.2.1 Maintenance Menu.....	31
4.2.2.2 Report Menu	32
4.2.2.3 Provisioning Menu	33
4.2.2.4 Network Management Menu	35
4.2.2.5 System Menu	36
4.2.2.6 User Menu.....	37
User Management.....	37
4.2.2.7 About Menu	37
5. Configuring CPE Devices	38
5.1 Default TR069 Settings.....	38
5.2 Linux based routers.....	40
5.3 Vigor DrayOS routers	41
6. Exercise – Part 1: Register CPE devices to ACS 2	44
6.1 Video Demonstration	44
6.2 Preliminary Configuration	44
6.2.1 Configure Router LAN	45
6.2.2 Configure Access Point LAN.....	48
6.2.3 Configure Router WAN Interfaces	49
6.3 Log into VigorACS Server	51
6.4 Register CPE Devices to VigorACS 2	52
6.4.1 Register DrayTek Routers.....	52
Step 1 – Enable TR069 Server	52
Step 2 – Configure TR069.....	52
Step 3 – Configure CPE Client Settings.....	53
Step 4 – Enable STUN Settings if Required.	54
6.4.2 Register DrayTek Access Point to ACS 2.....	55
6.4.3 Verify that CPE devices have Registered to ACS 2	58
7. Exercise – Part 2: Managing CPE Devices in VigorACS 2	59
7.1 Google Maps Key (Optional)	59
7.2 Creating Networks in ACS 2	61
7.2.1 Create Training Lab Network	61
7.2.2 Create Brisbane Office Network	62
7.3 Move CPE Devices into the Networks.....	63
8. Exercise – Part 3: Create VPN Tunnels Using VigorACS 2	66

8.1 Create VPN tunnel Between Vigor2862Lac and Vigor2926 Router	66
8.2 Check VPN tunnel Configuration in the Routers.....	71
8.2.1 Vigor2862Lac Router VPN Status.....	71
8.2.1 Vigor2926 Router VPN Status	72
9. Exercise – Part 4: Generate Reports in VigorACS 2.....	73
Appendix	76

(Blank)

Course Outline

- What is VigorACS 2
 - Video Demonstration
 - Benefits of using VigorACS 2
 - System Requirements
- How does VigorACS 2 Work
- VigorACS 2 Features
- Getting Started with VigorACS 2
 - Logging into VigorACS 2
 - Menu Options Overview
- CPE Configuration
- Exercises
 - Register CPE Devices
 - Managing CPE Devices
 - Create VPN tunnels using VPN Wizard
 - Creating Reports

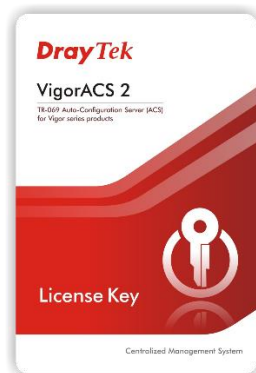
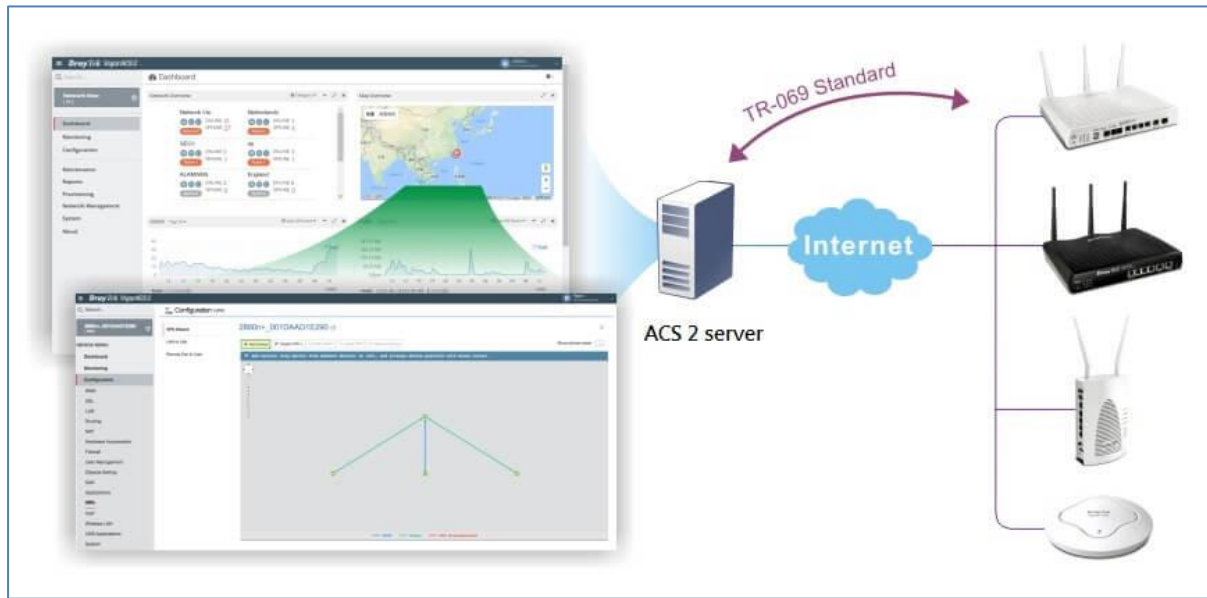
(Blank)

1. What is VigorACS 2

VigorACS 2 is a TR-069 based centralized management system for DrayTek Vigor devices.

With a user-friendly interface, it allows System Integrators or Network Administrators to configure, monitor and manage DrayTek devices remotely from the comfort of their offices or homes.

VigorACS 2 provides a user-friendly interface with a responsive display which automatically adjusts and arranges content to suit a variety of devices such as PC's, tablets or phones.



The software package is produced by DrayTek and licence keys are available from 25 nodes to 5,000 nodes.

1.1 VigorACS 2 Highlights

The list below summarises the key features for this Centralized Management System for DrayTek Vigor devices.

- Automatic remote service provisioning for DrayTek's Vigor devices
- Real-time Status Monitoring
- Scheduled firmware upgrades
- Device performance reporting and system logging
- Drag and drop VPN configuration wizard
- Flexible and secure CPE grouping
- Scheduled back-up and restore of configuration data
- TR-069 compliant
- AP & Wireless Management
- Responsive Web Design (RWD) enables viewing on various screen sizes

1.2 Video Demonstration

VPN tunnels are created quickly and easily by using VigorACS as shown in the video below:

Creating VPN tunnels using DrayTek VigorACS SI

This video is available on YouTube at the following URL:

<https://youtu.be/Lg1tG9jKbQk>



Note: This video is based on the earlier version of ACS (VigorACS SI), but VPN tunnel creation using the wizard is similar in VigorACS 2.

1.3 Benefits of VigorACS 2

There are many benefits of using VigorACS 2 for managing small to large networks. Service providers can offer dynamic services such as home networking that are centrally managed by ACS. Also support calls will be reduced since customer devices will be monitored and any issues can be resolved quickly before they become a major problem. A summary of the benefits includes:

- Time and cost savings for the businesses/organisations
- More reliable and secure networks
- Less travelling for network administrators
- Network alarm and report for better management decisions
- Customer satisfaction
- Extra income source for IT service providers

1.3.1 Time and Cost Saving Examples for VigorACS 2

There are many benefits that the VigorACS 2 can offer, two of these are time savings in creating multiple VPN tunnels and multiple firmware upgrades. The two tables below show the time and cost savings for creating VPN tunnels and firmware upgrade for 2 scenarios: one medium network with 20 nodes and one large network with 500 nodes. It compares the time taken to carry out the task manually to the time taken by using VigorACS 2. You can see that there is a substantial time saving which is reflected in cost savings.

Time and Cost Savings Creating Multiple VPN Tunnels

Network Size	20 nodes		500 nodes	
Method	On site	VigorASC 2	On site	VigorACS 2
Time usage per node	10 mins	0.5 mins	10 mins	0.5 mins
Total time usage	3 hrs & 20 mins	10 mins	83 hrs & 20 mins	4 hrs & 10 mins
Total time saved	3 hrs & 10 mins		79 hrs & 10 mins	
Cost Saving (assuming IT Admin's rate is \$150/hr)	\$475		\$11,875	

Time and Cost Savings Performing Multiple Firmware Upgrades

Network Size	20 nodes		500 nodes	
Method	On site	VigorASC 2	On site	VigorACS 2
Time usage per node	10 mins	0.25 mins	10 mins	0.25 mins
Total time usage	3 hrs & 20 mins	5 mins	83 hrs & 20 mins	2 hrs & 5 mins
Total time saved	3 hrs & 15 mins		81 hrs & 15 mins	
Cost Saving (assuming IT Admin's rate is \$150/hr)	\$488		\$12,188	

1.4 Supported Devices List

As at October 2018 the devices supported in VigorACS 2 are shown in the list below. More products will be added to the list in future updates.

Model	Firmware Version
Vigor2120	V3.8.6
Vigor2132	V3.8.0
Vigor2760	V3.8.2.3
Vigor2762	V3.8.8
Vigor2830	V3.6.8.7
Vigor2830v2	V3.8.1.2
Vigor2832	V3.8.7
Vigor2860	V3.8.9
Vigor2862	V3.8.9
Vigor2912	V3.8.6
Vigor2925	V3.8.9
Vigor2926	V3.8.9
Vigor2952	V3.8.9
Vigor3220	V3.8.9
VigorAP 710	V1.2.3
VigorAP 810	V1.2.3
VigorAP 900	V1.2.3
VigorAP 902	V1.2.3
VigorAP 910C	V1.2.3
Vigor1000	V1.5.4.2
Vigor2130	V1.5.4.2
Vigor2710	V3.6.9
Vigor2850	V3.6.8.6
Vigor2920	V3.6.9
Vigor3900	V1.4.0
Vigor2960	V1.4.0
Vigor300B	V1.4.0
Vigor130	V3.8.2
VigorSwitch P1280	V2.3.0
VigorSwitch G1280	V2.3.0
VigorSwitch P2280	V2.3.0
VigorSwitch G2280	V2.3.0

1.5 Minimum System Requirements

Server

	50 nodes	500 nodes	5K nodes	10K nodes	20K nodes
Operating System	Windows / Linux	Windows / Linux	Only Linux	Only Linux	Only Linux
Operating System Bits	64	64	64	64	64
CPU	Intel Core i3-7300 Processor (4M Cache, 4.00 GHz, Cores: 2, Threads: 4)	Intel Core i7-7700K Processor (8M Cache, 4.2 GHz, Cores: 4, Threads: 8) Intel Xeon Processor E3-1280 V6 (8M Cache, 3.90 GHz, Cores: 4, Threads: 8) Intel Xeon Processor E3-1280 V6 (8M Cache, 3.90 GHz, Cores: 4, Threads: 8)	Intel Core i7-6850K Processor (15M Cache, 3.60 GHz, Cores: 6, Threads: 12) Intel Xeon Processor E5-1650 V4 (15M Cache, 3.60 GHz, Cores: 6, Threads: 12) Intel Xeon Processor E5-1650 V4 (15M Cache, 3.60 GHz, Cores: 6, Threads: 12)	Intel Xeon Processor E5-2687W V4 (30M Cache, 3.00 GHz, Cores: 12, Threads: 24)	Intel Xeon Processor E7-8894 v4 (60M Cache, 2.40 GHz, Cores: 24, Threads: 48)
Memory	3G	4G	8G	14G	20G
Storage	400G	4T	8T	14T	20T

Minimum memory requirement: 2GB for VigorACS 2.

(see <https://www.draytek.com/en/products/central-management/vigoracs-2/> on system requirements tab to get more details)

Client

- Firefox/Chrome/Opera/Safari/IE/Edge

Operating System

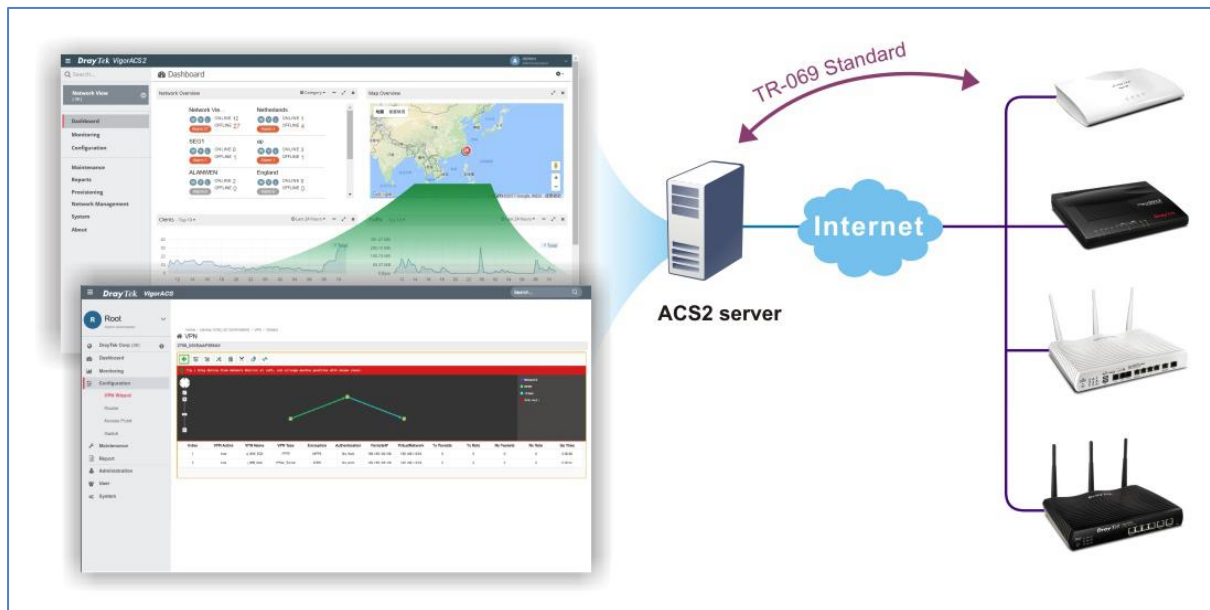
- 64-bit Microsoft Windows 7 / Windows 8 / Windows 10
- 64-bit openSUSE is recommended / Other Unix / Linux distribution version with OpenJDK / MariaDB (MySQL)

(For over 5,000 nodes it is recommended to use a Linux server).

2. How does VigorACS 2 Work

VigorACS 2 utilises the TR-069 Standard for communication between the ACS 2 server and the CPE devices. You can have any number of DrayTek devices on the Internet that can be managed by the ACS server.

TR-069 is an application layer protocol for remote management of end user devices. It was developed for automatic configuration of modems, routers, gateways, access points etc. by using an Auto Configuration Server.



2.1 Terminology

ACS - Auto Configuration Server - software that manages devices remotely.

CPE - Customer Premises Equipment - any equipment used by customers which can be managed by the ACS. CPE is commonly called a device.

Parameters Required for Communication Between the ACS server and the CPE Devices

- **ACS URL** - an Internet address of the ACS server.
- **Periodic Inform Interval** – The time period before the CPE device contacts the ACS server.
- **Username and password** – Used to authenticate the CPE device on the ACS server.

2.2 TR-069 Communication Process

The connection between the CPE device and the ACS 2 server is not permanent. The CPE device establishes the connection with the ACS only at specific points in time determined by the Periodic Inform Interval. It usually lasts several seconds exchanging all necessary messages between the CPE and the ACS 2 server. This short exchange of messages is called a provisioning session.

Note: The session can be started only by the CPE device. However, the ACS server can send a request to establish connection, that is Connection Request, which makes the CPE device contact the ACS server. This connection request is used when changes in the configuration have to be deployed immediately. Instead of waiting for the CPE device to connect, the ACS server can inform the CPE in advance of a need to connect to the server, and implement changes.

2.2.1 Provisioning Session Steps

- **Session initialization**

The session is always initialized by the device that connects to the ACS.

- **Authentication**

The ACS server must verify a username and a password provided by the device to continue the session.

- **Device identification**

Devices are identified on the basis of information sent during initialization of the provisioning session. Namely, a device's serial number and manufacturer's unique identifier that together constitute a main identifier of the device in the ACS. A MAC address is not used as the identifier but it is saved by the ACS, making it easier to find the device in the ACS GUI later on.

- **Tasks execution on the device**

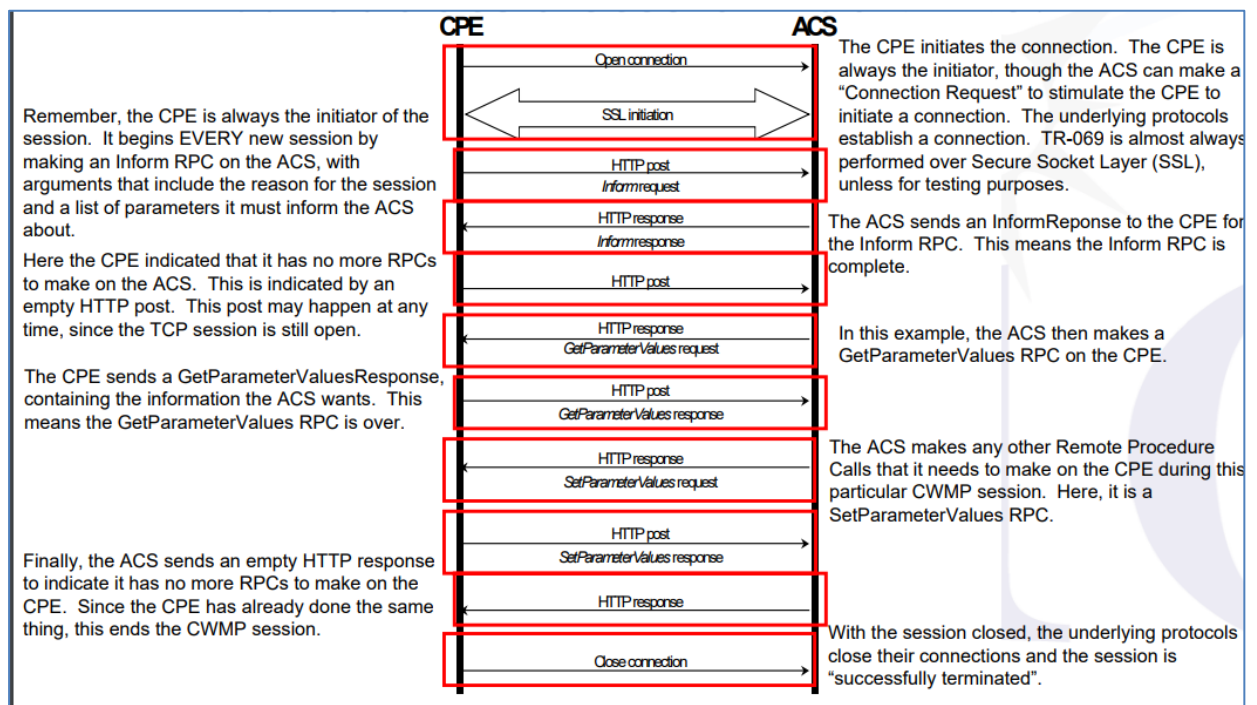
When the device is identified and its communication part ends, a key phase of the session starts - the ACS server orders various tasks on the device. These might include reading or saving parameters, performing diagnostics, rebooting or ordering file transfers.

- **Session closure**

When all planned tasks have been ordered, the CPE device closes the session. Any further tasks need the initialization of a new session.

The diagram below shows the process involved in a TR-069 session.

(Source: https://www.iol.unh.edu/sites/default/files/knowledgebase/hnc/TR-069_Crash_Course.pdf)



TR-069 Session

3. VigorACS 2 Features

3.1 Auto Provisioning

VigorACS 2 allows CPEs, when installed in remote networks, to receive pre-configured data such as IP, PPPoE, VoIP parameters, etc. from the ACS server.

Network administrators can schedule provisioning of new profiles, firmware upgrades or backup/restore configurations for selected CPE's to occur at specific times. Operations such as configuring VPN connections, VoIP settings, uploading new profiles, etc. can be scheduled to take place at the same time and in the same way as required.

Provisioning can be carried out per network group (Global Parameter), or per device (CPE Set Parameters). The "CPE Keep Parameter" feature restores configuration changes should they be accidentally removed by a network administrator.

Auto Provisioning reduces the cost of on-site support and ensures network uniformity.



3.2 Real-Time Monitoring

VigorACS 2, displays real-time information of CPE's including uptime, firmware version, resource usage, client number, etc.

In addition, error conditions such as lost connectivity of CPEs, WAN, LAN, and VPN connections will be highlighted on the dashboard. VigorACS 2 can also be configured to send notifications of the error conditions to the Network Administrator.

Logs generated by VigorACS 2 provide details of events executed including device name, MAC address, Device IP, Command Key, and time stamp for the event. Other events recorded in the logs include: file downloads, reboot, parameter changes, etc.

DrayTek VigorACS2 Livedemo System Administrator

Search...

Root Network (372)

NETWORK MENU

- Dashboard
- Monitoring
- Alarm
- Logs
- Configuration

SYSTEM MENU

- Maintenance
- Reports

Monitoring > Alarm

search No. / Device Name / MAC Time Interval : 2017/03/08 to 2017/04/07

Alarm 349 History

Export All Delete Delete All

No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message
77899	Not Ack	2017/04/07 10:14:37 AM	3900_001DAAA92508	001DAAA92508	Critical	Device Loss Connect
77898	Not Ack	2017/04/07 10:14:24 AM	2960_001DAAC08638	001DAAC08638	Critical	Device Loss Connect
77897	Not Ack	2017/04/07 10:14:18 AM	Mig			
77896	Not Ack	2017/04/07 10:14:17 AM	Tu			
77895	Not Ack	2017/04/07 10:14:15 AM	29			

Notification Options: Mail, SMS, Log

Real-Time Monitor

3.3 Device Maintenance

VigorACS 2 allows regular maintenance tasks such as firmware upgrades, configuration backups, restorations and device reboots to be automated and be carried out from a central console.

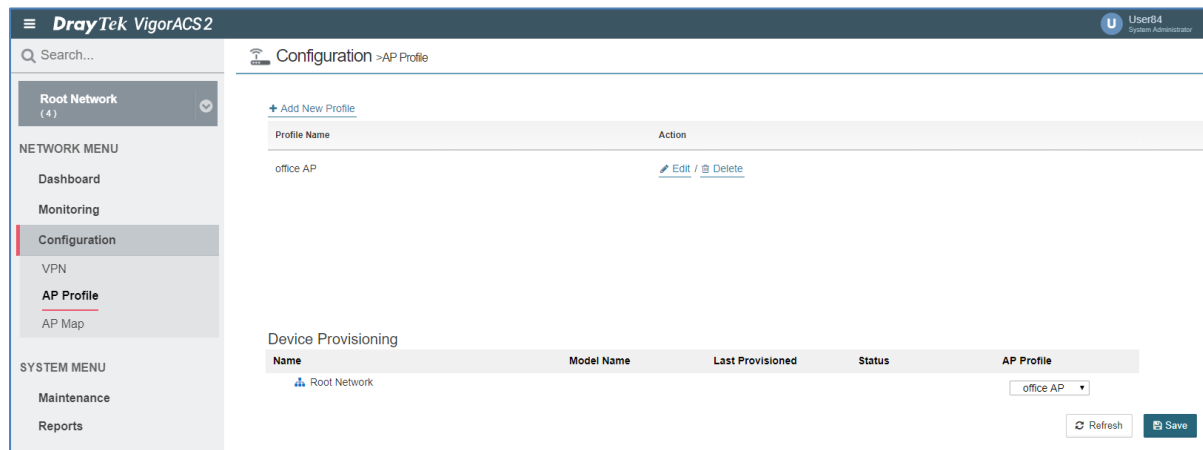
For example, firmware upgrades can be applied to a single device or a batch of devices. They can also be scheduled to start at a convenient time.

