

DrayTek

VigorConnect

The Management Software Connects Your Vigor Devices

USER'S GUIDE

V1.3

VigorConnect

The Management Software Connects Your Vigor Devices

User's Guide

Version: 1.3

Firmware Version: V1.9.1

Date: May 22, 2024

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, 11 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.

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

Customer Remedies

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

No Other Warranties

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

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

Table of Contents

Part I Introduction	I
Chapter 1 Introduction	2
1.1 Introduction	2
1.2 Installation	3
Chapter 2 Getting Started	7
2.1 Accessing to Web User Interface	7
2.2 Changing Password	9
2.3 Dashboard	10
2.3.1 Dashboard for Root Network	10
2.3.2 Dashboard for a Device	10
2.3.3 Menu Bar	12
2.3.4 Root Network and Selected CPE	13
2.3.5 Set Password, Two-factor Authentication, and Log Out.....	14
2.3.6 Auto Refresh, Manual Refresh, and Widget	18
2.3.7 Overviews.....	19
2.3.8 Icons Used in VigorConnect.....	21
Applications.....	22
A.1 How to Create a New Network?.....	22
A.2 How to Assign a New Added Device to a Network?	24
Part II System and User Settings Management.....	27
Chapter 3 System Menu.....	28
3.1 System Parameter	28
3.2 Logs.....	30
3.3 ACS	32
3.4 Service Control	33
3.5 Syslog Setup	33
3.6 Reboot System	34
Chapter 4 User Menu	35
4.1 User Management.....	36
4.2 External Authentication Server	38
4.3 Mail Server	40
4.4 SMS Server	42
Chapter 5 About VigorConnect	43
5.1 Update.....	43
5.2 License Agreements	43
Applications.....	45
A.1 How to Create a Network for Managing Devices?.....	45
A.2 How to Change the Network of a Device?.....	46
A.3 How to Add a User?	49
Part III General Settings for Managing Device	51
Chapter 6 Network Management	52
6.1 Setting.....	52
Chapter 7 Maintenance Menu.....	57
7.1 Scheduled Backup	57
7.1.1 Networks & Devices.....	57
7.1.2 Backup Settings Profile	58
7.2 Configuration Restore.....	61
7.2.1 Apply to Devices	61
7.2.2 Restore Settings Profile.....	62
7.3 Firmware Upgrade.....	64
7.4 Device Reboot	68
7.4.1 Networks & Devices.....	68

7.4.2 Reboot Settings Profile.....	69
7.5 Schedule Profile	71
7.6 File Manager	72

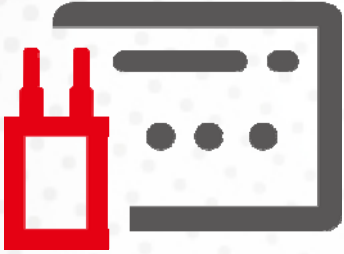
Part IV Network Menu for Root Network 74

Chapter 8 Root Network Menu	75
8.1 Dashboard for the Root Network.....	75
8.2 Monitoring Menu	76
8.2.1 Alarm.....	76
8.2.2 VPN.....	78
8.2.3 Logs	80
8.2.4 Devices.....	81
8.2.5 Floor Plan	83
8.2.6 Rogue AP Detection	88
8.2.7 Flow	90
8.3 Configuration Menu	91
8.3.1 Wireless Wizard	91
8.3.2 Mesh	95
8.3.3 AP Profile	99
8.3.4 Switch Alert Setup	104
8.3.5 Flow Alert Setup	104
8.3.6 VPN Analytics Setup.....	107

Part V Device Menu for a CPE..... 112

Chapter 9 Device Menu	113
9.1 Dashboard for CPE	113
9.2 Monitoring Menu	115
9.2.1 Alarm for a Switch.....	115
9.2.2 Logs for a Switch	116
9.2.3 Flow for a Switch	117
9.2.4 Alarm for an AP	119
9.2.5 Logs for an AP.....	121
9.3 Configuration.....	122
9.3.1 VLAN Settings for a Switch.....	122
9.3.2 sFlow Settings for a Switch	127
9.3.3 PoE	128
9.3.4 SysLog Settings for a Switch	131
9.3.5 Mesh for an AP	132
9.3.6 SysLog Settings for an AP.....	134

Part I Introduction



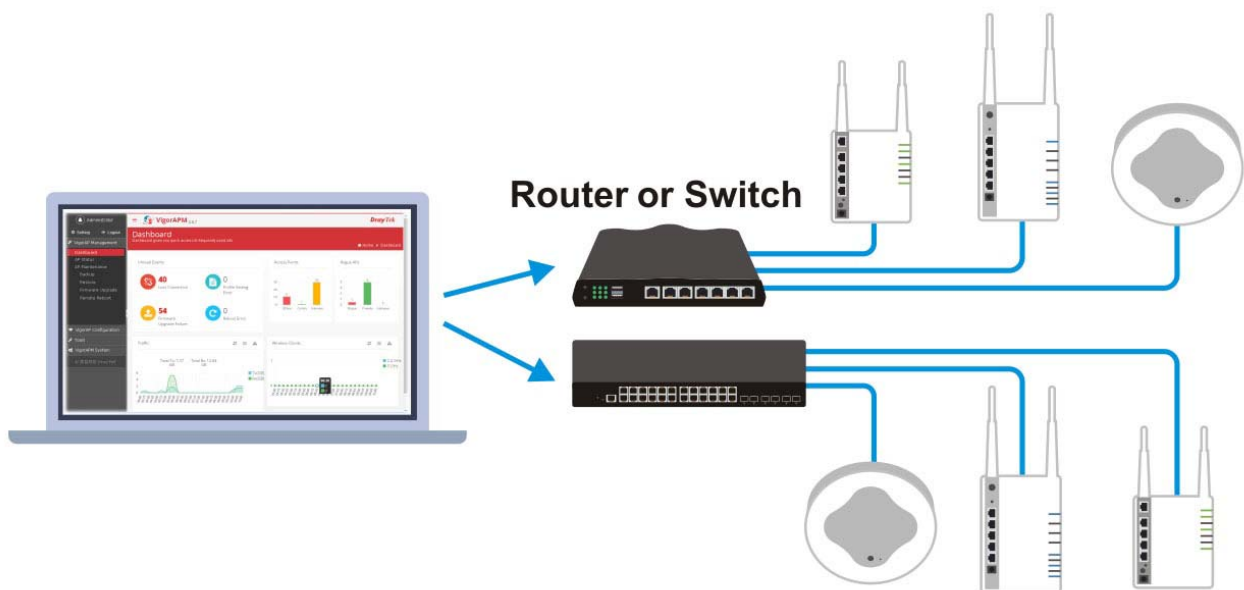
Chapter 1 Introduction

1.1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

VigorConnect, a central AP management software, is able to manage VigorAPs connected to Switch/Router. With VigorConnect, an administrator can modify the wireless settings, perform firmware upgrade, backup / restore settings related to VigorAP via a PC easily without accessing into the web page of VigorAPs one by one.

The following figure shows how VigorConnect manages VigorAPs via switch or router:



VigorConnect can manage VigorAP up to 100 devices.

System Requirements for VigorConnect Server

- OS: Windows 7 and later
- CPU: 1.2GHz Quad Core 64 bits CPU
- Memory: 2GB memory (DDR4)
- HDD: 1GB storage
- Browser: Firefox, Chrome, Opera, Safari, IE, Edge

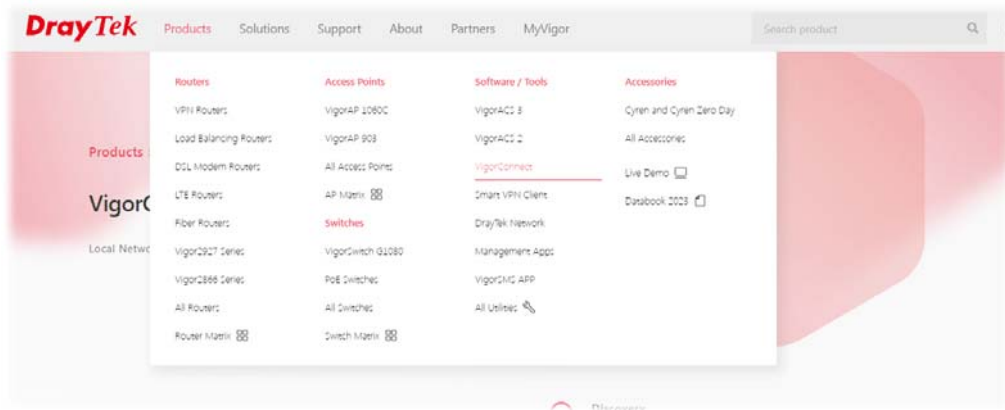
System Requirements for VigorConnect Client

- OS: Windows 7 and later
- Browser: Firefox, Chrome, Opera, Safari, IE, Edge

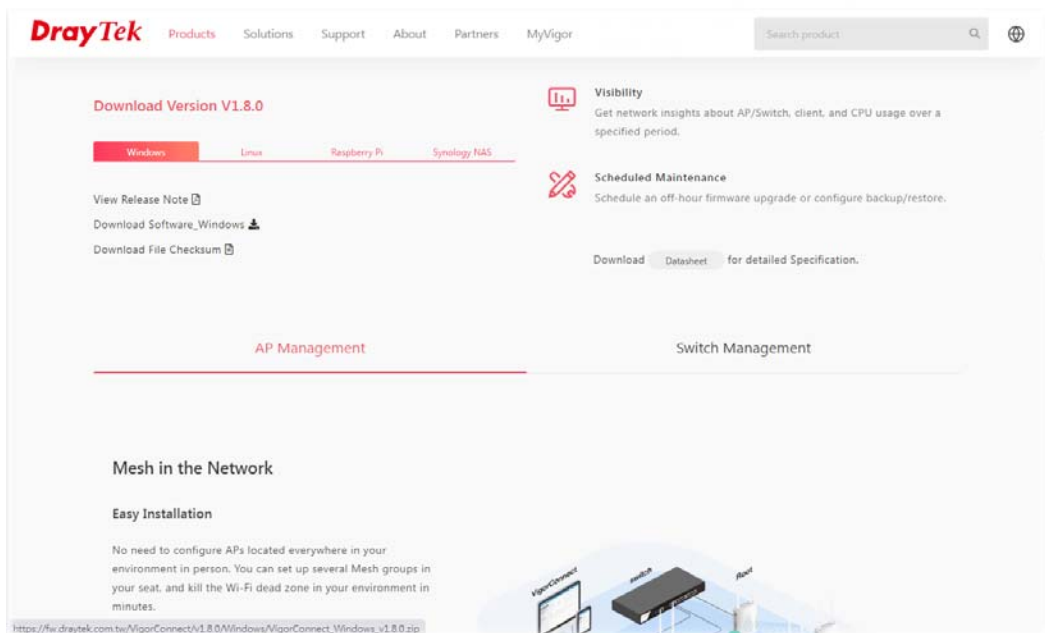
1.2 Installation

Follow the steps below.

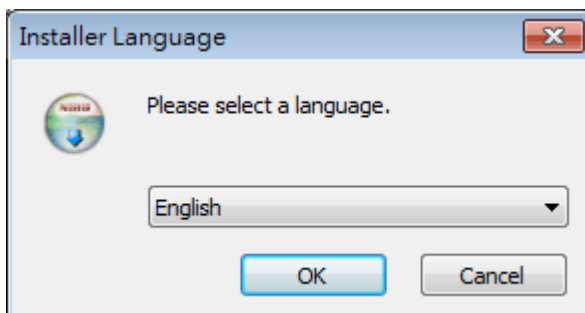
1. Visit www.draytek.com.
2. Open **Products>>Software/ Tools>>VigorConnect**.



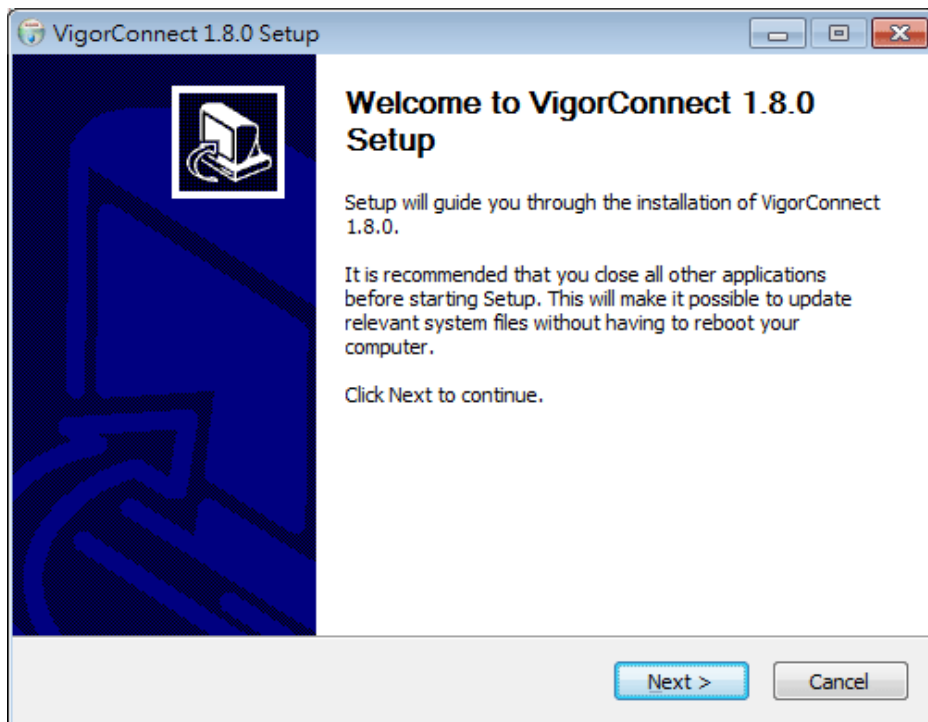
3. Scroll this page to find out **Download Software_Windows**.



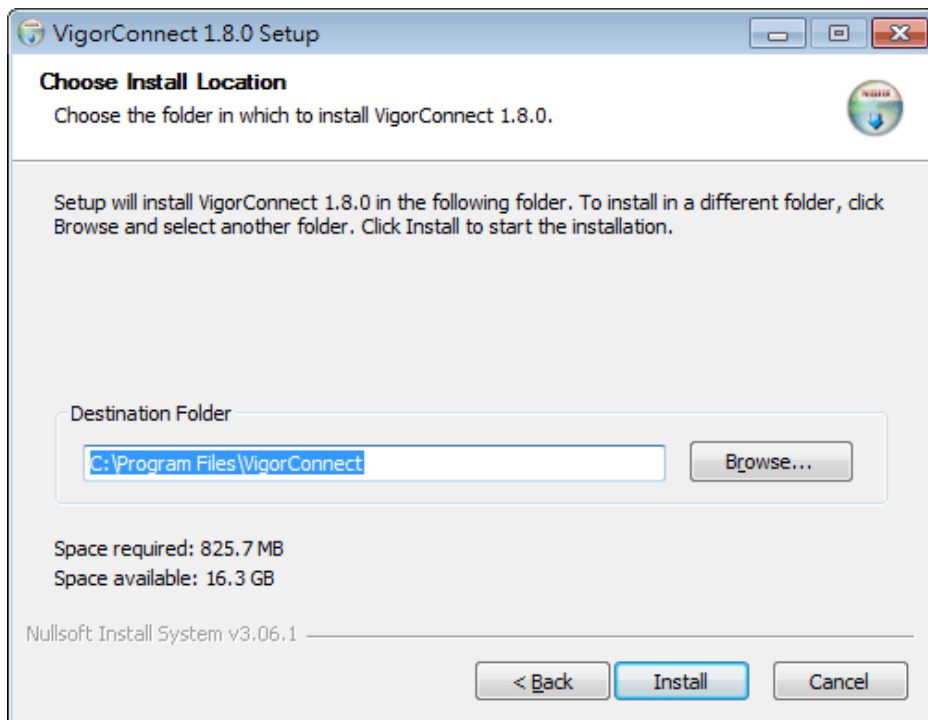
4. Download **VigorConnect** onto your computer.
5. Run the installer. Specify the language you want.



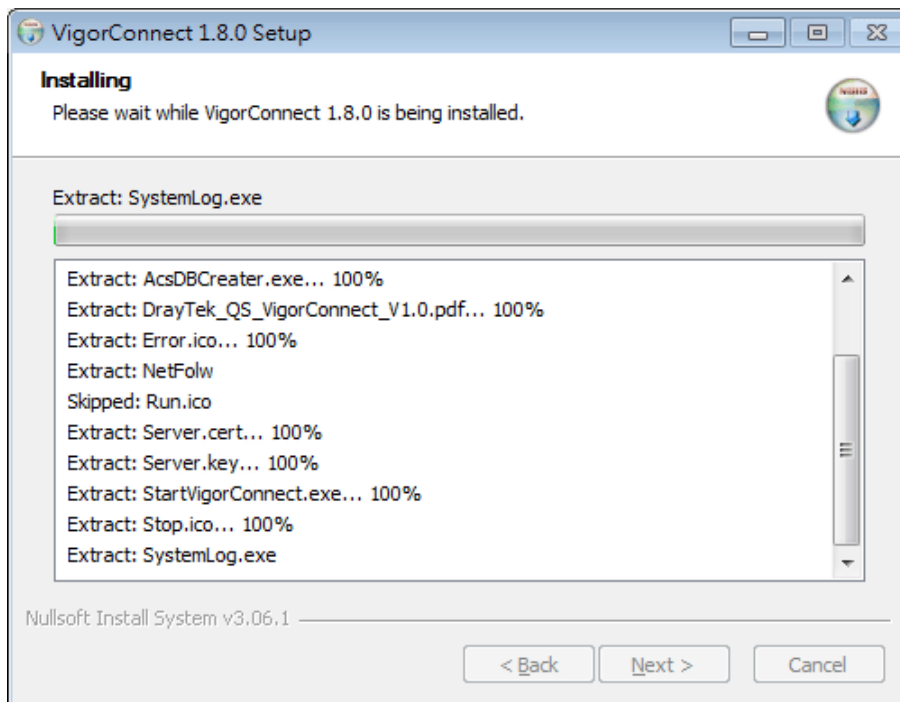
6. When the following dialog appears, click **Next**.



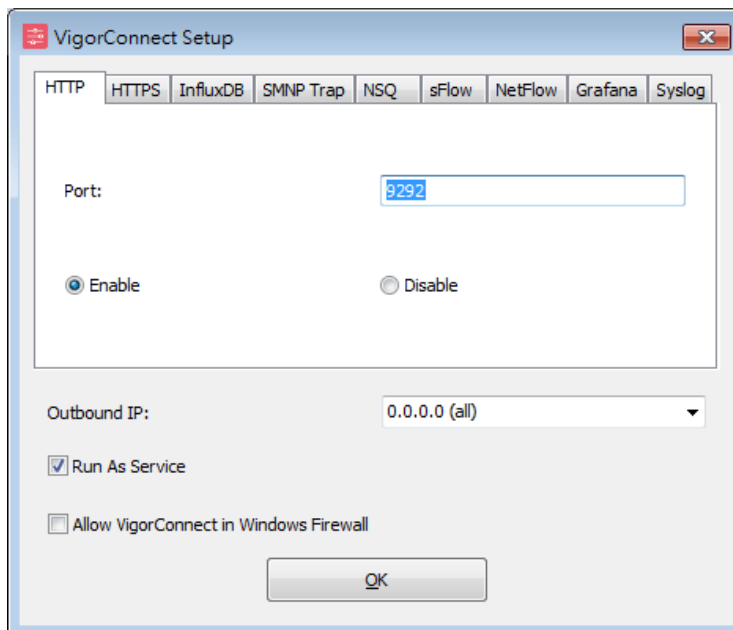
7. Specify the destination folder and click **Install**.



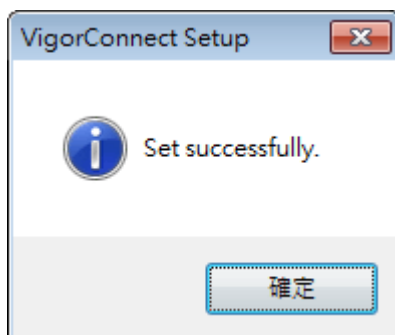
8. Wait for required files installing onto your computer.



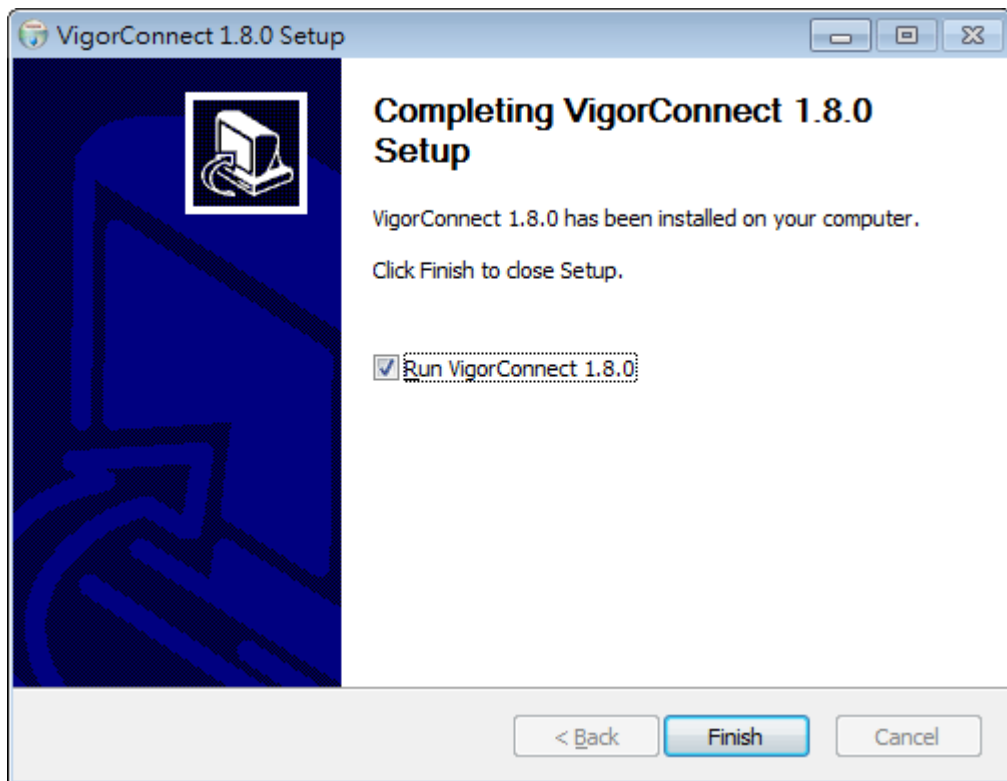
9. Then, the setup dialog with default values will appear. Click each tab to check the settings. It is recommended to use the default values. Then, click **OK**.



10. When the following dialog appears, simply click **OK**.



11. Check the box of Run VigorConnect and click **Finish**.

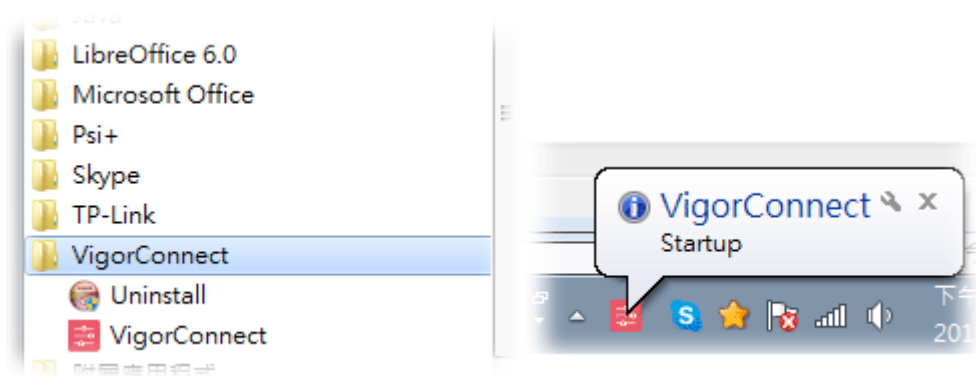


Chapter 2 Getting Started

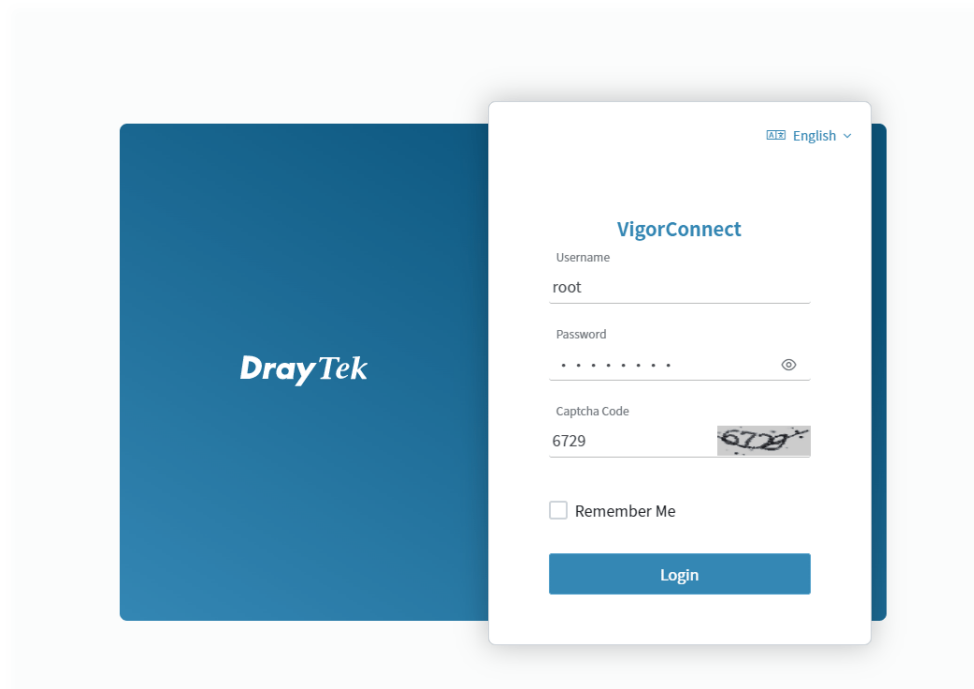
2.1 Accessing to Web User Interface

All functions and settings of this access point must be configured via web user interface. Please start your web browser (e.g., Firefox).

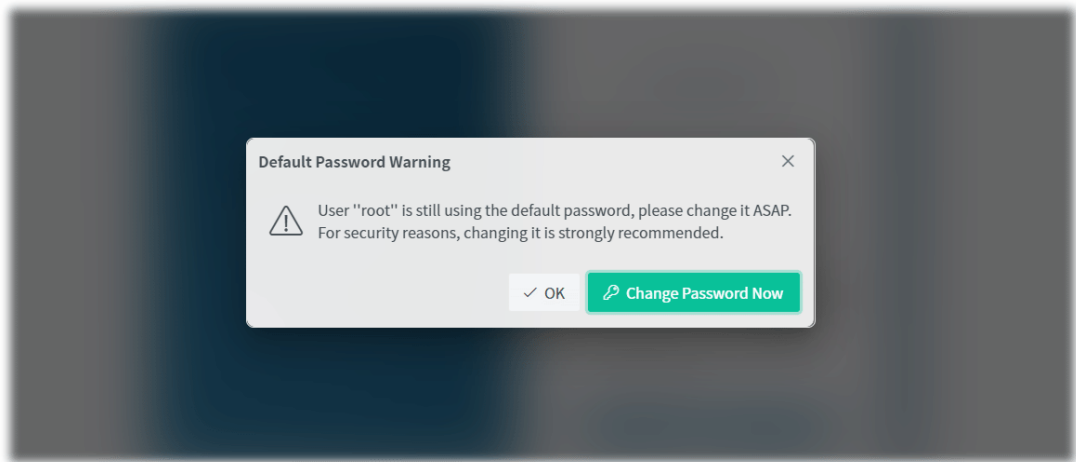
1. Double click the **VigorConnect** icon on the desktop or open **Programs >> VigorConnect>> VigorConnect**.



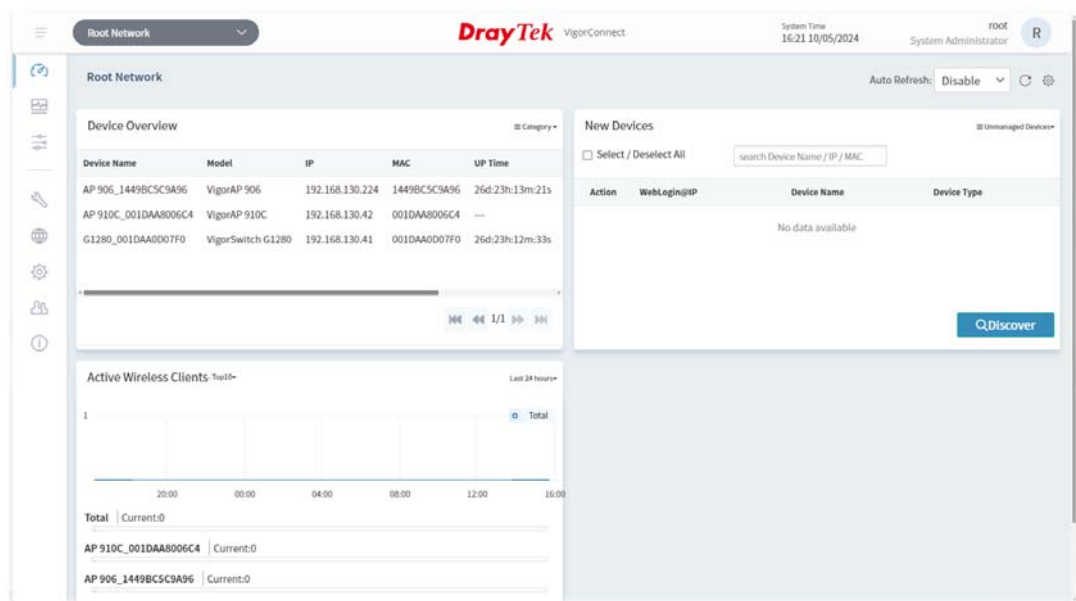
2. Please enter "root/admin123" as the Username/Password and enter validation code. Then, click **Login**.



3. For the first time to access into VigorConnect, Vigor system will ask you to change the login password. If you want to use the default password, simply click **Cancel** to access into the main screen.



4. Now, the **Main Screen** will appear.



5. The web page can be logged out by clicking **Log Out** on the top right of the web page. Or, logout the web user interface according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting of auto logout if you want.

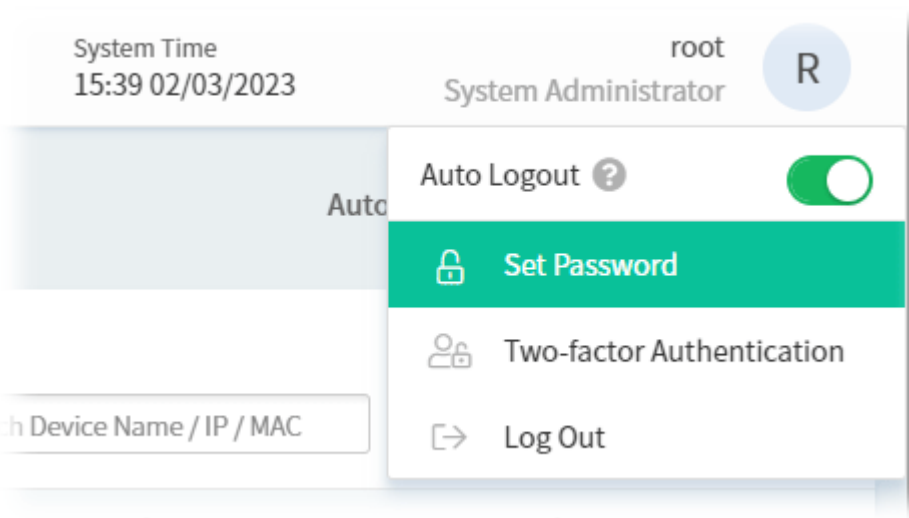
Note:

If you fail to access the web configuration, please go to the section "Trouble Shooting" for detecting and solving your problem.

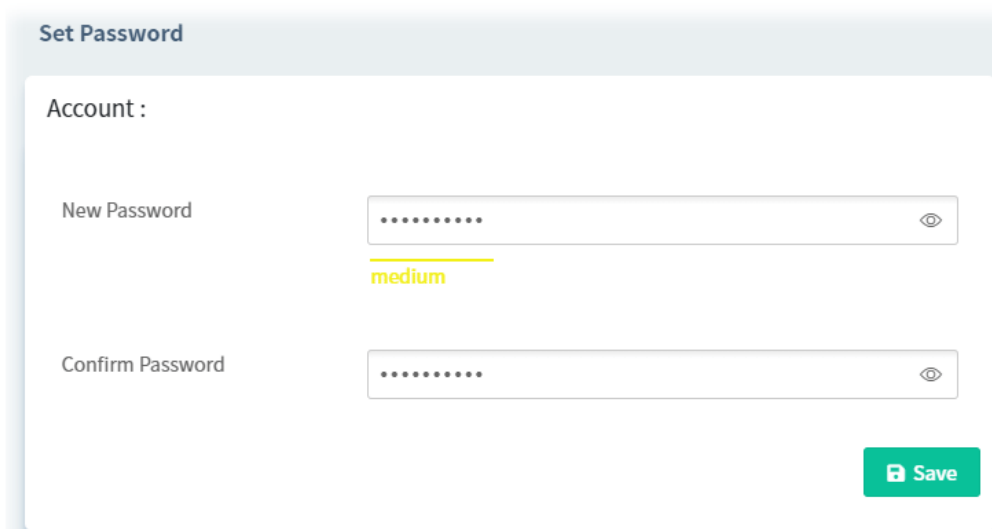
For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.2 Changing Password

1. Please change the password for enhancing the security.
2. Click the top-right corner to list the drop down menu. Choose **Set Password**.