SYSTEM MENU

- Maintenance**
 - Scheduled Backup
 - Configuration Restore
 - Firmware Upgrade
 - Device Reboot
 - System Password Reset
 - Schedule Profile
 - File Manager

3.4 AP Management

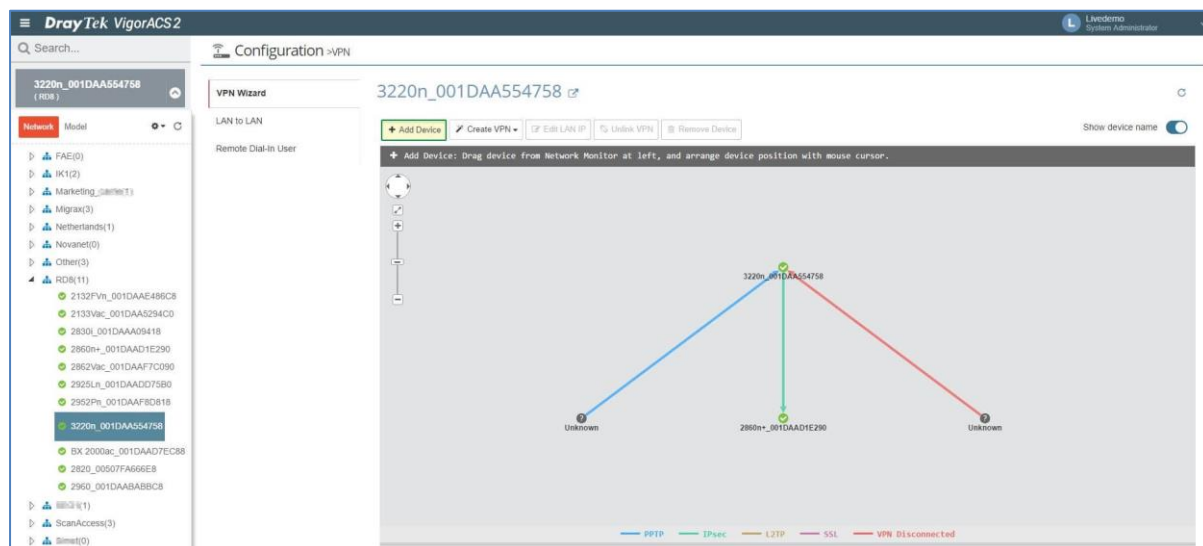
The AP management feature in VigorACS 2 allows monitoring and configuration of DrayTek Vigor access points. Access Point settings such as SSID, security, load balancing rules can be pre-configured into an AP profile, and be automatically applied to Vigor Access points that have joined the network. The AP Map function allows a floor plan to be uploaded to VigorACS 2 and APs placed on it. This is useful for mapping and placement of APs.



AP Management

3.5 VPN Wizard

VigorACS 2 provides an easy method to create VPN tunnels between two CPE's. Simply drag the icon of one CPE and drop it onto another to create a VPN tunnel between the two CPEs within seconds. Selectable options include the type and encryption method for the VPN tunnel.



VPN Wizard

3.6 Alarm & Log Management

VigorACS 2 records real time alarms and sends alert messages about fault conditions of all CPEs to specified phone or email accounts. The types of alarm reports include date, time, alarm type, level and acknowledge status. You can examine the alarm details and system logs to determine the nature of the faults, and hopefully clear them without leaving your place and racing to the sites.

A Log View page displays two types of information: Device Action and System status. The Device Action page lists network activity data of the CPEs such as download, reboot, parameters, objects added or deleted by VigorACS SI, etc. With these records, you can check what had happened to each CPE and when.

The System page displays the changes made to the CPEs by the VigorACS SI including network names, CPEs' names, CPEs' locations, etc.

No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type
140	Not Ack	2017/10/23 01:28:20 PM	AP 902_001DAA3D578A	001DAA3D578A	Critical	Device Loss Connection	Device Loss Connection
139	Not Ack	2017/10/23 01:28:18 PM	2925_001DAA564650	001DAA564650	Critical	Device Loss Connection	Device Loss Connection
130	Not Ack	2017/10/18 01:03:25 PM	2925_001DAA563920	001DAA563920	Critical	Device Loss Connection	Device Loss Connection
126	Not Ack	2017/10/17 05:18:01 PM	2860Ln_001DAA5B1800	001DAA5B1800	Critical	Device Loss Connection	Device Loss Connection

Alarms

ID	Device ID	MAC Address	Device IP	Action	Action ID	Time
4	AP 902_001DAA3D578A	001DAA3D578A	192.168.101.25	Inform	42	2017/10/23 12:55:16 PM
4	AP 902_001DAA3D578A	001DAA3D578A	192.168.1.2	Inform	41	2017/10/23 12:01:33 PM
40	AP 902_001DAA3D578A	001DAA3D578A	192.168.1.2	Inform	40	2017/10/23 11:42:00 AM
39	AP 902_001DAA3D578A	001DAA3D578A	192.168.1.2	Inform	39	2017/10/23 11:27:32 AM
38	2925_001DAA564650	001DAA564650	192.168.101.25	Inform	38	2017/10/23 11:27:18 AM
37	2925_001DAA563920	001DAA563920	192.168.101.26	Inform	37	2017/10/18 12:55:54 PM
36	2925_001DAA564650	001DAA564650	192.168.101.25	Inform	36	2017/10/18 12:54:55 PM

Logs Generated

3.7 Reports

VigorACS 2 provides a range of reports for network administrators to monitor traffic conditions and activities of all CPEs. These reports cover the following performance details:

- Device summary
- Status of CPEs
- LAN/WAN statistics & graphical charts
- Firmware versions
- CPE IP overview (LAN/WAN)



3.8 User Management

User Management provides 5 privilege levels for users to log into VigorACS 2. These are: System Administrator (the highest), Group Administrator, Administrator, Operator, and View Only Operator (the lowest). User accounts can also be assigned to a group and management authority for certain devices (by network) be assigned to a user group.

Five-level User Authority

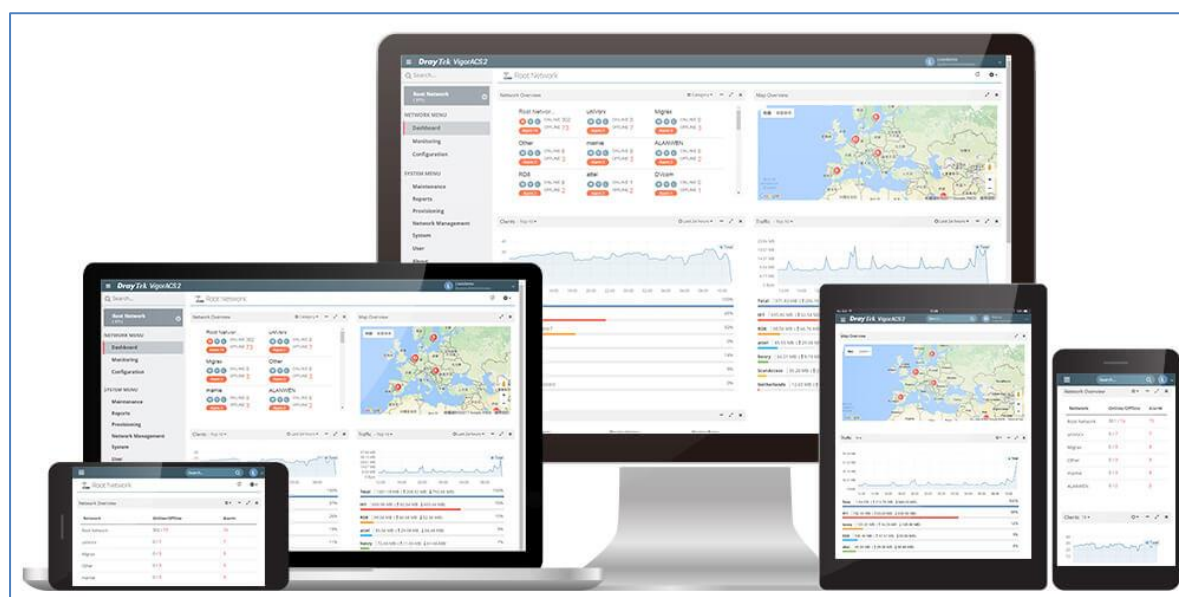
The screenshot shows the 'User Management' page in the DrayTek VigorACS2 web interface. On the left is a sidebar menu with options like Root Network, Maintenance, Reports, Provisioning, Network Management, System, and User. The 'User' section is expanded, showing 'User Management' as the active option. The main area displays a table of users with columns for Username, Role, Status, Mail Notify, SMS Notify, Email, Telephone, and Description. A pyramid diagram on the right illustrates the five privilege levels: System Administrator (top, blue), Group Administrator (green), Administrator (yellow), Operator (orange), and View only operator (bottom, red).

Username	Role	Status	Mail Notify	SMS Notify	Email	Telephone	Description
root	System Administrator	Active	✓	-	root@draytek.com		System Administrator
admin	Administrator	Active	-	-	admin@draytek.com		Administrator
Kevin	System Administrator	Active	✓	✓	kevin.draytek@draytek.com	+886 2 2345 6789	A test account
ga	Group Administrator	Active	-	-			
op	Operator	Active	-	-			
uitester	System Administrator	Active	-	-			UI Test
ap_sa	System Administrator	Active	-	-			
ap_admin	Administrator	Active	-	-			
ap_op	Operator	Active	-	-			
ap_gadmin	Group Administrator	Active	-	-			
ap_vop	View Only Operator	Active	-	-			
dni	View Only Operator	Active	-	-			
liveadmin	System Administrator	Active	-	-			

User Management

3.9 RWD Design

Responsive Web Design (RWD) enables viewing on various screen sizes, including PC's, tablets, smartphones etc. The screen display automatically adjusts to suit the size and type of screen used.



RWD Design

4. Getting Started with VigorACS 2

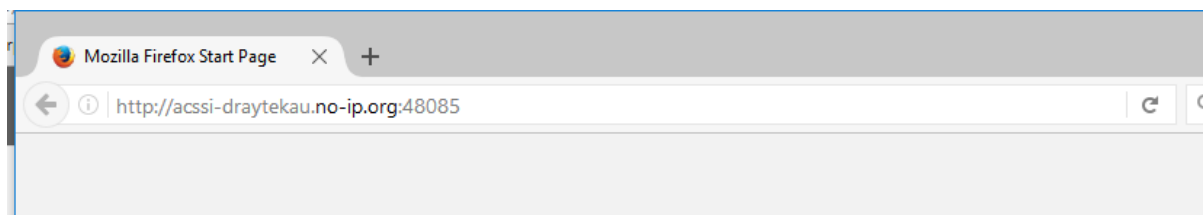
For this section we will go through how to use VigorACS 2 after it has been installed. For the exercises, we will be using a pre-installed version of VigorACS 2. Installation and configuration of the server will be covered in another course.

Note: Vigor ACS 2 version 2.2.2 will be used in this document.

4.1 Logging into VigorACS 2 web page.

To Log into VigorACS 2, 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 2. For example, if HTTPS is defined as 48085, then the URL will be “localhost:48085”.

For example, use the web browser to connect to: <http://acssi-draytekau.no-ip.org:48085>



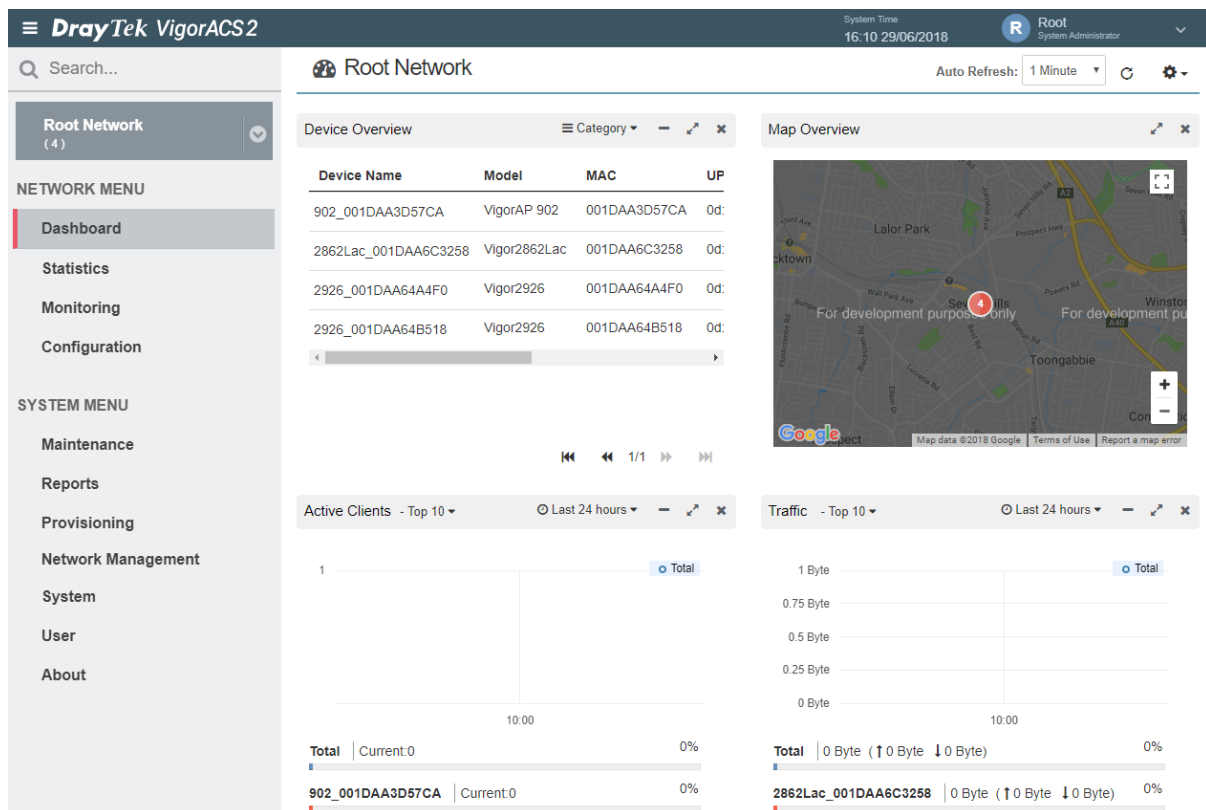
Enter the username, password and Validation code.

The default Username is “root”

Click on **Login** to access VigorACS 2

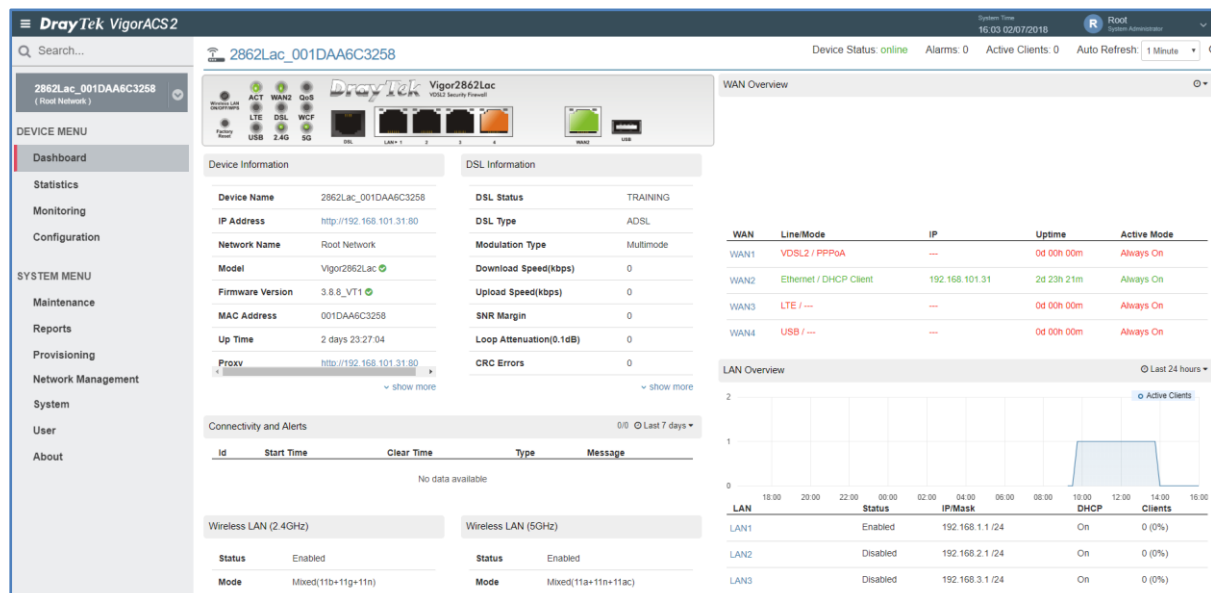
The diagram illustrates the login process for VigorACS 2. It shows two versions of the login page. The left page is the initial state with empty input fields: 'User Name', 'Password', and 'Validation Code'. A red 'Login' button is at the bottom. The right page shows the fields filled with the default credentials: 'root' for the username, a masked password for the password, and '6934' for the validation code. A blue arrow points from the left page to the right page, indicating the transition after login. Both pages have a copyright notice at the bottom: 'Copyright © 2017 DrayTek Corp. All Rights Reserved.'

After logging into VigorACS 2, you will be presented with the Dashboard view as shown in the diagram below:



Dashboard View - Alarm / traffic / clients status in one glance

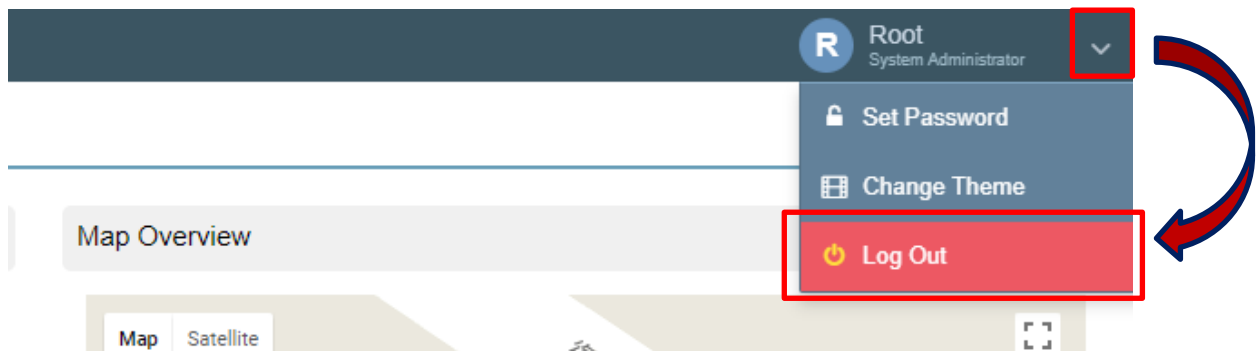
Selecting any CPE device gives the CPE view, which provides more detailed information and graphs to help you to understand the system status at a glance.



CPE View

4.2 Logging out from VigorACS 2 Web Page

To logout of ACS 2, click on pulldown menu at the top right corner of the page. Now click on the “**Log Out**” option.



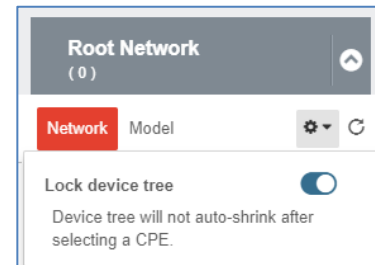
4.2 VigorACS 2 Menu Options

VigorACS 2 has two top level main menus. These are:

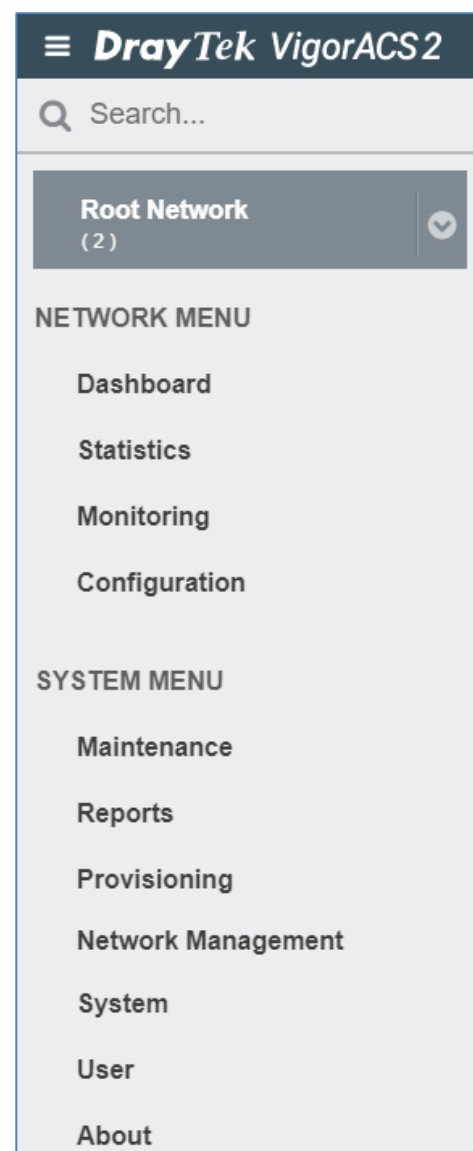
1. **Network Menu**
2. **System Menu**

Other menu options available are:

- Drop-down network tree by network/device filter.
- Lock device tree makes swapping between devices simpler.



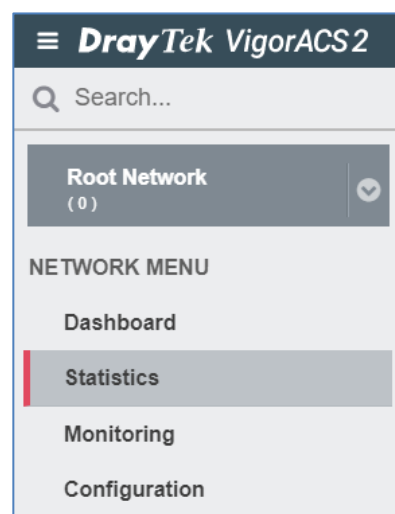
After logging into VigorACS 2 you will be presented with menu options at the left of the screen.



4.2.1 Network Menu

This menu has 4 sub menus:

- Dashboard
- Statistics
- Monitoring
- Configuration

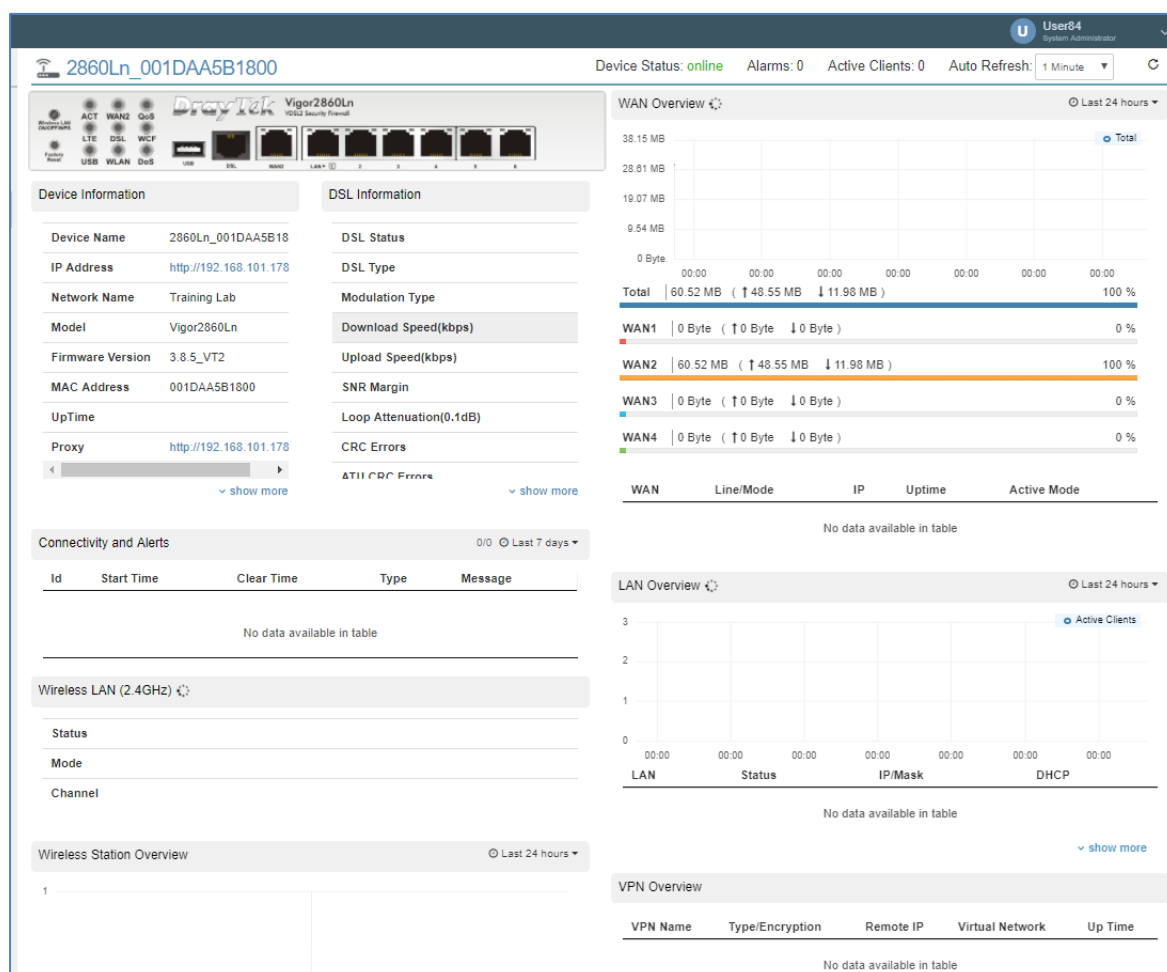


4.2.1.1 Dashboard Menu

The Dashboard menu provides detailed information on the status of a network of CPE devices.

For CPE devices Device information and DSL or WAN information are displayed.

Statistics are provided for WAN overview, LAN overview, VPN overview or Wi-Fi activity. The details presented will vary by the type of CPE device being managed.



Additional shortcuts are also available here for CPE configuration backup and restore

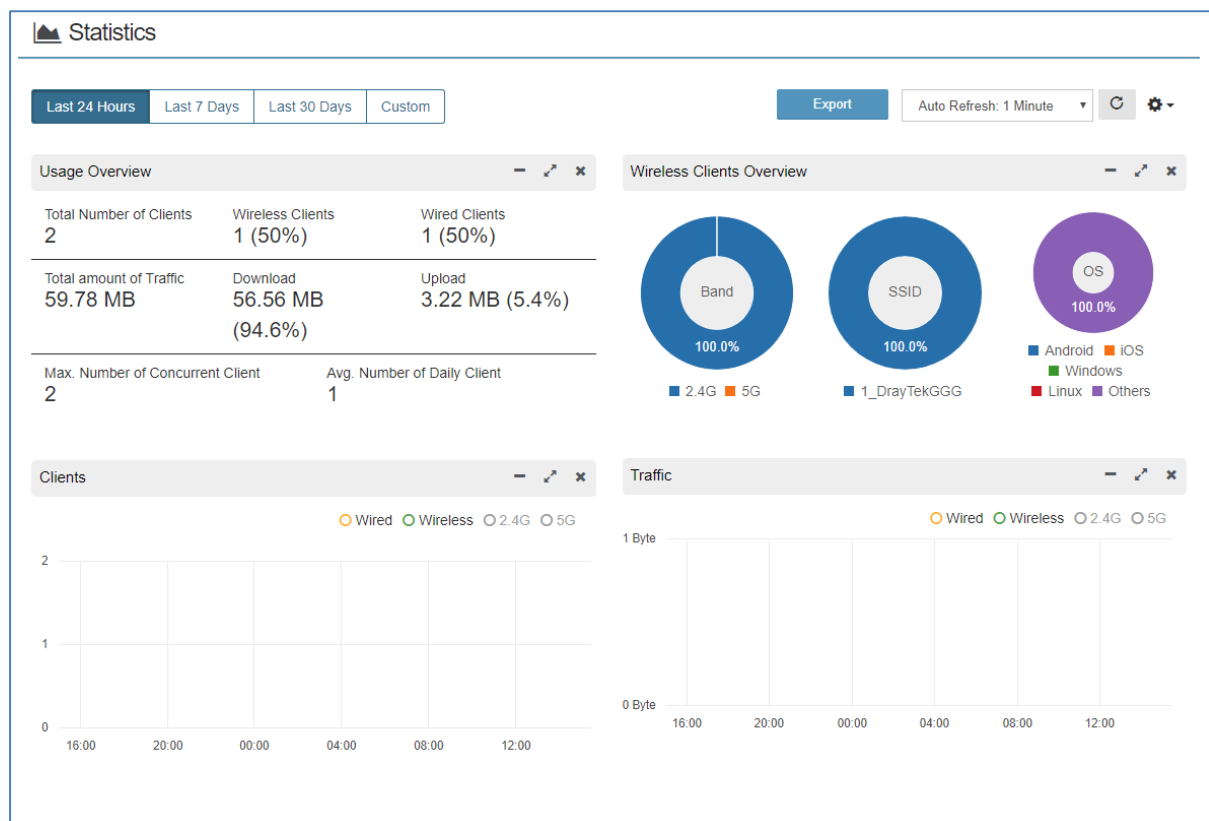
Quick Tools

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

4.2.1.2 Statistics Menu

The statistics for all the devices listed under the root network is displayed. It includes usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. Time periods that can be viewed are: Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period).

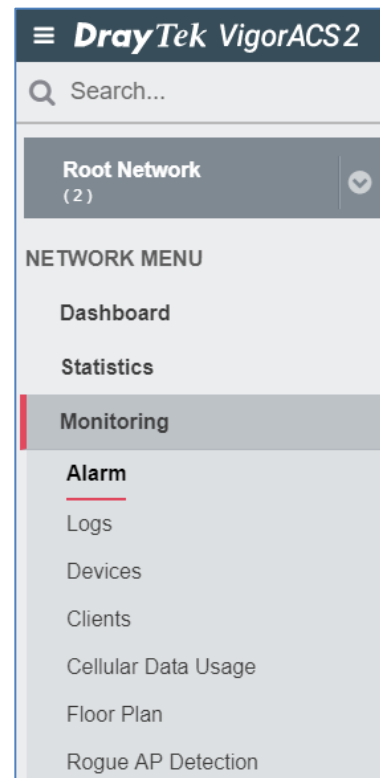
In addition, the statistics can be exported as “.XLS” file by clicking on the Export button.



4.2.1.3 Monitoring Menu

Seven sub menus are available within the Monitoring menu:

- Alarm
- Logs
- Devices
- Clients
- Cellular Data Usage
- Floor Plan
- Rogue AP Detection



Alarm View

Provides details of alarms generated for CPE devices e.g. lost connection. Five levels of alarms are displayed depending on the severity. These are:

- Critical
- Major
- Minor
- Warning
- Normal

User84
System Administrator

Monitoring > Alarm

search No. / Device Name / MAC

Time Interval : 2017/09/24 to 2017/10/24

Alarm 1

History

Export All

Delete

Delete All

⏮

<

1

/ 2

>

⏭

⏹

⚙

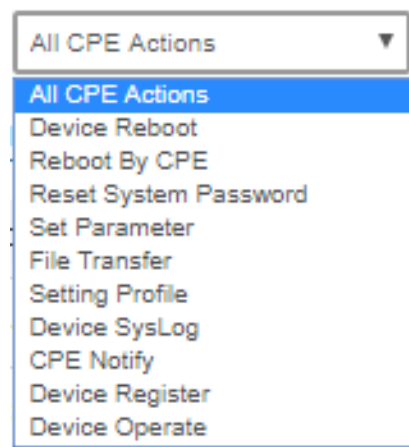
No.	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type	Ack Status	
☐	126	2017/10/17 05:18:01 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Not Ack
☐	122	2017/10/17 05:10:31 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Not Ack
☐	117	2017/10/17 04:54:08 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Not Ack
☐	109	2017/10/17 04:28:34 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Not Ack
☐	102	2017/10/17 04:08:28 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Acked
☐	96	2017/10/17 03:19:50 PM	2860Ln_001DAA5B1800	001DAA5B1800	▲ Critical	Device Loss Connection	Device Loss Connection	Not Ack

Log View

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

ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
44	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	44	2017/10/24 03:27:42 PM
43	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	43	2017/10/24 03:26:16 PM
34	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	34	2017/10/17 05:15:12 PM
30	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	30	2017/10/17 04:51:03 PM
29	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	29	2017/10/17 04:48:36 PM
22	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	22	2017/10/17 04:00:34 PM
19	2860Ln_001DAA5B1800	1	001DAA5B1800	192.168.101.178	Inform	19	2017/10/17 03:30:24 PM

The log view can be filtered by a specific CPE action if required.



Devices View

Use this view to get 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 devices under the selected network group.

Device	IP Address	MAC Address	Model	Network	Status	Up Time	F/W Version	Current Client	Current Traffic
2860Vn+_001DAABC4CF8	192.168.100.121	001DAABC4CF8	Vigor2860Vn+	Root Network	online	0d:0h:0m:0s	3.8.7_VT4	0 (Local Wireless: 0)	0 Byte (↑ 0 Byte ↓ 0
2862Lac_001DAA6C3258	192.168.101.64	001DAA6C3258	Vigor2862Lac	Root Network	online	0d:0h:0m:37s	3.8.8_VT1	1 (Local Wireless: 1)	0 Byte (↑ 0 Byte ↓ 0

Clients View

This page displays general information (such as hostname, MAC address, IP address, name of connected devices, type, SSID, connection time, and etc.) for wireless / wired clients which connect to CPEs under the selected network group.

Monitoring > Clients									
Last 24 Hours Last 7 Days Last 30 Days Custom Create Report									
Search Hostname / MAC / IP Device: All selected (2) Type: All SSID:									
Total Number of Clients: 3 Rows 10 1 / 1									
Hostname	MAC Address	IP Address	Connected Device	Connected Device MAC	OS	Type	SSID	ConnectionTime	Traffic
Herve-PC	00241dc0b6f7	192.168.1.10	2860Vn+_001DAABC4CF8	001DAABC4CF8		WIRED		0d 10h 14m 11s	322.84KB(↑133.08KB
DESKTOP-EE8RAF1	18d6c704dfd6	192.168.1.10	2862Lac_001DAA6C3258	001DAA6C3258		WIRED		0d 21h 08m 32s	39.00MB(↑2.18MB ↓3
Roy	303a64b6d6c2	192.168.1.11	2862Lac_001DAA6C3258	001DAA6C3258		WIRELESS_2.4g	1_DrayTekGGG	0d 20h 05m 21s	21.10MB(↑1.16MB ↓1

Cellular Data Usage

This page displays traffic information including data used, data cycle, status, percentage, downloaded data, uploaded data for LTE devices. The LTE data Quota can also be monitored.

Monitoring > Cellular Data Usage

Root

System Administrator

LTE Data Usage Overview

Data Used

0 Byte

Data Cycle

04/08 - 04/14

Status: NORMAL

0% of 500MB

1 Byte

Total

0 Byte

04-08

04-09

04-10

Device

Total

Download

Upload

2862Lac_001DAA6C3258

0 Byte

0 Byte

0 Byte

Quota Settings

Data Usage Alarm

Data Quota

500

MB

Trigger Alarm When

90

% of Quota (450.00 MB)

Usage Reached

Alarm Serverity Level

Critical

Data Usage Cycle

Weekly

Monthly

Custom

Weekly Reset Day

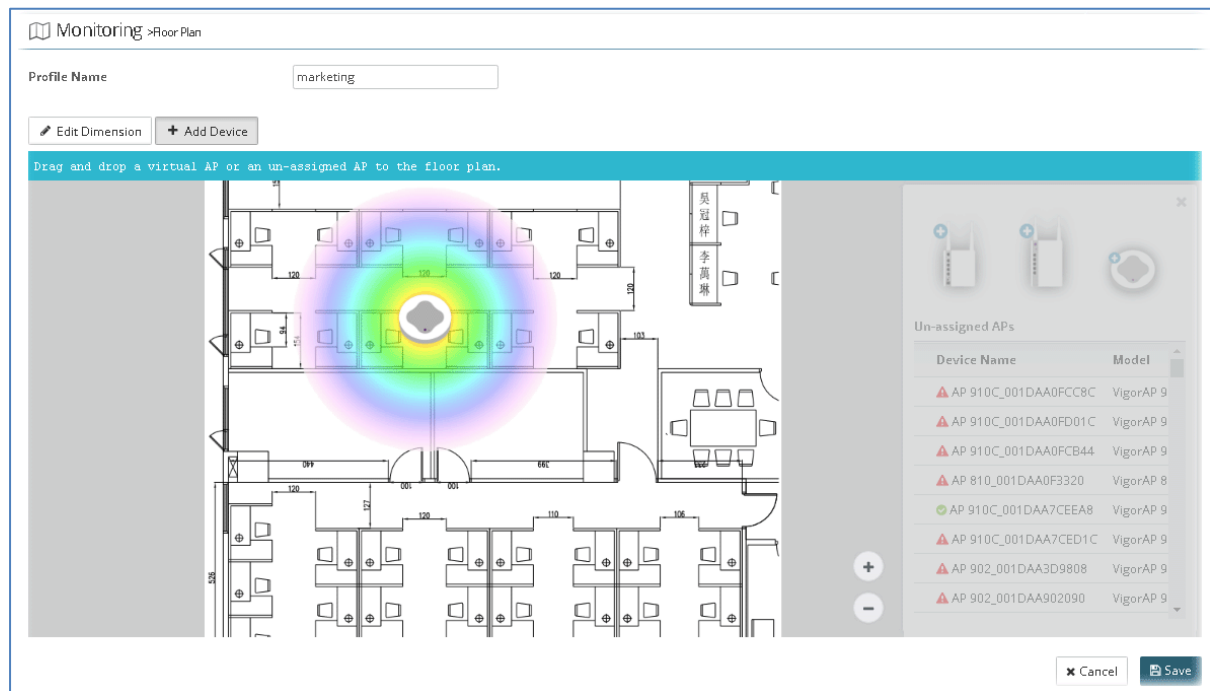
Sunday

Cancel

Save

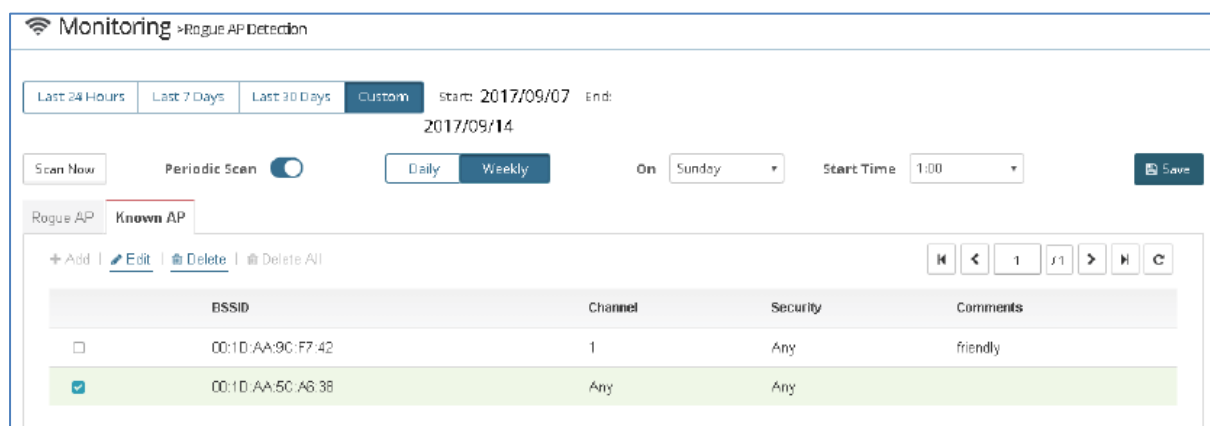
Floor Plan View

Use this view to determine the best location for VigorAP in building. Drag and drop available VigorAP icon from the list to the floor plan to see the wireless coverage.



Rogue AP Detection View

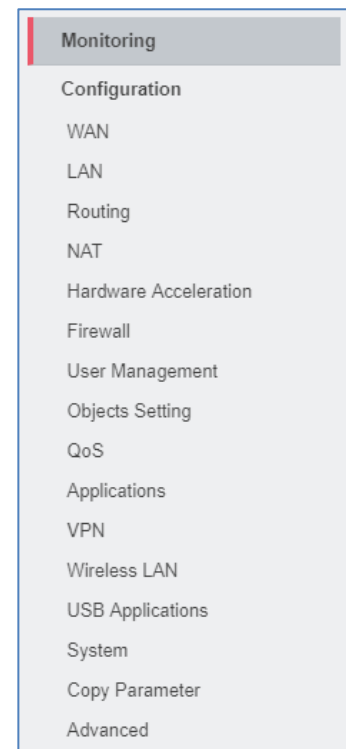
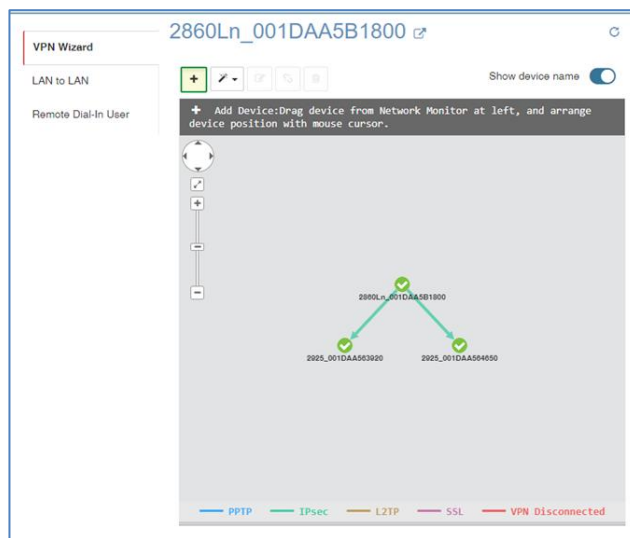
Information detected by Vigor Access Points is displayed on this page. Rogue AP's and known AP's are shown in different colours.



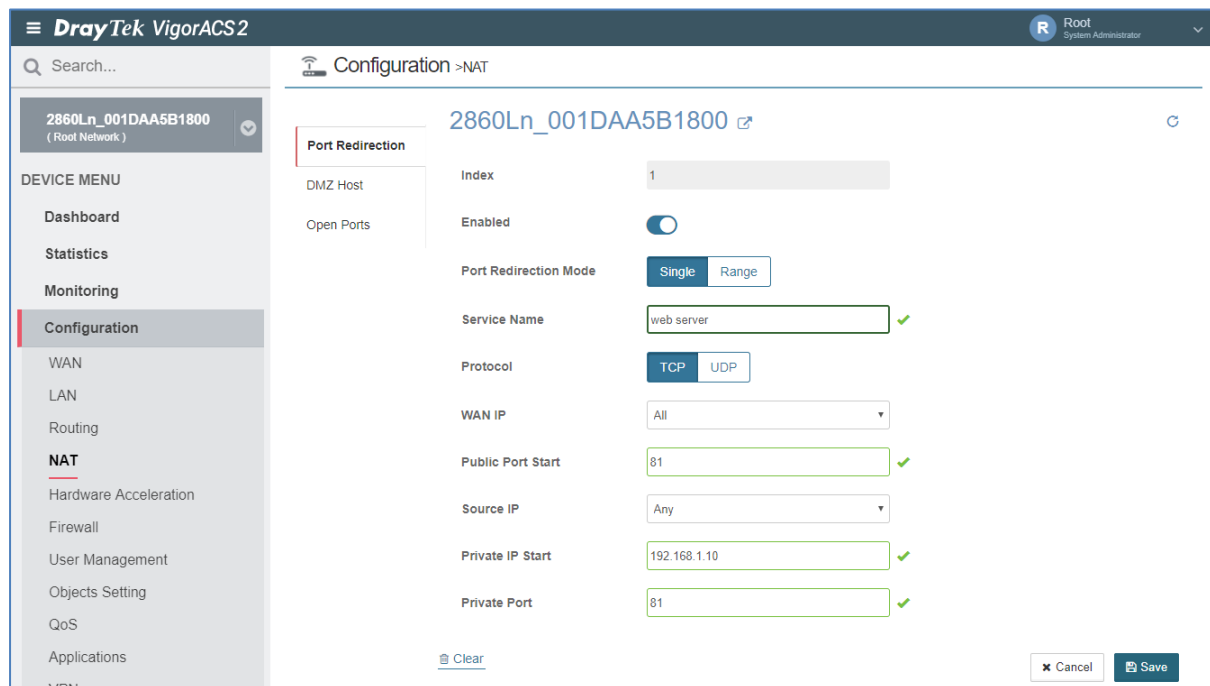
4.2.1.3 Configuration Menu

The configuration menu allows CPE devices to be configured by selecting the required parameter.

It includes the **VPN** wizard to automatically create a VPN tunnel between two routers. Simply drag and drop one router icon over the other router to create a VPN tunnel.



For example, selecting **Configuration>>NAT>>Port Redirection** brings up the following page for the Vigor2860Ln router. Parameters can be modified and saved to the CPE device.



4.2.2 System Menu

The SYSTEM MENU has 7 sub menus:

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

SYSTEM MENU

Maintenance

Reports

Provisioning

Network Management

System

User

About

4.2.2.1 Maintenance Menu

The Maintenance sub menu allows you to carry out various tasks on CPE devices such as configuration backup/restore, firmware upgrades etc.