3. A Set Password page is shown as follows. Enter a new password and re-enter the password to confirm the setting.

A screenshot of the 'Set Password' page. The page title is 'Set Password'. Under the heading 'Account:', there are two password input fields. The first is labeled 'New Password' and the second is labeled 'Confirm Password'. Both fields contain masked characters (dots) and have an eye icon to toggle visibility. Below the 'New Password' field, there is a yellow bar indicating the password strength as 'medium'. At the bottom right of the form, there is a green 'Save' button with a lock icon.

4. Click **Save**.
5. Now, the password has been changed. Next time, use the new password to access the Web User Interface of VigorConnect.

2.3 Dashboard

2.3.1 Dashboard for Root Network

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

The screenshot shows the DrayTek VigorConnect dashboard for the Root Network. The interface includes a sidebar menu (A), a top navigation bar (B) with a dropdown menu, a top right area (C) showing system time and user information, and a main content area (E) with a 'Device Overview' table, a 'New Devices' section, and an 'Active Clients' chart. A 'QDiscover' button is visible in the bottom right of the main content area.

Device Name	Model	MAC	UP Time	Firmware Version	LA
AP 1000C_001DA04F06C	VigorAP 1000C	001DA04F06C		1.4.1	0
AP 903_00507FF19216	VigorAP 903	00507FF19216	---	1.4.6	0
GZ280x_001DA043C7BA	VigorSwitch GZ280x	001DA043C7BA	---	2.8.2	0
P2280_001DA0CB609	VigorSwitch P2280	001DA0CB609		2.6.6	0
PQ2121xb_1449DC50G73D	VigorSwitch PQ2121xb	1449DC50G73D	---	2.8.0_RC2	0

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

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

C: System Time - Displays the system time.

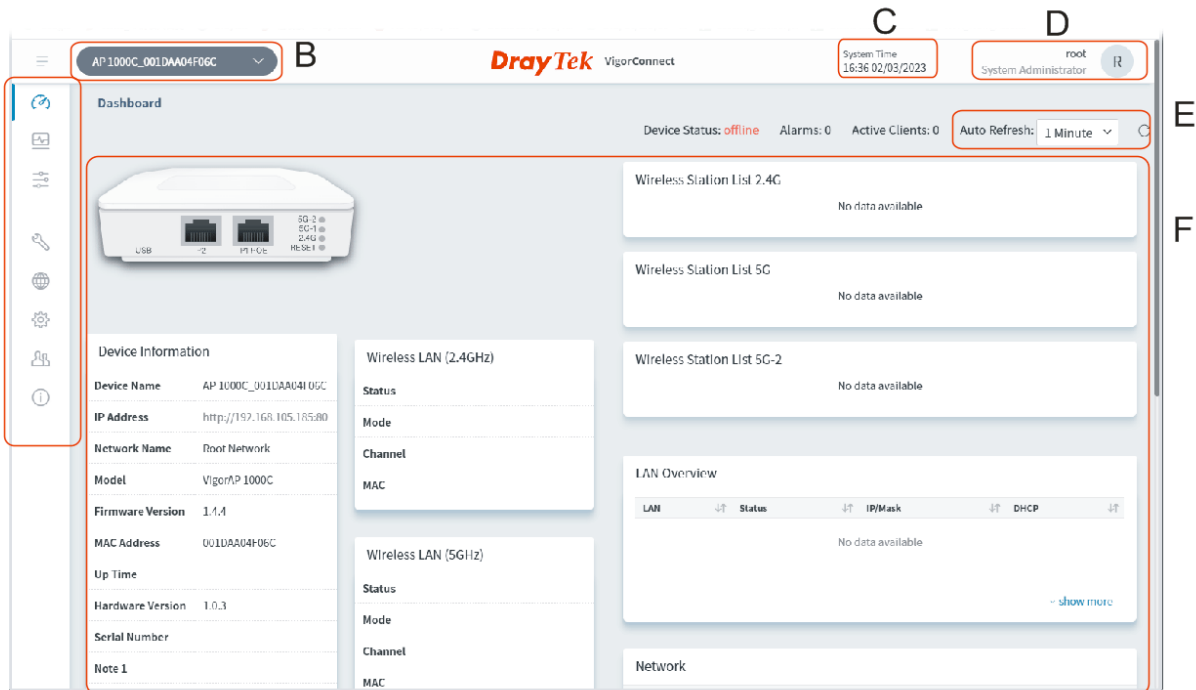
D: Selections - Displays current used account and offer selections for setting password, two-factor authentication, and logout.

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

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

2.3.2 Dashboard for a Device

This page offers device information such as system resource, connectivity and alerts for the selected device, wireless LAN configuration, wireless station overview, LAN overview, Network Status, Operation Mode, Connectivity and Alerts, and Quick Tools for the selected device.



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

B: Display Tab - Displays current selected item, e.g., root network, group network and device model.

C: System Time - Displays the system time.

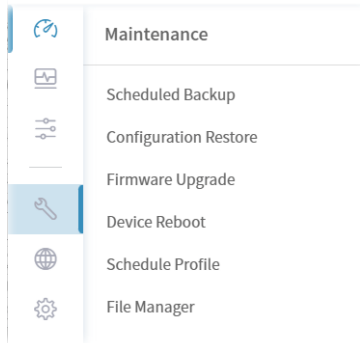
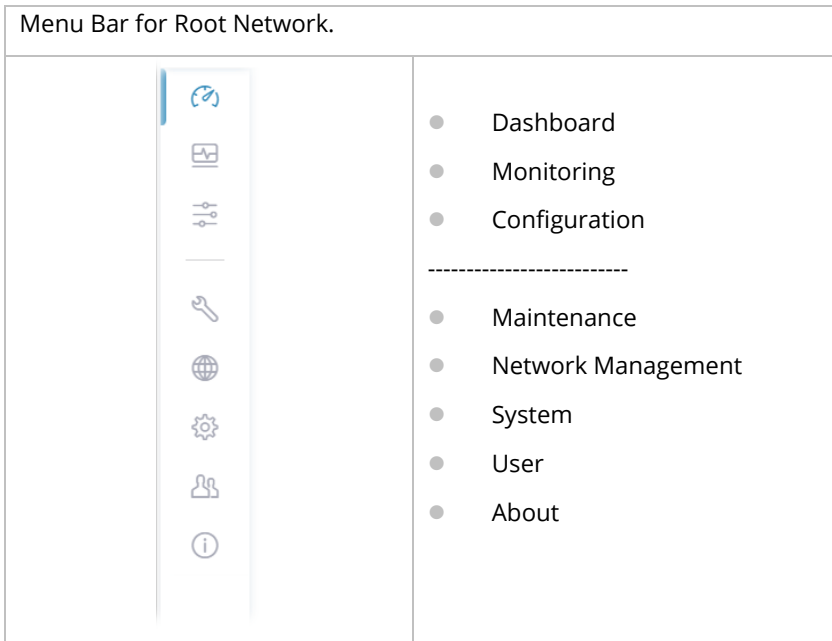
D: Selections - Displays current used account and offer selections for setting password, two-factor authentication, and logout.

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

F: Information - Displays information related to the device, wireless LAN, LAN, wireless stations, etc., of the selected device.

2.3.3 Menu Bar

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



Move the mouse cursor to each icon to open the drop down menu list.

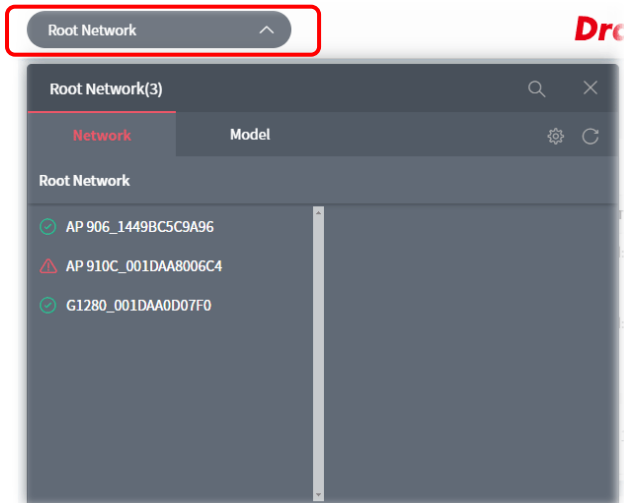
Select the menu item and access into the configuration web page.

2.3.4 Root Network and Selected CPE

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

2.3.4.1 The Display Tab, Root Network

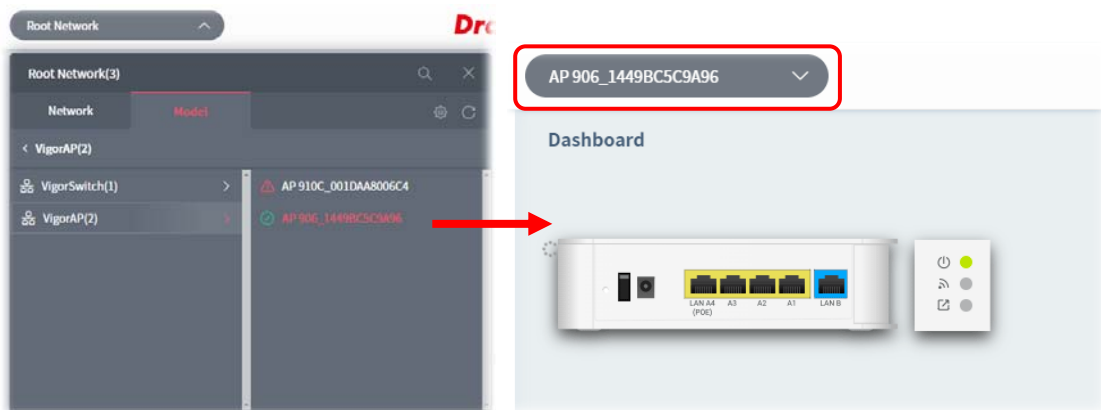
Click the **Display Tab** to display a drop-down list. This tab will display the root network or the name of the selected CPE based on your selection. In default, Root Network will be shown on the Display Tab.



When the **Display Tab** shows a 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.

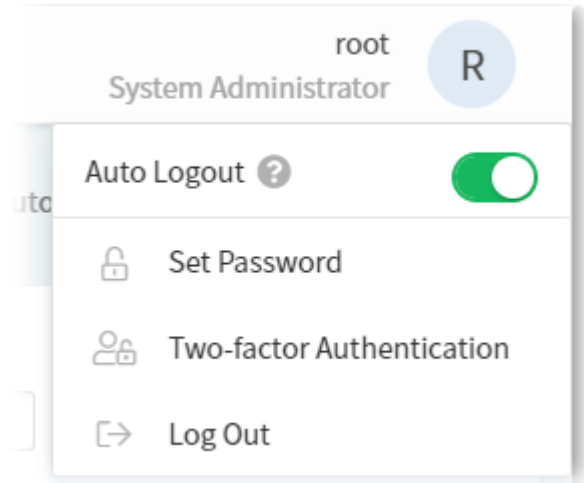
2.3.4.2 The Display Tab, CPE Device

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.



2.3.5 Set Password, Two-factor Authentication, and Log Out

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



2.3.5.1 Set Password

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

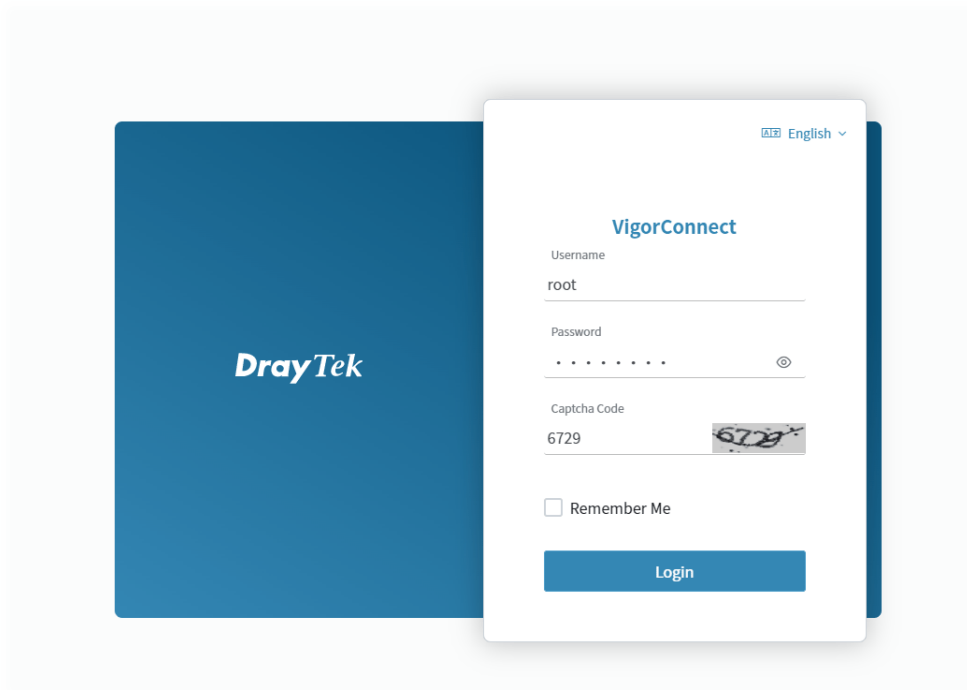
A screenshot of the 'Set Password' form. The form has a title 'Set Password' at the top left. Below the title, there is a label 'Account :'. The main part of the form contains two input fields: 'New Password' and 'Confirm Password'. Each input field has a small eye icon on the right side, indicating a toggle for password visibility. At the bottom right of the form, there is a green 'Save' button.

2.3.5.2 Two-factor Authentication

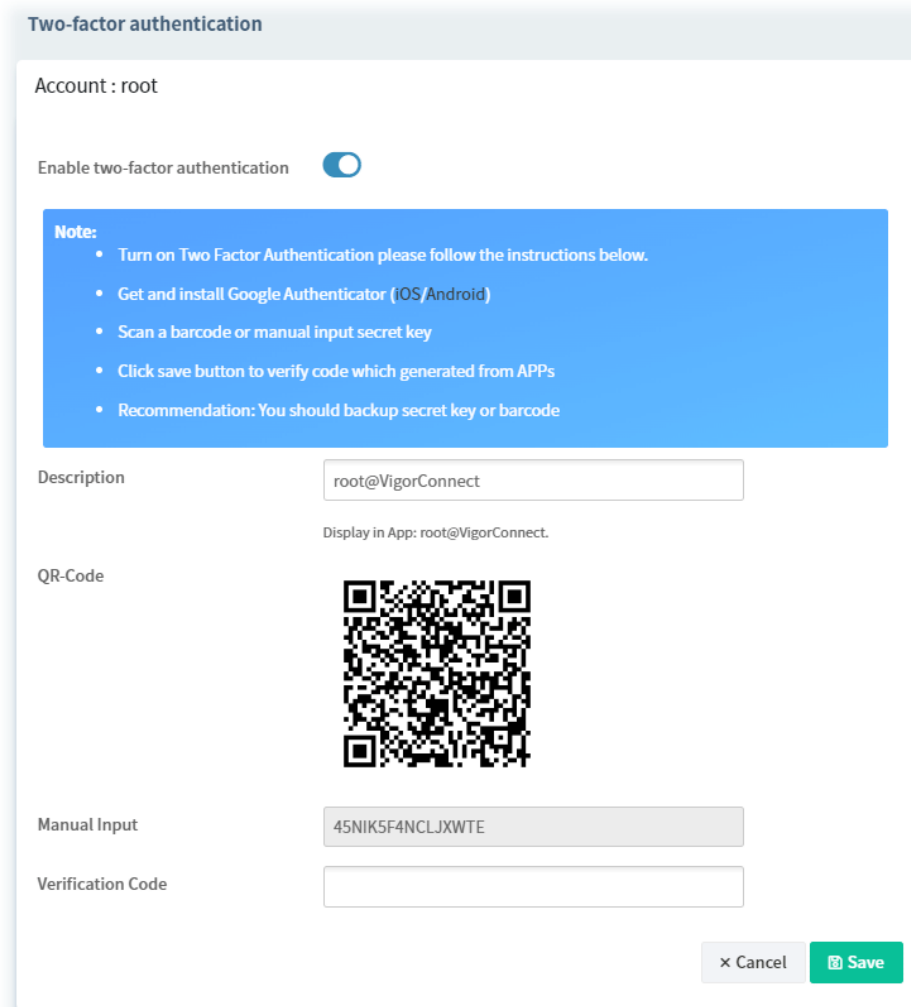
Usually, the system administrator can access into VigorConnect by using user account and password. If network security is highly concerned, two-factor authentication will be strongly recommended.

For using two-factor authentication for accessing VigorConnect;

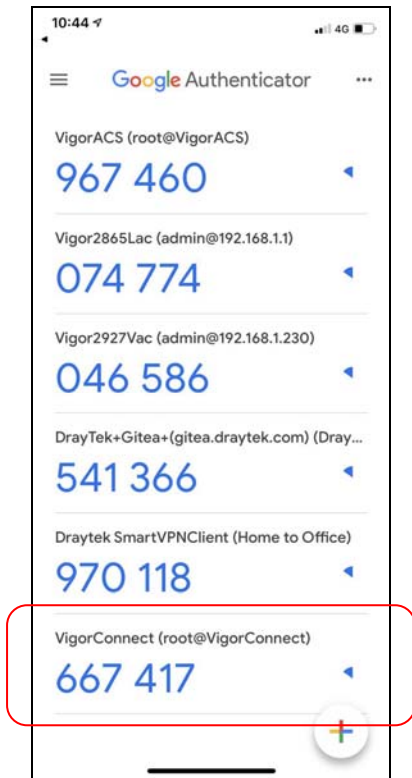
1. Get and install **Google Authenticator** (iOS/Android) first.
2. Login VigorConnect by using the user account and password.



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



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

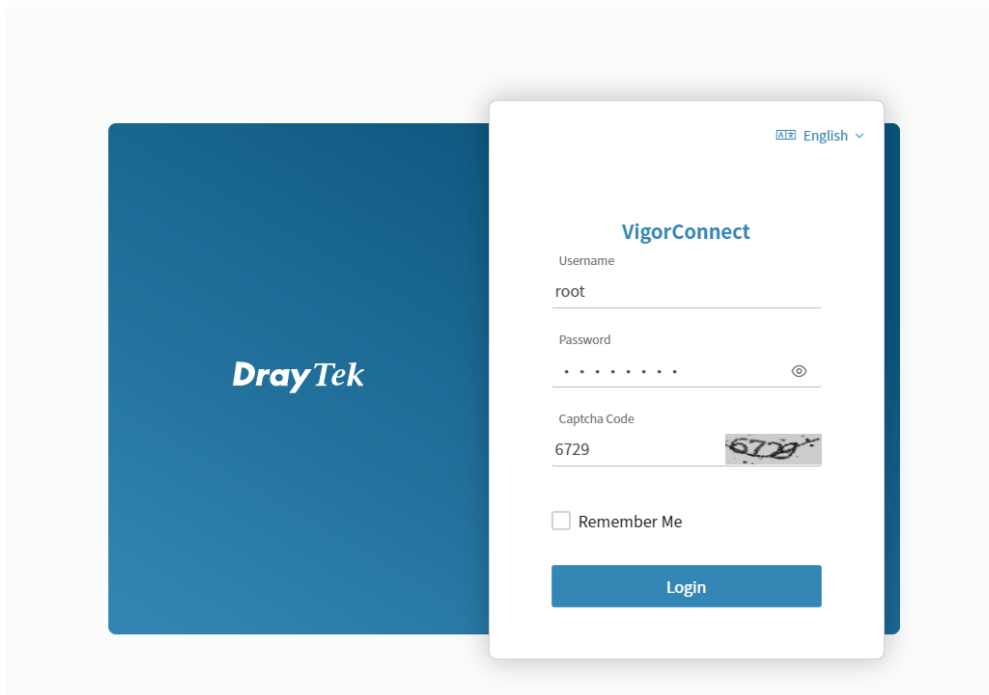


5. A key will be created randomly on the cell phone. Enter that key on the box of **Verification Code** and click the **Save** button.

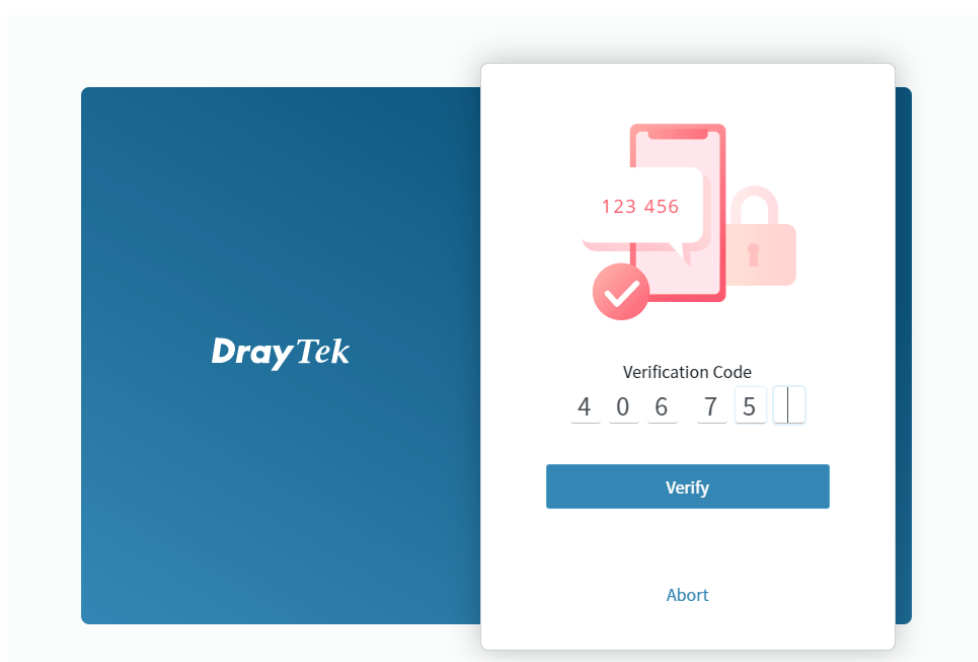
The image shows a screenshot of the 'Two-factor authentication' configuration page. At the top, it says 'Account : root'. Below that, there is a toggle switch for 'Enable two-factor authentication' which is turned on. A blue note box contains the following instructions: 'Note: • Turn on Two Factor Authentication please follow the instructions below. • Get and install Google Authenticator (IOS/Android) • Scan a barcode or manual input secret key • Click save button to verify code which generated from APPs • Recommendation: You should backup secret key or barcode'. Below the note, there are several input fields: 'Description' with the value 'root@VigorConnect', 'QR-Code' with a QR code, 'Manual Input' with the value '45NIK5F4NCLJXWTE', and 'Verification Code' with the value '667417'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

6. Logout VigorConnect.

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

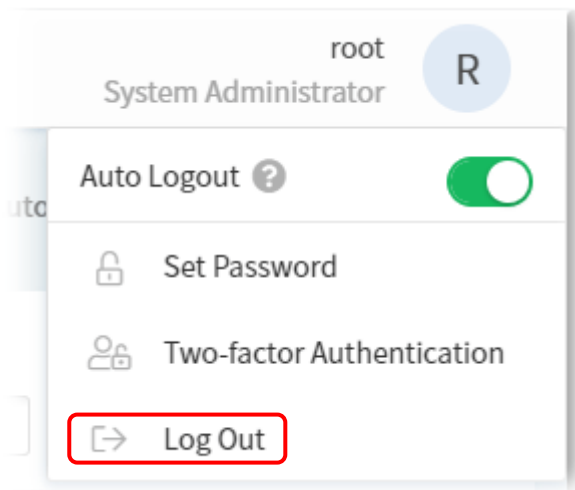


After clicking the Login button, the *second* login web page appears. Please enter the verification code (created randomly) obtained from the APP (Google Authenticator) on your cell phone and click the Verify button.

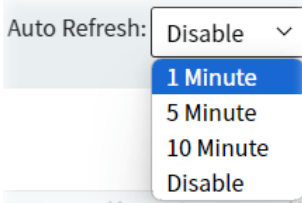
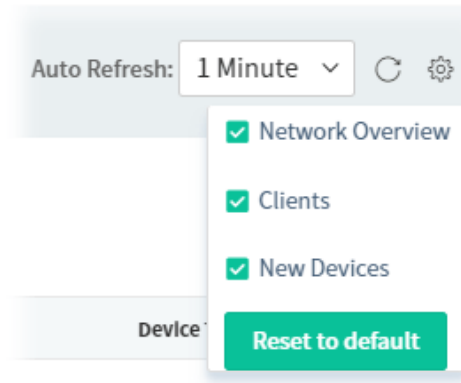


2.3.5.3 Logout VigorConnect

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

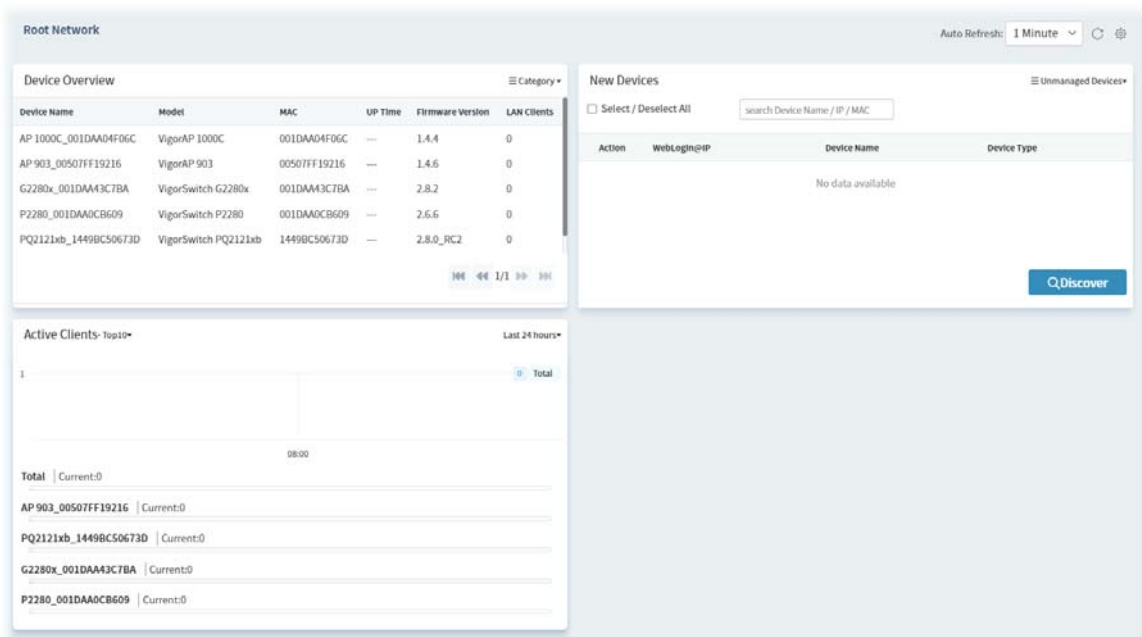


2.3.6 Auto Refresh, Manual Refresh, and Widget

Item	Description
Auto Refresh	<p>Select the time interval for refresh the web page automatically.</p> 
Manual Refresh	Click to refresh the web page immediately.
Widget	<p>There are four display views to select, including Network Overview, Clients, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard.</p> 

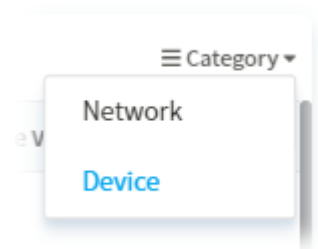
2.3.7 Overviews

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



2.3.7.1 Device Overview

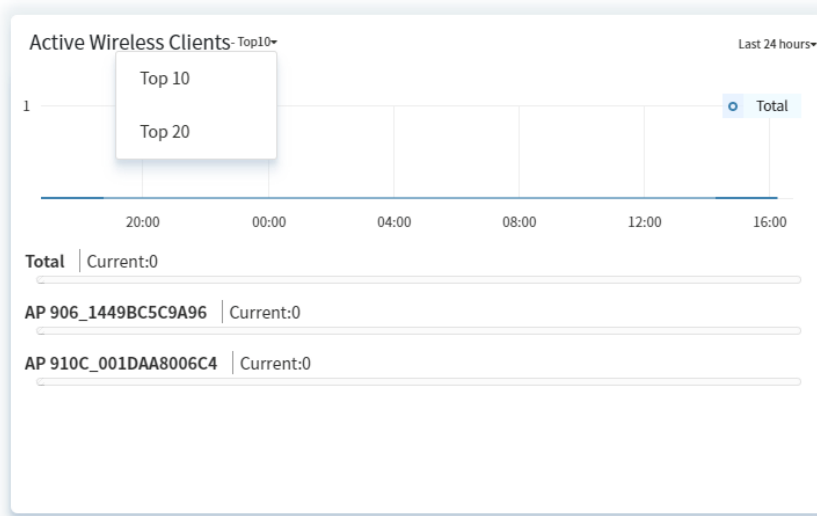
This area displays the Device Overview.

Item	Description
Category	<p>Switch between Network or Device.</p> 

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.

2.3.7.2 Active Wireless Clients

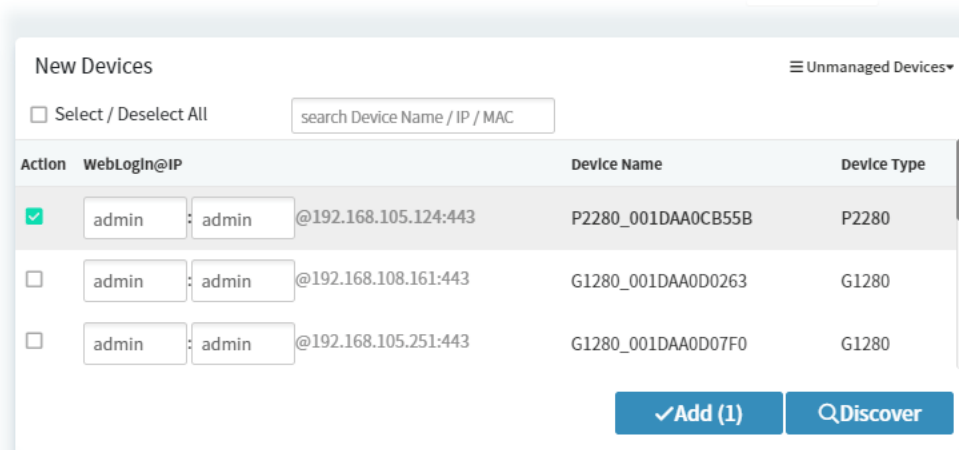
This area displays the top 10 clients or top 20 clients accessing into VigorConnect during the last 24 hours, 7 days or 30 days.



Item	Description
Last 24 hours	Use the drop down list to specify the time period, last 24 hours, 7 days or 30 days.

2.3.7.3 New Devices

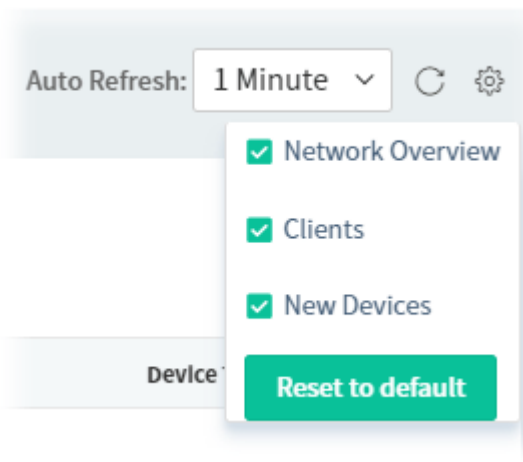
Click **Discover** to search new devices (AP or switches). The new device(s) can be found and displayed on the list.






Item	Description
Select/Deselect All	Check the box to enable the function of Select All or Deselect All.
<input type="checkbox"/>	Click the button to select a device.
Add	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.

2.3.7.4 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.



2.3.8 Icons Used in VigorConnect

Item	Description
+	Add a new device.
	Switch these two icons by click the mouse cursor on it.  - means "Enable".  - means "Disable".

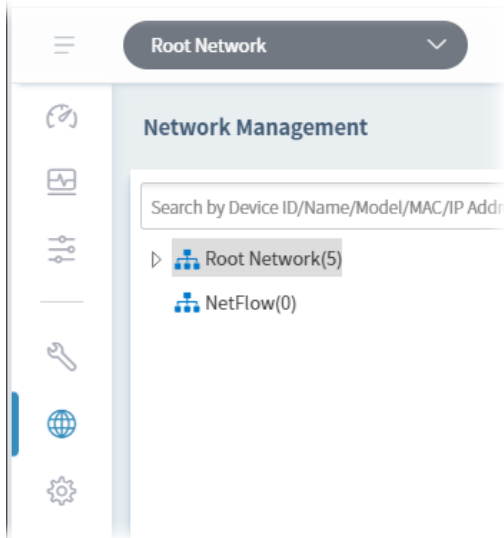
Applications

A.1 How to Create a New Network?