SYSTEM MENU

Maintenance

Scheduled Backup

Configuration Restore

Firmware Upgrade

Device Reboot

System Password Reset

Schedule Profile

File Manager

 **Maintenance** > Firmware Upgrade

User Group : RootGroup

Firmware Upgrade Job List

[+ Add](#)

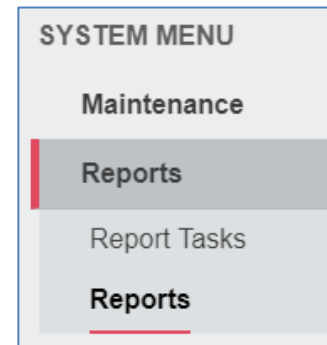
Name	Status	Model	FW Version	FW File	Schedule	Start Date	Action
sample	Disabled	Vigor2760n	3.1.1.1_RC6	v2k7v_a_3.1.1.1_RC6.all	Any	N/A	Edit
5555	Disabled	44	44	./RootGroup/ap900_r4669_1153RC3.all	Any	N/A	Edit
AP902	Enabled	VigorAP 902	1.2.0RC6a	./RootGroup/ap902_r6078_1171.all	15:05-18:43	N/A	Edit
Period_2860	Disabled	Vigor2860ac	3.8.5_RC5a	./RootGroup/v2860std_r51496_001.all	Any	N/A	Edit

Firmware Upgrade

4.2.2.2 Report Menu

This menu option allows you to create custom reports for CPE devices. You can select individual CPE devices or all devices for the report.

Reports can be created for various parameters including traffic, firmware, network, status and information.



Report

Create a Report

Report 3

VigorACS Report

Status Overview Report

Device Total Count:4

Severity	Device Name	MAC Address	IP	Model
Normal	DrayTek_001DAA_Vigor2860Ln_001DAA	001DAA5B1800	192.168.101.178	Vigor2860Ln
Normal	DrayTek_001DAA_Vigor2925_001DAA56	001DAA563920	192.168.101.26	Vigor2925
Normal	DrayTek_001DAA_Vigor2925_001DAA56	001DAA564650	192.168.101.25	Vigor2925
Normal	DrayTek_001DAA_VigorAP	001DAA3D578A	192.168.1.2	VigorAP 902

Status Overview Report for all CPE Devices

4.2.2.3 Provisioning Menu

Provisioning functions allow CPE devices to be configured simultaneously instead of configuring each CPE individually. For example, you can to update all customer routers with an updated firewall rule.

Usually an XML file needs to be created with the required configuration parameters. This file is then used to update the selected CPE devices.

“CPE Keep Parameters” will cause the CPE device to reload the VigorACS 2 configuration parameters in case a user accidentally modifies the CPE device configuration.

SYSTEM MENU

Maintenance

Reports

Provisioning

Network & Devices

Global Parameters

CPE Set Parameters

CPE Keep Parameters

Provisioning > Network & Devices

User Group : RootGroup

Name	Profile Id
Root Network(4)	Empty
Brisbane Office(1)	Block YouTube v1
Training Lab(3)	Block YouTube v1

Network & Devices – Select Configuration File to Apply to CPE Devices

Provisioning > Global Parameters

User Group : RootGroup

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

Profile Name	Model	Always Keep	Revision	Last Modification At	Action
Empty		No	0	0001/01/01 12:00:00 AM	Edit Delete View Log
KFC project-Global Setting		No	1	2017/10/18 11:55:09 AM	Edit Delete View Log
KFC project-Global Objects-Groups		No	1	2017/10/18 01:20:06 PM	Edit Delete View Log
Block YouTube v1		No	1	2017/10/18 01:29:51 PM	Edit Delete View Log

Global Parameters – Upload or import XML Configuration Files

Root
System Administrator

Provisioning > CPE Set Parameters

Device :

Primary ViewParameter List

WAN

LAN

LAN Subnet

VLAN

DHCP Option Setup

NAT

Object Settings

QoS

Firewall

VoIP

Routing

Wireless

System

Applications

Index

1

Enable VLAN

☒

Subnet

LAN1

VLAN Tag Enable

☒

VLAN Tag ID

10

VLAN Tag Priority

0

VLAN Members

Physical LAN Ports

☒ P1 ☒ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6

2.4G Wireless LAN

☒ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

5G Wireless LAN

☒ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

CPE Set Parameters – Create Custom XML file for CPE device based on its MAC Address or IP Address

4.2.2.4 Network Management Menu

The Network Management menu allows the creation of networks under the Root network and CPE devices can be moved into each network. This helps in managing CPE devices located in different locations.

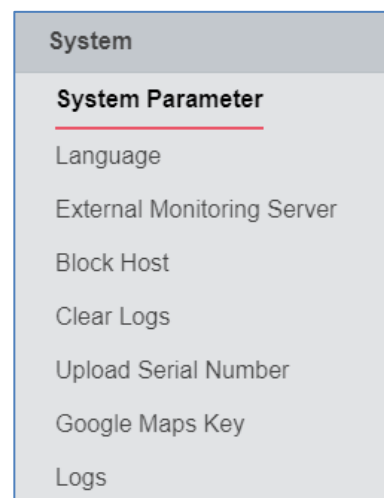
In the example shown below, we create two networks: Brisbane Office and Training Lab and have the CPE devices shown within each network.

The screenshot displays the 'Network Management' interface. On the left, a tree view shows the hierarchy: Root Network(4) > Brisbane Office(1) > 2925_001DAA563920 > Training Lab(3) > 2860Ln_001DAA5B18. The main area is divided into 'Setting' and 'Map' tabs. The 'Setting' tab is active, showing a configuration form for a device. The form includes fields for Device ID (1), Network ID (3), Model Name (Vigor2860Ln), Device Name (2860Ln_001DAA5B1800), Note 1, Note 2, Serial number, MAC Address (001DAA5B1800), Location (128 station road seven hills), IP (192.168.101.178), Phone No., Port (8069), Domain Name, and URI (/cwm/CRN.html). There are also buttons for 'Delete This Device', 'Change Network', 'Change Username/Password', 'Status' (Disable/Enable), and 'Known Device' (Known/Unknown).

Network Management – Allows CPE Devices to be Grouped into Networks

4.2.2.5 System Menu

The System menu allows VigorACS 2 system parameters to be modified. This includes how VigorACS 2 performs certain functions, language used, log handling etc.



System > System Parameter		
ID	Name	Value
74	EnableFirmwareCheck	true
73	HealthierWebFolder	web
72	HealthierExposelp	192.168.100.92
71	EnableSendCPENotify	true
70	ShowTreeCount	100
68	DisableSaveInformLog	false
67	EnableAutoChangeWebPort	true
66	CheckCPEValidByNetworkUser	false
65	New_DeleteOldDeviceBySameIP	false
64	CheckCPEValidByAuthKey	false
63	EnableBackUpCheck	false
62	EnableRecordActionLog	true
61	TimeFormat	1
60	EnableForceSetCPEPeriodicInformInterval	true
59	CPEPeriodicInformInterval	900
58	FWUpgradeFailInterval	86400
57	EnableChangeNetworkByNetworkUser	true
56	UseStunAddressForVpn	false

Reset to default

Cancel Save

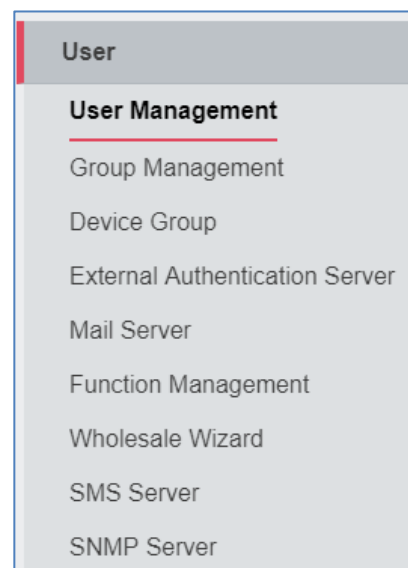
System Parameter - Used to control how VigorACS 2 Performs Certain Functions

4.2.2.6 User Menu

The User menu has a number of functions to control access to the ACS 2 server and notifications for network administrators.

The User Management ensures security by only allowing users with the appropriate privileges to view or modify server parameters as well as CPE parameters.

Up to 200 customized profiles can be created for users controlled under User Management.



Five-level User Authority

The screenshot displays the 'User Management' interface in the DrayTek VigorACS2 system. On the left is a 'SYSTEM MENU' with options like Maintenance, Reports, Provisioning, Network Management, System, and User. The 'User' menu is selected, showing 'User Management' as the active option. The main area contains a table of users with columns for Username, Role, Status, Mail Notify, SMS Notify, Email, Telephone, and Description. A pyramid diagram on the right illustrates the five levels of user authority:

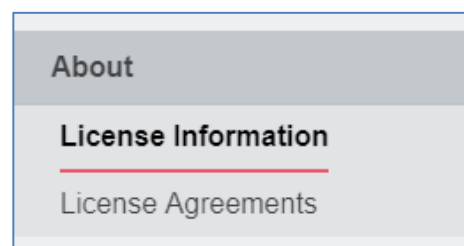
- System Administrator** (Top level, teal)
- Group Administrator** (Second level, green)
- Administrator** (Third level, yellow)
- Operator** (Fourth level, orange)
- View only operator** (Bottom level, red)

Username	Role	Status	Mail Notify	SMS Notify	Email	Telephone	Description
root	System Administrator	Active	✓	-	111@draytek.com		System Administrator
admin	Administrator	Active	-	-	admin@draytek.com		Administrator
Kevin	System Administrator	Active	✓	✓	kevin@draytek.com	+886 123456789	A test account
ga	Group Administrator	Active	-	-			
op	Operator	Active	-	-			
uitester	System Administrator	Active	-	-			UI Test
ap_sa	System Administrator	Active	-	-			
ap_admin	Administrator	Active	-	-			
ap_op	Operator	Active	-	-			
ap_gadmin	Group Administrator	Active	-	-			
ap_vop	View Only Operator	Active	-	-			
dni	View Only Operator	Active	-	-			
liveadmin	System Administrator	Active	-	-			

User Management

4.2.2.7 About Menu

This menu provides License information for the VigorACS 2 installation as well as details of any licence agreements in relation to the software.



5. Configuring CPE Devices

Once VigorACS 2 has been installed, you can configure the DrayTek CPE devices so that they will be registered with the ACS server and be managed. Note that Linux based routers have different menu options to DrayOS Vigor routers. The following sections provide the configuration parameters required for each type of CPE devices.

5.1 Default TR069 Settings

5.1.1 ACS Server Settings

ACS Server URL `http://Server Address:Port/ACSServer/services/ACSServlet`

For example, if the Server Address is *acssi-draytekau.no-ip.org* and the http port is 48084, we enter the following URL for the ACS Server:

`http://acssi-draytekau.no-ip.org:48084/ACSServer/services/ACSServlet`

ACS Username `acs`
ACS Password `password`

The ACS username and password are configured in the Network Management page of VigorACS 2 server as shown in the diagram below.

The screenshot shows the DrayTek VigorACS2 web interface. The 'Network Management' section is active, displaying a list of networks. The 'Root Network(2)' is selected, and the 'Setting' tab is active. The configuration form for the network is shown, with the 'User Name' and 'Password' fields highlighted by a red box. The 'User Name' field contains 'acs' and the 'Password' field contains 'password'. A 'Save' button is visible at the bottom right of the form.

Field	Value
Network ID	2
Name	Root Network
Location	
User Name	acs
Password	password

5.1.2 CPE Client Settings

CPE URL <http://WAN IP address:Port #/cwmp/creq>
(This automatically generated by the router)

CPE Username Vigor

CPE Password password

This can be customised in **Network Management** page after selecting the required CPE device.

The screenshot displays the DrayTek VigorACS2 web interface. On the left is a sidebar menu with sections for 'DEVICE MENU' (Dashboard, Statistics, Monitoring, Configuration) and 'SYSTEM MENU' (Maintenance, Reports, Provisioning, Network Management, System, User, About). The 'Network Management' option is selected. The main content area shows the configuration for a device named '2862Lac_001DAA6C3258'. The 'Setting' tab is active, showing various fields for device identification and client settings. A red box highlights the 'CPE Client User Name' and 'CPE Client Password' fields, which are set to 'vigor' and 'password' respectively. Other visible fields include Device ID (2), Network ID (2), Model Name (Vigor2860Vn+), Device Name (2860Vn+_001DAA6C3258), MAC Address (001DAA6C3258), CPE Client IP (192.168.100.121), CPE Client Port (8069), and CPE Client URI (/cwm/CRN.html). The Management Protocol is set to 'ACS default (http)' and the Management Port is 80. A 'Save' button is located at the bottom right of the configuration area.

5.2 Linux based routers

This section covers the TR069 settings in DrayTek Linux based routers such as the Vigor2960, Vigor3960 or Vigor300B.

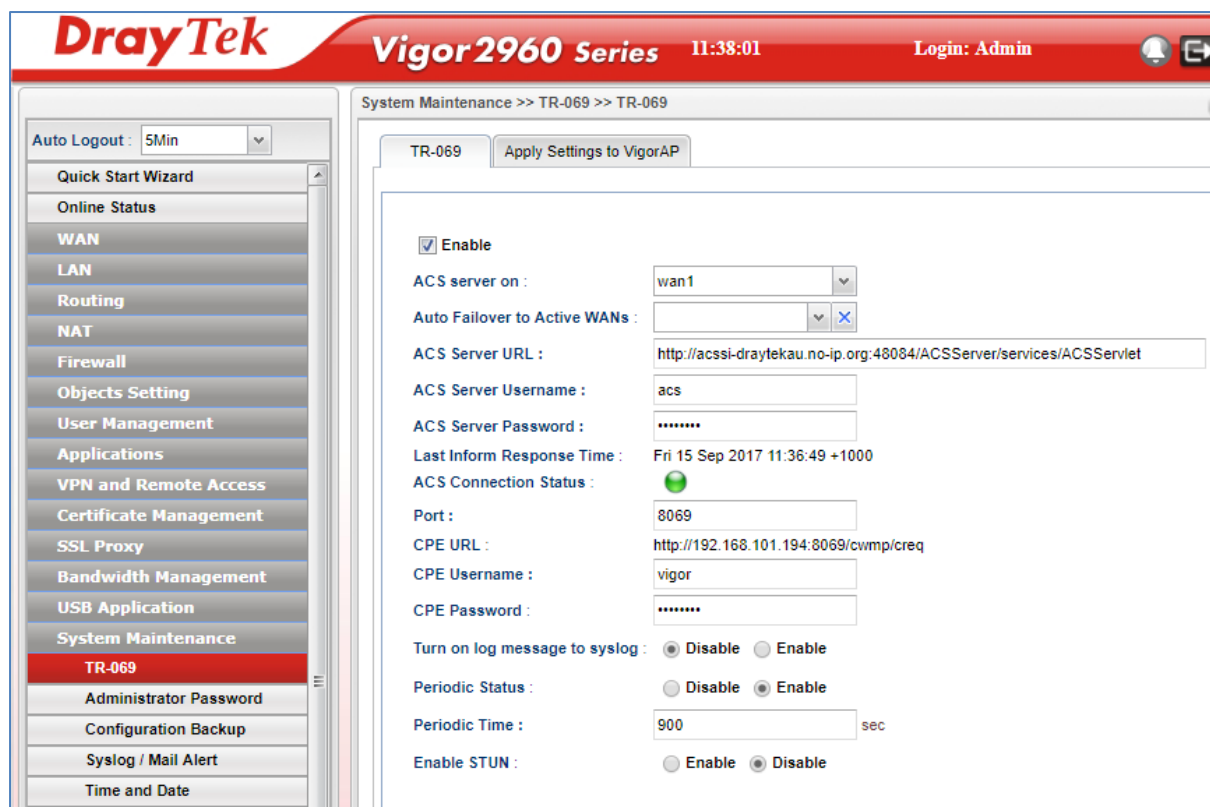
You will need to enter the following parameters:

ACS Server URL `http://Server Address:Port/ACSServer/services/ACSServlet`

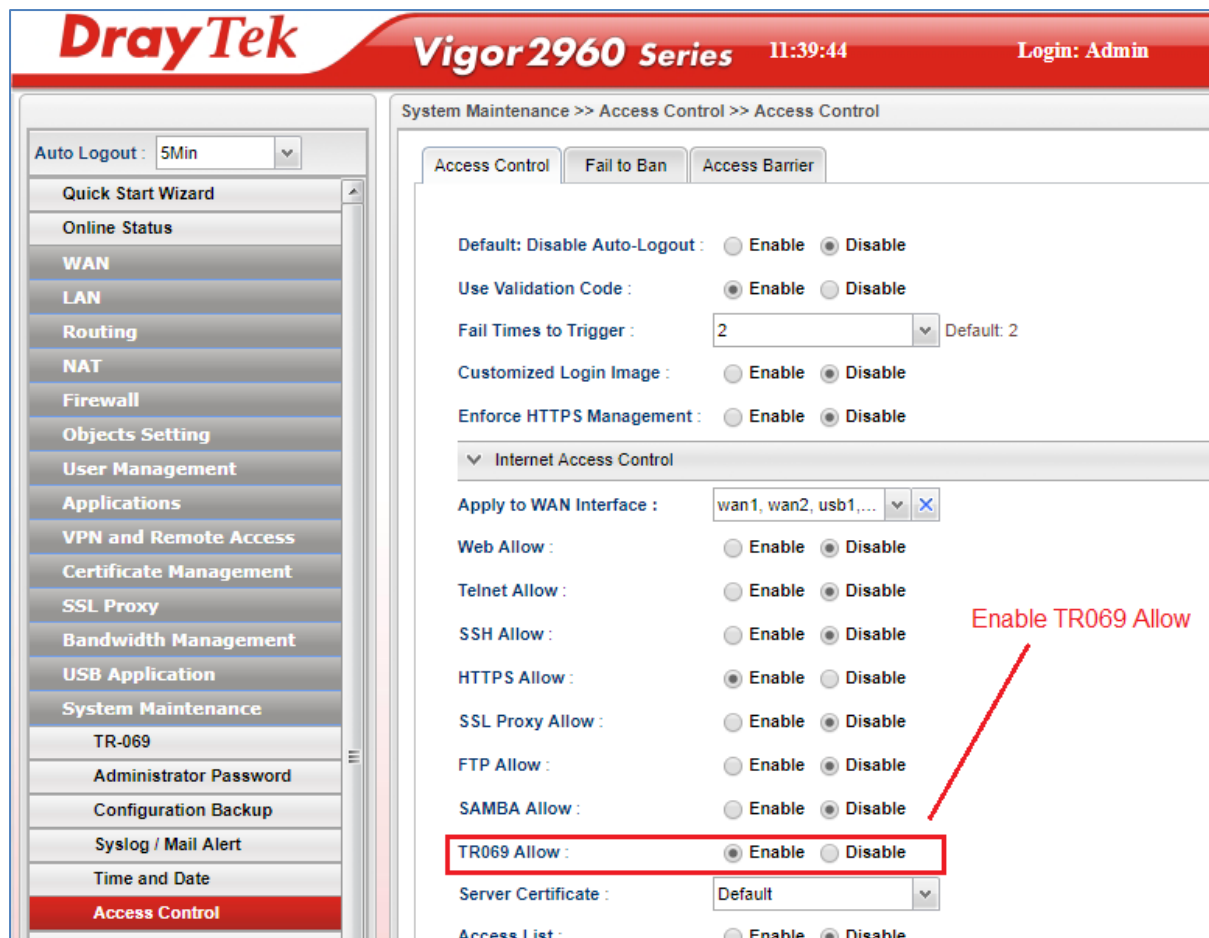
For example, if the Server Address is *acssi-draytekau.no-ip.org* and the http port is 48084, we enter the following URL for the ACS Server:
`http://acssi-draytekau.no-ip.org:48084/ACSServer/services/ACSServlet`

ACS Username acs

ACS Password password



You will also need to allow TR069 in the Internet Access control settings. To do this, select the enable option for the “TR069 Allow” option as shown in the diagram below.



5.3 Vigor DrayOS routers

The TR069 setting in DrayTek Vigor routers such as the Vigor2762, Vigor2862, Vigor2926 as well as others is shown in the diagrams below:

You will need to enter the following parameters:

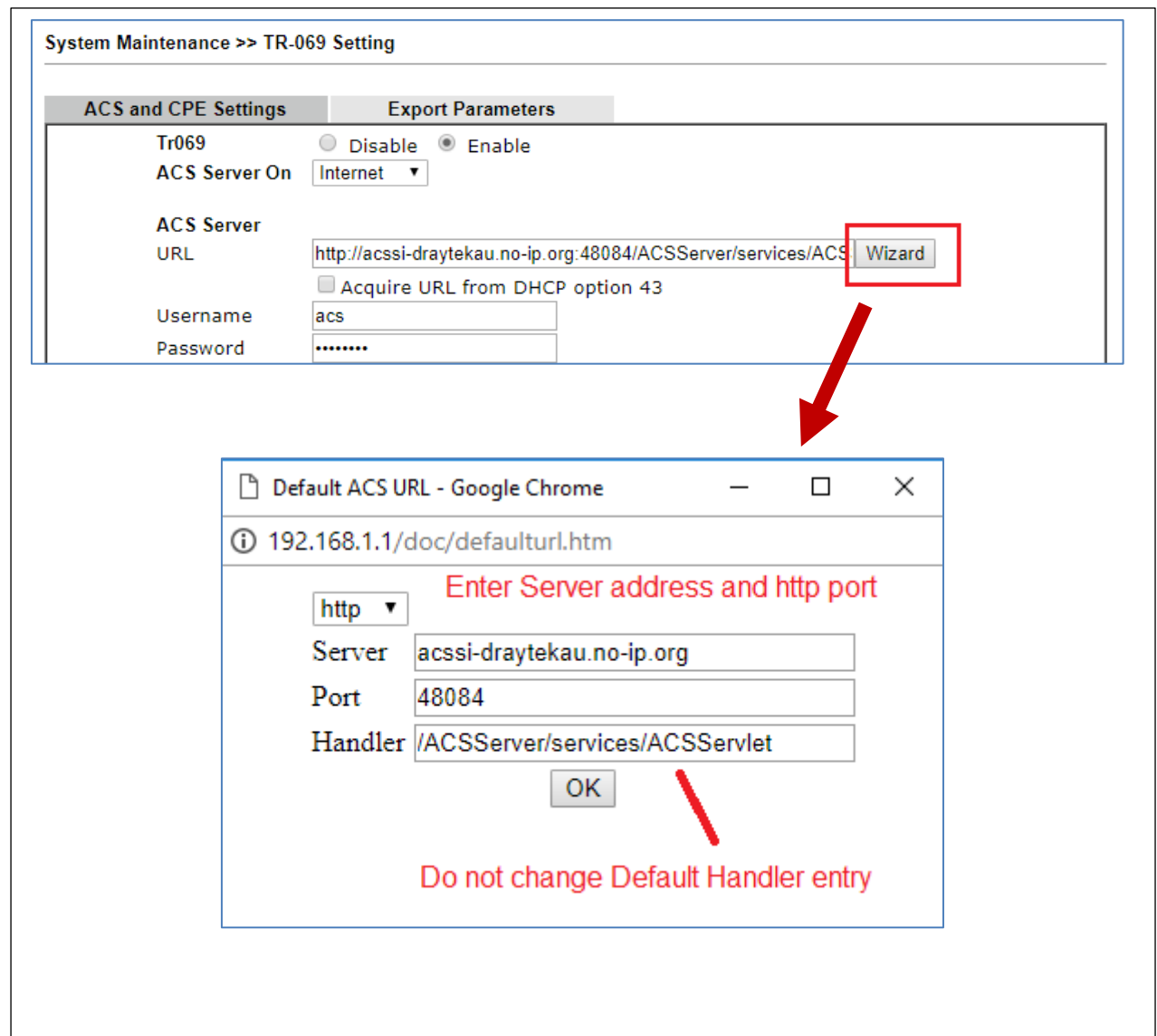
ACS Server URL `http://Server Address:Port/ACSServer/services/ACSServlet`

For example, if the Server Address is *acssi-draytekau.no-ip.org* and the http port is 48084, we enter the following URL for the ACS Server:
`http://acssi-draytekau.no-ip.org:48084/ACSServer/services/ACSServlet`

ACS Username `acs`
ACS Password `password`

The ACS Server URL can be created by using the wizard button. In the pop-up menu enter the ACS server address, and HTTP or HTTPS port and select http or https from the pull-down menu. The Handler should be left at the default setting.