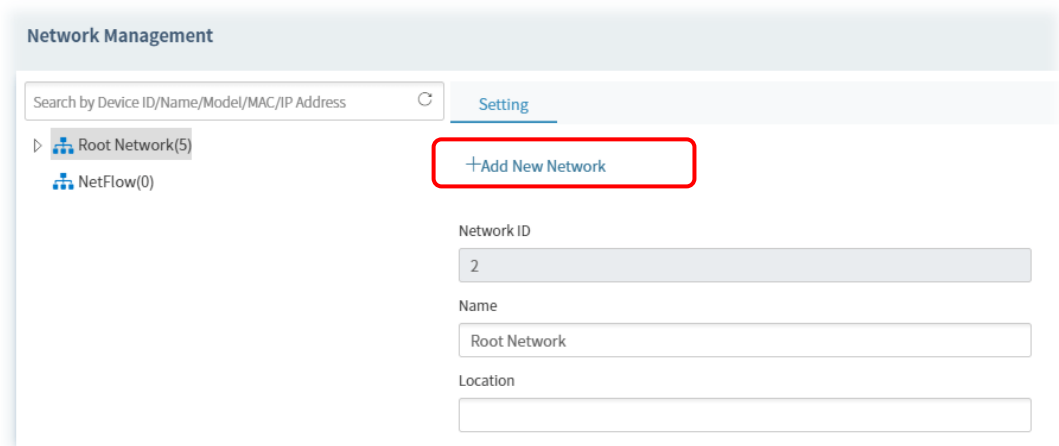
VigorConnect allows the administrator to build several networks (and sub-network) for different devices under the *root network*.

Only the administrator has the right to create a new user group.

1. From the MENU bar, click **Network Management**.



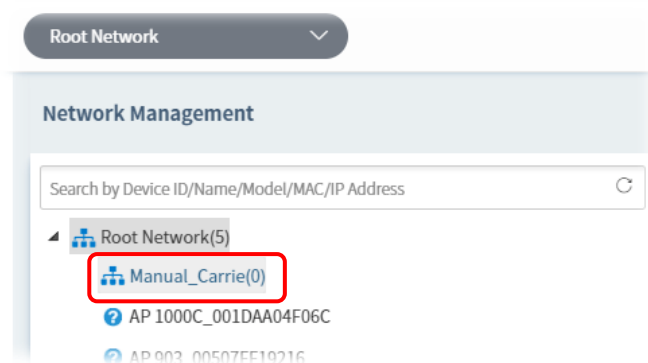
2. When the following page appears, click the link of **+Add New Network**.



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

- 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.

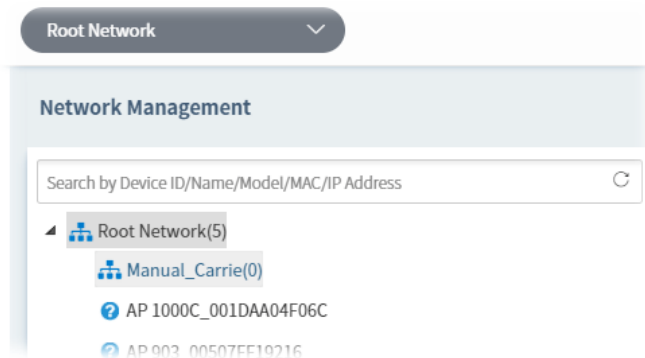
4. Click **+Add** to save the settings. The new created network will be seen under the **Root Network**.



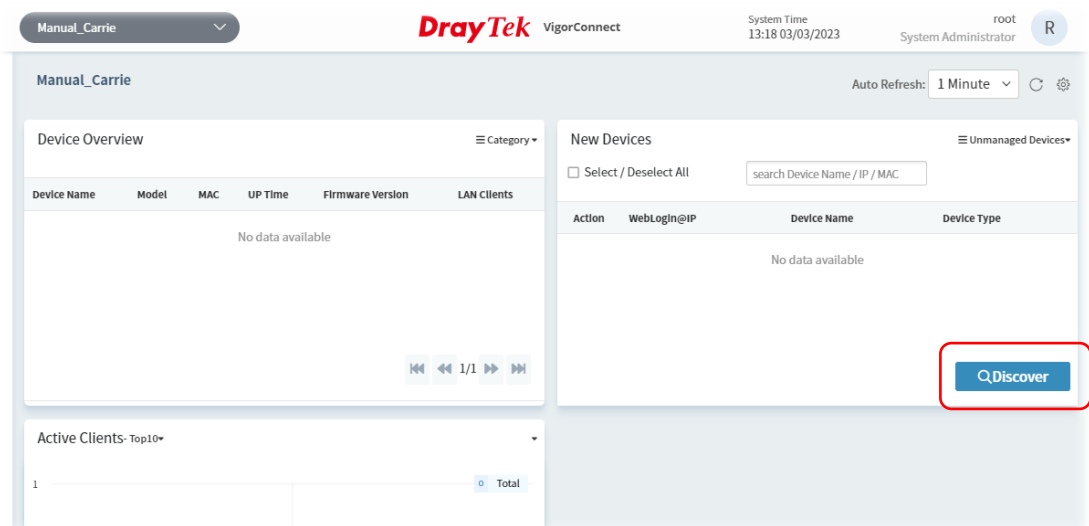
A.2 How to Assign a New Added Device to a Network?

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

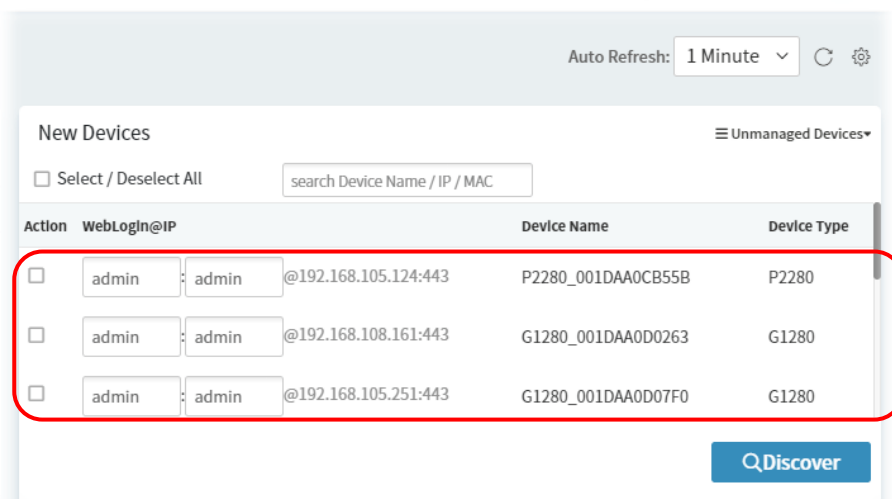
1. Open the dashboard of the network (e.g., Marketing_Carrie) created in A-1.



2. On the dashboard, click **Discover** under the field of New Devices. Vigor system will search nearby AP/switch and display the device(s) on this page.



3. Later, scanned devices will be shown under the field of New Devices.



4. Check the one(s) which will be managed under the specified network (e.g., Marketing_Carrie) and click **Add**.

The screenshot shows the 'New Devices' interface. At the top right, there is a toggle for 'Unmanaged Devices'. Below this, there is a 'Select / Deselect All' checkbox and a search box labeled 'search Device Name / IP / MAC'. The main area contains a table with three rows of device information. The third row is highlighted in light green and has a red border around it, indicating it is selected. At the bottom right, there are two buttons: 'Add (1)' and 'Discover'.

	admin	:	admin	@192.168.105.161:443	P2121_001DAA4CE9BC	P2121
<input type="checkbox"/>	admin	:	admin	@192.168.105.98:80	G1080_00507FF1BB79	G1080
<input checked="" type="checkbox"/>	admin	:	admin	@192.168.105.212:443	Q2121X_1449BC506AA4	Q2121X

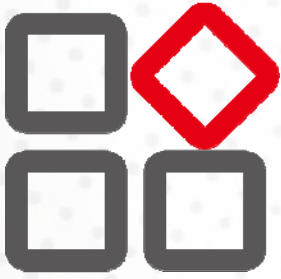
5. Then, the selected devices will be shown under **Device Overview**.

The screenshot shows the 'Manual_Carrie' interface. At the top, there is a toggle for 'Category'. Below this, there is a 'Device Overview' section. The main area contains a table with one row of device information. At the bottom right, there are navigation buttons and a page indicator '1/1'.

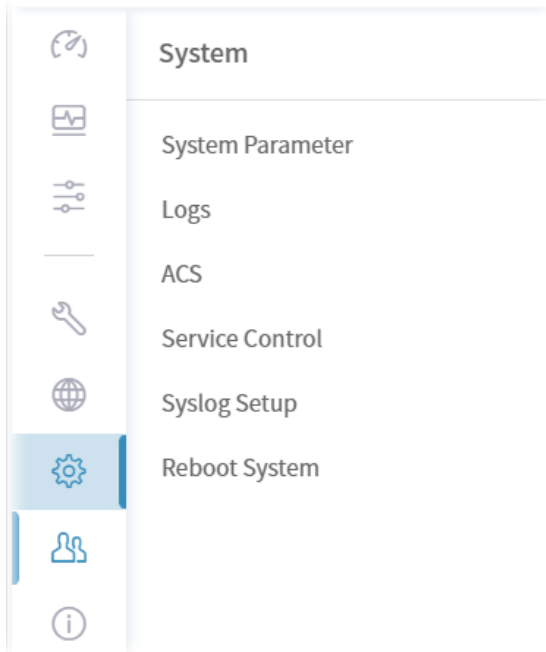
Device Name	Model	MAC	UP Time	Firmware Version	LAN Clients
Q2121x_1449BC506AA4	VigorSwitch Q2121x	1449BC506AA4	---	2.8.1	0

This page is left blank.

Part II System and User Settings Management



Chapter 3 System Menu



3.1 System Parameter

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

The screenshot shows a web page titled 'System / System Parameter'. It contains a table with the following data:


ID	Name	Value
1	EnableValidateCodeCheck	true
2	EnableFirmwareCheck	true
3	ShowTreeCount	100
4	FWUpgradeFailInterval	86400
6	LogsRetentionDays	365
7	AutoDetectRouterName	false
1001	HTTP Port	9292
1002	Enable HTTP	true
1003	HTTPS Port	4433
1004	InfluxDB HTTP Port	8089
1005	InfluxDB DB Port	8091
1006	SNMP Trap Port	162
1007	Enable SNMP Trap	true
1008	NSQ Port	4150
1009	sFlow Port	6343
1010	sFlow Sampling Rate	400

At the bottom of the page, there is a 'Reset to default' link, a 'Cancel' button, and a 'Save' button.

These parameters are explained as follows:

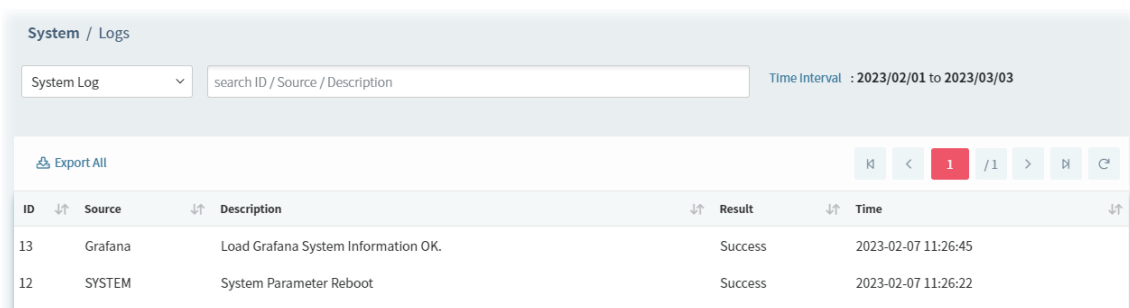
Item	Description
------	-------------

1	EnableValidateCodeCheck True – Enable the function of validating code check on the login page. False – Disable the function. It is the default value.
2	EnableFirmwareCheck True - VigorConnect 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.
3	ShowTreeCount Set how many devices will be shown on the home device tree. Default value is 100.
4	FWUpgradeFailInterval If the firmware upgrade failed, the next firmware upgrade will execute after the time interval configured here. Default value is 86400 seconds.
6	LogsRetentionDays VigorConnect will store the log for a while (the number of days defined here).
7	AutoDetectRouterName If enabled (choosing true), the system will detect the name of the device automatically while allowing the registration from the device or doing the VigorConnect online check.
1001	HTTP Port Set the HTTP port number for VigorConnect. The default is 9292.
1002	Enable HTTP Enable or disable the HTTP service for VigorConnect. The default is true (enabled).
1003	HTTPS Port Set the HTTP port number for VigorConnect. The default is 4433.
1004	InfluxDB HTTP Port Set the HTTP port number for InfluxDB. The default is 8089.
1005	InfluxDB DB Port Set the HTTP port number used by InfluxDB. The default is 8091.
1006	SNMP Trap Port Set the port number used by the SNMP Trap. The default is 162.
1007	Enable SMNP Trap Enable or disable the HTTP service for VigorConnect. The default is true (enabled).
1008	NSP Port Set the port number used by the NSQ Server. The default is 4150.
1009	sFlow Port Set the port number used by the sFlow Collector. The default is 6343.
1010	sFlow Sampling Rate Set the sFlow sampling rate. The default is 400.
1011	sFlow Counter Sampling Interval Set the sampling interface for sFlow counter. The range is from 0 to 300. The unit is second. Default value is 30.
1012	Enable sFlow Enable or disable the sFlow server. The default is disabled (false).

1013	NetFlow IPFIX Port Set the port number used by the NetFlow IPFIX Collector.
1014	NetFlow IPFIX Active Timeout Set the active Timeout for NetFlow IPFIX Collector. The default is 300 (unit is second).
1015	NetFlow IPFIX Inactive Timeout Set the inactive Timeout for NetFlow IPFIX Collector. The default is 15 (unit is second).
1016	Enable sFlow Enable or disable the sFlow server. The default is disabled (false).
1017	Grafana HTTP Port Set the HTTP Port for NetFlow IPFIX Collector. The default is 15 (unit is second).
1018	Grafana HTTP Port Set the HTTP Port for NetFlow IPFIX Collector. The default is 15 (unit is second).
1019	Syslog Port Set the port number used by the Syslog Server. The default is 514.
1020	Syslog Retention Days Set the Retention Days for Syslog. The range is from 10 to 180 days. The default is 30.
1021	Enable Syslog Enable or disable the Syslog service. The default is enabled (true).
1022	etcd Listen Client Port Set the listen client port number used by the etcd Server. The default is 2379.
1023	etcd Listen Peer Port Set the listen peer port number used by the etcd Server. The default is 2380.
1024	Security Pack Enable or disable the security pack. The default is disabled (false).
	Reset to default Click the link to reset all of the system parameters with factory default values.
Save	Save the current settings.

3.2 Logs

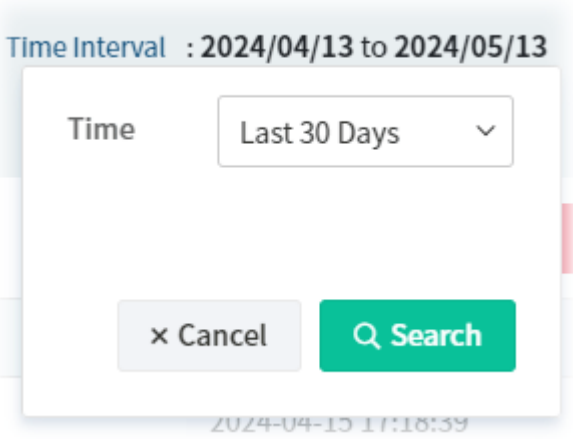
Information displayed here shall be useful for the administration to viewing the status for user access.



The screenshot shows the 'System / Logs' interface. At the top, there is a dropdown menu for 'System Log' and a search box for 'search ID / Source / Description'. The 'Time Interval' is set to '2023/02/01 to 2023/03/03'. Below the search area, there is an 'Export All' button and a pagination control showing '1 / 1'. The main content is a table with the following columns: ID, Source, Description, Result, and Time.

ID	Source	Description	Result	Time
13	Grafana	Load Grafana System Information OK.	Success	2023-02-07 11:26:45
12	SYSTEM	System Parameter Reboot	Success	2023-02-07 11:26:22

These parameters are explained as follows:

Item	Description
System Log / Login Log /	Click one of the types to display log of System and Login.
Search ID / Source / Description	Specify the conditions (type the ID number, username, the IP address or overview) for log searching.
Time Interval	<p>Select a time interval. The log within the period will be shown on the page.</p> 
System Log	Display the ID number, description, result and time.
Login Log	Display the log information, including ID, username, authentication, login IP, status, login time and logout time for clients accessing into VigorConnect.
Export All	Log information can be exported as a file.

3.3 ACS

With the following configuration, VigorConnect (the client) can deliver the complete information to VigorACS for displaying the NetFlow charts after collecting the required data.

These parameters are explained as follows:

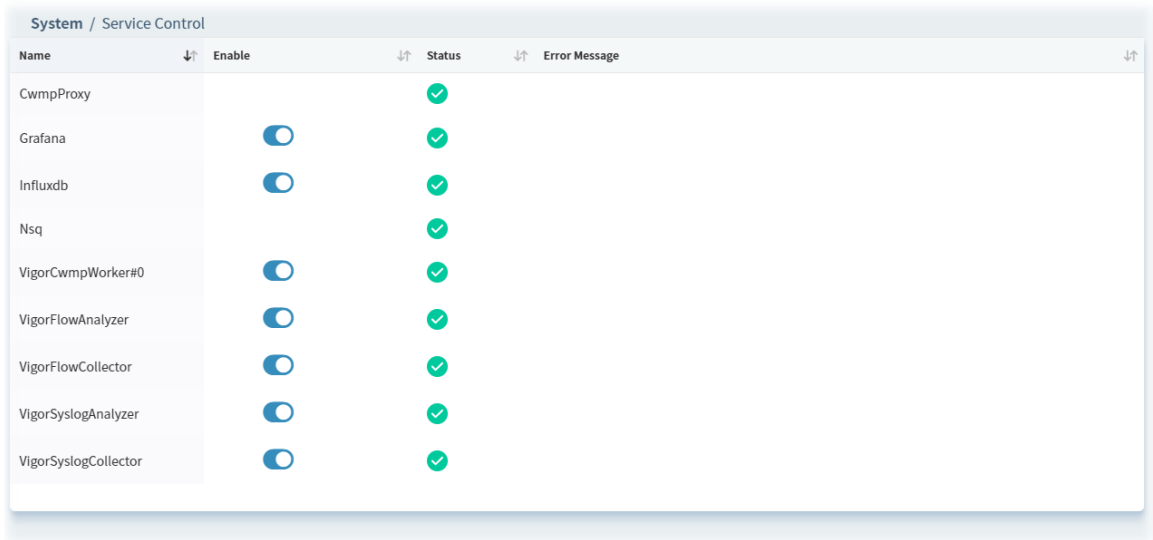
Item	Description
ACS Server	
Status	Displays the current status (X or ✓) of registering to VigorACS. If successful registration, a tick will be shown instead after clicking Save.
Enable Server	Click to enable the function of connecting to VigorACS server.
Register Server	Enter the IP or domain name of VigorACS server. VigorConnect will be registered to VigorACS after clicking Save .
Browse Server	Usually, it will be the same as the Register Server.
Port	Enter the port number used for connecting VigorConnect and VigorACS server.
Username	Enter the name for accessing VigorACS server.
Password	Enter the password for accessing VigorACS server.
Keep Alive (seconds)	Enter the values (seconds) for keeping the network connection between VigorConnect and VigorACS server.
ACS Type	Select one of the ACS types for building connection between VigorConnect and VigorACS server. <ul style="list-style-type: none"> ● Standalone ● Cloud
Enable STUN	Click to enable the function of the STUN server.
STUN Port	Enter the port value used for the STUN server.

VigorConnect	
Username / Password	The settings are generated by VigorConnect automatically. It is recommended to use the default setting.
Save	Save the current settings.

3.4 Service Control

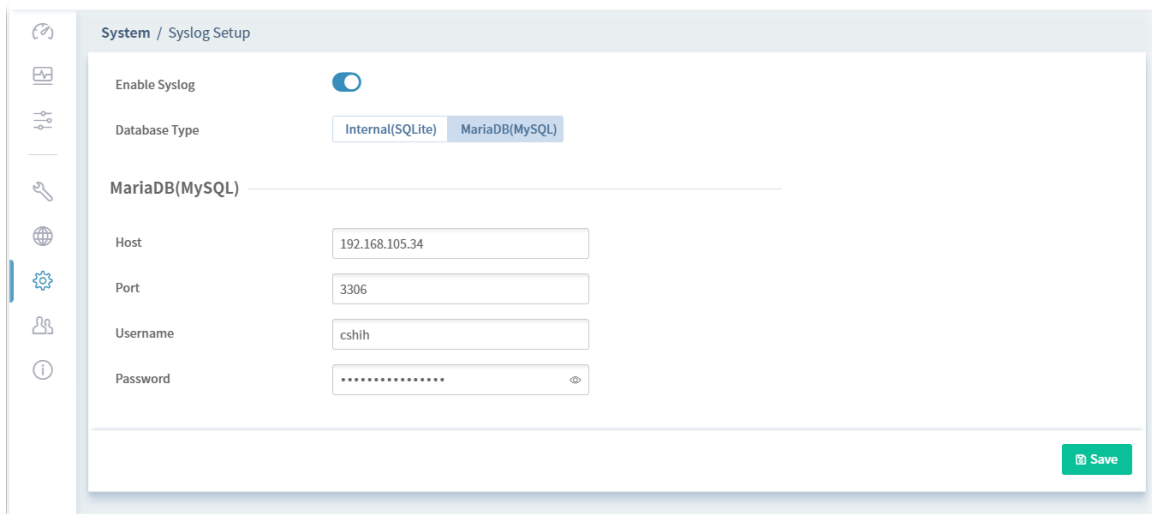
VigorConnect will apply various services to generate various data and chart.

In general, use the default settings in this page.



3.5 Syslog Setup

VigorConnect allows recording logs by internal or external databases.



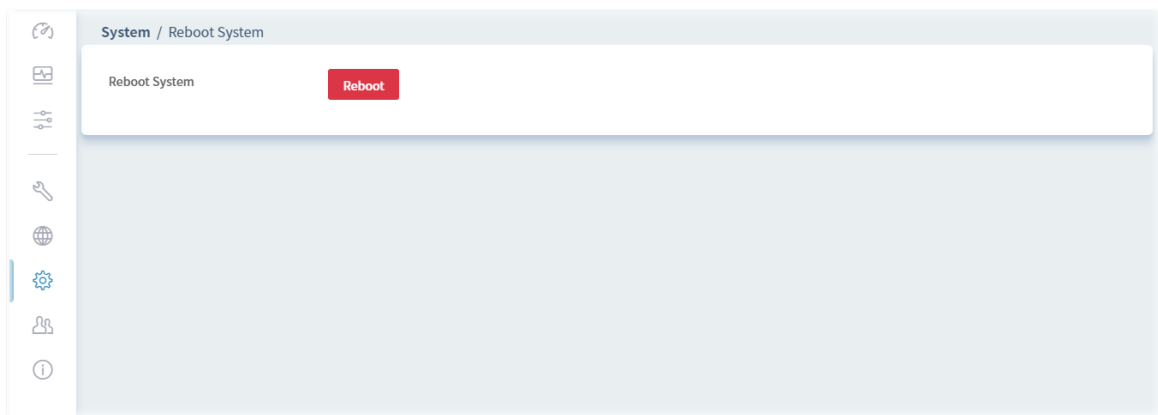
These parameters are explained as follows:

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

Enable Syslog	Click to enable recording the log for the system configuration to the Syslog.
Database Type	Select the (internal or external) database type. <ul style="list-style-type: none"> ● Internal(SQLite) ● MariaDB(MySQL)
MariaDB(MySQL)	
Host	Enter the host name of the database.
Port	Enter the port number used for the database.
Username	Enter the user name which is set while installing MariaDB for VigorConnect.
Password	Enter the password which is set while installing MariaDB for VigorConnect.
Save	Save the current settings.

3.6 Reboot System

Click **Reboot** to restart VigorConnect with current configuration.

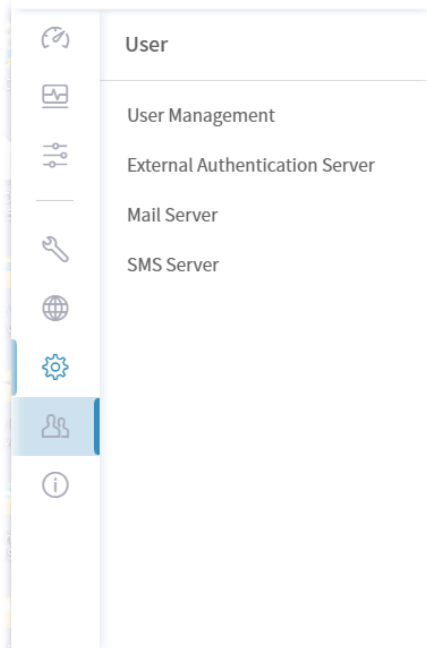


Chapter 4 User Menu

VigorConnect allows a user to manage AP devices through VigorConnect 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 VigorConnect.

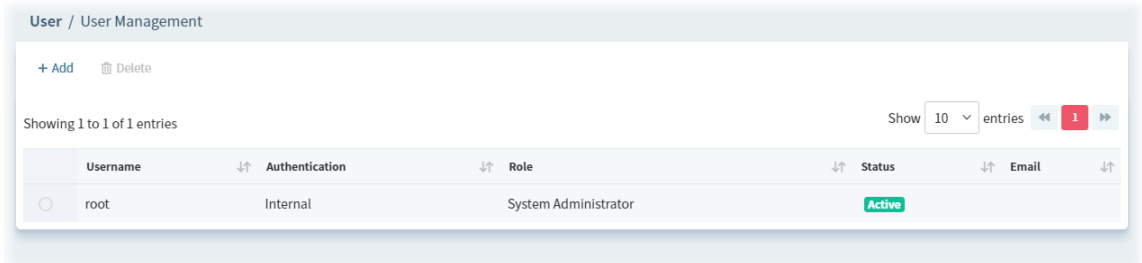
This chapter will guide you to define users. It can be set with different roles (at present, only System Administrator is allowed); each role has different administration authority.

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



4.1 User Management

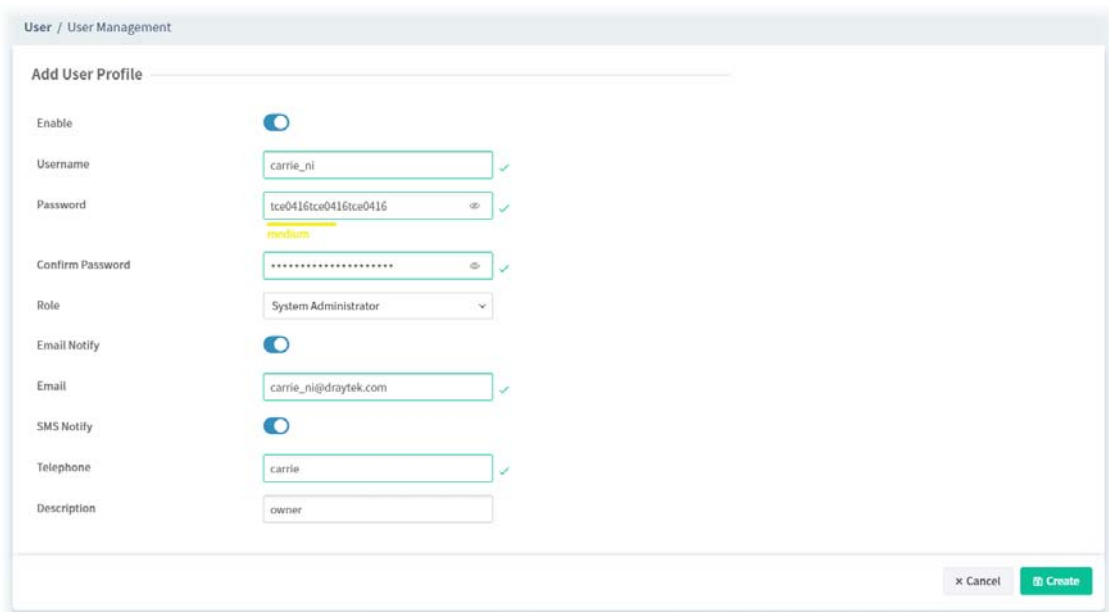
To add, delete a user or check information for a user, open **User >> User Management**. This page displays basic information including username, authentication, role, status (active, inactive), and email address for the user.



These parameters are explained as follows:

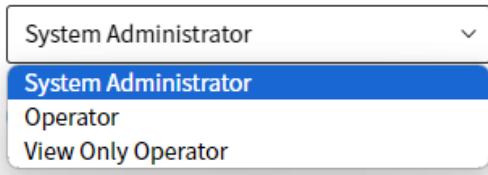
Item	Description
+Add	Click to add a user.
Delete	Click to remove the selected user.

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



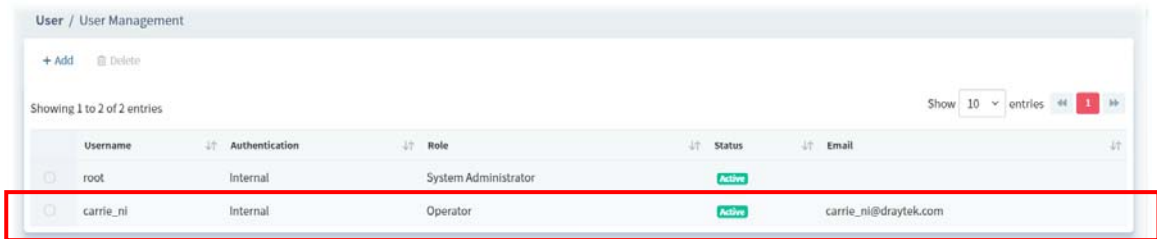
These parameters are explained as follows:

Item	Description
Enable	Click to enable / disable the user profile.
Username	Enter a name for the new user.
Password	Enter the password for the user.
Confirm Password	Enter the password same as above 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.

	<p>System Administrator – Have the highest authority.</p>  <p>Operator – Have the low authority higher than View Only Operator. It allows to modify settings for some web user interface.</p> <p>View Only Operator – Have the lowest authority. For example, the user can view the web user interface but has no right to edit the pages.</p>
Email Notify	Click to enable the email notification function.
Email	Enter the email for communication between the user and VigorConnect server.
SMS Notify	Click to enable the SMS notification function.
Telephone	Type the telephone number for receiving the SMS notification.
Description	Enter a brief description for the user.
Cancel	Discards current settings.
Create	Click it to create a new user profile 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., `carrie_ni`) and click it.



The screenshot shows the 'User / User Management' interface. At the top, there are '+ Add' and 'Delete' buttons. Below that, it says 'Showing 1 to 2 of 2 entries' and 'Show 10 entries'. The table has columns for Username, Authentication, Role, Status, and Email. Two users are listed: 'root' (System Administrator, Active) and 'carrie_ni' (Operator, Active, Email: carrie_ni@draytek.com). The 'carrie_ni' row is highlighted with a red border.

Username	Authentication	Role	Status	Email
root	Internal	System Administrator	Active	
carrie_ni	Internal	Operator	Active	carrie_ni@draytek.com

4.2 External Authentication Server

VigorConnect uses LDAP profile as the external authentication server.

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 will be used to authenticate VPN connection attempts.

Active Directory (AD) is a directory service from Microsoft that supports LDAP queries.

These parameters are explained as follows:

Item	Description
Enable	Click to enable / disable the external authentication server.
Choose User Role at Registration	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> <div style="border: 1px solid gray; padding: 2px;">System Administrator</div> <div style="background-color: #0070C0; color: white; padding: 2px;">System Administrator</div> <div style="border: 1px solid gray; padding: 2px;">Operator</div> <div style="border: 1px solid gray; padding: 2px;">View Only Operator</div> </div> <p>System Administrator – Have the highest authority.</p> <p>Operator – Have the low authority higher than View Only Operator. It allows to modify settings for some web user interface.</p> <p>View Only Operator – Have the lowest authority. For example, the user can view the web user interface but has no right to edit the pages.</p>
Server IP Address	Enter the IP address of the authentication server (LDAP server).
Authentication Server Type	Select the server type. At present only Active Directory/LDAP is available.
Destination Port	Enter the port number for the server. The default value is 389.
Use SSL	Click to use Secure Sockets Layer (SSL) for LDAP traffic.
Bind Type	Select from one of 3 bind types: Simple Mode – Initiate bind operation (authentication) without performing user search. This mode can be used when all users belong to the same

	<p>branch in the LDAP structure.</p> <p>Anonymous – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user search. This mode can be used when not all users belong to the same branch and the server allows anonymous searches.</p> <p>Regular Mode – Same as Anonymous mode, except that the DN and password are sent to the server. This mode can be used when not all users belong to the same branch and the server does not allow anonymous searches.</p> <p>For the regular mode, you'll need to Enter the Regular DN and Regular Password.</p>
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 .
+Add	Up to 5 LDAP profiles can be created. These profiles would be used with User Management for different purposes in management.
Save	Save the current settings.

To add a new Active Directory / LDAP profile, click **+Add**.

User / External Authentication Server

Profile Name

Common Name Identifier

Base Distinguished Name

Additional Filter


Note:

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

Group Distinguished Name

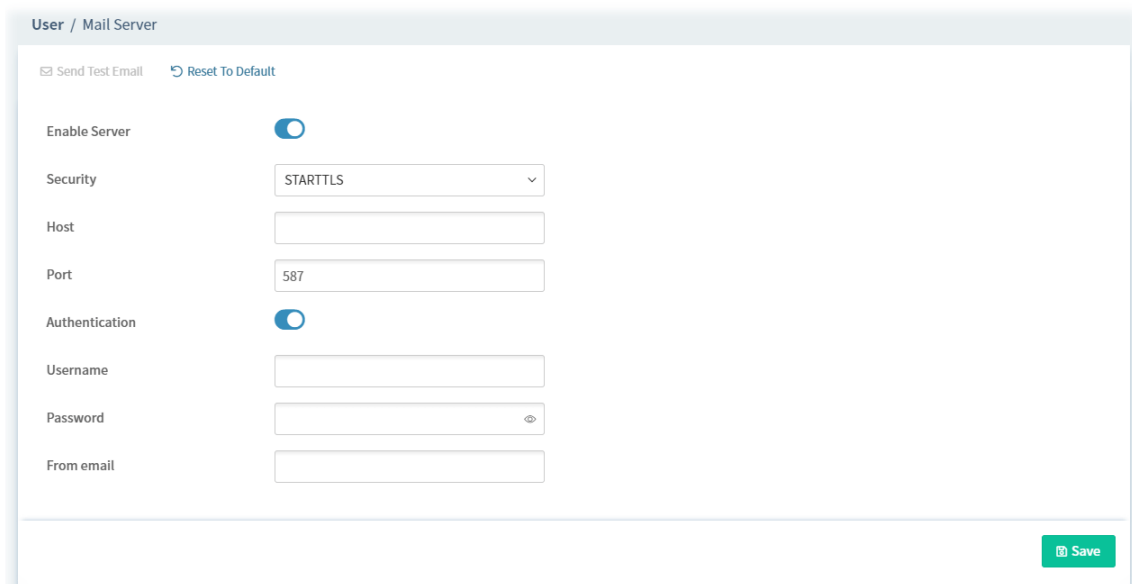
These parameters are explained as follows:

Item	Description
Profile Name	Enter a name for identification.
Common Name Identifier	The common name attribute, which is typically "cn" in most LDAP configurations.
Base Distinguished Name	<p>The starting point of user search in the LDAP directory, for example, dc=draytek,dc=com.</p> <p><input type="button" value="🔍"/> – click this icon to display a list of valid DNs in the LDAP directory.</p>
Additional Filter	<p>Additional filter to be applied to the search request to identify eligible users.</p> <p>For example,</p> <p>– "OpenLDAP: (gidNumber=500)"</p>

	<p>Here group ID 500 is the group of dial-in users.</p> <ul style="list-style-type: none"> - "ActiveDirectory: (msNPAllowDialin=TRUE)" <p>The msNPAllowDialin attribute indicates that the user has permission to dial in remotely.</p>
Group Distinguished Name	<p>The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com.</p> <p> - click this icon to display a list of valid DN's in the LDAP directory.</p>
Cancel	Discards current modification.
Save	Save the current settings.

4.3 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.



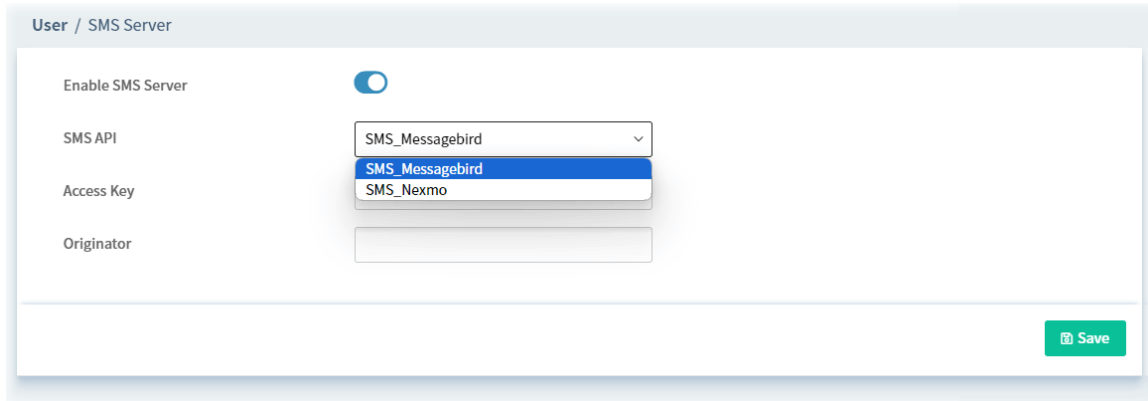
These parameters are explained as follows:

Item	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.
Reset To Default	Click to reset the mail server to default settings.
Enable Server	Click to enable /disable the SMTP server.
Security	Choose None, STARTTLS or SSL / TLS for the security of the mail transferring.
Host	Enter the IP address of the SMTP server.
Port	Type the port number of the SMTP server.

Authentication	Click to activate/disable this function while using e-mail application.
Username	Enter the user name for authentication.
Password	Enter the password for authentication.
From email	Enter the e-mail address as the sender.
Save	Save the current settings.

4.4 SMS Server

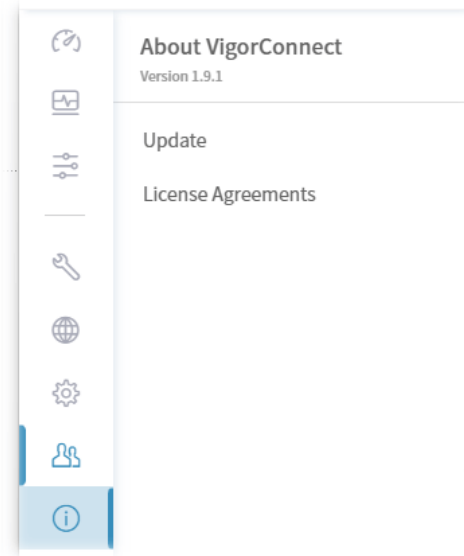
It is used to configure the SMS server for sending notification. When a CPE in a group encounters an event which can be classified as the level defined in this page, a SMS will be sent out for notification.



These parameters are explained as follows:

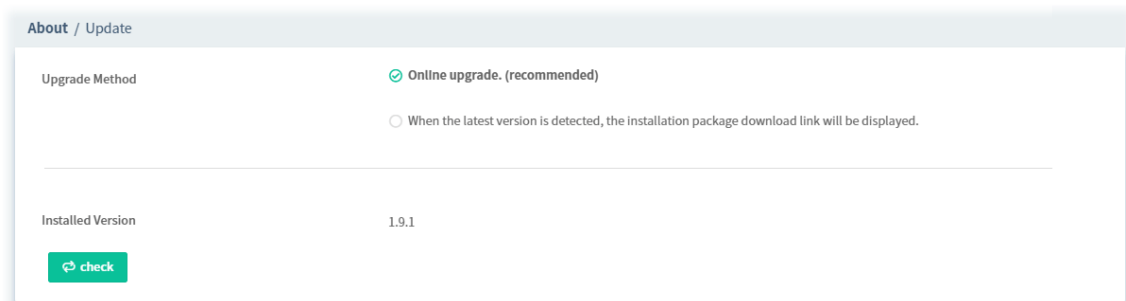
Item	Description
Enable SMS Server	Click to enable /disable the SMS server.
SMS API	Use the drop down list to choose an ISP for sending SMS.
Access Key	Enter the key value based on the information from the service provider.
Originator	Enter the name/value based on the information from the service provider.
Save	Save the current settings.

Chapter 5 About VigorConnect



5.1 Update

This page offers information for the newest version of VigorConnect.



Available settings are listed as follows:

Item	Description
Upgrade Method	Online upgrade. - After clicking it, you will be notified when the latest version is available. When the latest... - After clicking it, the system will display the newest version available for you to download and upgrade for VigorConnect.
Installed Version	Display the current software version installed.

5.2 License Agreements

This page displays relational license information required by VigorConnect.

DrayTek VigorConnect

System time: 14:21 11/05/2024 root System Administrator

License Agreements

Root Network

Apache License, Version 2.0			MIT		
Name	Author	Web Site	Name	Author	Web Site
client_golang	prometheus	🔗	go-socks5	armon	🔗
go-oidc	coreos	🔗	go-ini	vaughan0	🔗
cobra	spf13	🔗	golink	matishishao	🔗
go-proxyproto	pires	🔗	diskv	peterbourgon	🔗

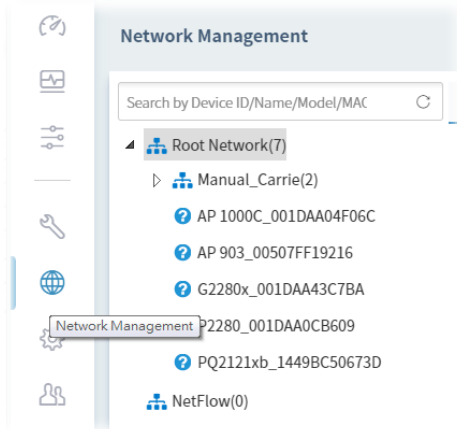
BSD 3-clause License			BSD license		
Name	Author	Web Site	Name	Author	Web Site
protobuf	golang	🔗	gosnmp	gosnmp	🔗
mux	gorilla	🔗	goputil	shirou	🔗
flock	golrs	🔗	Crypt2go	Andre Burgaud	🔗
zoinl	zickey	🔗	Handlers		🔗

GNU General Public License v3.0			ISC License		
Name	Author	Web Site	Name	Author	Web Site
slimdb	sonyarouje	🔗	goip2-golang	oschwald	🔗
			FTP	Julien Laffaye	🔗

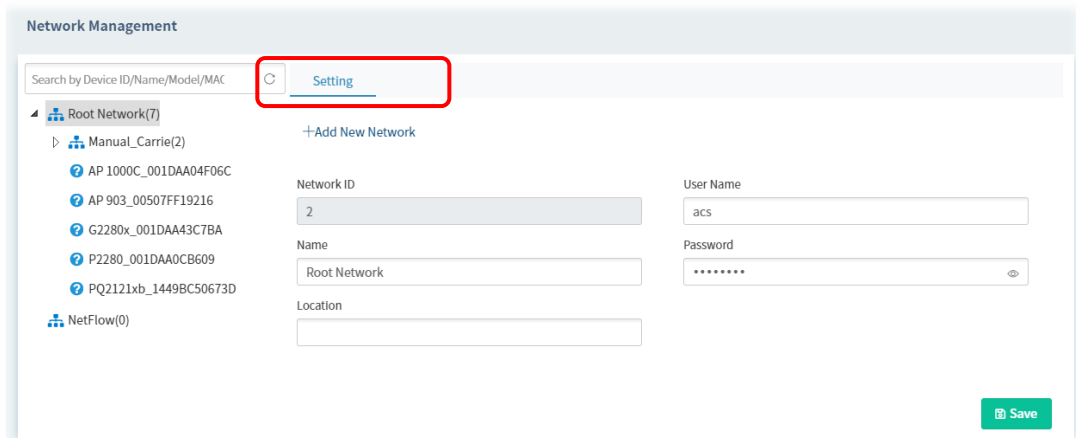
Applications

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

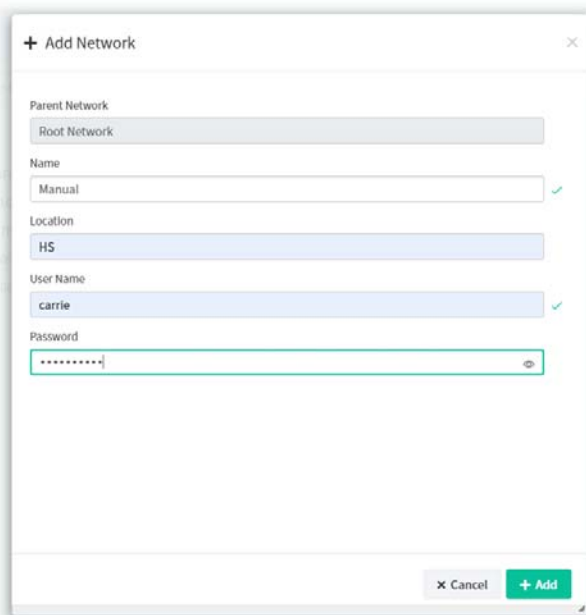
1. Open **Network Management**.



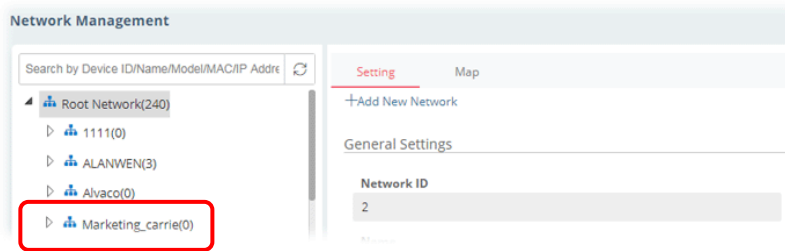
2. Click **+Add New Network** on the **Setting** page.



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

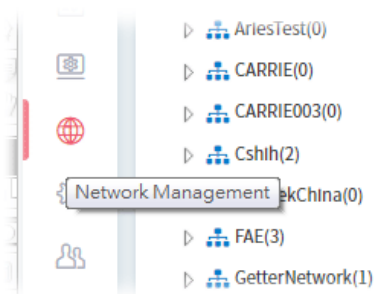


4. Click **Add**.
5. The new network has been created and displayed on the tree view.

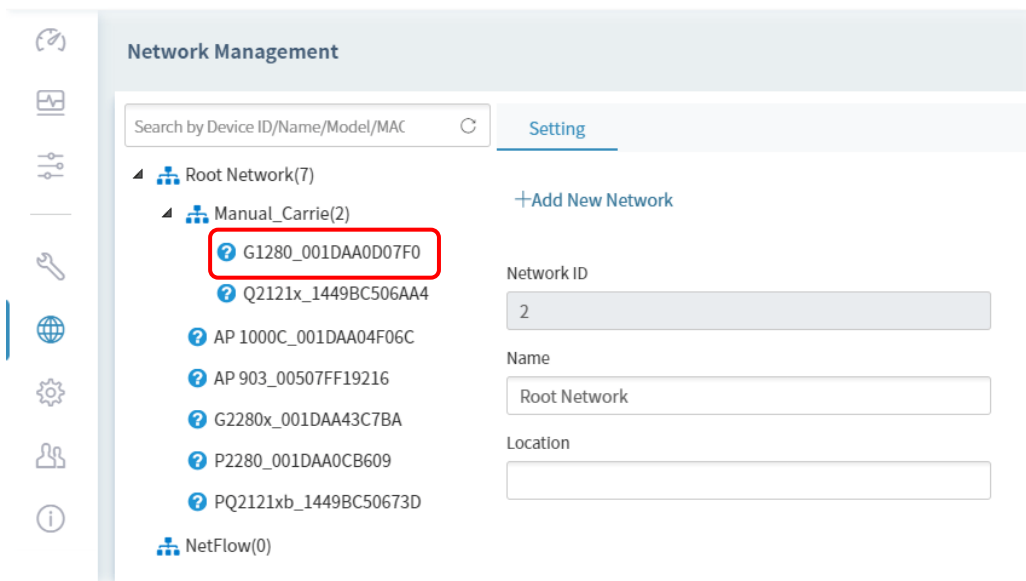


A.2 How to Change the Network of a Device?

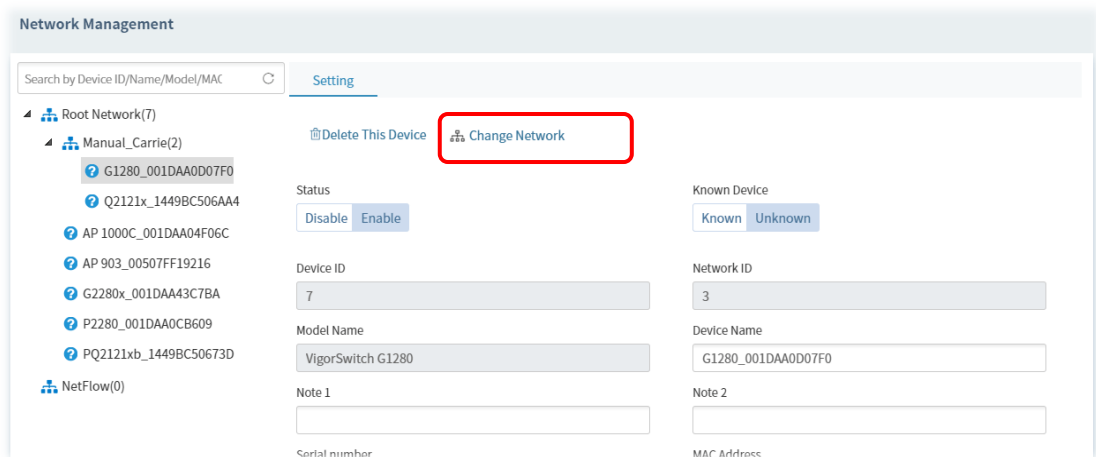
1. Open **Network Management**.



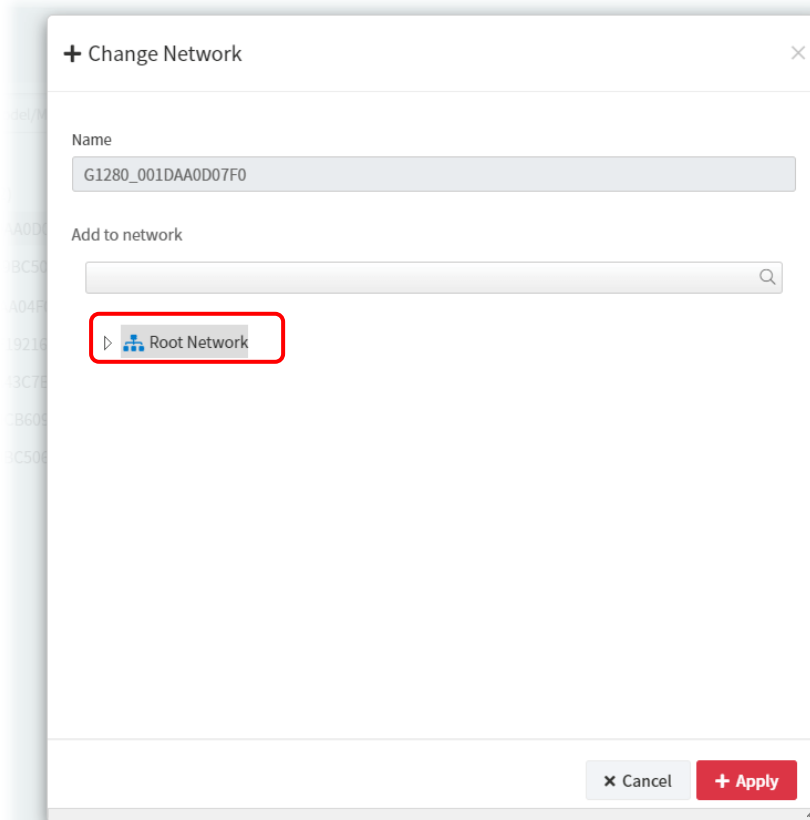
2. Choose and click a device displayed on the Network tree view (e.g., G1280 under Manual_Carrie).



3. From the following page, click **Change Network**.



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

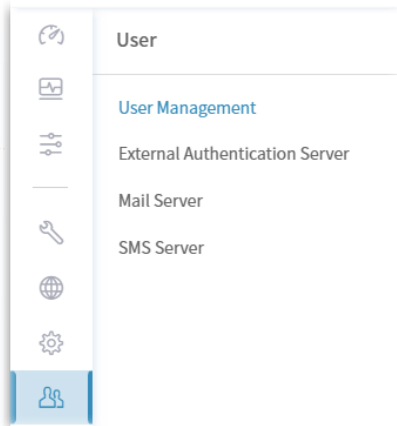


5. The selected device has been grouped under the specified network (**Root Network**, in this case).

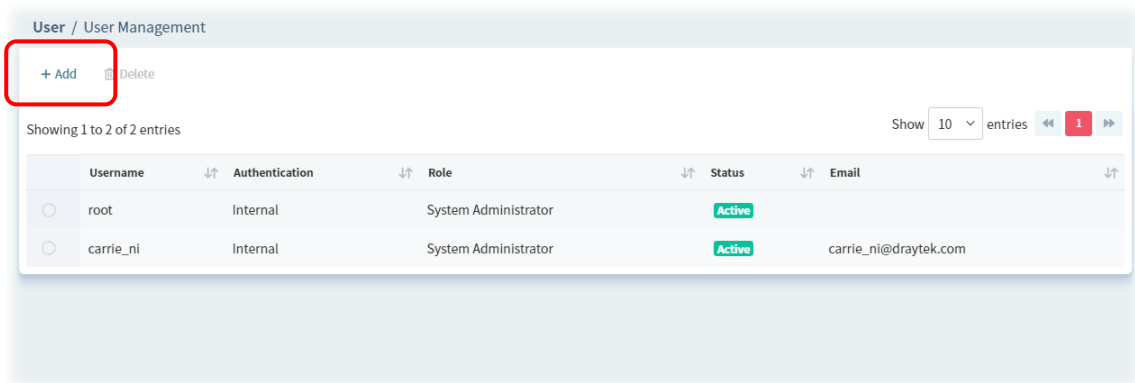
The screenshot displays the 'Network Management' interface. On the left, a tree view shows a hierarchy: 'Root Network(7)' expanded to show 'Manual_Carrie(1)', which contains several devices. The device 'G1280_001DAA0D07F0' is highlighted with a red box. Below this are 'NetFlow(0)'. On the right, the 'Setting' tab is active, showing options to 'Delete This Device' and 'Change Network'. The 'Status' section has 'Disable' and 'Enable' buttons. The 'Device ID' field contains '7', and the 'Model Name' field contains 'VigorSwitch G1280'. A 'Note 1' field is also present.

A.3 How to Add a User?

1. Open **User>>User Management**.



2. Click **+Add**.



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


A screenshot of the 'Add User Profile' form in the 'User / User Management' interface. The form has the following fields:



- Enable:
- Username: ✓
- Password: ✓ (Strength: medium)
- Confirm Password: ✓
- Role: ✓
- Email Notify:
- Email: ✓
- SMS Notify:
- Telephone: ✓
- Description:

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

4. Click **Create**.

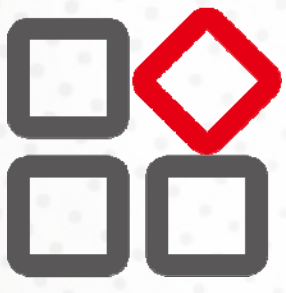
User / User Management

+ Add  Delete

Showing 1 to 3 of 3 entries Show entries  **1** 

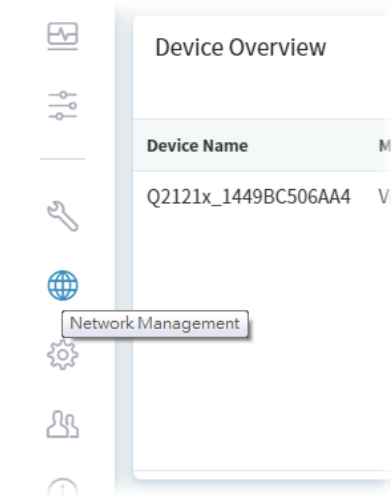
	Username	Authentication	Role	Status	Email
<input type="radio"/>	root	Internal	System Administrator	Active	
<input type="radio"/>	carrie_ni	Internal	System Administrator	Active	carrie_ni@draytek.com
<input checked="" type="radio"/>	TestForCo	Internal	System Administrator	Active	carrie@draytek.com

Part III General Settings for Managing Device



Chapter 6 Network Management

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



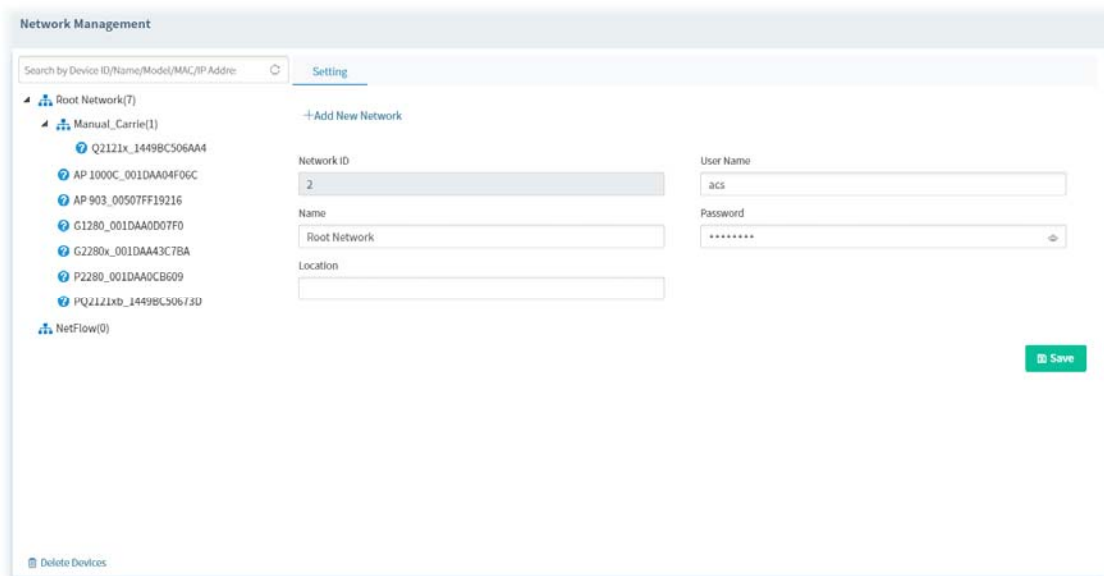
It can

- Add new network (s) for new client which will be managed by VigorConnect.
- Delete existed network if the client will not be managed by VigorConnect.
- Modify the name and location of the network for management.

6.1 Setting

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

6.4.1.1 Settings for Root Network



These parameters are explained as follows:

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

Search by device ID/name/model/MAC/IP Address	Enter the ID, name, model, MAC address, or 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 VigorConnect randomly for the selected network.
Name	Display the name of the parent network. You can modify it if required.
Location	Type the location (e.g., HsinChu, New York) for such network.
User Name	Display the name of the selected network. Change it if required.
Password	Display the password of the selected network. Change it if required.
Save	Click to save the change.

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

The screenshot shows a dialog box titled '+ Add Network'. It contains the following fields and values:

- Parent Network:** Root Network
- Name:** Manual (with a green checkmark)
- Location:** HS
- User Name:** carrie (with a green checkmark)
- Password:** A masked field with a toggle icon to show/hide the password.

At the bottom right of the dialog, there are two buttons: 'Cancel' and '+ Add'.

These parameters are explained as follows:

Item	Description
Parent Network	Display the name of the root network. New created network will be the sub-network of the parent network. In default, Root Network is the parent network for any new created network.
Name	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 .
User Name	Enter a login name (e.g., <i>carrie</i>) for the new network which will be used for communication between Vigor device and VigorConnect.
Password	Enter a password (e.g., <i>admin123</i>) for this new network.
Cancel	Discards current modification.
+Add	Save the current settings and exit the page.

6.1.1 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:

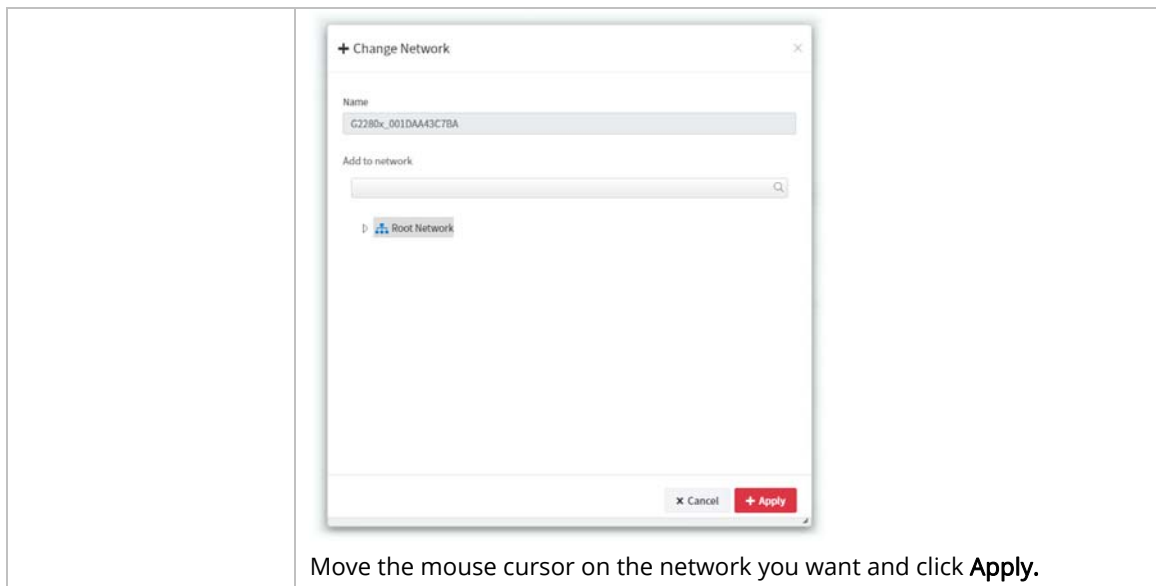
- Modify the name of the device for easy identification and management by VigorConnect.
- Modify the location of the device easily.
- Modify the user name/password of certain device (non-DrayTek device) to be managed by VigorConnect.
- Enable or disable the management of the device for VigorConnect.
- Select certain protocol (e.g., http/https) for the device (CPE) for management.

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

The screenshot shows the 'Network Management' interface. On the left, a tree view shows 'Root Network(7)' with several sub-networks. The selected device 'G2280x_001DAA43C7BA' is highlighted. The main area displays the settings for this device, including a search bar, a 'Setting' tab, and various input fields and buttons for configuration.

These parameters are explained as follows:

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

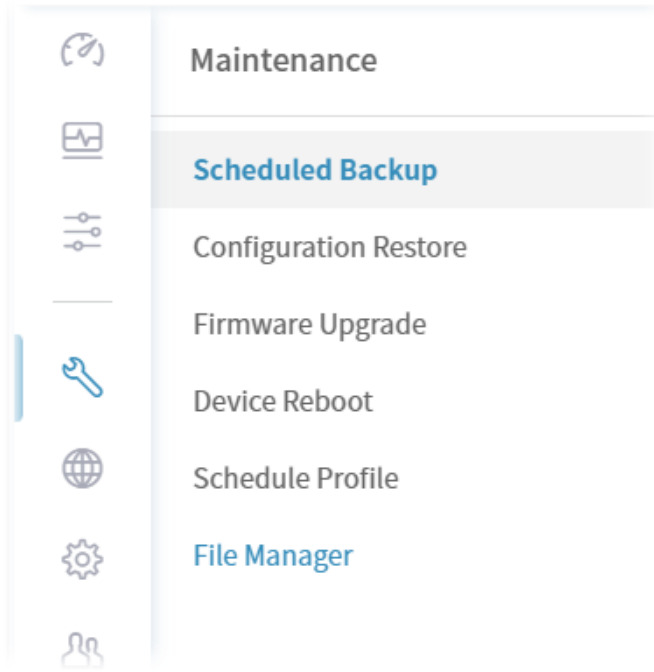


General Settings	
Status	<p>Disable – The selected device will be hidden on the tree view.</p> <p>Enable – The selected device can be displayed on the tree view.</p>
Known Device	<p>Known – The selected CPE is known (👤) to VigorConnect.</p> <p>Unknown – If the selected CPE is new added device, it will be identified as Unknown.</p>
Network ID	Displays the ID number of the network.
Model Name / Device Name	<p>Model Name – Display the model name of the selected device. Model name cannot be changed.</p> <p>Device Name – Display the name of the device for identification. It can be changed if required.</p>
Note 1 / Note 2	<p>Note 1 – Displays brief description for the selected device.</p> <p>Note 2 – Displays brief description for the network.</p>
Serial number / MAC Address	<p>Serial number – Enter a number for identification of the device.</p> <p>MAC Address – Display the MAC address of the device.</p>
Location	Displays 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	Displays a number for management port. If required, click the Edit button to enter a port number that will be used for accessing into the web user interface of the CPE.
Management Protocol	Choose CEP default, HTTPS or HTTP.
CPE Client IP / Port / URI	Display the IP address, port number and URI.
CPE Client User Name / Password	<p>Display the username and password that VigorConnect can use to access into the CPE.</p> <p>Edit - Click to change the username and password.</p>

This page is left blank.