Click **OK** to save.



For **CPE Client settings**, select either **Http** or **Https** option.

The URL is generated automatically based on the router WAN IP address.

You can customise the port, username and password, however these must match the settings in the VigorACS 2 server as described in section 5.1.2 CPE Client Settings.

Periodic Inform settings can be enabled if required.

STUN settings will need to be enabled if the CPE device is behind NAT or firewall. Enter the ACS 2 server address for the STUN server.

System Maintenance >> TR-069 Setting

Off IR6

Dashboard
Wizards
Online Status

WAN
LAN
Load-Balance/Route Policy
NAT
Hardware Acceleration
Firewall
User Management
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
Wireless LAN
SSL VPN
USB Application
System Maintenance
System Status
TR-069
Administrator Password
User Password
Login Page Greeting
Configuration Backup
SysLog / Mail Alert
Time and Date
SNMP
Management
Self-Signed Certificate
Reboot System
Firmware Upgrade
Activation
Internal Service User List
Diagnostics

Central Management
VPN
AP
Switch

ACS and CPE Settings Export Parameters

Tr069 ☐ Disable ☒ Enable

ACS Server On

ACS Server
URL Wizard
☐ Acquire URL from DHCP option 43

Username
Password
Test With Inform Event Code

Last Inform Response Time : Fri Sep 15 3:31:34 2017 ●

CPE Client
☒ Http ☐ Https
URL
Port
Username
Password

Periodic Inform Settings
☐ Disable ☒ Enable
Interval Time second(s)

STUN Settings
☐ Disable ☒ Enable
Server Address
Server Port
Minimum Keep Alive Period second(s)
Maximum Keep Alive Period second(s)

Ensure that both “TR069 Server” and “Allow management from the Internet” are enabled as shown in the diagram below.

The TR069 port can be customised on this menu as well.

System Maintenance >> Management ?

IPv4 Management Setup IPv6 Management Setup

Router Name

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

Internet Access Control
☒ Allow management from the Internet
Domain name allowed

☐ FTP Server
☒ HTTP Server
☒ HTTPS Server
☒ Telnet Server
☒ TR069 Server
☐ SSH Server
☒ Disable PING from the Internet

Management Port Setup
☒ User Define Ports ☐ Default Ports

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

TLS/SSL Encryption Setup
☒ Enable TLS 1.2
☒ Enable TLS 1.1
☒ Enable TLS 1.0
☐ Enable SSL 3.0

6. Exercise – Part 1: Register CPE devices to ACS 2

6.1 Video Demonstration

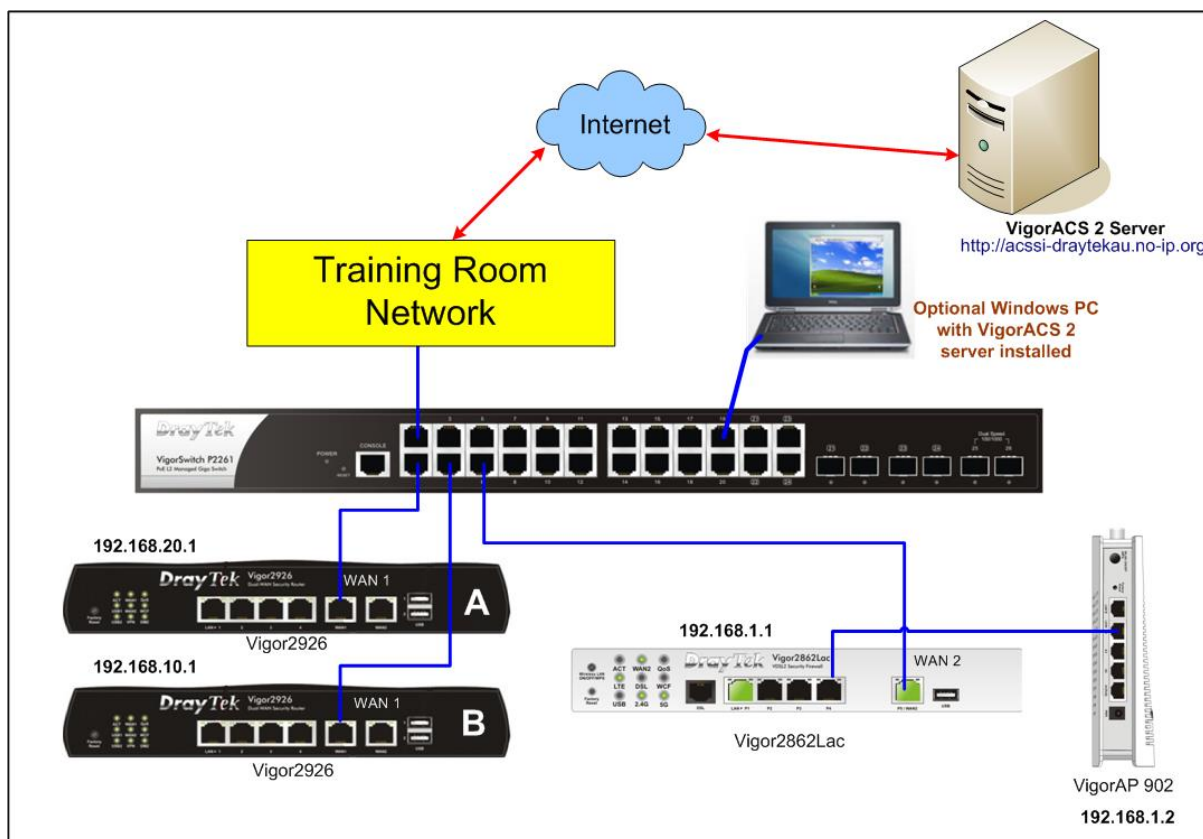
How to Register a CPE device into DrayTek VigorACS SI

This video covers the steps required to configure the DrayTek Vigor routers to register with VigorACS server as discussed in section 5. It is available on YouTube at the following URL:

<https://youtu.be/GNSJIWvFW2g>

6.2 Preliminary Configuration

For this exercise, we will register three routers and an access point to VigorACS 2 using the following network topology shown in the diagram below. You will be advised if you will be connected to the VigorACS 2 Server on the internet or a local Windows PC with VigorACS 2 server installed.



Connect the WAN port of each device to the VigorSwitch as shown in this diagram. You can connect any LAN port of the AP902 to one of the Vigor2862Lac LAN ports. Also ensure that the VigorSwitch is reset to factory default settings to avoid any issues connecting to the network.

Note: Before proceeding to the next step, reset all the routers and access point to factory default settings by pressing the factory reset button for at least 5 seconds or until the ACT LED starts to flash rapidly.

(At factory defaults, the router IP address is 192.168.1.1 and username/password is admin/admin)

6.2.1 Configure Router LAN

Before we start we need to configure a unique LAN IP subnet for each router as shown in the diagram above. Follow the instructions below to configure each router LAN.

Vigor2862Lac

This router should be at factory default settings so the settings for LAN 1 should appear as shown below.

- Go to “LAN >> General Setup” configuration menu to verify settings.
- Click on Details page to view LAN 1 details.

DrayTek Vigor2862 Series

LAN >> General Setup

General Setup

Index	Status	DHCP	DHCPv6	IP Address	Details Page	IPv6
LAN 1	V	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☐	☒	☒	192.168.2.1	Details Page	IPv6
LAN 3	☐	☒	☒	192.168.3.1	Details Page	IPv6
LAN 4	☐	☒	☒	192.168.4.1	Details Page	IPv6
LAN 5	☐	☒	☒	192.168.5.1	Details Page	IPv6
LAN 6	☐	☒	☒	192.168.6.1	Details Page	IPv6
LAN 7	☐	☒	☒	192.168.7.1	Details Page	IPv6
LAN 8	☐	☒	☒	192.168.8.1	Details Page	IPv6

Vigor2862 Series

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration
For NAT Usage

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

LAN 1 IPv6 Setup

DHCP Server Configuration
☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 192.168.1.10
IP Pool Counts: 200 (max. 1021)
Gateway IP Address: 192.168.1.1
Lease Time: 86400 (s)
☒ Clear DHCP lease for inactive clients periodically

DNS Server IP Address
Primary IP Address:
Secondary IP Address:

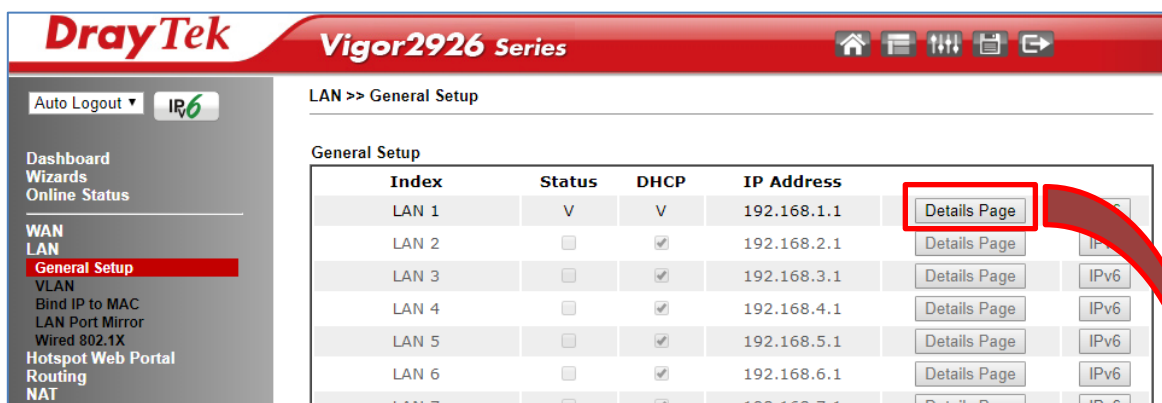
Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN1 Virtual IP to the same domain IP.

OK

Vigor2926 (A)

Configure the router to have the LAN 1 IP address of **192.168.10.1** as shown below.

- Log into the router (A) using the default login details (192.168.1.1 admin/admin)
- Go to “LAN >> General Setup” configuration menu.
- Click on Details page.
- Under Network Configuration, Change the IP address to 192.168.10.1
- Under DHCP Server Configuration
 - Change start address to 192.168.10.10
 - Change Gateway IP Address to 192.168.10.1
- Click **OK** to save the settings.



LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration
For NAT Usage

IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

LAN 1 IPv6 Setup

DHCP Server Configuration
☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 192.168.10.10
 IP Pool Counts: 200 (max. 1021)
 Gateway IP Address: 192.168.10.1
 Lease Time: 86400 (s)
☒ Clear DHCP lease for inactive clients periodically

DNS Server IP Address
 Primary IP Address:
 Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change **HA** LAN1 Virtual IP to the same domain IP.

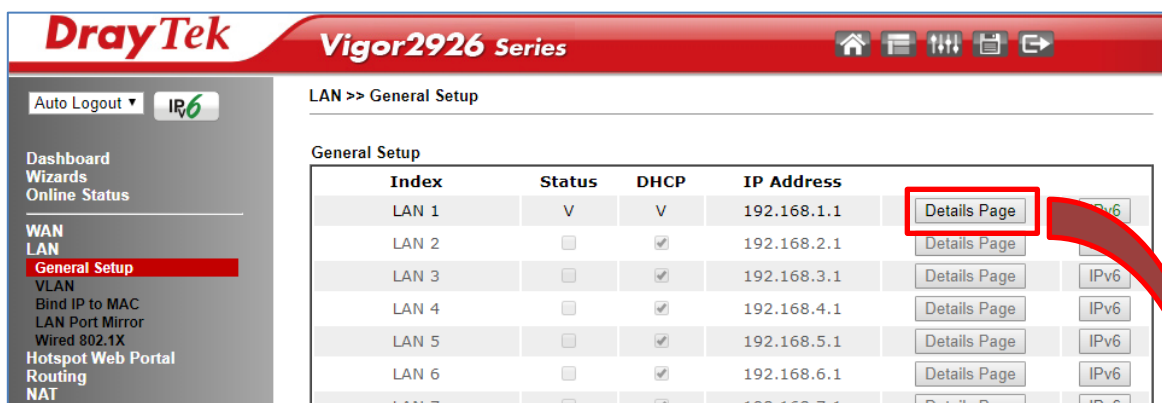
OK

Index	Status	DHCP	IP Address	Details Page	IPv6
LAN 1	V	V	192.168.10.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6
LAN 3	☒	☒	192.168.3.1	Details Page	IPv6

Vigor2926 (B)

Configure the router to have the LAN 1 IP address of **192.168.20.1** as shown below.

- Log into the router (**B**) using the default login details (192.168.1.1 admin/admin)
- Go to “LAN >> General Setup” configuration menu.
- Click on Details page.
- Under Network Configuration, Change the IP address to 192.168.20.1
- Under DHCP Server Configuration
 - Change start address to 192.168.20.10
 - Change Gateway IP Address to 192.168.20.1
- Click **OK** to save the settings.



LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration
For NAT Usage

IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable

LAN 1 IPv6 Setup

DHCP Server Configuration

☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 192.168.20.10

IP Pool Counts: 200 (max. 1021)

Gateway IP Address: 192.168.20.1

Lease Time: 86400 (s)

☒ Clear DHCP lease for inactive clients periodically

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN1 Virtual IP to the same domain IP.

OK

LAN >> General Setup

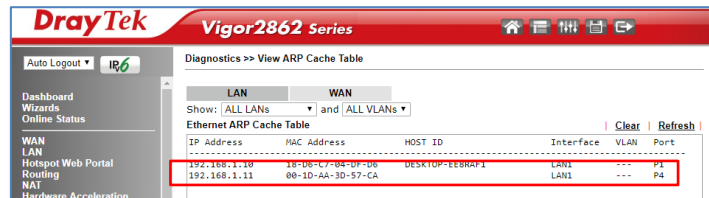
General Setup

Index	Status	DHCP	IP Address	Details Page	IPv6
LAN 1	V	V	192.168.20.1	Details Page	IPv6
LAN 2	☐	☒	192.168.2.1	Details Page	IPv6
LAN 3	☐	☒	192.168.3.1	Details Page	IPv6

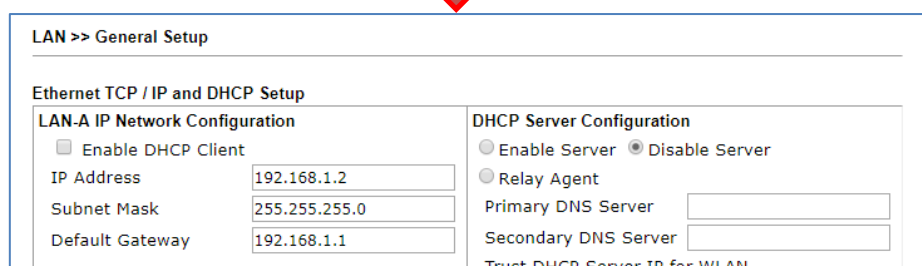
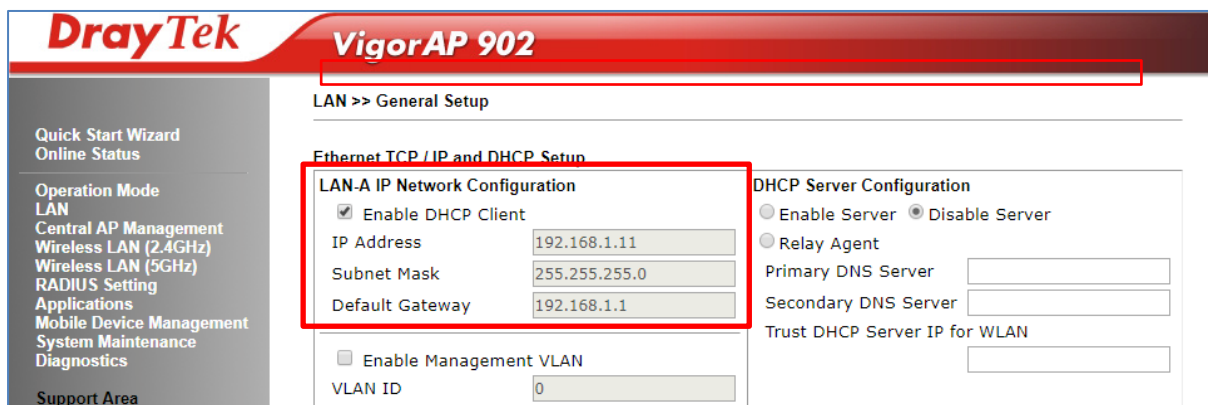
6.2.2 Configure Access Point LAN

The VigorAP902 access point will have DHCP enabled by default making it difficult to manage the unit. Disable the DHCP client setting and assign a static IP address using the steps below.

- Connect the VigorAP902 to one of the LAN ports in the Vigor2862Lac router.
- Log into the Vigor2862Lac router.
- Go to “**Diagnostics >> View ARP Cache Table**” in the router. You should see an entry there for the VigorAP902. In the example below, the IP address is 192.168.1.11 connected to router port P4.
- Alternatively, you can use **Central Management >> AP >> Dashboard** to find the IP address



- Use the current IP address of the VigorAP902 to log into access point. (The username/password is *admin/admin*).
- Disable DHCP Client.
- Change the IP address to **192.168.1.2** and default gateway to 192.168.1.1.
- Click **OK** to save the settings.



6.2.3 Configure Router WAN Interfaces

Configure each router (Vigor2862Lac, Vigor2926) to connect to the network using Ethernet WAN connection. Configure each WAN to use DHCP as shown in the instructions below:

Vigor2862Lac

Configure WAN 2 and connect to the VigorSwitch.

- Log into the router and go to **WAN >> Internet Access** menu.
- For WAN 2 select **Static or Dynamic IP** from the pull-down menu.
- Click on **Details Page**.
- On the next page select **Enable** and **Obtain IP address automatically**.
- Click **OK** to save.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6
WAN4		USB	None	Details Page	IPv6

Note: 1. Device on USB port 1 applies WAN3 configuration.

WAN >> Internet Access

WAN 2

PPPoE | **Static or Dynamic IP** | PPTP/L2TP | IPv6

☒ Enable ☐ Disable

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP:

PING Interval: minute(s)

WAN Connection Detection

Mode: ARP Detect

MTU: 1500 (Max:1500)

Path MTU Discovery: Detect

RIP Protocol

☐ Enable RIP

Bridge Mode

☐ Enable Bridge Mode

☐ Enable Full Bridge Mode

Bridge Subnet: LAN 1

TTL

Change the TTL value: Enable

WAN IP Network Settings | WAN IP Alias

☒ Obtain an IP address automatically

Router Name:

Domain Name:

☐ DHCP Client Identifier *

Username:

Password:

☐ Specify an IP address

IP Address:

Subnet Mask:

Gateway IP Address:

☒ Default MAC Address

☐ Specify a MAC Address

MAC Address: 00 1D AA 6C 32 5A

DNS Server IP Address

Primary IP Address: 8.8.8.8

Secondary IP Address: 8.8.4.4

*: Required for some ISPs

Note:

1. If enable firewall in bridge mode, IPv6 connection type would be change to DHCPv6 mode.
2. Bridge Subnet cannot be selected by Multi-WAN Interface at the same time.
3. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.
4. Full Bridge Mode supports forwarding packets with VLAN tags.
5. Full Bridge Mode doesn't support wireless LAN.

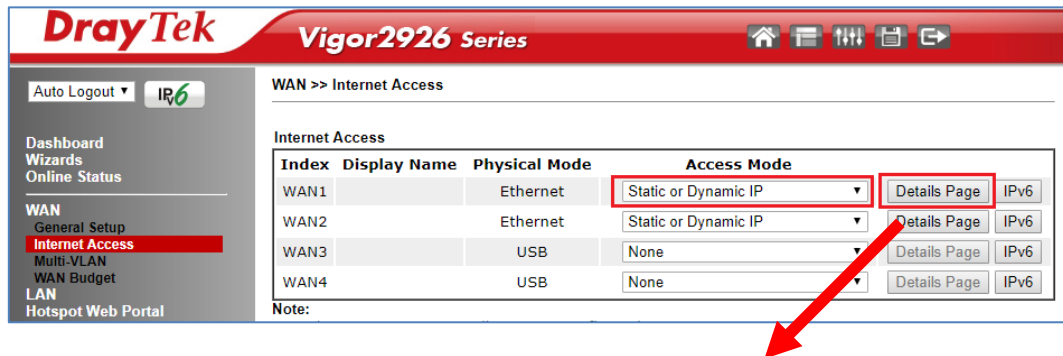
OK Cancel

Note: Note the router WAN IP address. This will be used to communicate with the router later.

Vigor2926

For each Vigor2926 router configure WAN 1 and connect to the VigorSwitch.

- Log into each router and go to **WAN >> Internet Access** menu.
- For WAN 1 select **Static or Dynamic IP** from the pull-down menu.
- Click on **Details Page**.
- On the next page select **Enable** and **Obtain IP address automatically**.
- Click **OK** to save.



WAN >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
☒ Enable ☐ Disable	WAN IP Network Settings WAN IP Alias ☒ Obtain an IP address automatically		

Router Name: *

Domain Name: *

☐ DHCP Client Identifier *

Username:

Password:

☐ **Specify an IP address**

IP Address:

Subnet Mask:

Gateway IP Address:

☐ **Default MAC Address**

☐ Specify a MAC Address

MAC Address: 00 · 1D · AA · E5 · 8A · BA

DNS Server IP Address

Primary IP Address: 8.8.8.8

Secondary IP Address: 8.8.4.4

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP:

PING Interval: 0 minute(s)

WAN Connection Detection

Mode: ARP Detect

MTU 1500 (Max:1500)

Path MTU Discovery: Detect

RIP Protocol

☐ Enable RIP

Bridge Mode

☐ Enable Bridge Mode

Bridge Subnet: LAN 1

*: Required for some ISPs

Note:

1. If enable firewall in bridge mode, IPv6 connection type would be change to DHCPv6 mode.
2. Bridge Subnet cannot be selected by Multi-WAN Interface at the same time.
3. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.

OK **Cancel**

Note: Note the router WAN IP address. This will be used to communicate with the router later.