Chapter 7 Maintenance Menu

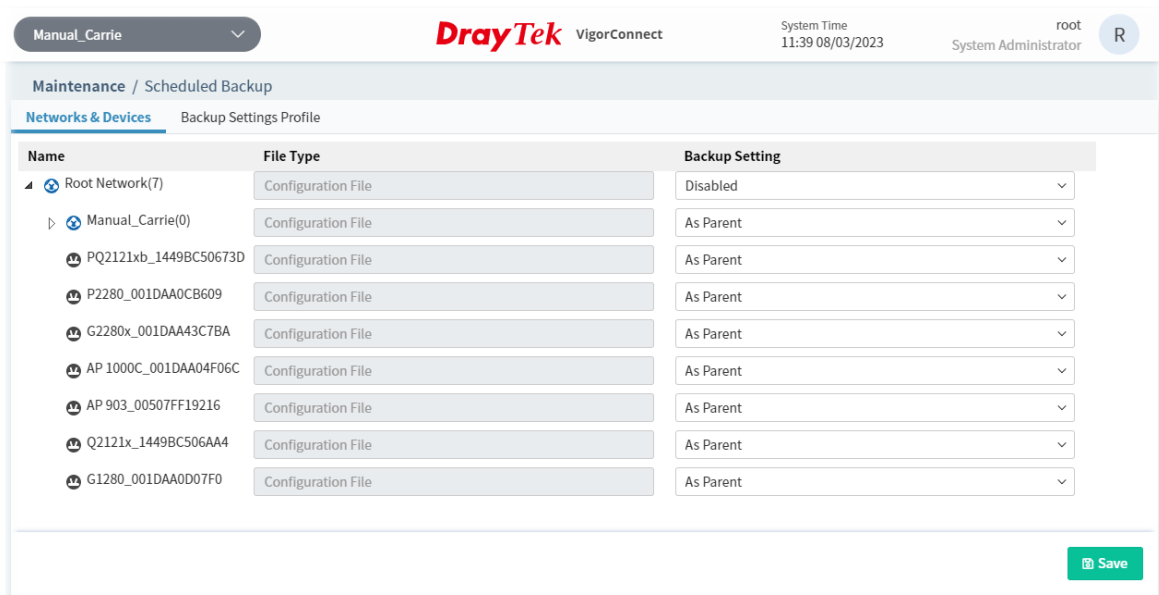
Settings in Maintenance can be applied onto numerous TR-069 CPEs instead of configuring settings for each CPE one by one.



7.1 Scheduled Backup

7.1.1 Networks & Devices

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 VigorConnect.



These parameters are explained as follows:

Item	Description
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 - The backup setting for the selected network / device is the same as the top setting. Disabled - No backup setting for the selected network / device. Default - Use the default backup setting for the selected network / device.
Save	Save the current settings.

7.1.2 Backup Settings Profile

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

The screenshot shows a web interface for 'Maintenance / Scheduled Backup'. It includes a breadcrumb 'Networks & Devices' and a sub-header 'Backup Settings Profile'. Below this is a '+ Add' button and a table with the following data:

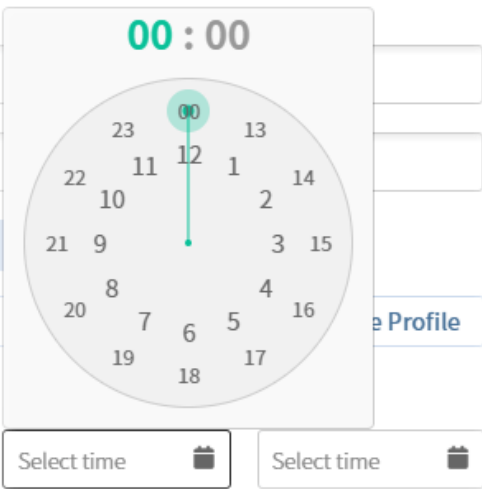
Name	Period(Days)	Type	Time Interval	Action
Default	1	The Last 20	Now	Edit Delete

These parameters are explained as follows:

Item	Description
+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.

These parameters are explained as follows:

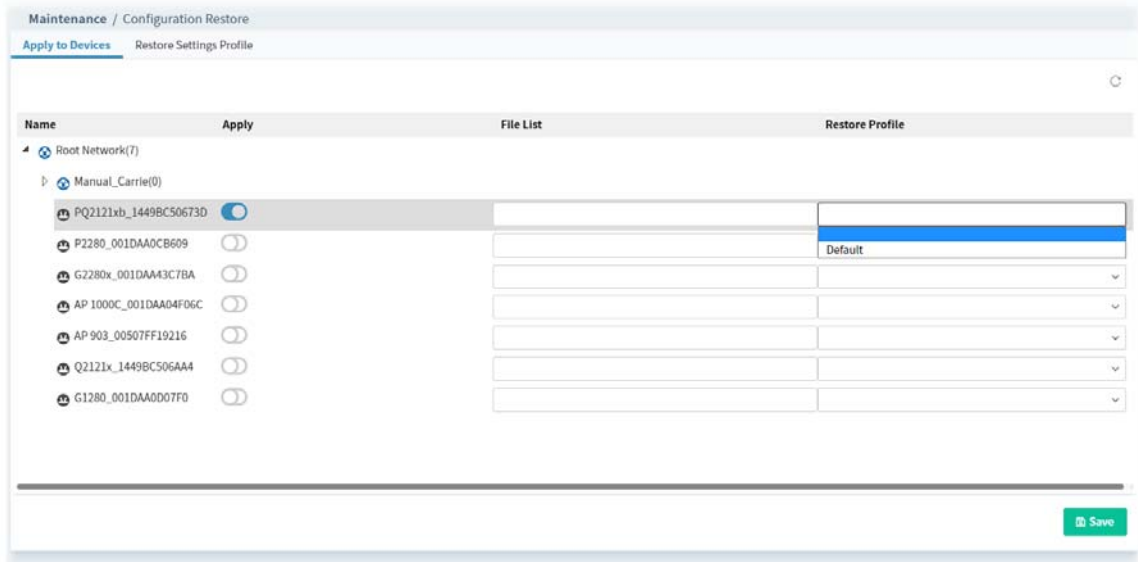
Item	Description
Name	Enter a name of the backup profile.
Backup Period(days)	The number typed here means the interval for the backup executed by VigorConnect. The unit is "day". If you type 1, that means the backup will be executed one time by one day.
Keep Files	Choose to keep all of the files (configuration files) or the last 20 files.
Backup Time	<p>Set a time interval for executing the backup work for networks and devices.</p> <ul style="list-style-type: none"> ● Now - The backup work will be executed immediately after clicking the Save button. ● Scheduled - The backup work will be executed at the specified time and date after clicking the Save button. ● Schedule Profile - The backup work will be executed according to the selected schedule profile after clicking the Save button.
Scheduled	<p>Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date – Click to enable the time setting. Date – Click to pop up a calendar to choose a date as the starting date.</p>

	<div data-bbox="619 226 1046 275" style="border: 1px solid #ccc; padding: 2px;">2023-03-08 ✓</div> <div data-bbox="619 282 1007 640" style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> < Mar > </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;"> 2023 > </div> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th>Su</th><th>Mo</th><th>Tu</th><th>We</th><th>Th</th><th>Fr</th><th>Sa</th></tr> </thead> <tbody> <tr> <td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr> <tr> <td>5</td><td>6</td><td>7</td><td style="background-color: #00a651; color: white;">8</td><td>9</td><td>10</td><td>11</td></tr> <tr> <td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td></tr> <tr> <td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr> <tr> <td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td></tr> </tbody> </table> </div>	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	
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																																						
<p>Schedule Profile</p>	<p>Choose a trigger profile from the drop down list. In which, VigorConnect offers default schedule profile.</p> <div data-bbox="595 775 970 1124" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <div style="border-bottom: 1px solid #ccc; padding-bottom: 2px;">reset_password_wizard</div> <div style="background-color: #007bff; color: white; padding: 2px;">reset_password_wizard</div> <div style="padding: 2px;">reboot_wizard</div> <div style="padding: 2px;">restore_wizard</div> <div style="padding: 2px;">backup_wizard</div> <div style="padding: 2px;">default</div> <div style="padding: 2px;">test1</div> <div style="padding: 2px;">test2</div> <div style="padding: 2px;">test3</div> <div style="padding: 2px;">test4</div> <div style="padding: 2px;">test5</div> <div style="padding: 2px;">test6</div> <div style="padding: 2px;">test7</div> <div style="padding: 2px;">tt1</div> </div>																																										
<p>Save</p>	<p>Save the changes on this page.</p>																																										

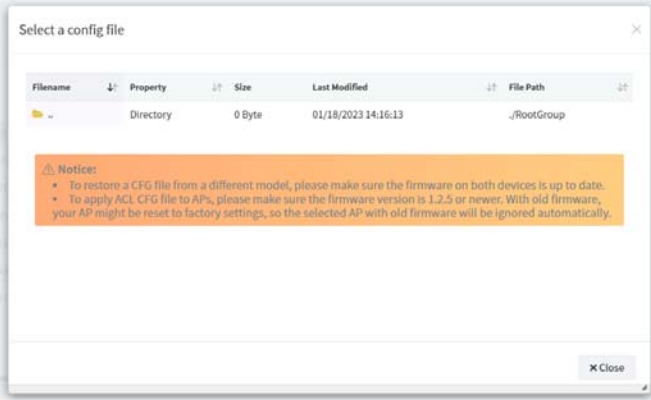
7.2 Configuration Restore

7.2.1 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 VigorConnect.

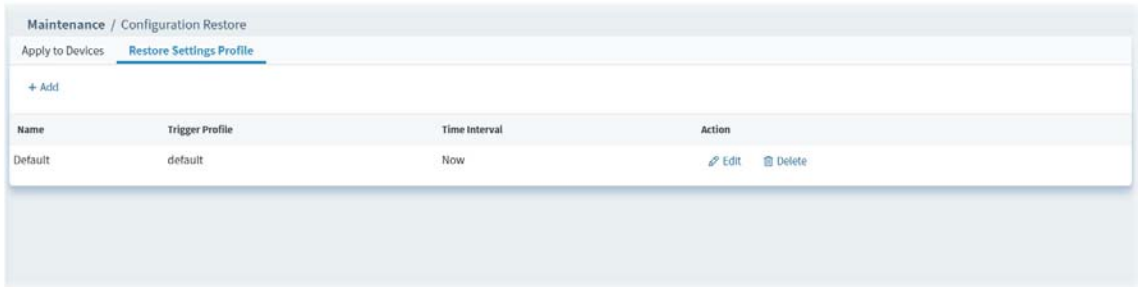


These parameters are explained as follows:

Item	Description
Apply	Click the icon to enable configuration restoration for the selected CPE.
File List	Open a dialog to choose one of the files for the file restoration of the selected CPE. 
Restore Profile	Choose a profile defined in Restore Settings Profile for applying onto the selected CPE. Default - Use the default restore setting for the selected network / device. Others - In addition to Empty and Default, profiles defined in Restore Settings Profile also will be listed in this drop-down list.
Save	Save the current settings.

7.2.2 Restore Settings Profile

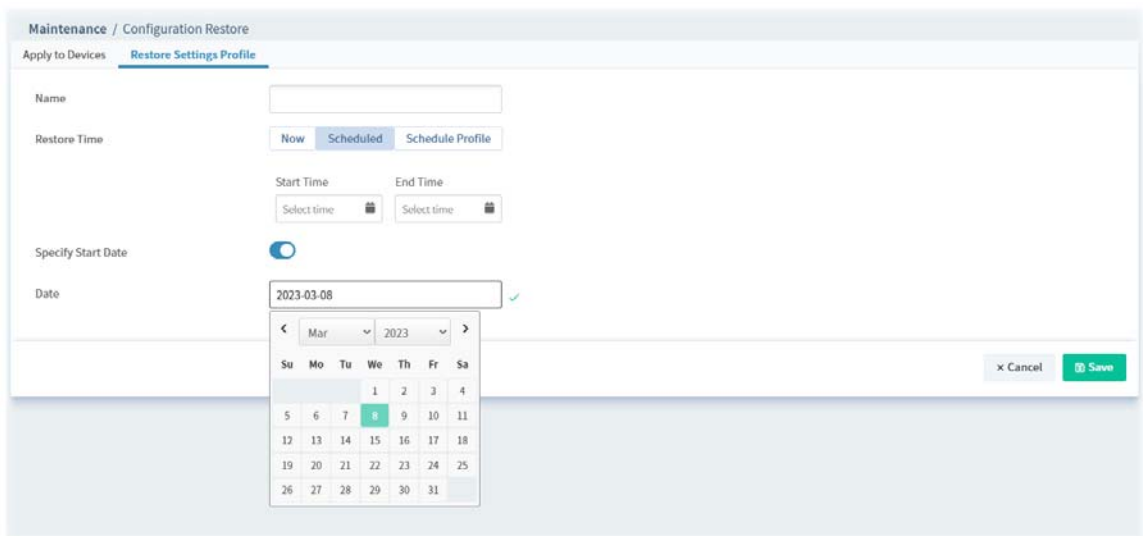
This page can determine the trigger time and method for firmware restoration.



These parameters are explained as follows:

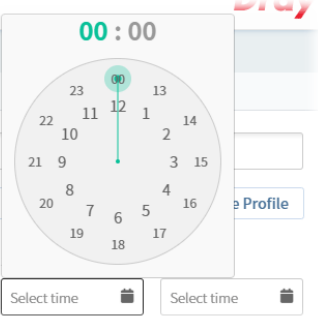
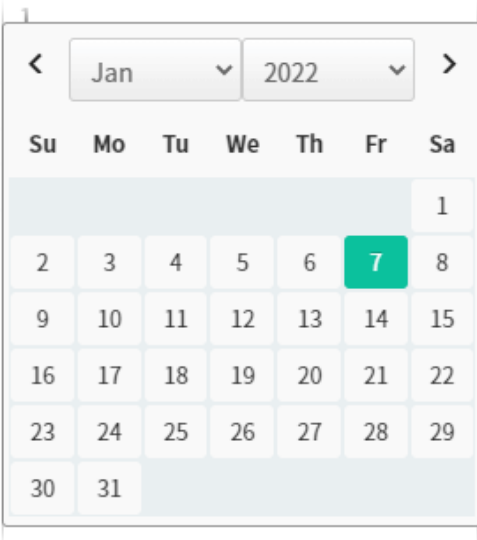
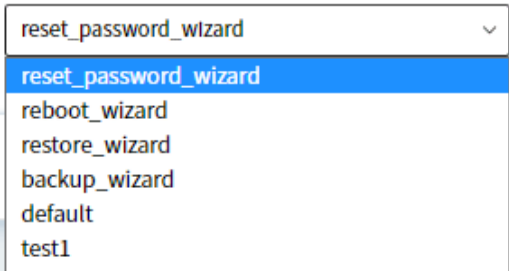
Item	Description
+Add	Click to create a new profile.
Name	Displays the name of the restore setting profile.
Trigger Profile	Displays the time schedule selected for the restore setting profile.
Time Interval	Displays the time period to trigger the setting restoration.
Action	Edit - Click to modify, change the selected profile. Delete - Click to delete the selected profile.

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



These parameters are explained as follows:


Item	Description
Name	Enter a name of the restore setting profile.
Restore Time	Set a time interval for restoring the configuration settings for networks and devices. <ul style="list-style-type: none"> Now - The setting restoring work will be executed immediately after clicking the Save button. Scheduled - The setting restoring work will be executed at the specified time and date after clicking the Save button. Schedule Profile - The setting restoring work will be executed according to the selected schedule profile after clicking the Save

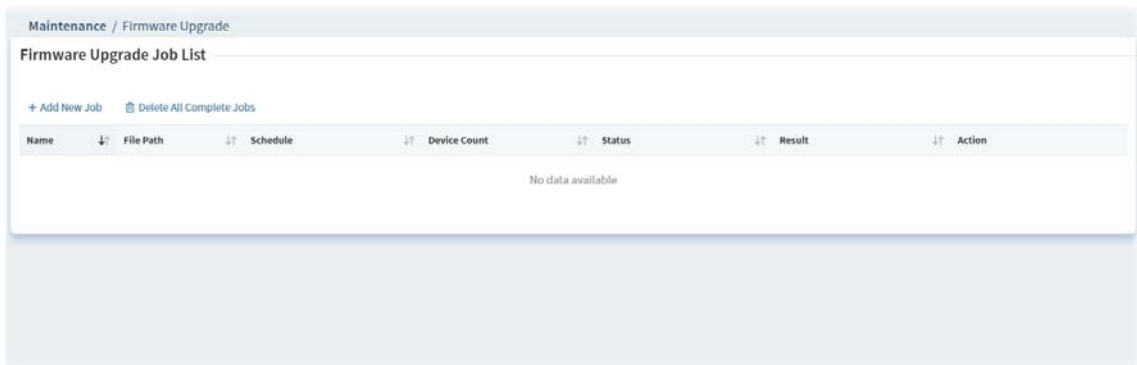
	button.
Now	The configuration restore will be executed after clicking Save .
Scheduled	<p>Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date – Click to enable the time setting.</p> <p>Date – Click to pop up a calendar to choose a date as the starting date.</p> 
Schedule Profile	<p>Trigger Profile – Choosing a trigger profile from the drop down list. In which, VigorConnect offers default schedule profile.</p> 
Cancel	Discard current settings and return to the previous page.
Save	Save the current settings.

7.3 Firmware Upgrade

When VigorConnect 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 VigorConnect server. If everything can match but software version not, VigorConnect will judge that the remote CPE requiring firmware upgrade. Next, VigorConnect 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 VigorConnect server uses to compare information coming from CPE router with the information stored in VigorConnect server's database.

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



These parameters are explained as follows:

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

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

Maintenance / Firmware Upgrade

Firmware Upgrade Job Settings

Name:

Status:

Upgrade Time:

Start Time:

End Time:

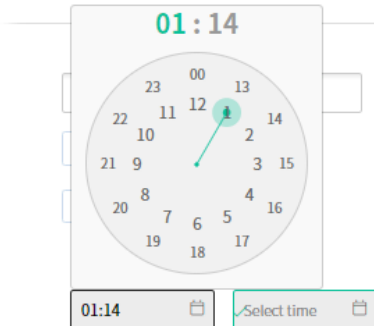
Date:

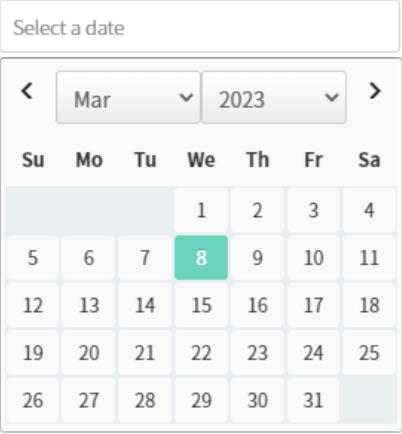
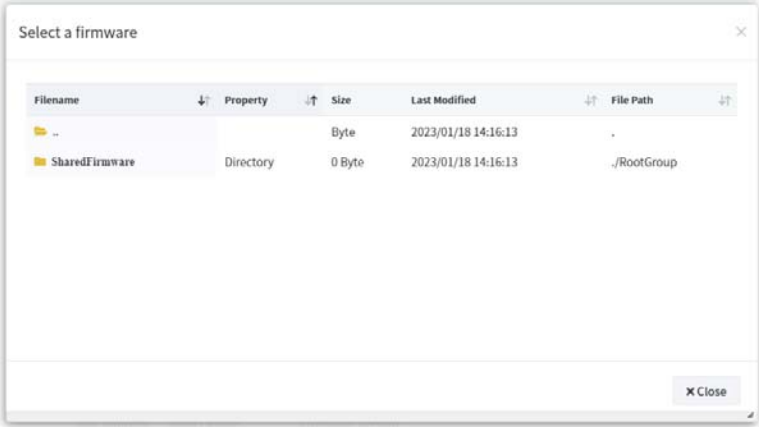
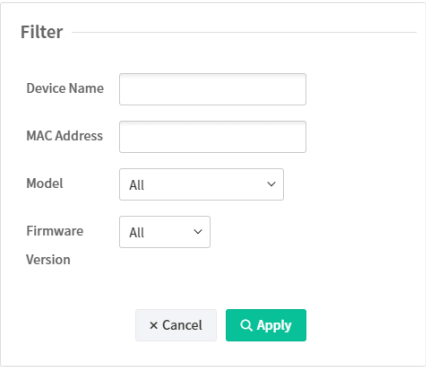
Apply Firmware:

Device to Upgrade ▾

Name	MAC Address	Model Name	Firmware Version
Root Network(7)			
Manual_Carrie(0)			

These parameters are explained as follows:

Item	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. <ul style="list-style-type: none"> ● Now - The firmware upgrade job will be executed immediately after clicking the Save button. ● Scheduled - The firmware upgrade job will be executed at the specified time and date after clicking the Save button.
Scheduled	<p>Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Date – Click to pop up a calendar to choose a date as the starting date.</p>

	
<p>Apply Firmware</p>	<p>Click to open a dialog to select a firmware file. VigorConnect will upgrade the selected CPE with the selected file.</p> 
<p>Device to Upgrade</p>	<p>Click the Filter icon to set the filtering conditions.</p> <p>Device to Upgrade ▾</p>  <p>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. Apply - After clicking Apply, the table below will show the devices according to filter conditions.</p>
<p>Table</p>	<p>Select one device or more devices to apply the firmware upgrade</p>

provision.

Name	MAC Address	Model Name	Firmware Version
Root Network(7)			
Manual_Carrier()			
AP 1000C_001DA04F06C	001DA04F06C	VigorAP 1000C	1.4.4
AP 903_00507FF19216	00507FF19216	VigorAP 903	1.4.6
G1280_001DAA0007F0	001DAA0007F0	VigorSwitch G1280	2.6.6
G2280x_001DAA43C7BA	001DAA43C7BA	VigorSwitch G2280x	2.8.2
P2280_001DAA0C8609	001DAA0C8609	VigorSwitch P2280	2.6.6

Model Name – Displays the model name for identification.

Firmware Version – Displays the firmware version that the model used currently.

Cancel

Discard current settings and return to the previous page.

Save

Save the current settings and exit the page.

7.4 Device Reboot

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

7.4.1 Networks & Devices

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

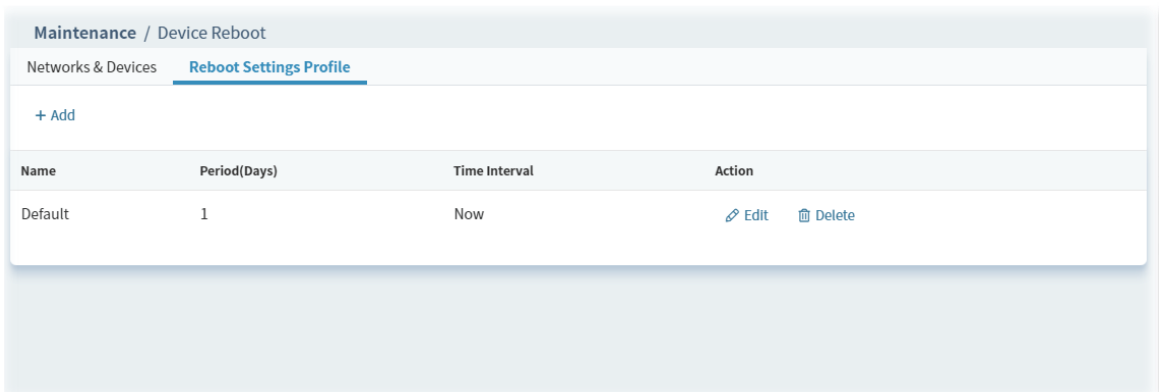
Name	Model Name	Firmware Version	Modem Version	Reboot Setting
Root Network(7)				Disabled
Manual_Carrie(0)				As Parent
PQ2121xb_1449BC50673D	VigorSwitch PQ2121xb	2.8.0_RC2	No DSL	As Parent
P2280_001DAA0CB609	VigorSwitch P2280	2.6.6		As Parent
G2280x_001DAA43C7BA	VigorSwitch G2280x	2.8.2	No DSL	As Parent
AP 1000C_001DAA04F06C	VigorAP 1000C	1.4.4	No DSL	As Parent
AP 903_00507FF19216	VigorAP 903	1.4.6	No DSL	As Parent
Q2121x_1449BC506AA4	VigorSwitch Q2121x	2.8.1	No DSL	As Parent
G1280_001DAA0D07F0	VigorSwitch G1280	2.6.6	No DSL	As Parent

These parameters are explained as follows:

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

7.4.2 Reboot Settings Profile

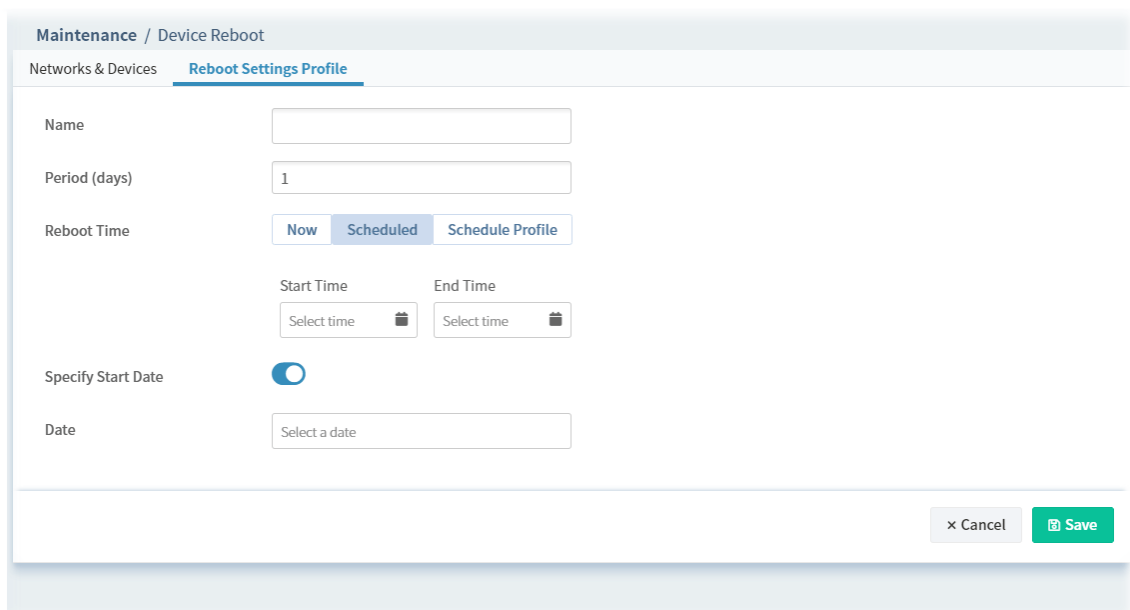
This page can determine the trigger time and method for device reboot.



These parameters are explained as follows:

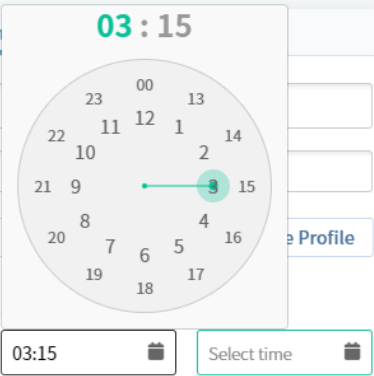
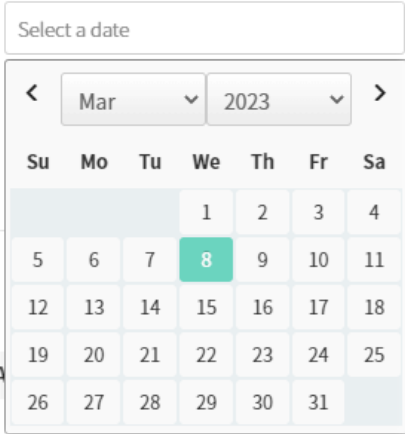
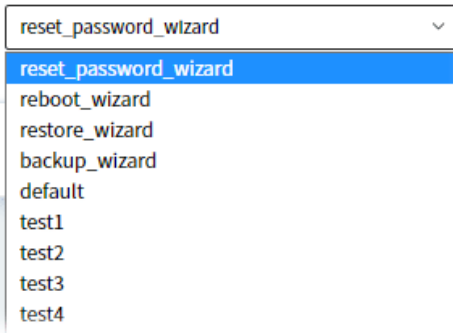
Item	Description
+Add	Click to create a new device reboot profile.
Edit	Click to edit / modify the settings for the selected profile.
Delete	Click to delete the selected profile.

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



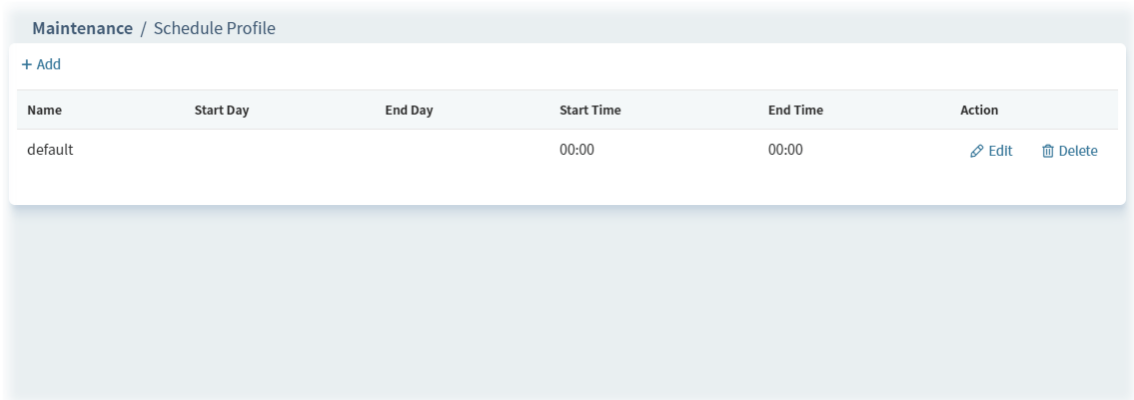
These parameters are explained as follows:

Item	Description
Name	Enter the name of the profile.
Period(days)	Determine the frequency for the CPE reboot by VigorACS. The default value is 1 day.
Reboot Time	Set a time interval for executing the device reboot. <ul style="list-style-type: none"> ● Now ● Scheduled

	<ul style="list-style-type: none"> ● Schedule Profile Now - The device reboot will be executed immediately after clicking the Save button. ● Scheduled - The device reboot will be executed at the specified time and date after clicking the Save button. ● Schedule Profile - The device reboot will be executed according to the selected schedule profile after clicking the Save button.
<p>Scheduled</p>	<p>Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.</p>  <p>Specify Start Date – Click to enable the time setting.</p> <p>Date – Click to pop up a calendar to choose a date as the starting date.</p> 
<p>Schedule Profile</p>	<p>Trigger Profile – Choosing a trigger profile from the drop down list. In which, VigorConnect offers default schedule profile.</p> 
<p>Cancel</p>	<p>Discard current settings and return to the previous page.</p>
<p>Save</p>	<p>Save the current settings.</p>

7.5 Schedule Profile

Schedule profiles can be set to apply to devices managed by VigorConnect. 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 VigorConnect.



These parameters are explained as follows:

Item	Description
+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.

The screenshot shows the configuration page for a schedule profile. It includes the following fields and controls:

- Profile Name:** A text input field.
- Date Type:** A dropdown menu currently set to 'Scheduled'.
- Start Date:** A date selection field with the placeholder 'Select a date'.
- Check End Date:** A toggle switch that is currently turned on.
- End Date:** A date selection field with the placeholder 'Select a date'.
- Time Type:** A dropdown menu currently set to 'Scheduled'.
- Start Time:** A time selection field with the placeholder 'Select time'.
- End Time:** A time selection field with the placeholder 'Select time'.

At the bottom right of the form, there are two buttons: a grey 'Cancel' button and a green 'Add' button.

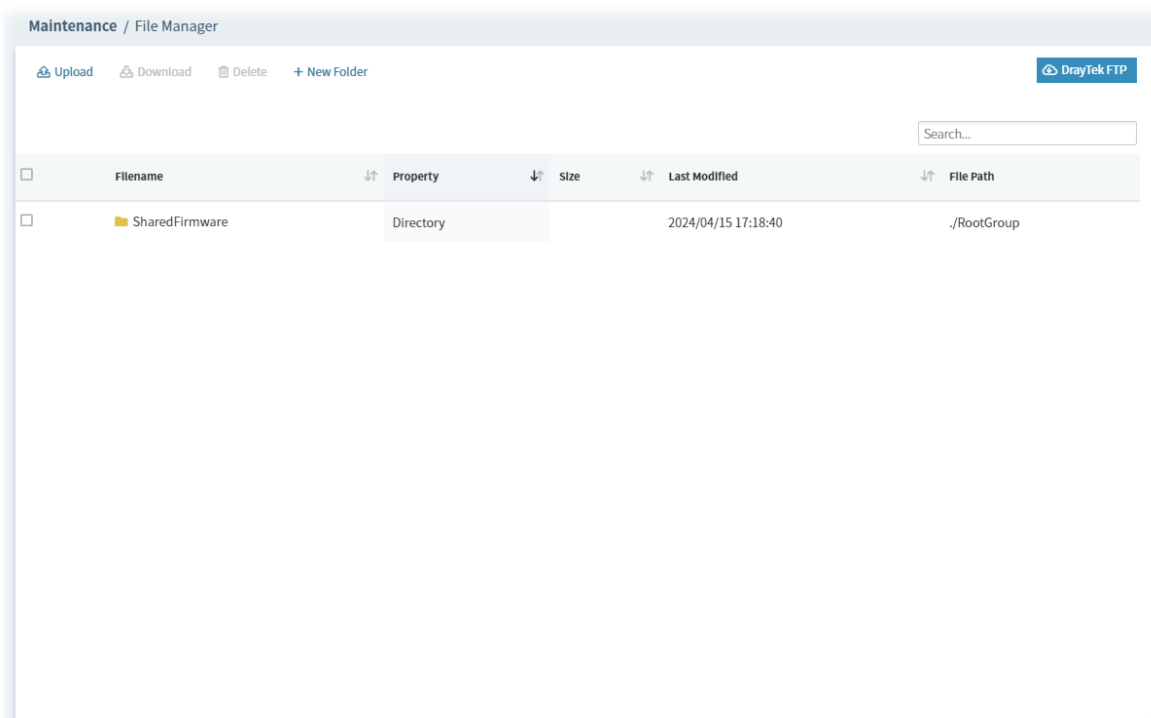
These parameters are explained as follows:

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

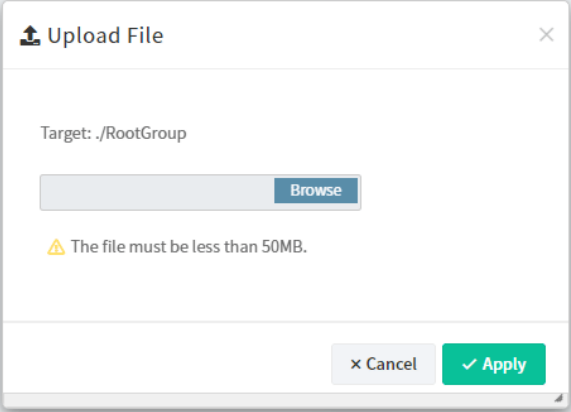
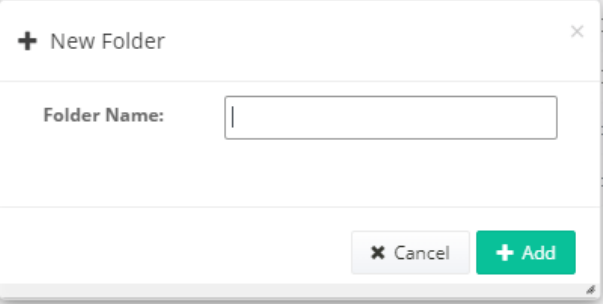
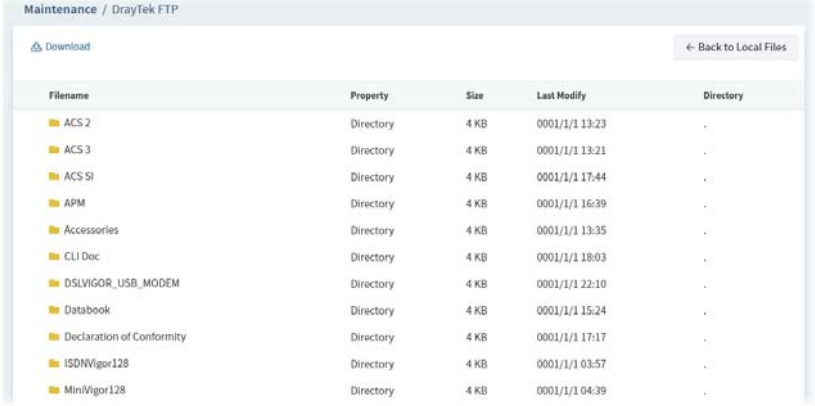
	upgrade) for the CPE will be performed immediately. Schedule – To specify a certain day to perform the job, choose this one and specify start day and end day respectively.
Start Day	Use the drop down calendar to specify the day you want to start the operation.
Check End Day	Click to enable the end day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

7.6 File Manager

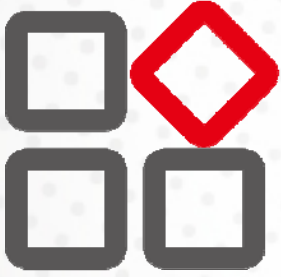
Firmware driver, configuration file for devices (VigorAP or Vigor switches) can be managed or classified with different folders.



These parameters are explained as follows:

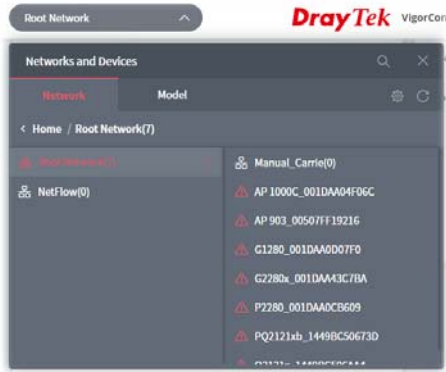
Item	Description
<p>Upload</p>	<p>Click to upload a file to VigorConnect server.</p> 
<p>Download</p>	<p>Download a driver (*.all, *.rst and etc.) related to CPE device from VigorACS 3 server.</p>
<p>Delete</p>	<p>Click to delete the selected profile.</p>
<p>New Folder</p>	<p>Create folders for files classification/management.</p> 
<p>DrayTek FTP</p>	<p>After clicking the link, the following page will appear for you to download file from DrayTek FTP directly.</p> 

Part IV Network Menu for Root Network



Chapter 8 Root Network Menu

Network contains two types, Root Network and User-defined Network. Use the drop-down menu on the top of the left side to select a network.

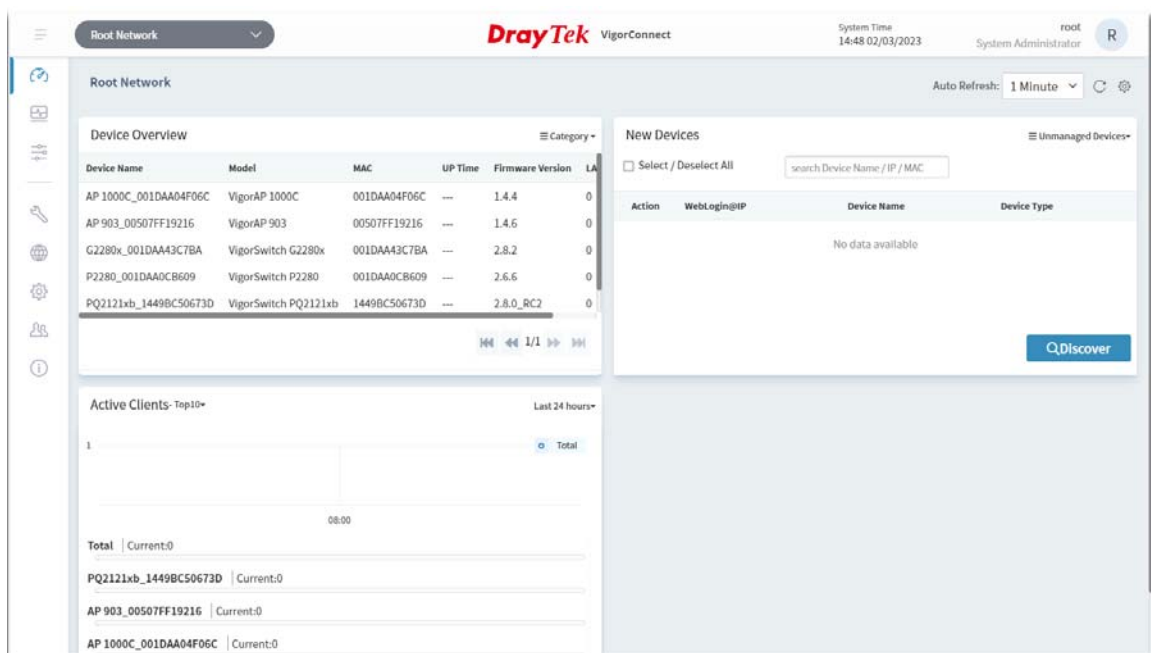


On the dashboard for root network, the Network menu contains:



8.1 Dashboard for the Root Network

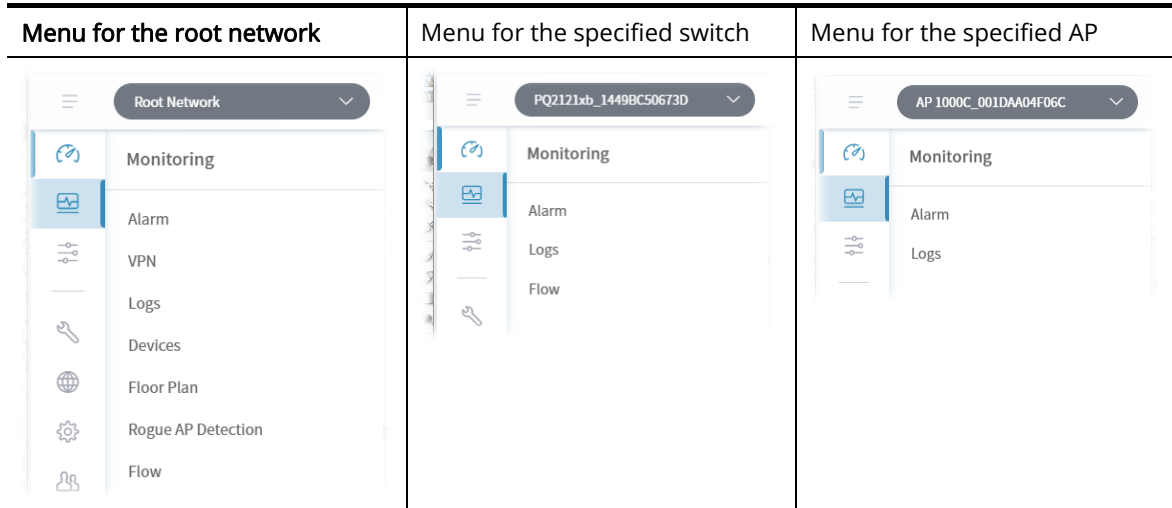
Dashboard shows the statistics of network overview, active clients and new devices.



8.2 Monitoring Menu

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

This section offers Monitoring menu items for the root network.



8.2.1 Alarm

Alarm message will be recorded on VigorConnect 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.

Monitoring / Alarm

search No. / Device Name / MAC Time Interval : 2023/02/06 to 2023/03/08

Alarm 7 History

Export All Delete Delete All 1 / 1

No.	Ack Status	Time	Device Name	MAC Address	Alarm Level	Alarm Message	Alarm Type	
<input type="checkbox"/>	17	Not Ack	2023-03-07 16:36:37	G1280_001DAA0D07F0	001DAA0D07F0	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	16	Not Ack	2023-03-03 13:59:12	Q2121x_1449BC506AA4	1449BC506AA4	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	15	Not Ack	2023-02-23 13:53:17	AP 1000C_001DAA04F06C	001DAA04F06C	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	14	Not Ack	2023-02-23 13:48:47	G2280x_001DAA43C7BA	001DAA43C7BA	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	13	Not Ack	2023-02-17 17:26:22	AP 903_00507FF19216	00507FF19216	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	12	Not Ack	2023-02-17 17:21:52	PQ2121xb_1449BC50673D	1449BC50673D	△ Critical	Device Loss Connection	Device Loss Connection
<input type="checkbox"/>	11	Not Ack	2023-02-17 15:02:22	P2280_001DAA0CB609	001DAA0CB609	△ Critical	Device Loss Connection	Device Loss Connection

These parameters are explained as follows:

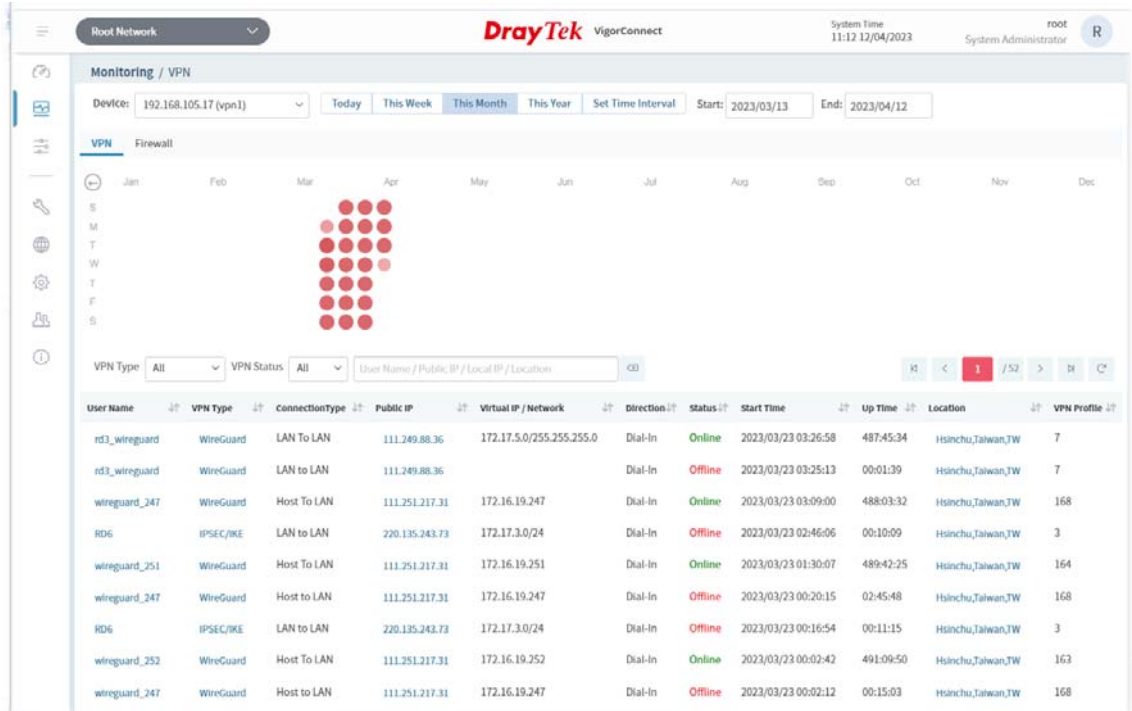
Item	Description
------	-------------

Alarm / History	Alarm – Display the alarm records recently. History – Display all the alarm records that have been solved and cleared.
Export All	Click this button to save alarm log as a XLS file.
Delete	Clear the alarm record which has been solved by VigorConnect.
Delete All	Clear all of the alarm records which have been solved by VigorConnect.
No.	Display the index number of the alarm. It is offered by VigorConnect 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 VigorConnect automatically.
Alarm Type	Displays the alarm message with the type specified.

8.2.2 VPN

8.2.2.1 VPN

This page displays various information (user name, VPN type, connection type, public IP, virtual IP/network, direction, status, start time, uptime, location, VPN profiles and etc.) by analyzing the VPN Log collected from the routers.



These parameters are explained as follows:

Item	Description
Device	Use the drop-down menu to select a device (router).
Today, This Week, This Month, This Year	Click each tab (different period) to display information about the selected device.
Set Time Interval	Click to set the time interval to display information about the selected device.
VPN Type	The default is All. Select the type to display information about the selected device.
VPN Status	The default is All. Select the status (all, offline, online) to display information about the selected device.

8.2.2.2 Firewall

This page displays the firewall information (time, action, username, direction, firewall rule, source IP, source port, destination IP, destination port, service, protocol, repeat and etc.) by analyzing the VPN Log collected from the routers.

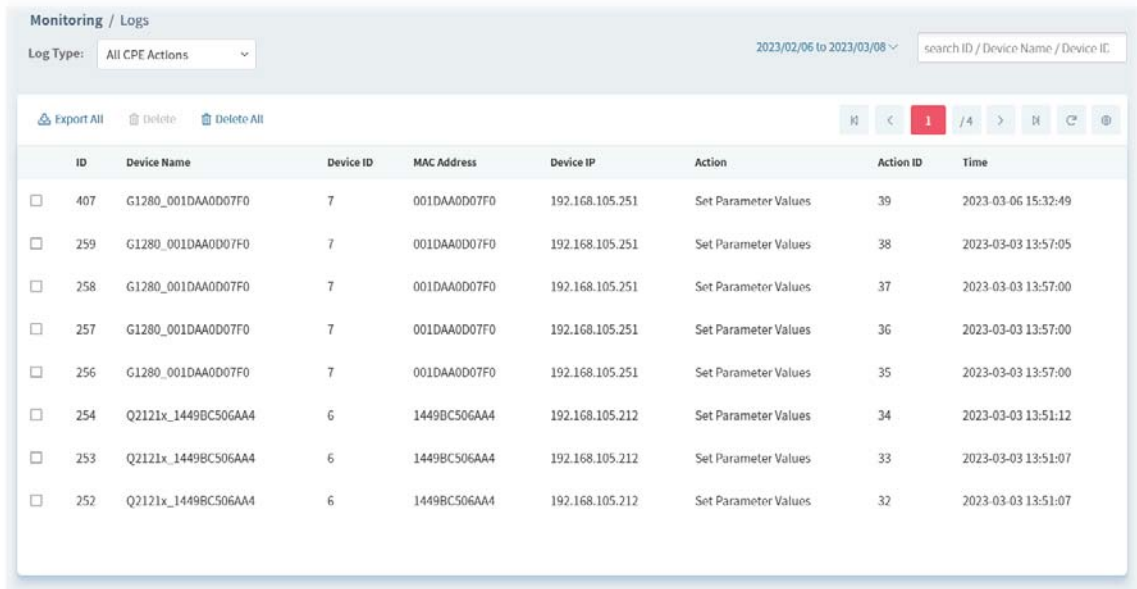
Time	Action	User Name	Direction	Firewall Rule	Source IP	Source Port	Dest IP	Dest Port	Service	Protocol	Repeat
2023/03/22 22:06:43	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	11015	172.16.2.8	995	email	TCP	1
2023/03/22 22:06:22	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	11004	172.16.2.8	995	email	TCP	1
2023/03/22 22:05:54	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10987	172.16.2.8	465		TCP	1
2023/03/22 22:05:36	Block	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-5	172.16.19.112	10980	172.16.0.1	80	HTTP	TCP	13
2023/03/22 18:51:39	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10714	172.16.2.8	995	email	TCP	1
2023/03/22 18:46:39	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10707	172.16.2.8	995	email	TCP	1
2023/03/22 18:41:38	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10690	172.16.2.8	995	email	TCP	1
2023/03/22 18:36:38	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10674	172.16.2.8	995	email	TCP	1
2023/03/22 18:31:40	Pass	dlin1	LAN/RT/VPN->LAN/RT/VPN	2-8	172.16.19.112	10667	172.16.2.8	995	email	TCP	1

These parameters are explained as follows:

Item	Description
Device	Use the drop-down menu to select a device (AP or switch).
Today, This Week, This Month, This Year	Click each tab (different period) to display information about the selected device.
Set Time Interval	Click to set the time interval to display information about the selected device.
Action	The default is All. Select the action (all, pass, block) to display information about the selected device.

8.2.3 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.



These parameters are explained as follows:

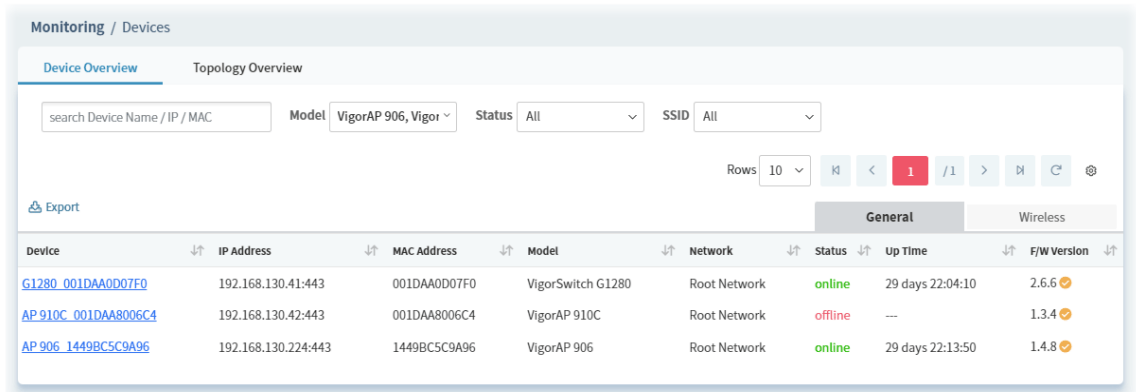
Item	Description
Log Type	Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Set Parameter, File Transfer, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page.
<input type="text" value="search ID / Device Name / Device ID"/>	Enter the condition for VigorConnect to search and display relational information.
Export	Click this button to save the log as an XLS file.
Delete	Clear the alarm record which has been solved by VigorACS.
Delete All	Clear all of the alarm records which have been solved by VigorACS.

8.2.4 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.

8.2.4.1 Device Overview



These parameters are explained as follows:

Item	Description
<input type="text" value="Search Device Name / IP / MAC"/>	Enter the condition for VigorConnect to search and display relational information.
Model	This area lists all of the devices that monitored by VigorConnect.
Status	<p>Online – This page displays information for the device which is online currently.</p> <p>Offline – This page displays information for the device which is offline currently.</p> <p>All – This page displays information for all of the devices no matter it is online or offline.</p>
SSID	<p>This area lists information for CPE with wireless features monitored by VigorACS.</p> <p>Check All to display all of the devices; or check the name of the device to display the information related to the selected device.</p> <p>SSID - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.</p>
Export	Click this button to save information for monitored devices as an XLS file.

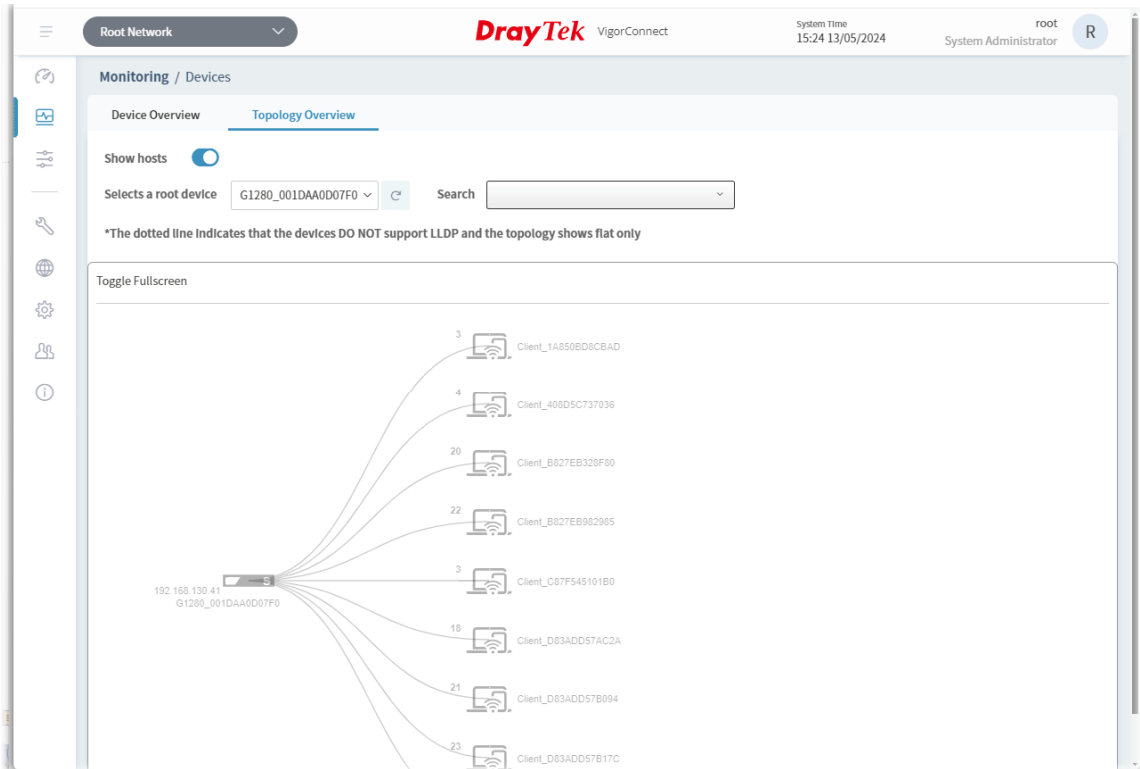
General / Wireless

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.

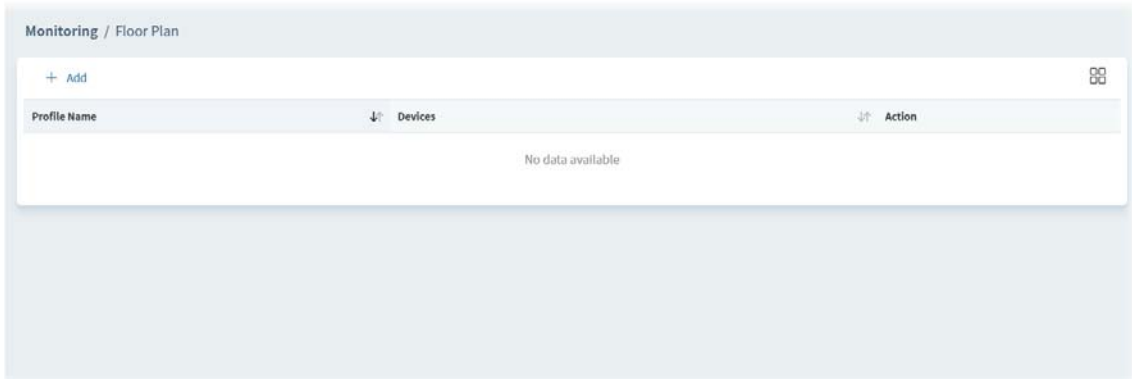
8.2.4.2 Topology Overview

This page shows the LLDP protocol information collected by VigorSwitch.



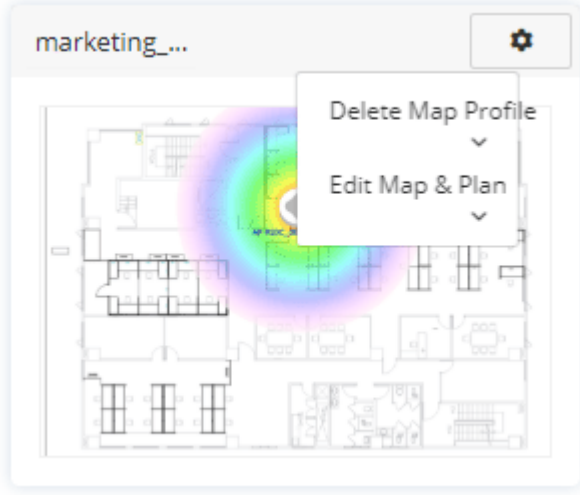


8.2.5 Floor Plan

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.



These parameters are explained as follows:

Item	Description
+Add	Creates a new profile.
	<p>Click to change to browse view. It displays all of the floor plan profiles with the map used.</p>  <p>You can click Add on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click Edit Map & Plan to perform the modification, or click Delete Map Profile to remove the selected floor plan profile.</p> 

Profile Name	Displays the name of the floor plan profile.
Devices	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., test6688) and click Browse to upload a map (e.g., AP_MAP.png). Click **Continue**.

Monitoring / Floor Plan

Profile Name: test6688 ✓

Upload Map: Floor_MAP.png

3. Click **Edit** to display the following figure.

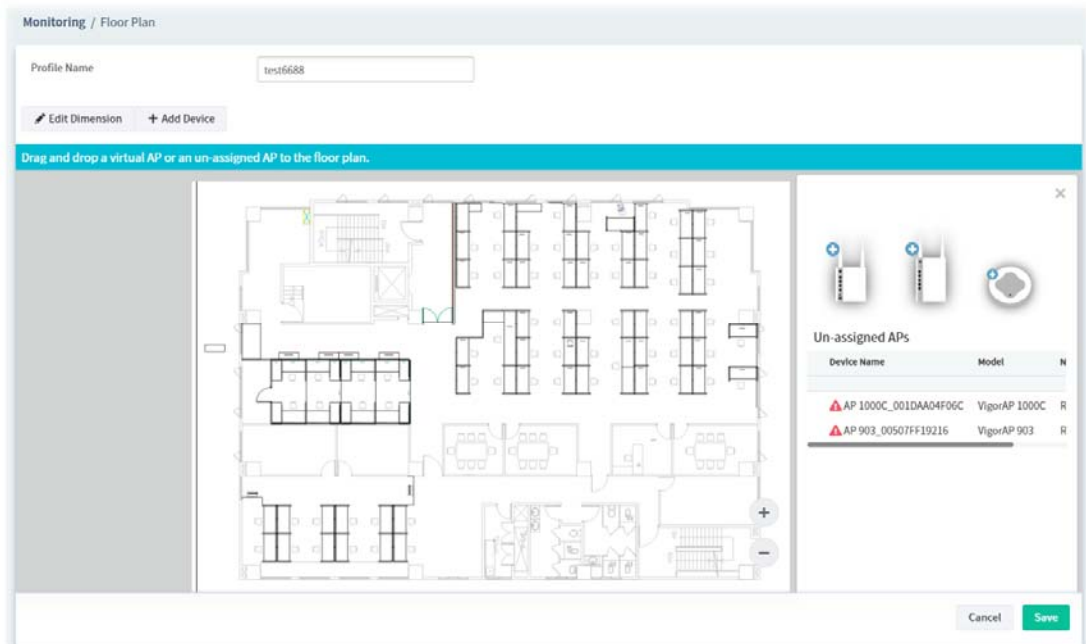
Monitoring / Floor Plan

Profile Name: test6688

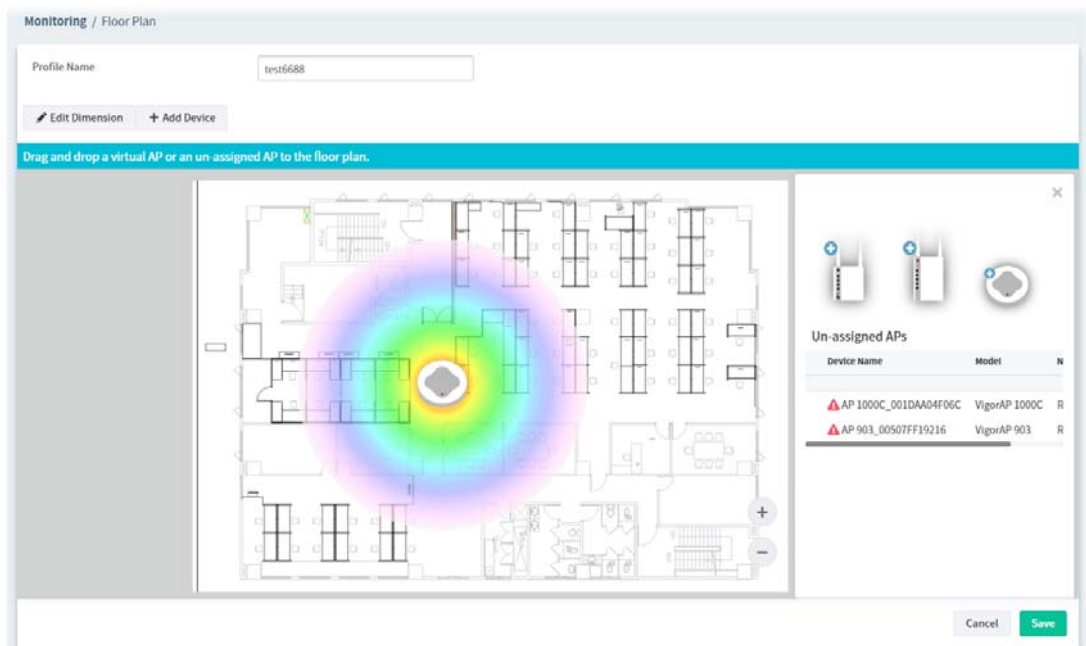
Edit Dimension – Draw a line and enter the distance of length / width of the map.

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

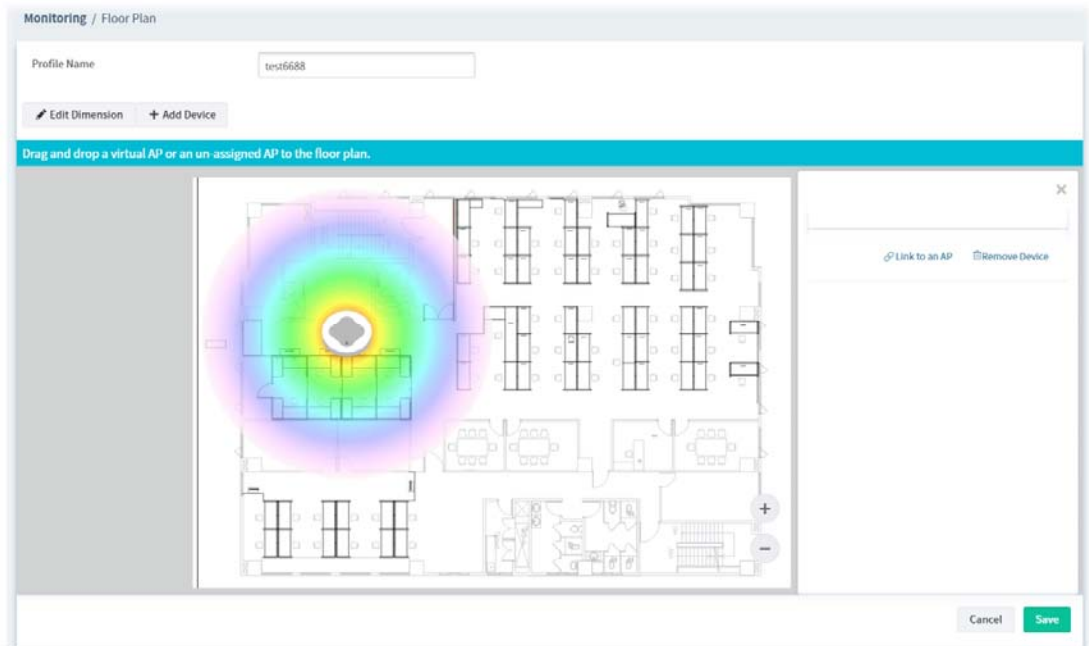
4. Click **+Add Device**. Available VigorAP icons and name list will be displayed on the right side of this page.