6.3 Log into VigorACS Server

Several VigorACS 2 accounts have been set up for the workshop. Use the details of the VigorACS server URL as well as your login details. For example:

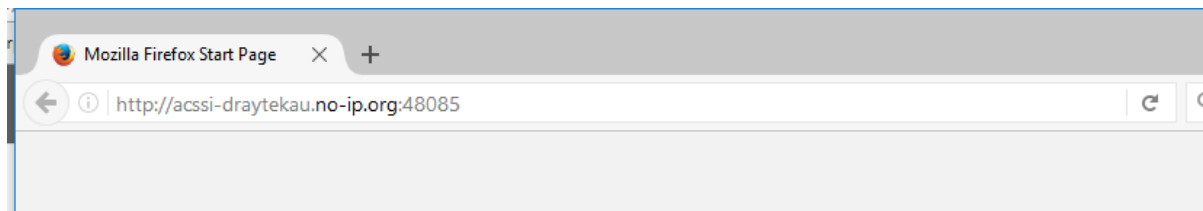
URL: `http://acssi-draytekau.no-ip.org:48085` (localhost:portnumber)
Username: `training`
Password: `xyz123`

Note: You will need to use the VigorACS Server URL to configure the TR-069 parameters in the CPE devices. If you have been supplied a laptop with VigorACS 2 pre-installed, the URL will be localhost:80 or the laptop IP address.

Logging into 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 HTTP port used is 48085, then the URL will be “localhost:48085”. (For supplied laptop HTTP port will be 80).

For example, use the web browser to connect to: <http://acssi-draytekau.no-ip.org:48085>
Or the IP address of your ACS2 Server e.g. 192.168.10.131 port 80



Enter the username and password given to you as well as the Validation code.

(Note: The default Username is “root”)

Click on **Login** to access VigorACS 2

The diagram illustrates the login process for VigorACS 2. It shows two versions of the login form, connected by a blue arrow indicating the flow from the initial state to the filled state.
Initial Login Form (Left):
- Title: Login to VigorACS 2
- Fields: User Name, Password, Validation Code
- Validation Code: 7081 (displayed in a red box)
- Remember me: ☐
- Login Button: A red button labeled 'Login'
- Footer: Copyright © 2017 DrayTek Corp. All Rights Reserved.
Filled Login Form (Right):
- Title: Login to VigorACS 2
- Fields: User Name (filled with 'root'), Password (masked with '.....'), Validation Code (filled with '6934', displayed in a red box)
- Remember me: ☐
- Login Button: A red button labeled 'Login'
- Footer: Copyright © 2017 DrayTek Corp. All Rights Reserved.

6.4 Register CPE Devices to VigorACS 2

For the following steps log into each router using each router WAN IP address once remote management is enabled in step 1 below. This will allow VigorACS 2 in the laptop to communicate with the router while TR069 is enabled.

6.4.1 Register DrayTek Routers

Step 1 – Enable TR069 Server

- Go to **System Maintenance>>Management** configuration menu in each of the routers (Vigor2862Lac and Vigor2926) enable TR069 Server.
- In Management Port Setup, leave TR069 port at 8069
- Click **OK** to save. *(The router will restart to save the settings)*

The screenshot shows the 'System Maintenance >> Management' configuration page for a DrayTek router. The page is divided into two main sections: 'IPv4 Management Setup' and 'IPv6 Management Setup'. Under 'IPv4 Management Setup', there are checkboxes for 'Default: Disable Auto-Logout', 'Enable Validation Code in Internet/LAN Access', 'Internet Access Control', 'Allow management from the Internet', 'Domain name allowed', 'FTP Server', 'HTTP Server', 'HTTPS Server', 'Telnet Server', 'TR069 Server' (highlighted with a red box), 'SSH Server', and 'Disable PING from the Internet'. Under 'IPv6 Management Setup', there is a 'Management Port Setup' section with radio buttons for 'User Define Ports' (selected) and 'Default Ports'. Below this, there are input fields for 'Telnet Port' (23), 'HTTP Port' (80), 'HTTPS Port' (443), 'FTP Port' (21), 'TR069 Port' (8069, highlighted with a red box), and 'SSH Port' (22). Each input field has its default value in parentheses. At the bottom, there is a 'TLS/SSL Encryption Setup' section with checkboxes for 'Enable TLS 1.2', 'Enable TLS 1.1', 'Enable TLS 1.0', and 'Enable SSL 3.0'.

Note: The TR069 port can be customised on this menu if required.

Step 2 – Configure TR069

Go to **System Maintenance>>TR069>>ACS and CPE Settings** configuration menu in each of the routers (Vigor2862Lac and Vigor2926) configure TR069 parameters.

- Select **Enable** for TR069
- Select **Internet** for ACS Server On
- Click on the **Wizard** button to create the ACS Server URL. In the pop-up menu enter the ACS server address and HTTP or HTTPS port and select **http** from the pull-down menu. The Handler should be left at the default setting. *(Refer to the diagram below for more details)*
- Click **OK** to save.

Note: The default login credentials for the ACS Server are:

Username: **acs**
 Password: **password**

The screenshot shows the 'System Maintenance >> TR-069 Setting' window. Under the 'ACS and CPE Settings' tab, the 'Tr069' section has 'Disable' selected. The 'ACS Server On' dropdown is set to 'Internet'. The 'ACS Server URL' field contains 'http://acssi-draytekau.no-ip.org:48084/ACSServer/services/ACS'. A red box highlights the 'Wizard' button next to the URL field. Below the URL field is a checkbox for 'Acquire URL from DHCP option 43'. The 'Username' field is 'acs' and the 'Password' field is masked with dots.

A red arrow points from the 'Wizard' button to a 'Default ACS URL - Google Chrome' dialog box. The dialog box shows the URL '192.168.1.1/doc/defaulturl.htm'. It has fields for 'http' (protocol), 'Server' (acssi-draytekau.no-ip.org), 'Port' (48084), and 'Handler' (/ACSServer/services/ACSServlet). A red arrow points to the 'Handler' field with the text 'Do not change Default Handler entry'. A yellow box on the right contains the text: 'If using the supplied laptop, enter laptop IP address for server and port 80'.

Step 3 – Configure CPE Client Settings

For **CPE Client settings**, select **http** option.

The URL is generated automatically based on the router WAN IP address.

Username: vigor

Password: password

(You can customise the port, username and password, however these must match the settings in the VigorACS 2 server).

- Enable **Periodic Inform Settings**.
- Set **Interval Time** to 900 seconds. *(Router will check for updates every 15 minutes)*

Step 4 – Enable STUN Settings if Required.

STUN settings will need to be enabled if the CPE devices are behind NAT or firewall.

- Enter the ACS 2 server address for the STUN server (*acssi-draytekau.no-ip.org*).
- Enter Server Port: 3478
- Minimum Keep Alive Period: 60 seconds
- Maximum Keep Alive Period: -1 seconds (*always on*)

The screenshot shows the 'System Maintenance >> TR-069 Setting' page. The left sidebar contains a navigation menu with options like Dashboard, WAN, LAN, Load-Balance/Route Policy, NAT, Hardware Acceleration, Firewall, User Management, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, Wireless LAN, SSL VPN, USB Application, System Maintenance, System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, SysLog / Mail Alert, Time and Date, SNMP, Management, Self-Signed Certificate, Reboot System, Firmware Upgrade, Activation, Internal Service User List, Diagnostics, Central Management, VPN, AP, and Switch. The main content area is titled 'System Maintenance >> TR-069 Setting' and has two tabs: 'ACS and CPE Settings' and 'Export Parameters'. Under 'ACS and CPE Settings', there are sections for 'Tr069' (with 'Disable' and 'Enable' radio buttons, 'Enable' is selected), 'ACS Server On' (with a dropdown menu set to 'Internet'), 'ACS Server' (with fields for 'URL', 'Username', and 'Password', and a 'Test With Inform' button), and 'CPE Client' (with 'Http' and 'Https' radio buttons, 'Http' is selected, and fields for 'URL', 'Port', 'Username', and 'Password'). Below these are 'Periodic Inform Settings' (with 'Disable' and 'Enable' radio buttons, 'Enable' is selected, and an 'Interval Time' field set to '900 second(s)') and 'STUN Settings' (with 'Disable' and 'Enable' radio buttons, 'Enable' is selected, and fields for 'Server Address', 'Server Port', 'Minimum Keep Alive Period', and 'Maximum Keep Alive Period'). The 'Last Inform Response Time' is displayed as 'Fri Sep 15 3:31:34 2017' with a green status indicator.

Click on “**Test With Inform**” button for the router to poll ACS 2 server. You should see a green status indicator if the ACS 2 server has responded.

Note: If you do not see the green status indicator for “Last Inform Response Time” Ensure that both “TR069 Server” and “Allow management from the Internet” are enabled as shown in the diagram for step 1 above.

6.4.2 Register DrayTek Access Point to ACS 2

Connect your laptop to the Vigor2862Lac router.

Configure Vigor2862Lac TR-069 settings for attached Access Point.

This method will auto configure the VigorAP902 with the TR069 settings.

- Go to **System Maintenance >> TR-069 Setting** menu.
 - In **Apply Settings to Aps** section select enable
 - Enter AP Password (*admin*)
 - Select **Apply Specific STUN Setting to Aps**
 - Select Enable
 - Enter VigorACS 2 server IP address
 - Keep Server port at 3478 and other settings at default values.

The screenshot shows the DrayTek Vigor2862 Series web interface. The left sidebar contains a menu with options like Dashboard, WAN, LAN, Hotspot Web Portal, Routing, NAT, Hardware Acceleration, Firewall, User Management, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, LTE, Wireless LAN (2.4 GHz), Wireless LAN (5 GHz), SSL VPN, USB Application, System Maintenance, System Status, **TR-069**, Administrator Password, User Password, Login Page Greeting, Configuration Backup, SysLog / Mail Alert, Time and Date, SNMP, Management, Panel Control, Self-Signed Certificate, Reboot System, Firmware Upgrade, Firmware Backup, Modem Code Upgrade, Activation, Internal Service User List, Dashboard Control, Diagnostics, Central Management, VPN, and AP.

The main content area displays the TR-069 settings. The 'CPE Client' section shows 'Http' selected, with a URL of 'http://192.168.101.31:8069/cwm/CRN.html', Port '8069', Username 'vigor', and Password '*****'. The 'Periodic Inform Settings' section shows 'Enable' selected with an interval of 900 seconds. The 'STUN Settings' section shows 'Enable' selected, with a Server Address of 'http://192.168.100.181', Server Port of '3478', Minimum Keep Alive Period of 60 seconds, and Maximum Keep Alive Period of -1 seconds.

The 'Apply Settings to Aps' section is highlighted with a red box. It shows 'Enable' selected for 'Apply Settings to Aps', with an AP Password of '*****'. The 'Apply Specific STUN Settings to Aps' section is also checked, with 'Enable' selected, and the same STUN settings as above: Server Address '192.168.101.36', Server Port '3478', Minimum Keep Alive Period '60' seconds, and Maximum Keep Alive Period '-1' seconds.

Alternative method to configure TR069 settings in VigorAP902

- Log into the VigorAP902 using the IP address 192.168.1.2
- Go to System Maintenance >> TR-069 Settings menu and enter the required settings.
- Click on the Wizard button.
- Click on the **Wizard** button to create the ACS Server URL. In the pop-up menu enter the ACS server address and HTTP or HTTPS port and select **http** from the pull-down menu. The Handler should be left at the default setting. (Refer to the diagram below for more details)
- Click **OK** to save.

Note: The default login credentials for the ACS Server are:

Username: *acs*
 Password: *password*

DrayTek VigorAP 902

System Maintenance >> TR-069 Settings

ACS Settings

URL: **Wizard**

Username:

Password:

Test With Inform: Event Code:

Last Inform Response Time :Thu Jan 01 1970 11:03:24 GMT+1100 (AUS Eastern Daylight Time)

CPE Settings

Enable: ☒

SSL(HTTPS) Mode: ☐

On:

URL:

Port:

Username:

Password:

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note : SSL(HTTPS) Mode only works when Vigor ACS SI is 1.1.6 and above version.
 Please set default gateway, no matter choose LAN-A or LAN-B.

Periodic Inform Settings

Enable: ☒

Interval Time: second(s)

STUN Settings

☐ Enable ☒ Disable

Server Address:

Server Port:

Minimum Keep Alive Period: second(s)

Maximum Keep Alive Period: second(s)

Default ACS URL - Google Chrome

192.168.1.1/doc/defaulturl.htm

Enter Server address and http port

Protocol: http

Server: 192.168.100.181

Port: 80

Handler: /ACSServer/services/ACSServlet

OK

Do not change Default Handler entry

If using the supplied laptop, enter laptop IP address for server and port 80

CPE Settings

- Select **Enable**.
- URL is auto generated. So, no need to change
- Leave port at 8069
- Enter Username: vigor
- Enter Password: password

Periodic Inform Settings

- Select Enable and set Interval Time to 900 seconds

STUN Settings

- Select Enable
- Enter the ACS 2 server address for the STUN server (*URL for your VigorACS 2 server*).
- Enter Server Port: 3478
- Minimum Keep Alive Period: 60 seconds
- Maximum Keep Alive Period: -1 seconds

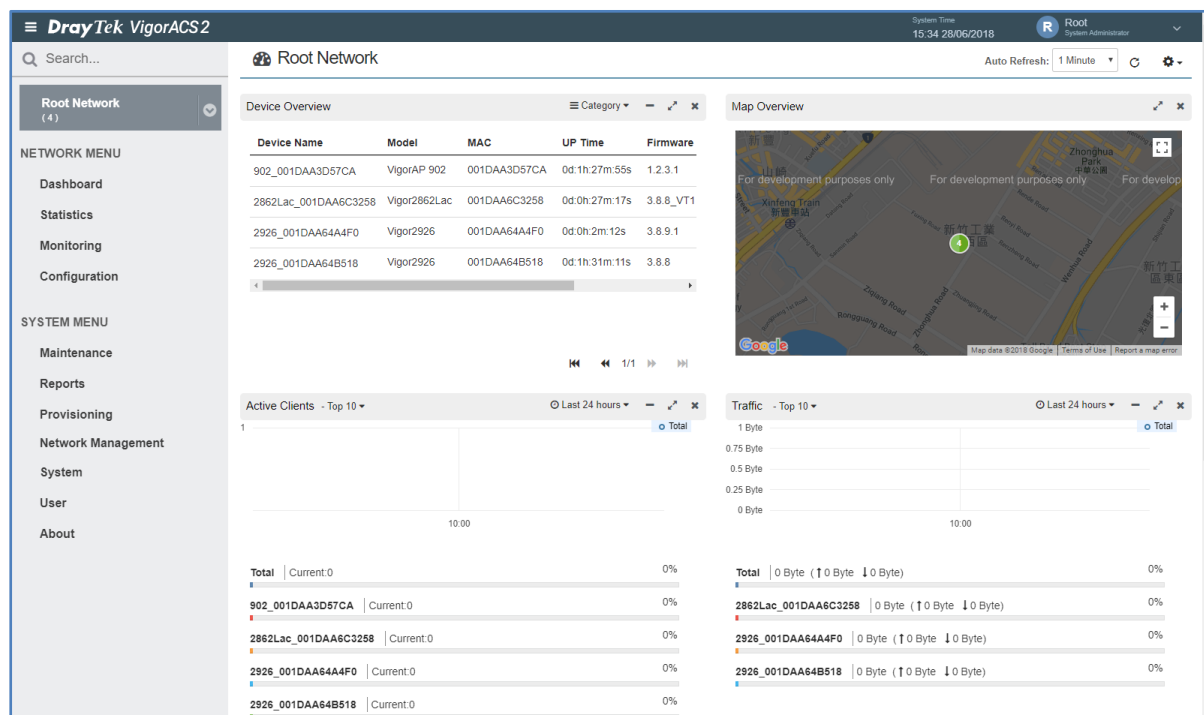
Click **OK** to save the settings.

6.4.3 Verify that CPE devices have Registered to ACS 2

To verify that all the CPE devices have successfully registered to ACS 2, log into ACS 2 console using the username and password provided.

You should see the **Root Network** page with 4 CPE devices listed.

Statistics for registered devices will also be displayed on this page as well as the Map Overview. The map does not show the local area and this will be configured in the next exercise.



At the bottom of the Root Network page is a list of new devices registered with ACS 2. By default, they all appear under the root network.

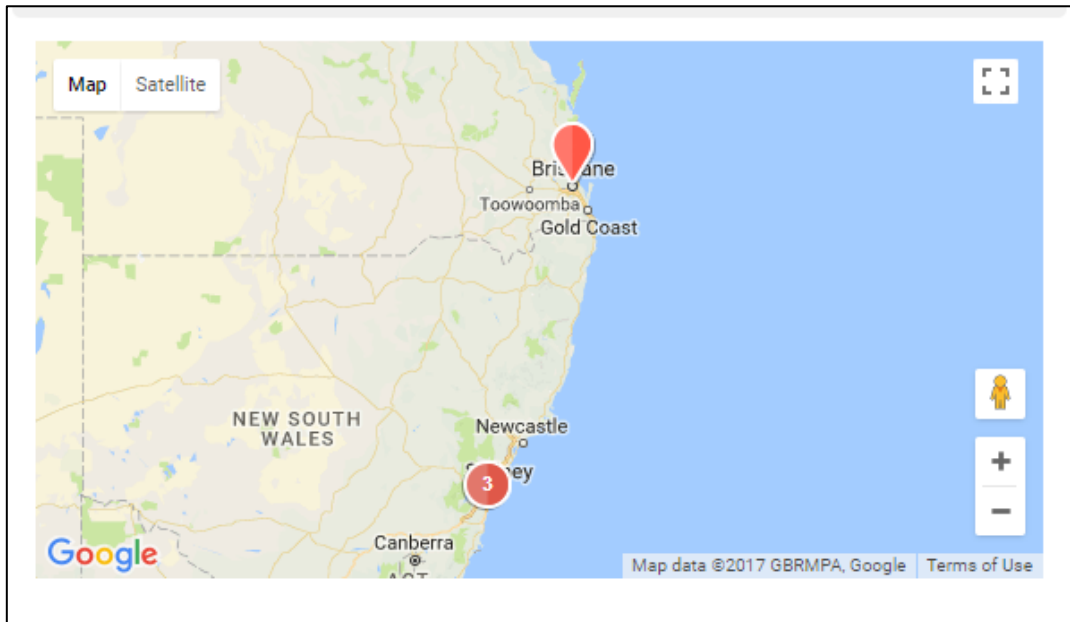
New Devices			
Action	IP Address	Device Name	Device Type
	192.168.1.2:80	902_001DAA3D57CA	VigorAP 902
	192.168.101.31:80	2862Lac_001DAA6C3258	Vigor2862Lac
	192.168.101.20:80	2926_001DAA64A4F0	Vigor2926
	192.168.101.29:80	2926_001DAA64B518	Vigor2926

7. Exercise – Part 2: Managing CPE Devices in VigorACS 2

For this exercise we will place the devices in two locations:

- Three CPE devices in the Seven Hills Office (Training Lab)
- One CPE device in the Brisbane Office.

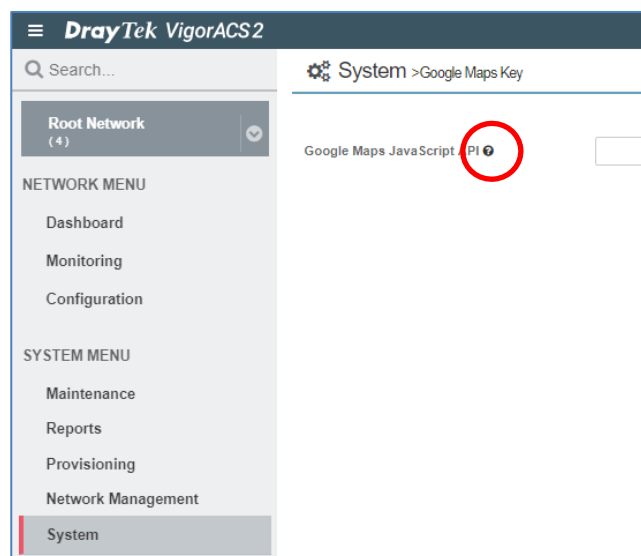
We will create the two networks and place the CPE devices into these networks. In addition, specify the locations of these devices so they appear in the correct location on Google Maps.



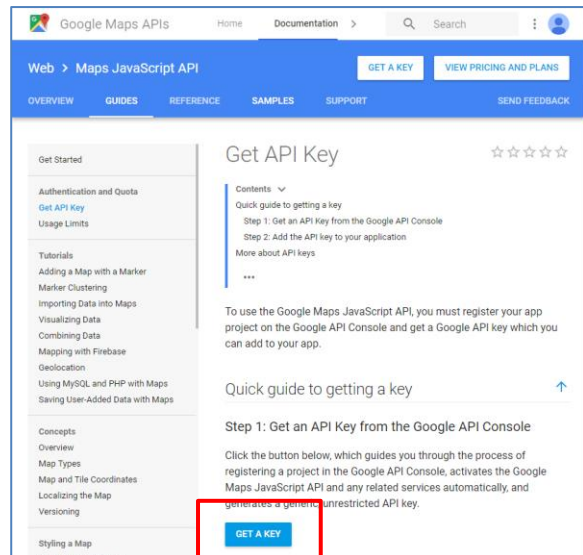
7.1 Google Maps Key (Optional)

Before using the API of Google Map, it may be necessary to apply and get a key from Google. Type the key in this page to activate the Google Map. After clicking Save, VigorACS will be granted permission to display the map on the dashboard. (This step is not required for this workshop exercise)

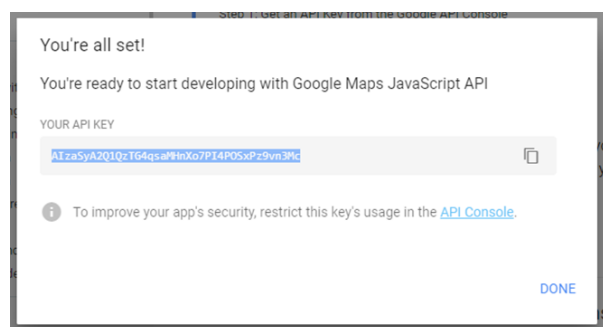
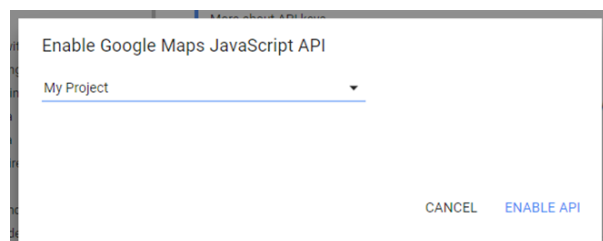
- In System menu click on Google Maps Key submenu.
- Click on the “?” to go to Google Maps API page



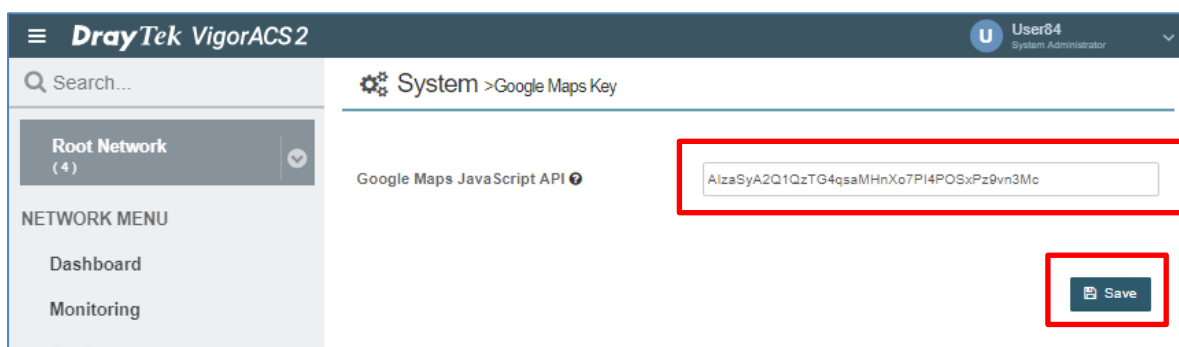
- Click on “Get a Key”



- Follow the prompts
- Once the key is generated, Copy and paste into ACS SI



- Click **Save**



7.2 Creating Networks in ACS 2

We will create two networks under the Root network: Training Lab & Brisbane Office.

7.2.1 Create Training Lab Network

In the ACS 2 console, under SYSTEM MENU, click on **Network Management** menu option.

- Click on **Add New Network**.

While on this page you can also enter the location of the Root Network so it will appear correctly in the Map view.

For the root network, change the location to Seven Hills, NSW, Australia so it will appear in Australia.

The screenshot shows the DrayTek VigorACS2 web interface. On the left, the 'SYSTEM MENU' is visible with 'Network Management' selected. The main content area is titled 'Network Management' and shows a list of networks under 'Root Network(4)'. A red box highlights the '+ Add New Network' button. Below this, the 'Setting' tab is active, showing fields for 'Network ID' (2), 'User Name' (acs), 'Name' (Root Network), 'Password' (password), and 'Location' (seven hills NSW AUstralia). A red arrow points from a text box to the 'Location' field.

Add location details so it will appear on the Map

Under Root Network, click on **Add New Network** and enter the following details:

- **Name:** Training Lab
- **Location:** Seven Hills, NSW, Australia
- **User Name:** acs1 (*Each network must have a unique username*)
- **Password:** password

Click on **Add** to save and add this network under the Root Network.

The screenshot shows the 'Setting' tab of a network management interface. At the top, there are two tabs: 'Setting' (active) and 'Map'. Below the tabs, there are three links: '+ Add New Network', 'Delete This Network', and 'Change Network'. The main form contains the following fields:

- Network ID:** A dropdown menu with the value '3' selected.
- User Name:** A text input field containing 'acs1'.
- Name:** A text input field containing 'Training Lab'.
- Password:** A text input field containing 'password'.
- Location:** A text input field containing 'Seven Hills, NSW, Australia'.

A 'Save' button is located at the bottom right of the form.

7.2.2 Create Brisbane Office Network

Under Root Network, click on **Add New Network** and enter the following details:

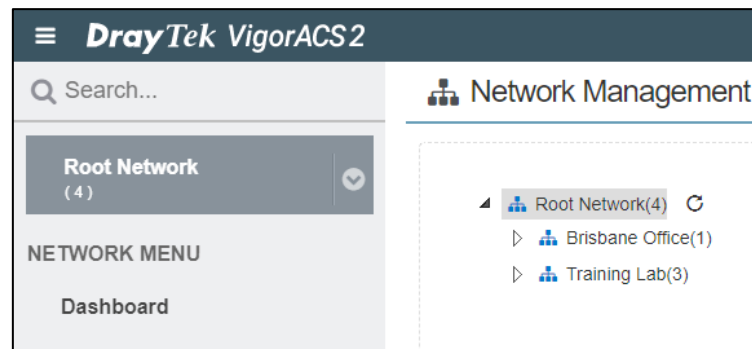
- **Name:** Brisbane Office
- **Location:** Brisbane
- **User Name:** acs2
- **Password:** password

Click on **Add** to save and add this network under the Root Network.

The screenshot shows the 'Network Management' interface with a dialog box titled '+ Add Network' open. The dialog box contains the following fields:

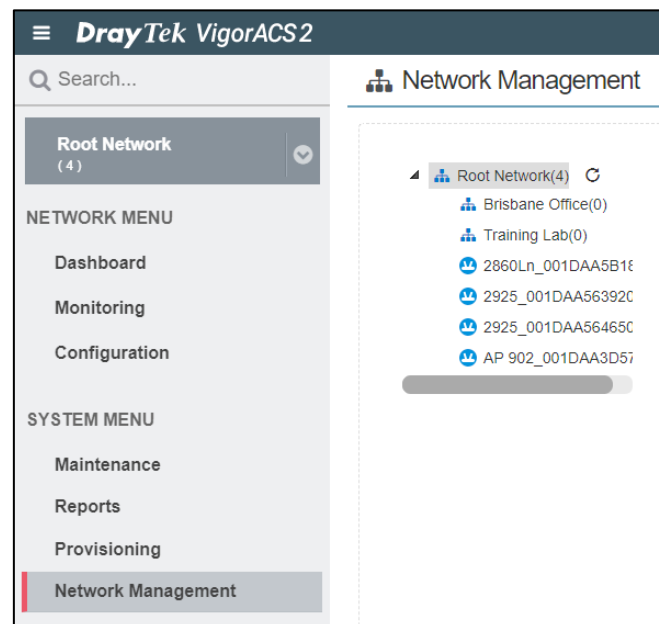
- Parent Network:** A dropdown menu with 'Root Network' selected.
- Name:** A text input field containing 'Brisbane Network' with a green checkmark icon to its right.
- Location:** A text input field containing 'Brisbane, Queensland'.
- User Name:** A text input field containing 'acs2' with a green checkmark icon to its right.
- Password:** A text input field containing 'password'.

Once the two networks are added you should see the two new networks appear under the root network.

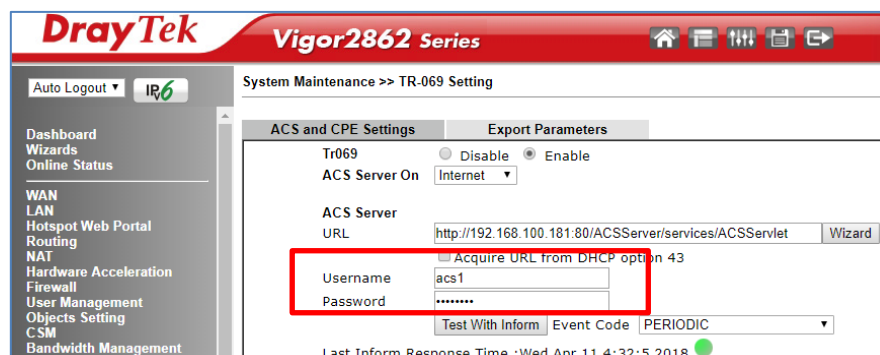


7.3 Move CPE Devices into the Networks

When the CPE devices are first registered with ACS 2, they will appear under the Root network. The two networks created in the previous step also appear under the Root Network and have the network icon next to the names.

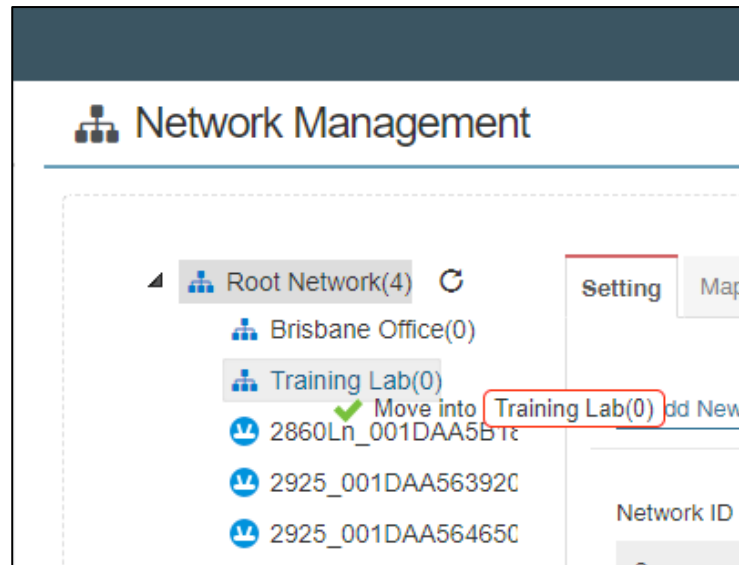


Changing the TR069 username in ACS server settings to the username for each network will move the device to that network when it registers. For example, for the Vigor2862Lac, change the username to acs1, will move it to the Training Lab in Seven Hills.



Another method is to drag the CPE device to the required network. For Windows version of VigorACS 2, this will work if ACS username is different to what is required for the network, but for Linux Version of VigorACS 2, the CPE must use the username for the network.

To move the CPE device, select the CPE from the page and drag into the required network as shown here.

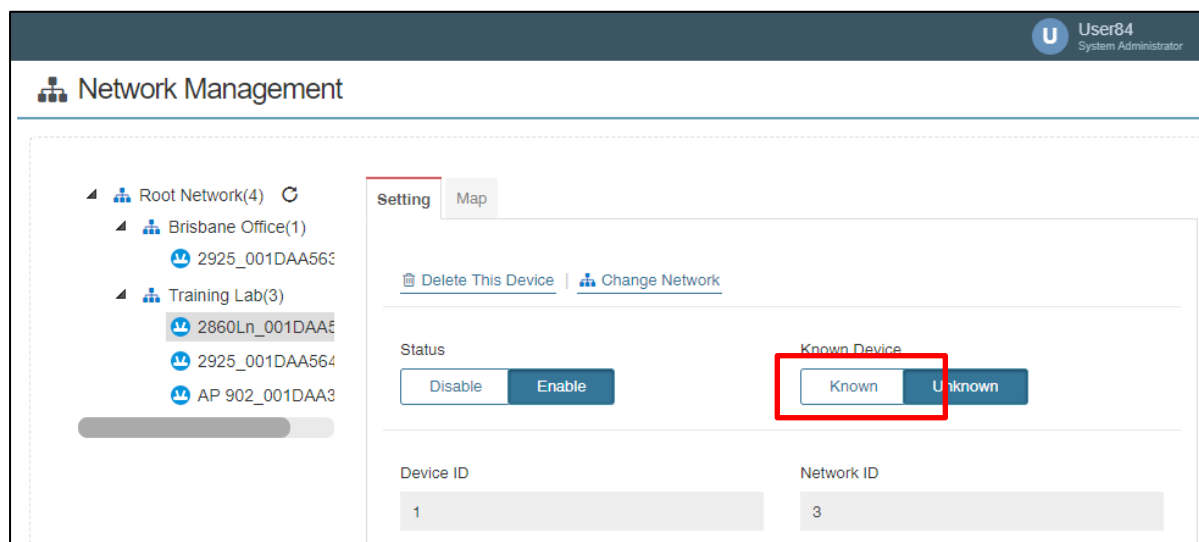


- Drag and drop the CPE devices into to the two networks:

Brisbane: Vigor2926

Training Lab: Vigor2862Lac, Vigor2926, VigorAP 902

When the CPE devices are first registered with ACS 2, they will be an “**Unknown**” device. Click on “**Known**” so that it can be monitored and managed.



- Click on each CPE device and select Known and enter the location address for each device so that it will appear correctly in the Map view.
- Click **Save** to save the settings

Network Management

Root Network(4)
 Brisbane Office(1)
 2925_001DAA563920
 Training Lab(3)
 2860Ln_001DAA5B1800
 2925_001DAA564650
 AP 902_001DAA3D578A

Setting | Map

Delete This Device | Change Network

Status: **Known Device**

Device ID: 1 Network ID: 3

Model Name: Vigor2860Ln Device Name: 2860Ln_001DAA5B1800

Note 1: Note 2:

Serial number: MAC Address: 001DAA5B1800

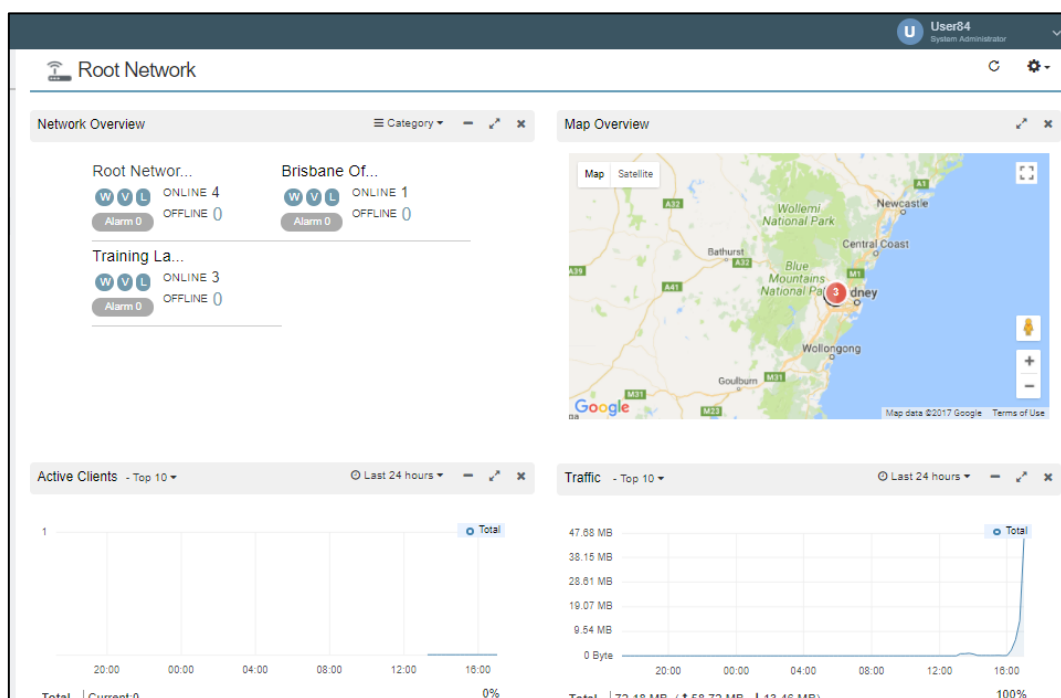
Location: 128 Station Road Seven Hills IP: 192.168.101.178

Phone No.: Port: 8069

Domain Name: URI: /cwm/GRN.html

Management Port: 80 User Name: vigor

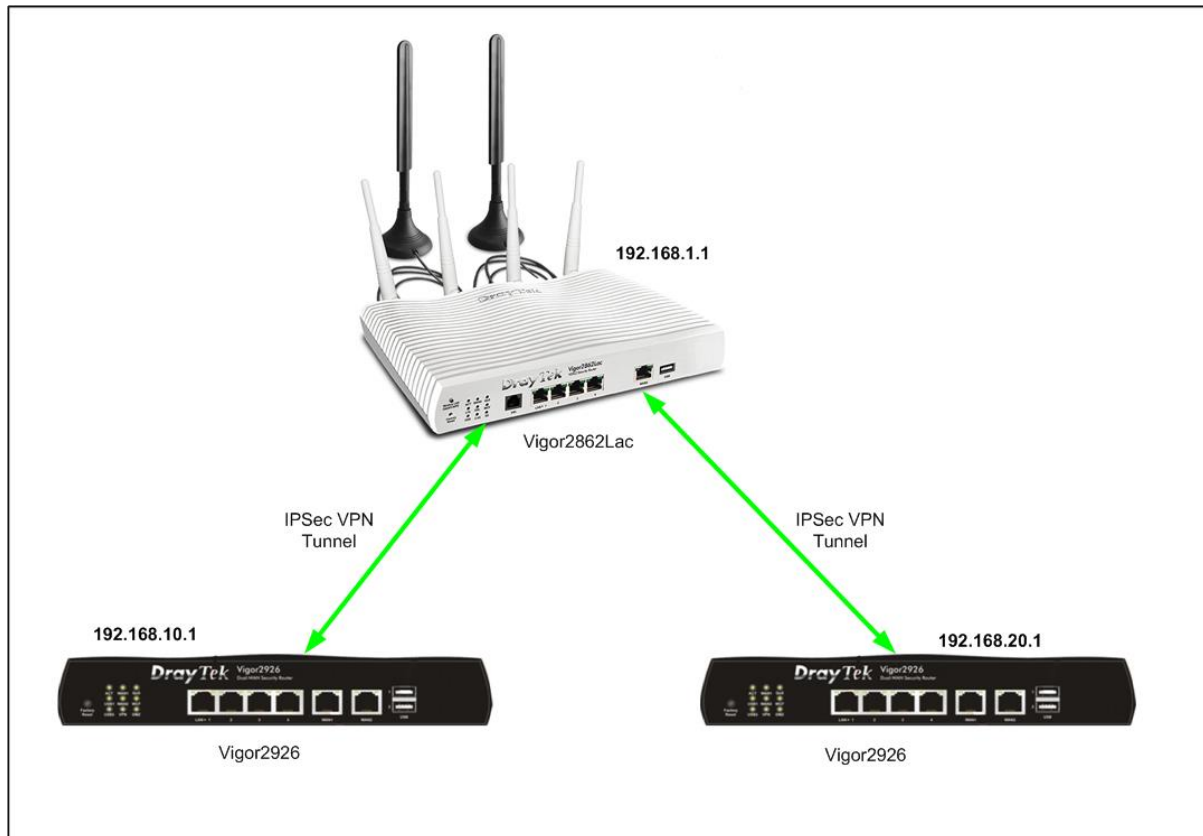
Management Protocol: Password: password



Dashboard View when set up Complete

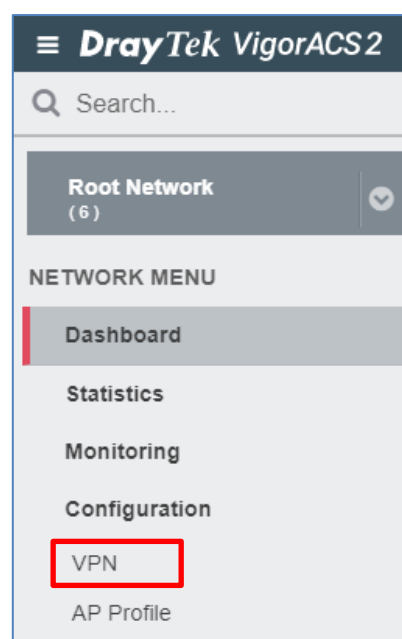
8. Exercise – Part 3: Create VPN Tunnels Using VigorACS 2

For this exercise, we will create two VPN tunnels between the routers as shown in the diagram below. Two IPSec VPN tunnels will be created between the Vigor2862Lac router and each of the Vigor2926 routers.

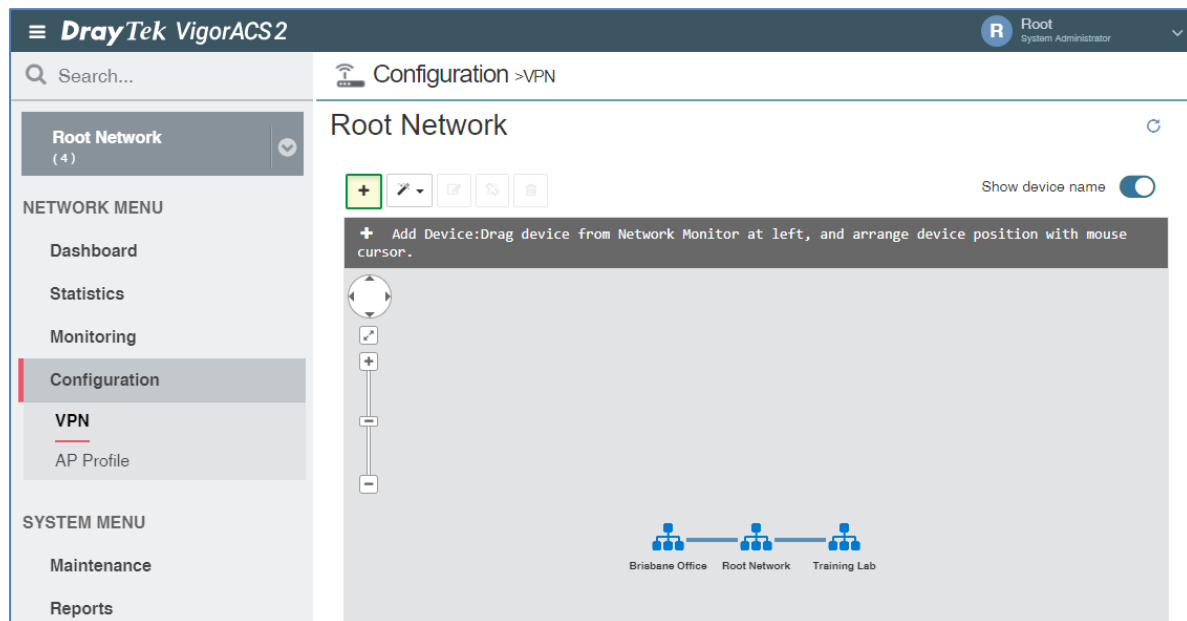


8.1 Create VPN tunnel Between Vigor2862Lac and Vigor2926 Router

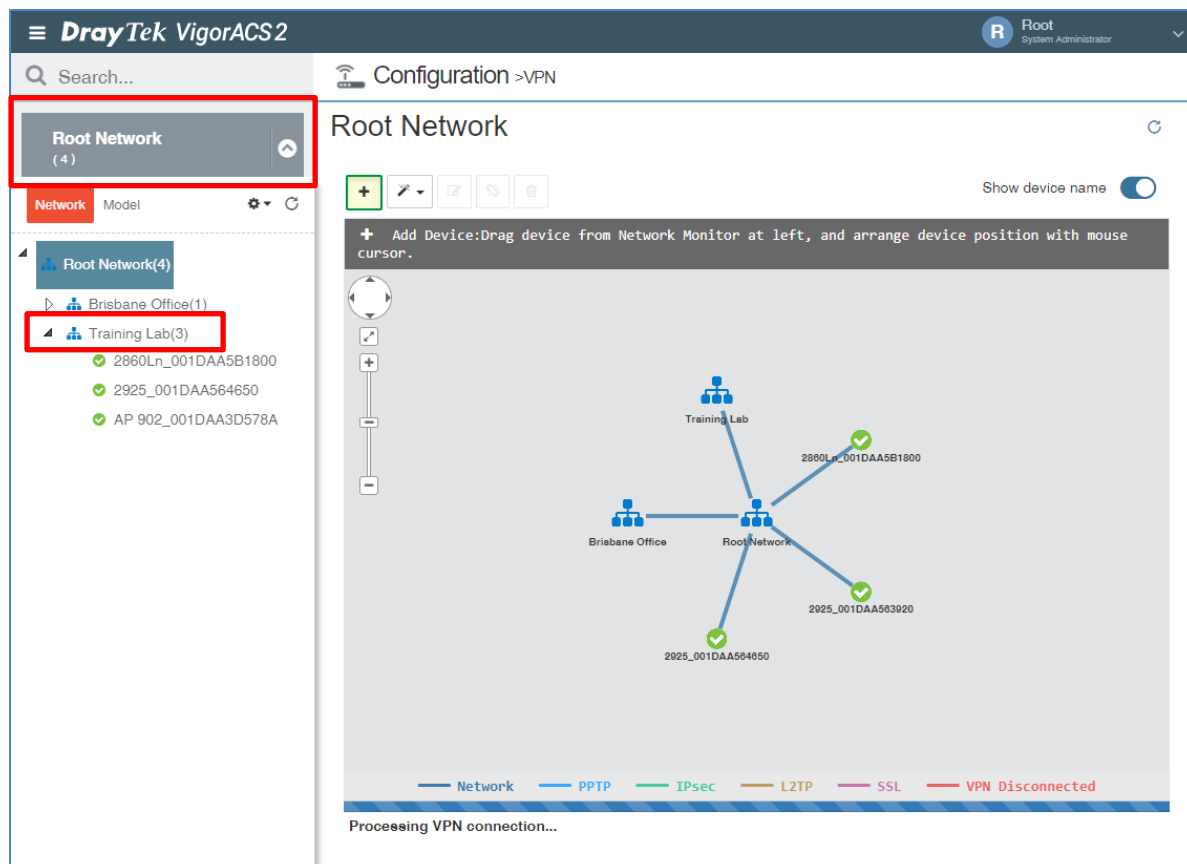
- In VigorACS 2 menu click on the **Configuration** sub menu under the Dashboard menu.
- Click on **VPN** menu option.