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.



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.

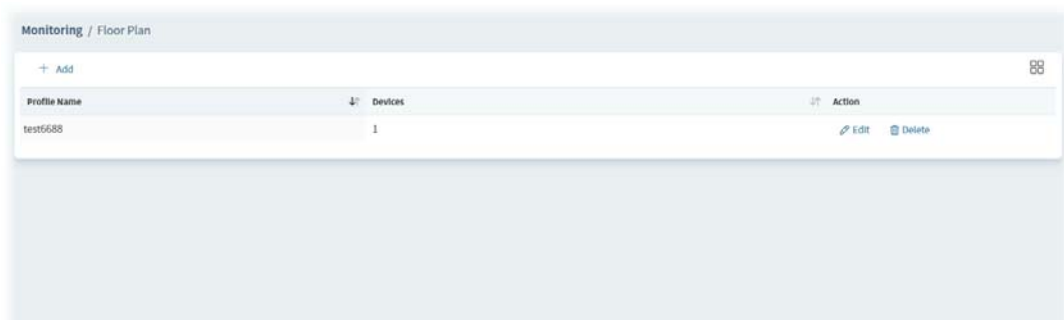


1. **Remove Device** – If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.
2. **Link to an AP** – If you satisfy the location of AP icon, click this link to select VigorAP. All of un-assigned AP names will be shown on the list. Choose the one you want and 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.



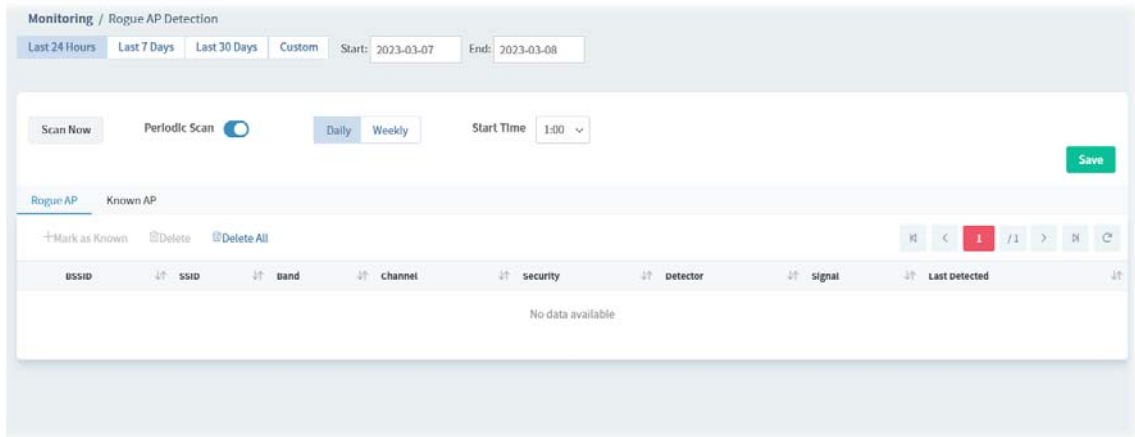
8. Click **Save**. The new created profile will be shown on the page.



8.2.6 Rogue AP Detection

Information detected by VigorAP can be displayed in this page. In which, the APs will be classified with rogue AP and known AP in different colors.

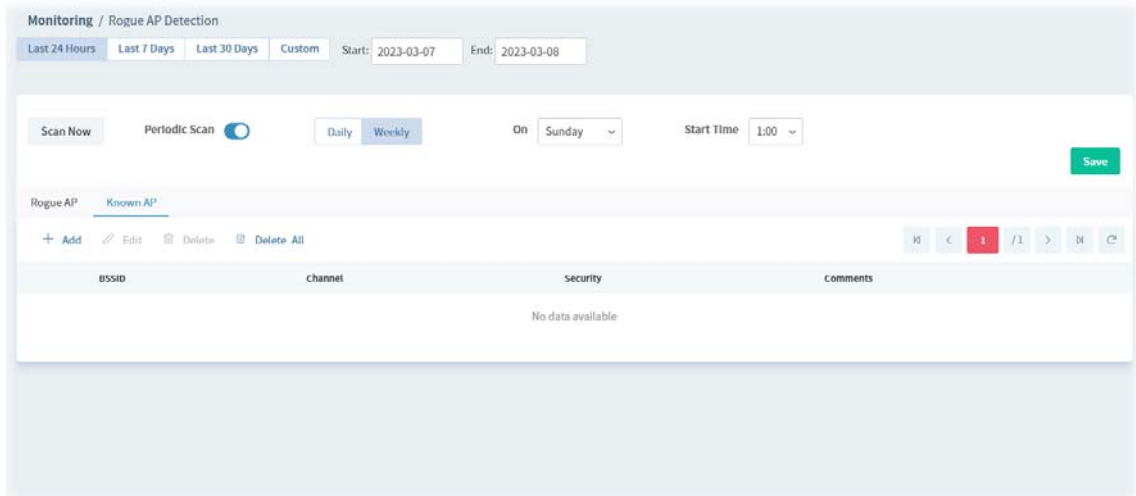
Click the **Rogue AP** tab to display the following page. All the APs detected will be treated as Rogue AP.



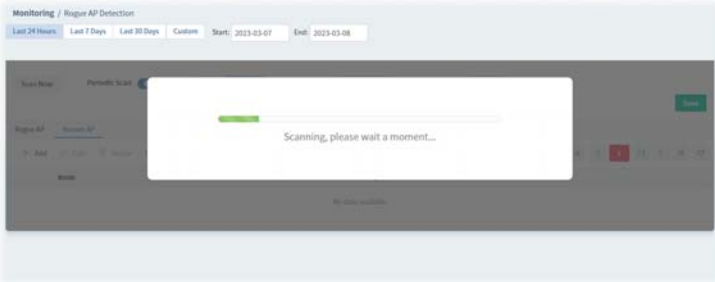
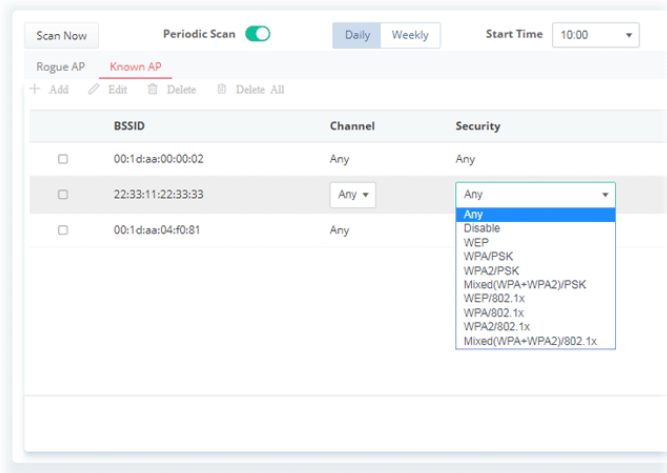
These parameters are explained as follows:

Item	Description
Last 24 Hours / Last 7 Days / Last 30 Days / Custom	Display the access point(s) detected within 24 hours, 7 days, 30 days or user defined days.
Scan Now	Perform device detection immediately.
Periodic Scan	<p>After enabling this feature, access points will be detected periodically based on the setting configured here.</p> <p>Daily – VigorConnect will detect access point on certain time every day.</p> <ul style="list-style-type: none"> ● Start Time – Specify a time point as starting time for device detection. <p>Weekly – VigorConnect will detect access point on certain time every week.</p> <ul style="list-style-type: none"> ● On – Choose the day to perform device detection. ● Start Time - Specify a time point as starting time for device detection.
+Mark as Known	Vigor access points can be detected and be shown in the table under Rogue AP. However, some of them might be known to you and should not be listed here. To solve this problem, simply click the access point and then click Mark as Known . The selected access point will be transferred and listed under Known AP.
Delete	Remove the selected access point from the list.
Delete All	Remove all of the access points from the list.

Click **Known AP** to display the following page. All the access points listed under this page will be treated as friendly AP.



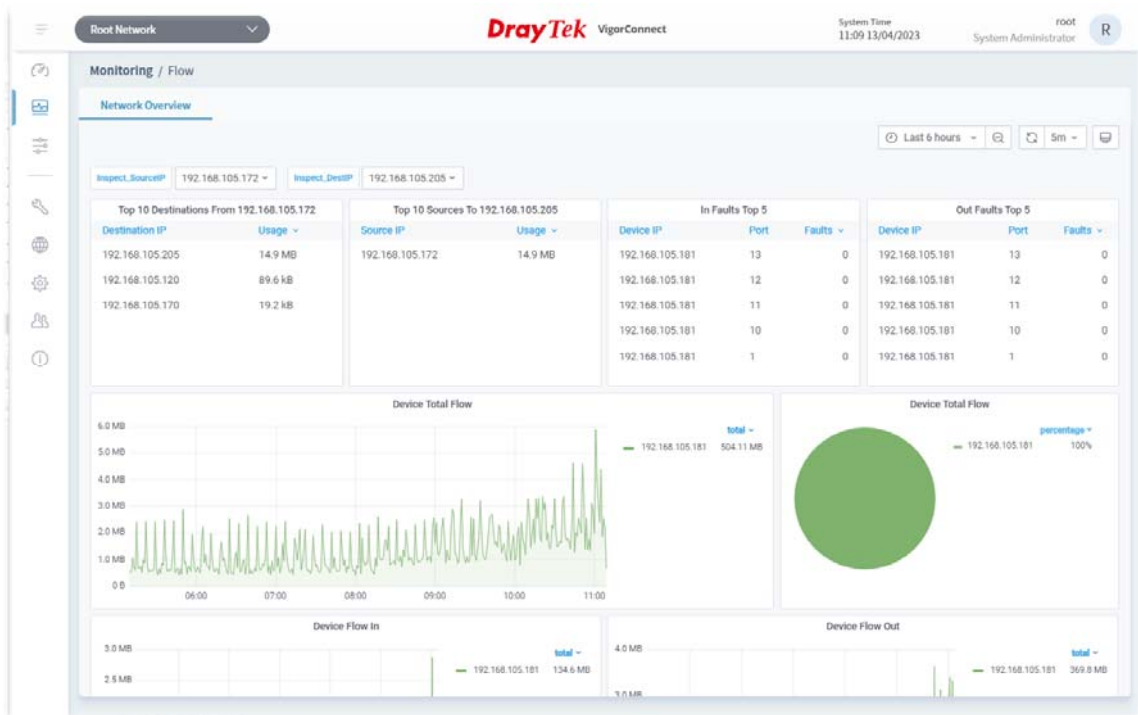
These parameters are explained as follows:

Item	Description
Scan Now	Perform device detection immediately. 
Add	Click to create a new entry for entering information for access point.
Edit	Change the settings for a selected access point. Select one of the access points. The Edit link will be available for clicking, then. After clicking it, channel, security and comments will be allowed to be modified with different values. 
Delete	Remove the selected access point from the list.

Delete All	Remove all of the access points from the list.
BSSID	Display the MAC address of the detected access point.
Channel	Display the channel used by the access point. Check the box of the selected access point and click Edit .
Security	Display the security mode used by the access point. It can be changed.
Comments	Display a brief explanation for the access point. It can be changed.
Save	Save the settings.

8.2.7 Flow

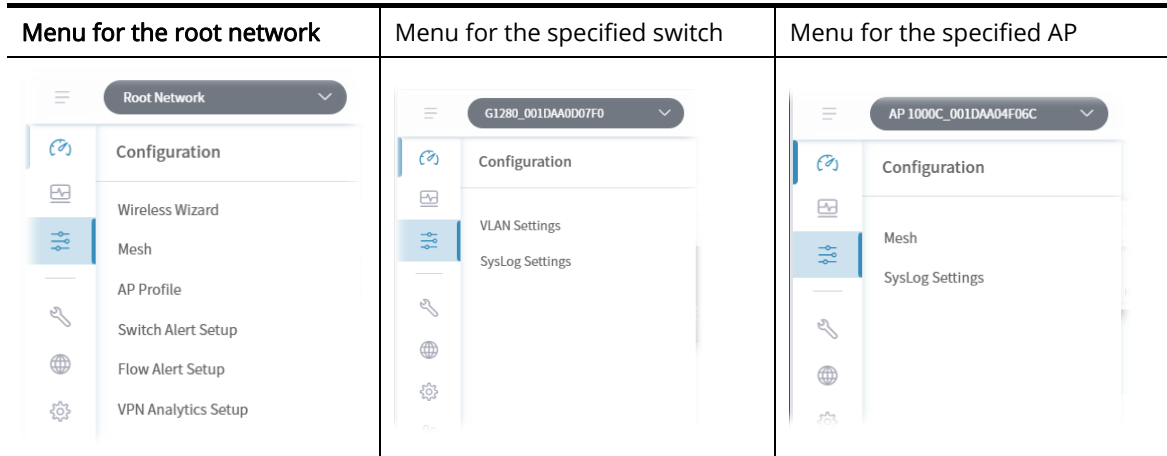
This page can display the network usage of the top 10 devices based on different conditions (Top 10 Destination From, Top 10 Sources To, In Faults Top 5, Out Faults Top 5, Device Total Flow, Device Flow In, Device Flow Out, Flow Top 10 Ports, Destination Flow Top 10, Source Flow Top 10 and Protocol Flow Top 10).



8.3 Configuration Menu

Configuration menu will vary for root network, user-defined network and specified CPE (AP/switch).

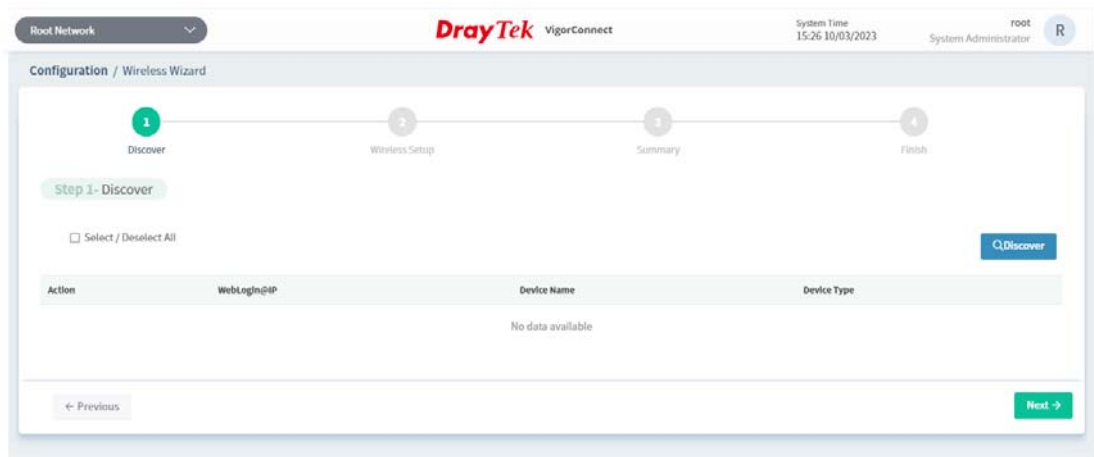
This section offers Configuration menu items for the root network.



8.3.1 Wireless Wizard

The wireless wizard offers a quick method to configure WLAN settings for a specified access point.

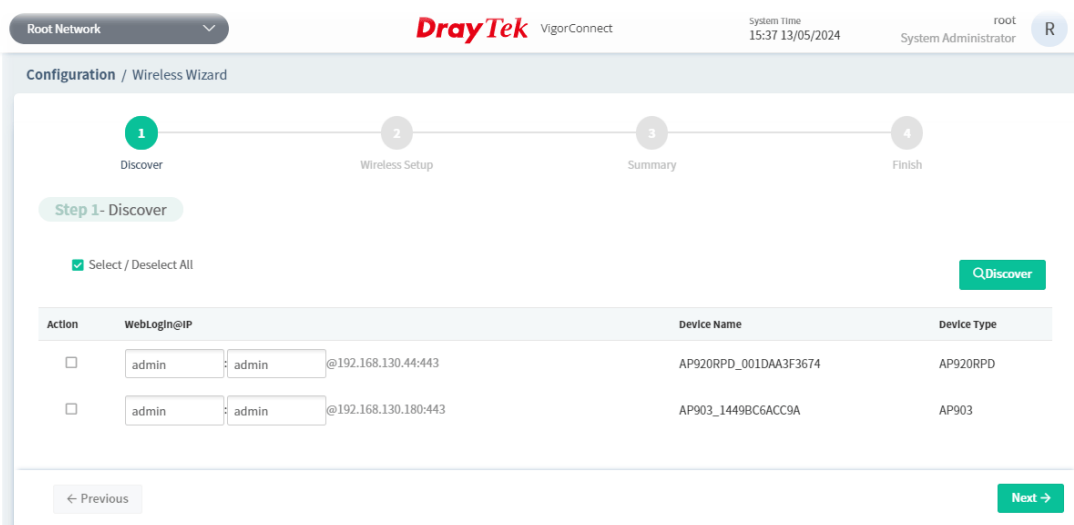
1. Open **Configuration>>Wireless Wizard**.



These parameters are explained as follows:

Item	Description
Discover	Click to search all the available devices.
Select/Deselect All	Check the box to select or deselect all the devices listed below the table.
Next	Click to access into next page.

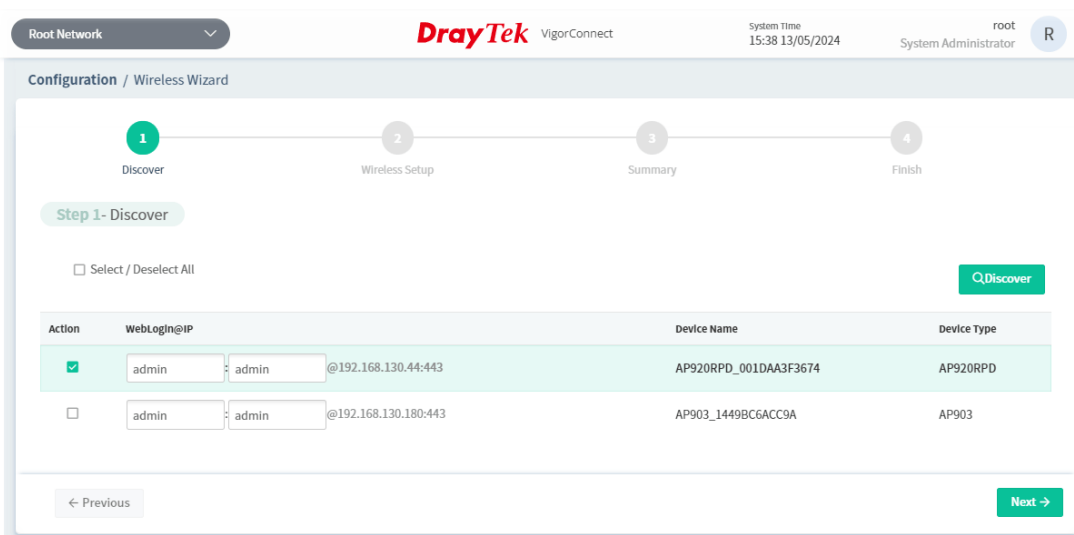
- Click **Discover**. Later available access points will be shown as the following page.



These parameters are explained as follows:

Item	Description
Action	Check the box to select the entry.
WebLogin@IP	Displays the username and password for the selected entry.
Device Name	Displays the name of the device.
Device Type	Displays the model type of device.
Next	Click to access into next page.

- Select the one(s) for wireless setup.



These parameters are explained as follows:

Item	Description
Next	Click to access into next page.

- Click **Next** to get the following configuration page.

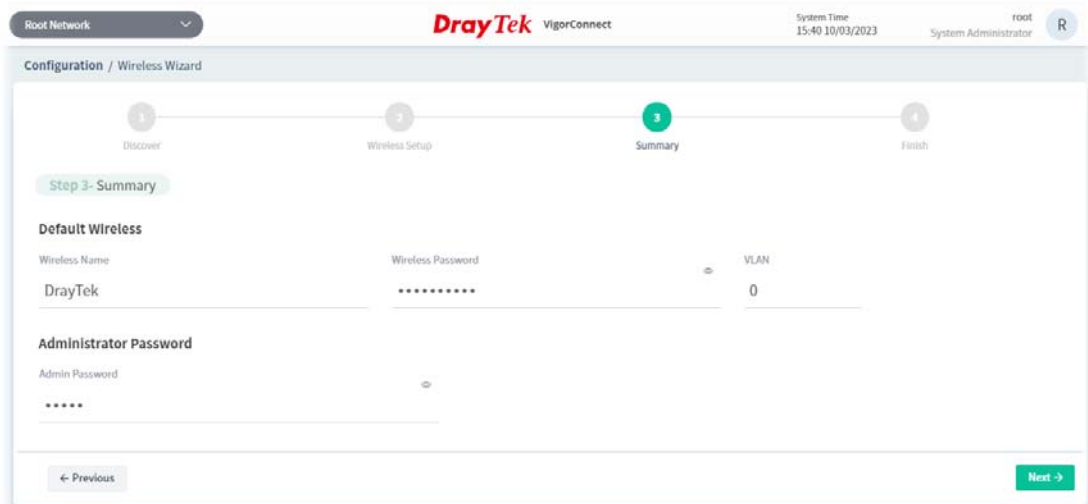
The screenshot shows the 'Wireless Wizard' configuration page in the DrayTek VigorConnect interface. It is currently on 'Step 2 - Wireless Setup'. The page is divided into sections for 'Default Wireless' and 'Administrator Password'. Under 'Default Wireless', there are input fields for 'Wireless Name' (pre-filled with 'DrayTek'), 'Wireless Password' (masked with asterisks), and 'VLAN' (pre-filled with '0'). Under 'Administrator Password', there are fields for 'Admin Password' and 'Confirm Password', both masked with asterisks. A '2nd Wireless' section is also present, featuring an 'Enable 2nd Wireless' toggle switch which is currently turned off. At the bottom of the page, there are 'Previous' and 'Next' navigation buttons.

These parameters are explained as follows:

Item	Description
Default Wireless	
Wireless Name	The system will display the default wireless name (e.g., DrayTek).
Wireless Password	The system will display the default wireless password (e.g., DrayTek123).
VLAN	Displays the default value (e.g., 0).
Administrator Password	
Admin Password	Displays the default value (e.g., admin). Change the value if required.
Confirm Password	Displays the default value (e.g., admin). Change the value if required.
2nd Wireless	
Enable 2nd Wireless	Click to enable the second wireless network connection.
2nd Wireless Name	Enter a string as the second wireless name.
2nd Wireless Password	Enter a string as the second wireless password.
2nd Wireless VLAN	Enter a value as the VLAN ID for the second wireless network connection.
2nd Bandwidth Limit	It is available when 2nd Wireless is enabled.
Enable 2nd Bandwidth Limit	Click to enable this feature. 2nd Upload Limit (bps) - Enter a value as the threshold for the upload limit. 2nd Download Limit (bps) - Enter a value as the threshold for the download limit.

2nd Station Control	It is available when 2nd Wireless is enabled.
Enable 2nd Station Control	Click to enable this feature. Then define the period for network connection and reconnection. <ul style="list-style-type: none"> ● 2nd Connect Time - ● 2nd Reconnect Time -
Previous	Click to return to the previous page.
Next	Click to access into next page.

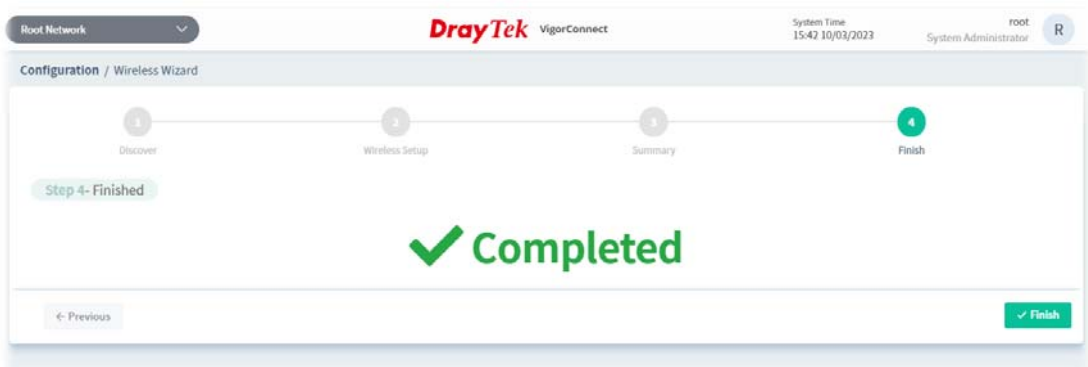
- After configuring the above settings, click **Next** to view the summary.



These parameters are explained as follows:

Item	Description
Previous	Click to return to the previous page.
Next	Click to access into next page.

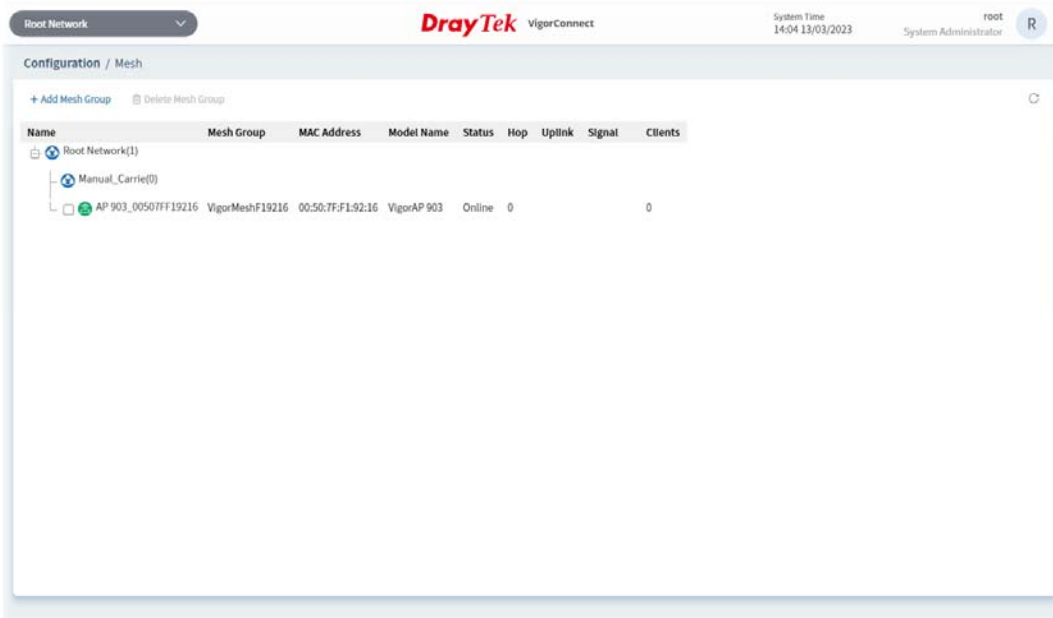
- If the summary is OK, click **Next**. Wait for the system to process the wireless settings. When the following page appear, click **Finish**.



8.3.2 Mesh

The mesh configuration is available for Vigor access point only.

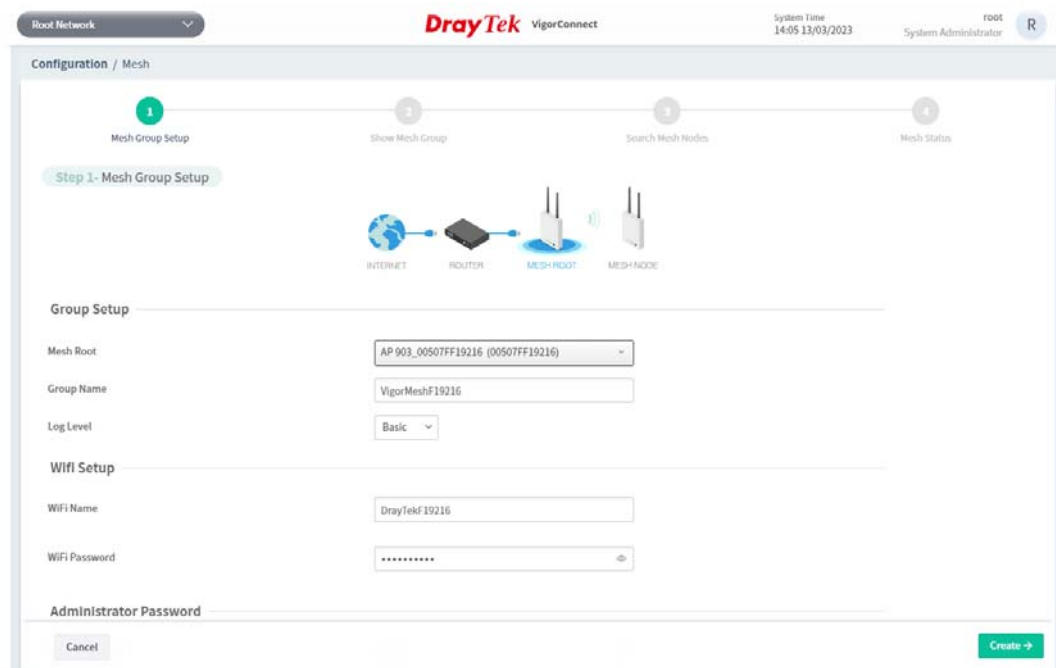
1. Click **+Add Mesh Group**.



These parameters are explained as follows:

Item	Description
+Add Mesh Group	Create a new mesh group.
Delete Mesh Group	Remove the selected mesh group.

2. The page of Step 1 will be shown as follows:

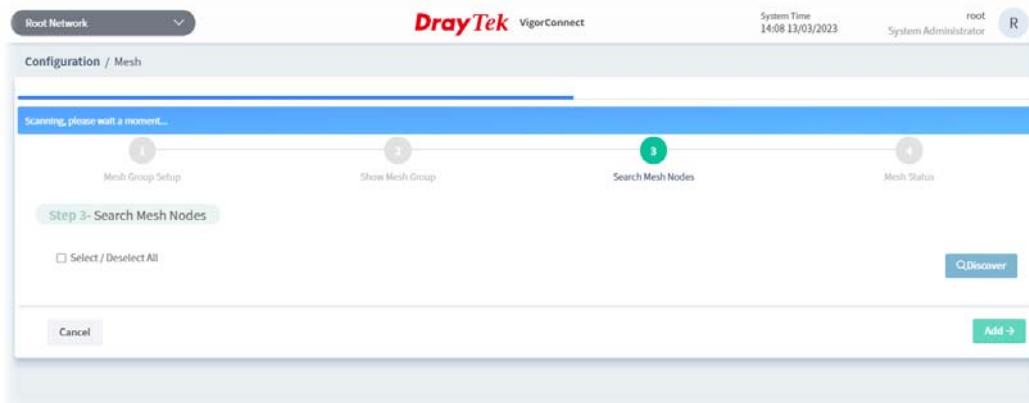


These parameters are explained as follows:

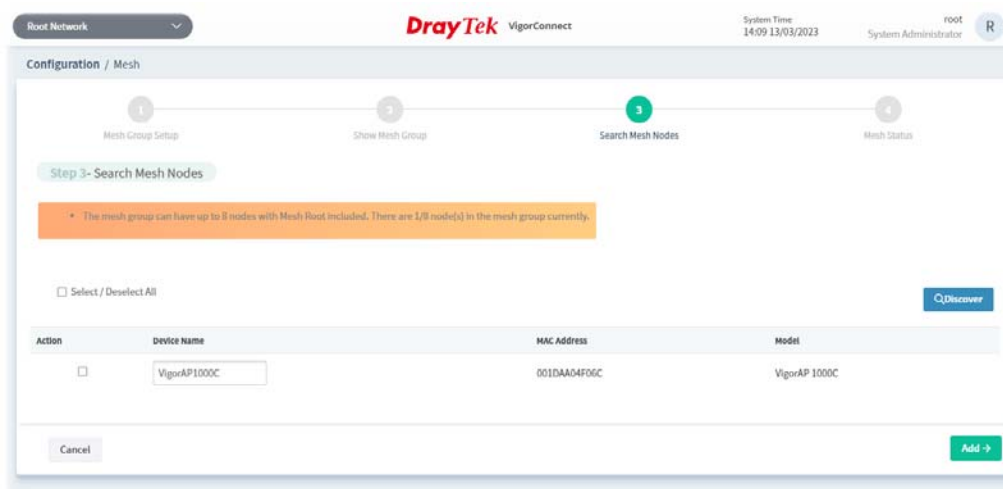
Item	Description
Group Setup	
Mesh Root	Use the drop down menu to select one of the device as the mesh root.
Group Name	Enter a name as the new mesh group.
Log Level	Choose Basic or Detailed . If Detailed is selected, more detailed operation information will be recorded on System Log .
Wifi Setup	
WiFi Name	Displays the wifi name defined for the mesh root.
WiFi Password	Displays the wifi password defined for the mesh root.
Administrator Password	
Admin Password	Displays the administrator password defined for the mesh root.
Confirm Password	Enter the password for confirmation.
Cancel	Click to exit the configuration page without saving the settings.
Create	Click to open next page.