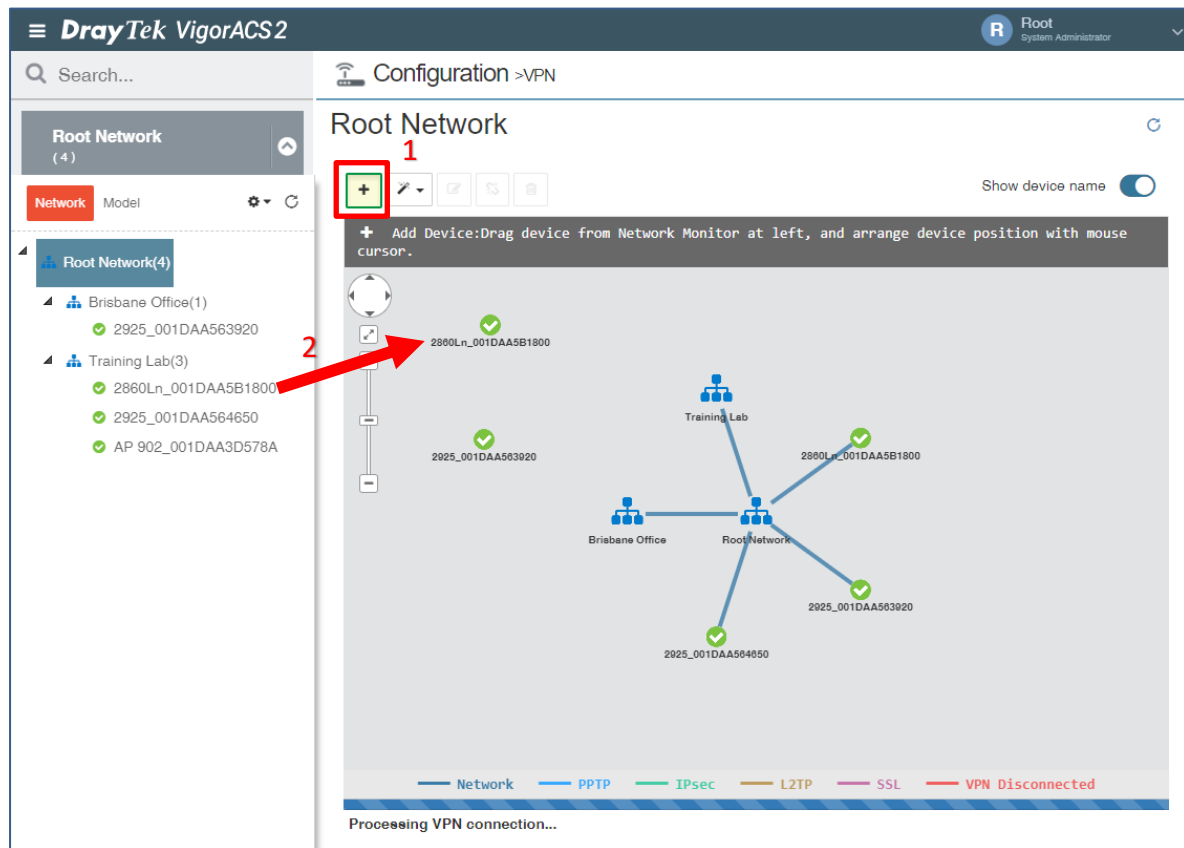
You should see a page appear like that below showing the VPN configuration screen for the Root Network.



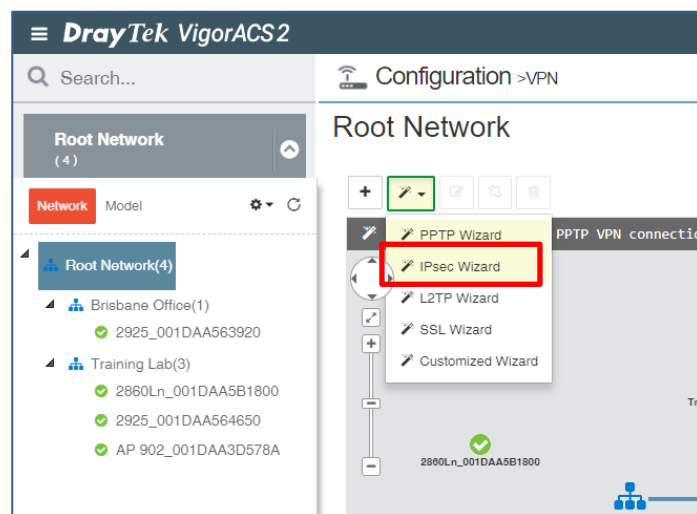
- Now click on the Root Network at the top of the menu bar and expand the networks below. You should see the routers appear in the diagram.



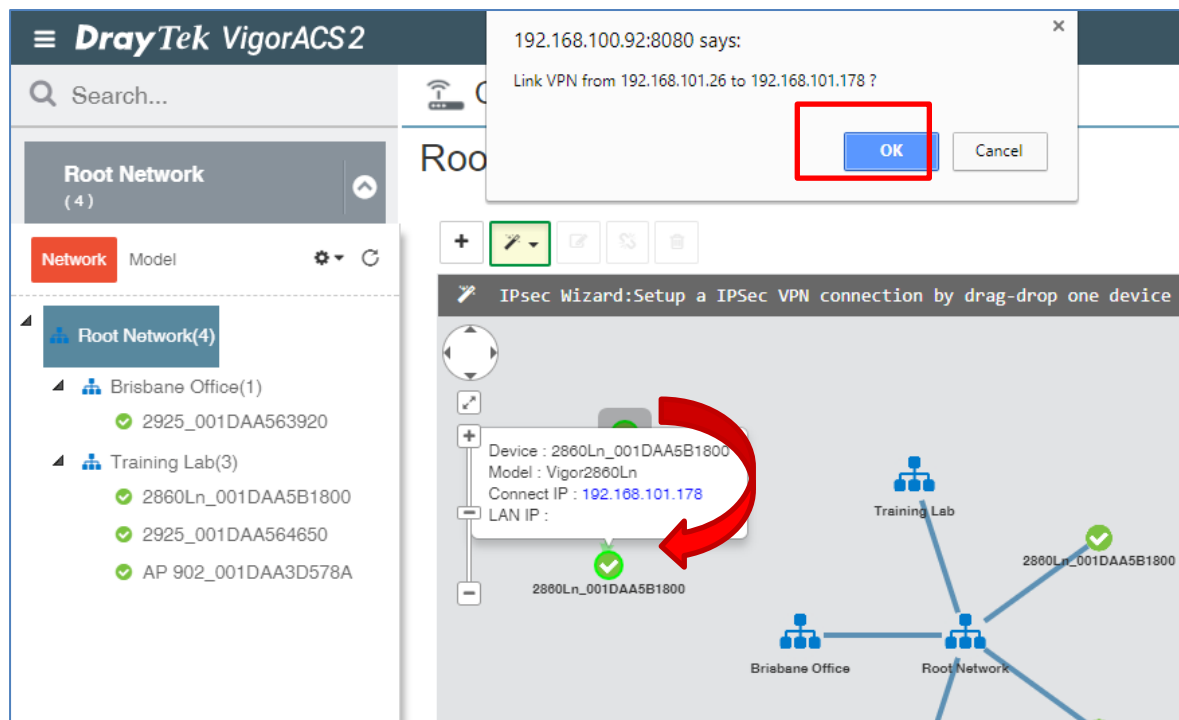
- Click on **[+]** to start adding devices to the VPN configuration page. (Step 1)
- Select the Vigor2862Lac router from the Training Lab network and drag into the VPN configuration page. (step 2)
- Similarly click the Vigor2926 router from the Brisbane network and drag to the VPN configuration page.



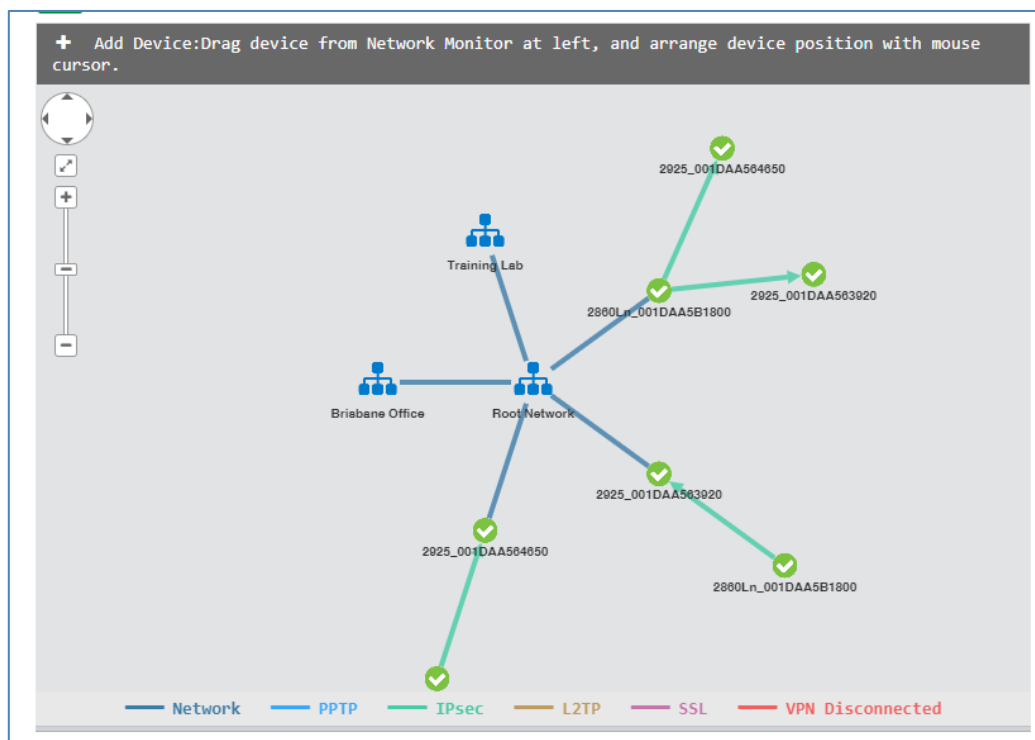
- Click on the pull-down menu and select IPsec Wizard.



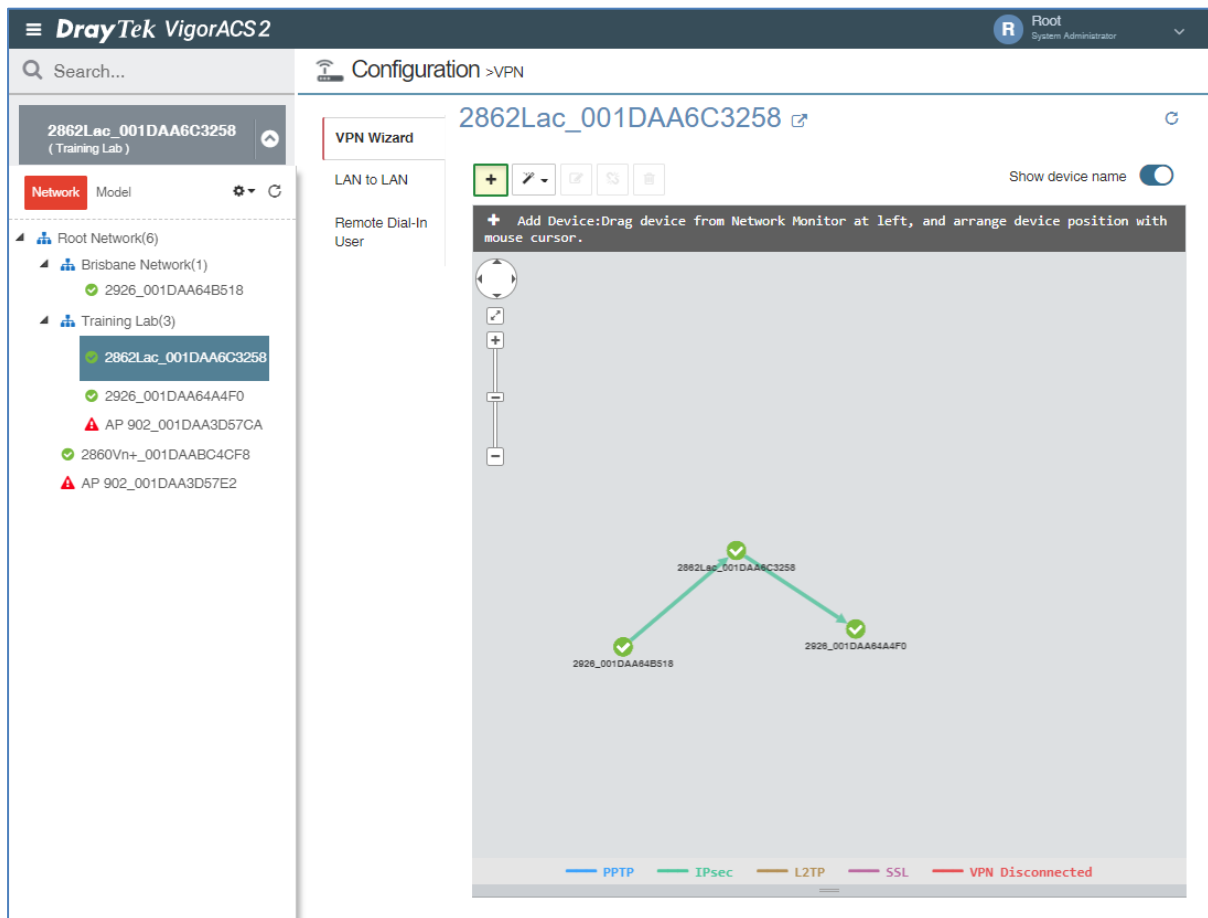
- Place mouse over the Vigor2862Lac router icon and drag over the Vigor2926 router icon.
- You should see a message appear indicating the VPN tunnel is being created.
- Click OK to create the VPN tunnel.



- Similarly create a VPN tunnel between the Vigor2862Lac and the other Vigor2926 router.
- You should see the VPN tunnels appear between the routers. The coloured lines indicate the type of VPN tunnel.



- Click on the Vigor2862Lac router in the Training Lab network to see all the VPN tunnels originating from this router.



8.2 Check VPN tunnel Configuration in the Routers

Once the VPN tunnels are configured using VigorACS 2 you can log into each router and confirm the VPN profiles created and connection status

8.2.1 Vigor2862Lac Router VPN Status

Log into the Vigor2862Lac router and go to **VPN and Remote Access >> LAN to LAN** menu. You should see two VPN profiles that have been created.

DrayTek Vigor2862 Series

Auto Logout **IPv6**

VPN and Remote Access >> LAN to LAN ?

LAN-to-LAN Profiles: [Set to Factory Default](#)

View: ☒ All ☐ Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	i_4F0_258	☒	Online	17.	???	☐	---
2.	i_258_518	☒	Online	18.	???	☐	---
3.	???	☐	---	19.	???	☐	---
4.	???	☐	---	20.	???	☐	---
5.	???	☐	---	21.	???	☐	---
6.	???	☐	---	22.	???	☐	---
7.	???	☐	---	23.	???	☐	---
8.	???	☐	---	24.	???	☐	---
9.	???	☐	---	25.	???	☐	---
10.	???	☐	---	26.	???	☐	---
11.	???	☐	---	27.	???	☐	---
12.	???	☐	---	28.	???	☐	---
13.	???	☐	---	29.	???	☐	---
14.	???	☐	---	30.	???	☐	---

Connection Management Status

DrayTek Vigor2862 Series

Auto Logout **IPv6**

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode: (i_4F0_258) 192.168.101.71

Backup Mode:

Load Balance Mode:

VPN Connection Status

LAN-to-LAN VPN Status

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
1 (i_4F0_258)	IPsec Tunnel 3DES-No Auth	192.168.101.71 via WAN2	192.168.10.0/24	0	0	2	24	0:3:25	Drop
2 (i_258_518)	IPsec Tunnel 3DES-No Auth	192.168.101.70 via WAN2	192.168.20.0/24	0	0	1	24	0:1:57	Drop

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

8.2.1 Vigor2926 Router VPN Status

Log into each Vigor2926 router and go to **VPN and Remote Access >> LAN to LAN** menu. You should see the VPN profiles that has been created.

Router A

DrayTek Vigor2926 Series

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: [Set to Factory Default](#)

View: ☒ All ☐ Online ☐ Offline ☐ Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	i_258_4F0	☒	Online	17.	???	☐	---
2.	???	☐	---	18.	???	☐	---
3.	???	☐	---	19.	???	☐	---

Connection Management Status

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode: (i_258_4F0) 192.168.101.64

Backup Mode:

Load Balance Mode:

VPN Connection Status

LAN-to-LAN VPN Status				Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 (i_258_4F0)	IPsec Tunnel 3DES-No Auth	192.168.101.64 via WAN1	192.168.1.0/24	1397	85.72	901	7.78	0:7:54 Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

Router B

DrayTek Vigor2926 Series

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: [Set to Factory Default](#)

View: ☒ All ☐ Online ☐ Offline ☐ Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	i_258_518	☒	Online	17.	???	☐	---
2.	???	☐	---	18.	???	☐	---

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode: (i_258_518) 192.168.101.64

Backup Mode:

Load Balance Mode:

VPN Connection Status

LAN-to-LAN VPN Status				Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime
1 (i_258_518)	IPsec Tunnel 3DES-No Auth	192.168.101.64 via WAN1	192.168.1.0/24	0	0	0	0	0:0:23 Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

9. Exercise – Part 4: Generate Reports in VigorACS 2

Create a report for firmware versions installed in CPE devices

- Go to **SYSTEM MENU**
- 1. Click on **Reports**.
 - a. Click on **Reports** submenu.
- 2. Click on **Create a Report** at the top of the page on the right.
- 3. Under “Select report type” select **Firmware**.
- 4. Select **Firmware Overview**.
- 5. Select all devices in Root Network.
- 6. Click on Query to generate the report.

DrayTek VigorACS2 System Time: 15:58 29/06/2018 Root System Administrator

Search... Report

Create a Report

+ Create new report

Select report type

Firmware Overview

Firmware Overview

Select devices

Model Name: ALL Modern Version: ALL Severity: ALL

Name	Model Name	Firmware Version
Root Network(4)		
902_001DAA3D57CA	VigorAP 902	1.2.3.1
2862Lac_001DAA6C3258	Vigor2862Lac	3.8.8_VT1
2926_001DAA64A4F0	Vigor2926	3.8.9.1
2926_001DAA64B518	Vigor2926	3.8.8

Cancel Query

Please input text here

Report 1

AdMvKuYKZW5kc3RyZWZlcmVudG9iaGoxIDAgb2JqPDwvR3J... 1 / 1

VigorACS Report

Firmware Overview Report

Device Total Count:4

Device Name	IP	Model	Firmware Version
2862Lac_001DAA6C3258	192.168.101.31	Vigor2862Lac	3.8.8_VT1
902_001DAA3D57CA	192.168.1.2	VigorAP 902	1.2.3.1
2926_001DAA64A4F0	192.168.101.20	Vigor2926	3.8.9.1
2926_001DAA64B518	192.168.101.29	Vigor2926	3.8.8

Optional Reports

You can also try generating other type of reports as in the examples below:

Create CPE Status Overview Report

+ Create new report

Select report type

Status Overview

Status
Status Overview

Select devices

Model Name
Modem Version
Severity

ALL
ALL
ALL

Name	Model Name	Firmware Version
Root Network(4)		
902_001DAA3D57CA	VigorAP 902	1.2.3.1
2862Lac_001DAA6C3258	Vigor2862Lac	3.8.8_VT1
2926_001DAA64A4F0	Vigor2926	3.8.9.1
2926_001DAA64B518	Vigor2926	3.8.8

VigorACS Report					
Status Overview Report					
Device Total Count:4					
Severity	Device Name	MAC Address	IP	Model	
Normal	2862Lac_001DAA6C3258	001DAA6C3258	192.168.101.31	Vigor2862Lac	
Normal	902_001DAA3D57CA	001DAA3D57CA	192.168.1.2	VigorAP 902	
Normal	2926_001DAA64A4F0	001DAA64A4F0	192.168.101.20	Vigor2926	
Normal	2926_001DAA64B518	001DAA64B518	192.168.101.29	Vigor2926	

NAT Graph Report

Select report type

NAT Graph

Traffic

NAT Graph

Select time interval

Preset

Custom

Start day

06/26/2018

End day

07/03/2018

Start time

12:00 AM

End time

11:59 PM

Select devices

Model Name

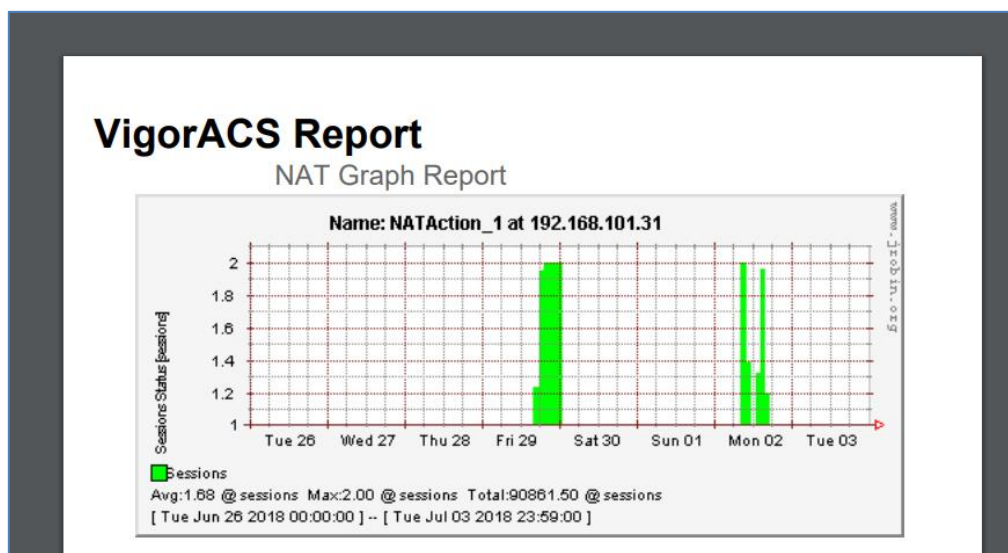
ALL

Modem Version

ALL

Severity

ALL



Appendix

Schematic layout to show where the Backup files are stored in the ACS 2