- After finishing settings on Step 1, clicking **Create** to get the following page. View and check the settings in this page.

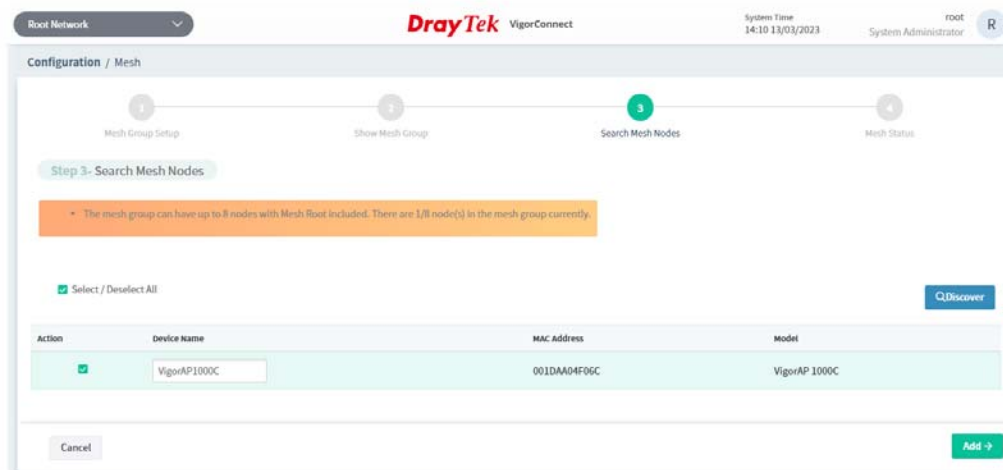
- If there is nothing to be changed, click **Next** to access the following page. Then VigorConnect will start to search mesh nodes automatically.



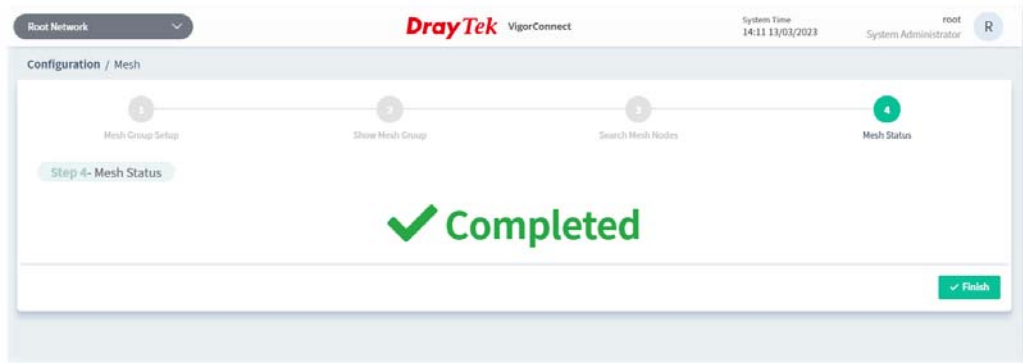
5. After finishing searching mesh nodes, available APs will be shown on the screen.



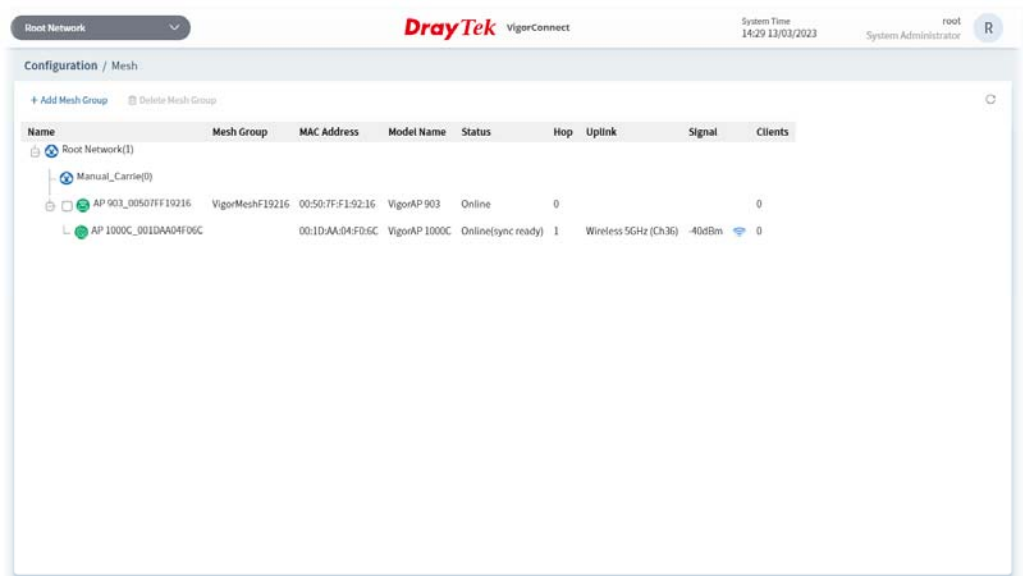
6. Select the access point which will be grouped under the mesh root. Then click **Add**.



7. Wait until the following page appears.



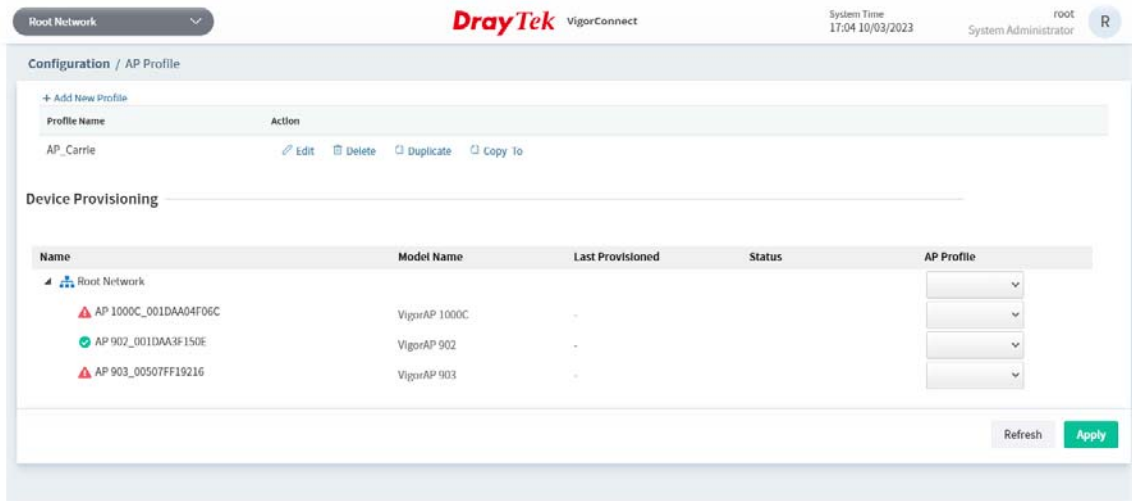
8. Click **Finish**. The mesh root and the mesh node grouped under the mesh root will be shown as follows.



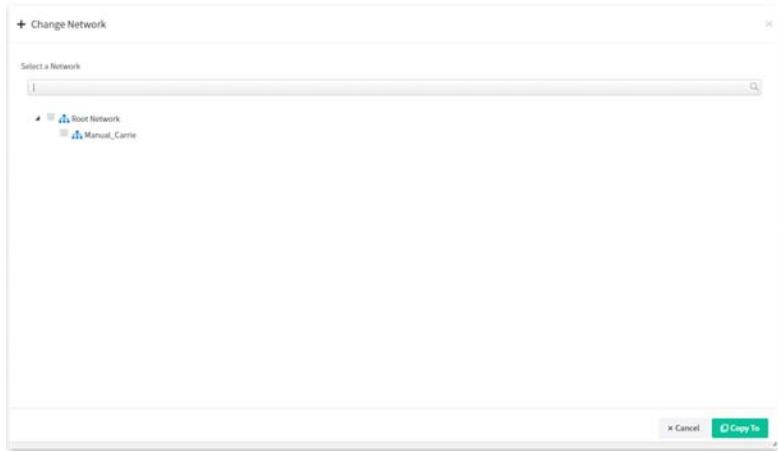
8.3.3 AP Profile

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 VigorConnect 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 VigorConnect. 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.



These parameters are explained as follows:

Item	Description
+Add New Profile	Create a new AP profile with basic settings.
Profile Name	Displays the name of AP profile.
Action	<p>Edit - Configure detailed settings for the selected AP profile.</p> <p>Delete - Delete the selected AP profile.</p> <p>Duplicate - Click to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).</p> <p>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).</p> 
Device Provisioning	Locate the access points for applying suitable AP profile.

	<p>Name – Display a tree view for model managed by VigorConnect.</p> <p>Model Name – Display the name of the model.</p> <p>Last Provisioned – Display the time that AP profile was applied to the selected device.</p> <p>Status – Display the status (updating, complete and “-”) of the AP.</p> <p>AP Profile – Choose an AP profile for applying to the selected AP. In which, “As Parent” means to apply the profile listed on the top to the selected AP.</p>
Refresh	Click to refresh current page.
Apply	Click to save the changes in this page.

8.3.3.1 Add an AP Profile

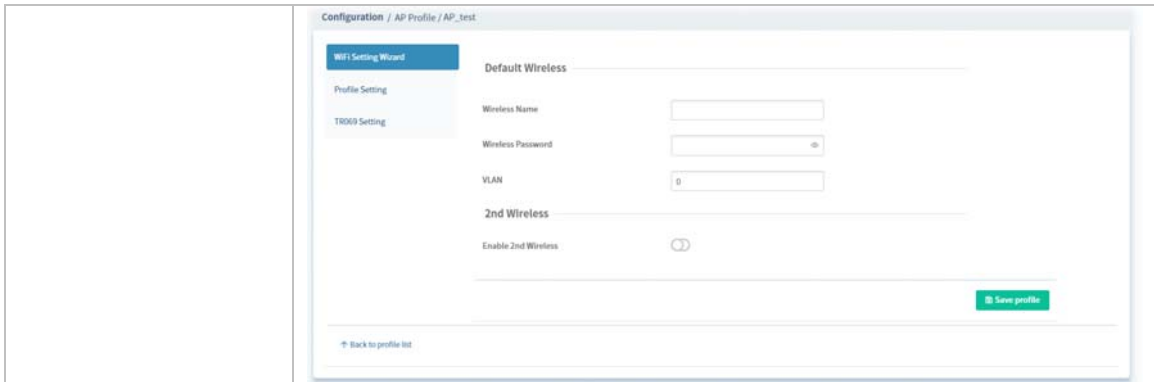
Click **+Add New Profile** to create a new AP profile.

Create a profile (named AP_Usage) with Quick setting mode.

Create a profile (named AP_Carrie) with Advanced setting mode.

These parameters are explained as follows:

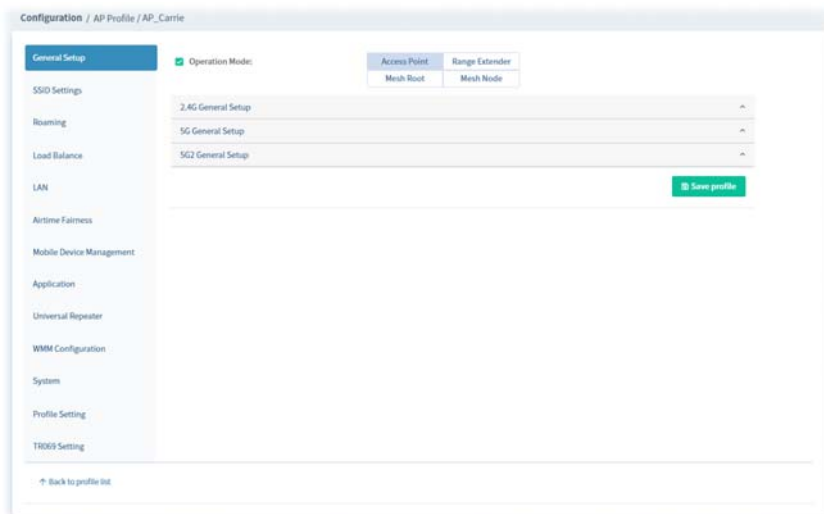
Item	Description
Profile Name	Enter a name of the profile.
AP Login Username	Enter a username for login the access point.
AP Login Password	Enter a password for login the access point.
Setting Mode	Quick - Only basic settings allowed for the AP profile. Below shows the AP profile with Quick setting mode.



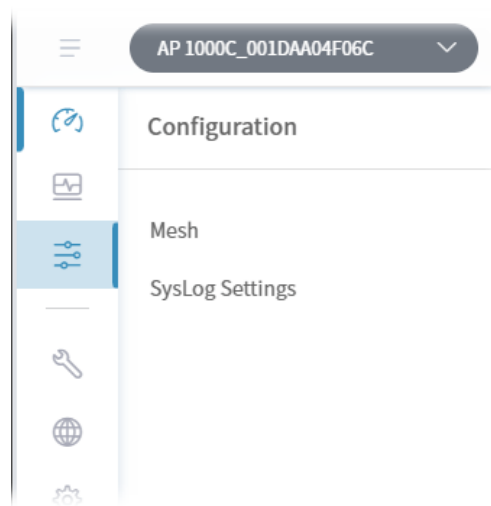
Advanced - All settings for the AP profile.

- **Select All** - Click to enable/disable the selection.

Below shows the AP profile with Advanced setting mode.



Once Mesh Root/Mesh Node is selected as the Operation Mode, the Mesh menu item will then appear on Configuration for the access point (if the devices support mesh function) for required configuration.

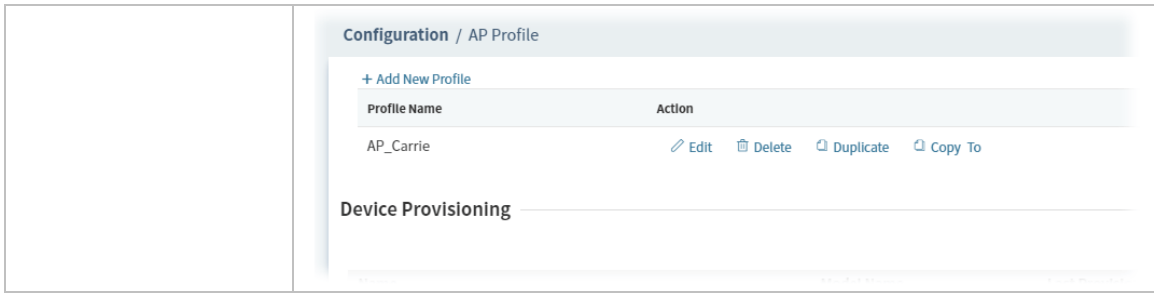


Back to profile list

Return to previous page, AP profile list.

Save

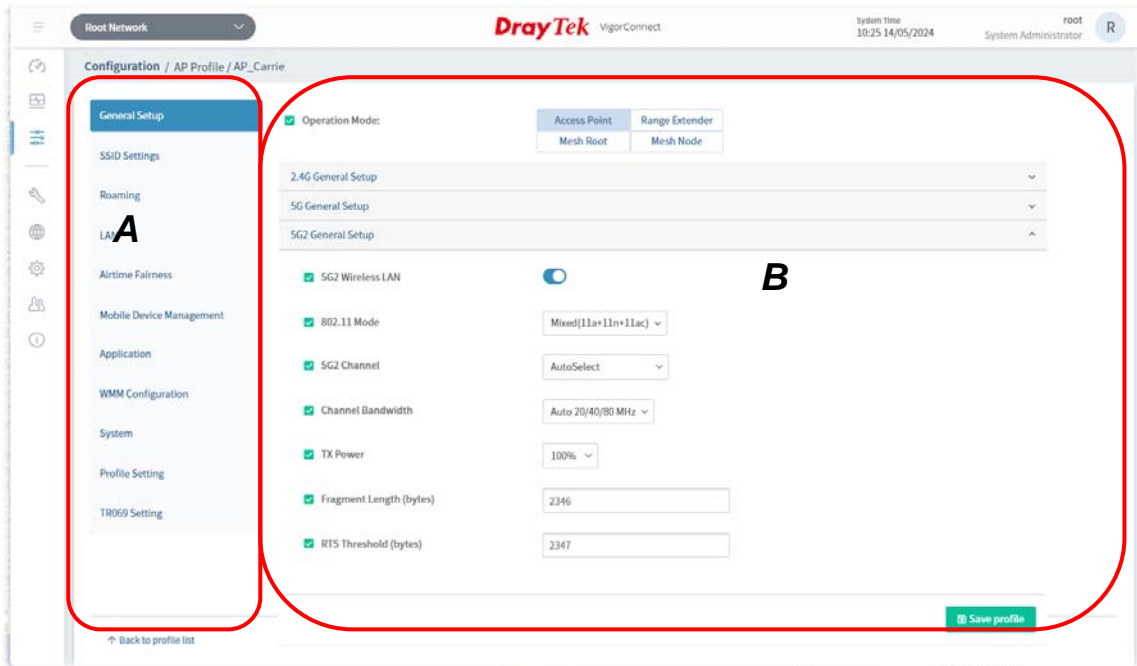
Save the settings and display the new profile on the AP profile list.



8.3.2.2 Edit an AP Profile


To configure detailed settings for each AP profile, click the **Edit** button for the selected profile.

Below shows the AP profile with Advanced setting mode.



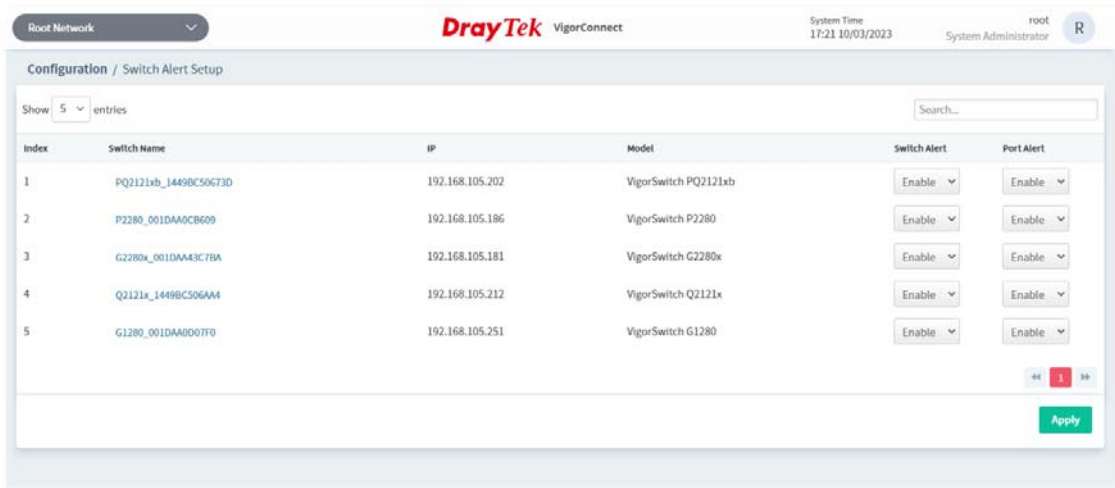
These parameters are explained as follows:

Item	Description
Area A - Menu Item	At present, the available menu items contain, <ul style="list-style-type: none"> ● General Setup ● SSID Settings ● Roaming ● LAN ● Airtime Fairness ● Mobile Device Management ● Application ● Universal Repeater ● WMM Configuration ● System ● Profile Setting ● TR069 Setting
Area B - Settings	This area will vary according to the item selected in Area A - Menu Item.
Save Profile	Click to save the settings.

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

8.3.4 Switch Alert Setup

VigorConnect will collect the SNMP trap coming from the VigorSwitch. If an alert event happens on VigorSwitch, the corresponding information will be sent to VigorConnect to send the alert messages.

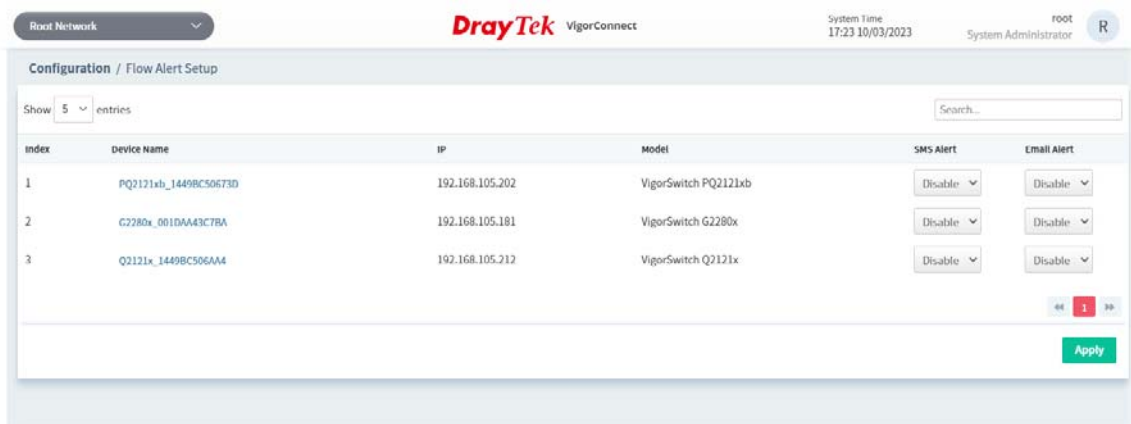


These parameters are explained as follows:

Item	Description
Switch Alert	Enable / Disable - Use the drop-down menu to enable or disable the function of sending an alert message to the recipient.
Port Alert	Enable / Disable - Use the drop-down menu to enable or disable the function of sending an alert message about port settings to the recipient.
Apply	Apply the settings configured above to each switch.

8.3.5 Flow Alert Setup

This page is to set different thresholds and flow values for each device. When an abnormality occurs, VigorConnect can quickly detect it and send an alert mail/SMS to the recipient (user/administrator) according to the sFlow analysis.



These parameters are explained as follows:

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

Device Name	Displays the device name of the VigorSwitch.
IP	Displays the IP address of the VigorSwitch.
Model	Displays the model name of the VigorSwitch.
SMS Alert	Disable - Select to disable the function of SMS alert. Enable - Select to enable the function of SMS alert.
Email Alert	Disable - Select to disable the function of e-mail alert. Enable - Select to enable the function of e-mail alert.
Apply	Apply the settings configured above to each switch.

To configure detailed settings of flow alerts for individual devices, click the name link under Device Name to open the setting page

These parameters are explained as follows:

Item	Description
User(s)	Select the user name(s) to which VigorConnect sends the alert.
Device Flow	Enable - Switch the toggle to enable/disable device flow control. Set the threshold for VigorConnect to collect the sFlow data. Frequency - The default is 30 minutes. Volume - The default is 1GB. The unit is GB/MB.
Port Flow	Port Flow attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Flow detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the threshold rate (volume set below). Enable - Switch the toggle to enable/disable port flow detection. Set the threshold for VigorConnect to collect the sFlow data. Frequency - The default is 30 minutes. Port(s) - Select the LAN port number. Volume - The default is 1GB. The unit is GB/MB.

Inspect Source Flow	<p>Enable - Switch the toggle to enable/disable the function of inspecting the source flow. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Volume - The default is 1GB. The unit is GB/MB.</p>
Inspect Destination Flow	<p>Enable - Switch the toggle to enable/disable the function of inspecting the destination flow. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Volume - The default is 1GB. The unit is GB/MB.</p>
Device Faults	<p>Enable - Switch the toggle to enable/disable the function of detecting the device faults. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
SYN Flood	<p>When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard SYN packets for a period of time as defined in Frequency. This is to prevent SYN packets from exhausting router resources.</p> <p>Enable - Switch the toggle to enable/disable SYN flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
ICMP Flood	<p>When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard ICMP packets for a period of time as defined in Frequency.</p> <p>Enable - Switch the toggle to enable/disable ICMP flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
TCP Flood	<p>When the arrival rate of TCP packets exceeds the Threshold value, the router will start to randomly discard TCP packets for a period of time as defined in Frequency.</p> <p>Enable - Switch the toggle to enable/disable TCP flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
UDP Flood	<p>When the arrival rate of UDP packets exceeds the Threshold value, the router will start to randomly discard UDP packets for a period of time as defined in Frequency.</p> <p>Enable - Switch the toggle to enable/disable UDP flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
Land Flood	<p>LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses set to that of the target system, which causes the target to reply to itself continuously.</p>

	<p>Enable - Switch the toggle to block/unblock LAND attacks. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
Tiny Fragment	<p>Enable - Switch the toggle to block/unblock the tiny fragment detection. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
Push ACK Flood	<p>Enable - Switch the toggle to enable/disable the push ACK flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
RST Flood	<p>Enable - Switch the toggle to enable/disable the RST flood defense. Set the threshold for VigorConnect to collect the sFlow data.</p> <p>Frequency - The default is 30 minutes.</p> <p>Threshold - The default is 100.</p>
Apply	Apply the settings configured above to each switch.

8.3.6 VPN Analytics Setup

VPN Analytics provides statistics and notifications for VPN connections by receiving and analyzing the Syslog from the CPE device. It is suggested to keep the VPN syslog only and delete the syslog for other functions to minimize storage usage.

8.3.6.1 General

This page is used for configuring the general settings for VPN analytics information.

The screenshot shows the 'VPN Analytics Setup' configuration page in the DrayTek VigorConnect web interface. The page is titled 'Configuration / VPN Analytics Setup' and has tabs for 'General', 'User Notification List', 'Service Name', and 'Email&SMS Format'. The 'General' tab is active.

Settings visible on the page include:

- Enable Analytics Setup:** A toggle switch currently turned off.
- Keep VPN Syslog Only:** A toggle switch currently turned on.
- Log Retention Days:** A text input field containing the value '90'.
- Notification Default Settings:**
 - Email Notification:** A toggle switch currently turned on.
 - SMS Notification:** A toggle switch currently turned off.
 - Notification Incident:** A dropdown menu currently set to 'Location Change'.

There are two informational boxes (blue background with white text) providing additional context:

- About VPN Analytics:** States that VPN Analytics provides statistics and notifications for VPN connections by receiving and analyzing syslog from the Router. It suggests keeping VPN syslog only and deleting other syslog to minimize storage usage.
- About Notification Incident:** Explains that the Notification Incident is 'per user' based and is the default setting for new users. It lists two options:
 - Location Change:** Send notification for the first connection of the day, and only send notification for following connection if the source location is different from the last connection. Please note, location is a wider scale than IP. A user may change IP but still falling in the same location.
 - IP Change:** Send notification for the first connection of the day, and only send notification for following connection if the source IP is different from the last connection.

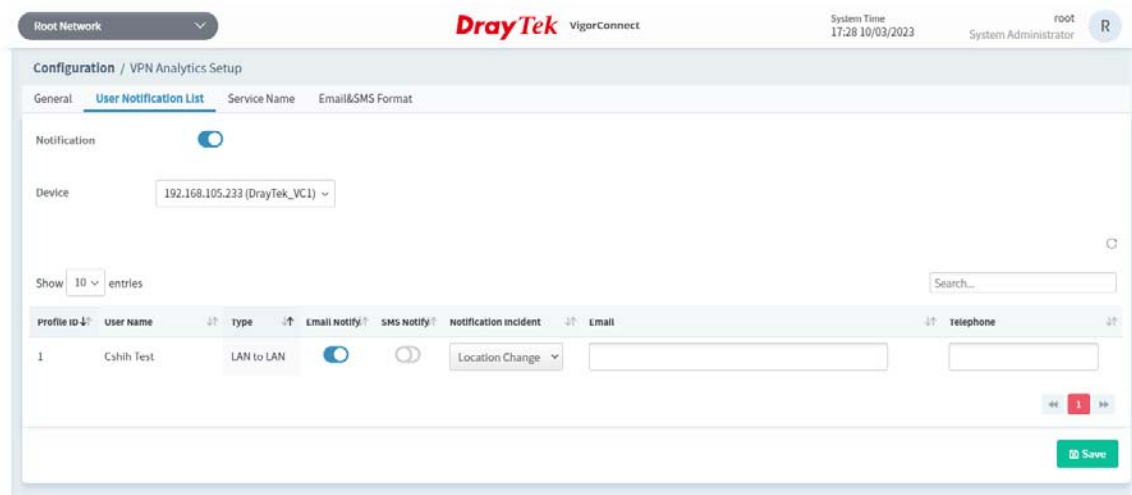
A 'Save' button is located at the bottom right of the configuration area.

These parameters are explained as follows:

Item	Description
Enable Analytics Setup	Click to enable/disable this VPN analytics setup page.
Keep VPN Syslog Only	Click to enable/disable the function of keeping VPN syslog only. If enabled, storage usage will be minimized as possible.
Log Retention Days	Set the days for the system to keep the log.
Notification Default Settings	
Email Notification	Click to enable/disable the function of sending a notification to the recipient by email.
SMS Notification	Click to enable/disable the function of sending a notification to the recipient by SMS.
Notification Incident	<p>Location Change - Send notification for the first connection of the day, and only send notification for the following connection if the source location is different from the last connection. Please note, location is a wider scale than IP. A user may change IP but still fall in the same location.</p> <p>IP Change - Send notification for the first connection of the day, and only send notification for the following connection if the source IP is different from the last connection.</p> <p>Always - Always send notifications when there's a VPN connection.</p> <p>Disable - Do not send notifications for VPN connections.</p> <p>This is the default setting that will be applied to new users. Each existing user setting can be customized in the User Notification List tab.</p>
Apply	Apply the settings configured above to each switch.

8.3.6.2 User Notification List

This page allows the system administrator to set the appropriate notification mechanism based on different VPN profiles.



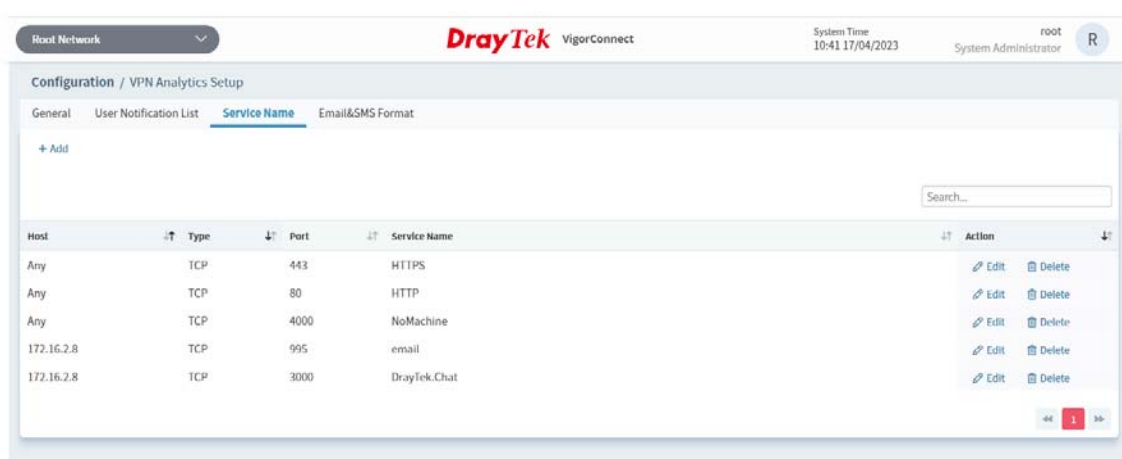
These parameters are explained as follows:

Item	Description
Notification	Click to enable/disable this notification setup page.
Device	Select a device. The VPN profiles configured for that device will be shown below.
User Name	Displays the name of the VPN profile.

Type	Displays the VPN type (e.g., LAN to LAN, Remote Dial-In).
Email Notify	Switch the toggle to enable/disable the function of email notify.
SMS Notify	Switch the toggle to enable/disable the function of SMS notify.
Notification Incident	Choose one of the notification incidents as the triggered event. When an incident occurs, a notification SMS/email will be sent out based on the address and telephone entered in this page.
Email	Enter the email address defined for the VPN profile.
Telephone	Enter the phone number defined for the VPN profile.
Save	Save the settings.

8.3.6.3 Service Name

The service name profile created here will be selected or applied on the page of **Monitoring>>VPN>>Firewall**. The default service names are HTTPS, HTTP, NoMachine, email, and DrayTek.Chat. Create available service names to meet the actual requirement.



These parameters are explained as follows:

Item	Description
+Add	Click to create a new service.
Host	Displays the IP address of the service.
Type	Displays the protocol set for the service.
Port	Displays the port number.
Service Name	Displays the name of the service.
Action	Edit - Click to modify the selected entry. Delete - Remove the selected entry.

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

The screenshot shows a web-based configuration interface for 'VPN Analytics Setup'. The 'Service Name' tab is active. It contains the following fields and controls:

- Host:** A text input field with a placeholder text: 'IPv4 format (EX: 123.12.1.1) or Any'.
- Type:** Three radio button options: 'TCP', 'UDP', and 'ICMP'.
- Port:** A text input field.
- Service Name:** A text input field.
- Buttons:** 'Cancel' and 'Save' buttons located at the bottom right of the form.

These parameters are explained as follows:

Item	Description
Host	Enter the IP address or the word of Any as the hostname.
Type	Set the protocol used for the host.
Port	Enter a port value used for the host.
Service Name	Define a name for the service.
Cancel	Discard current modification and return to the previous page.
Save	Save the current settings.

8.3.6.4 Email&SMS Format

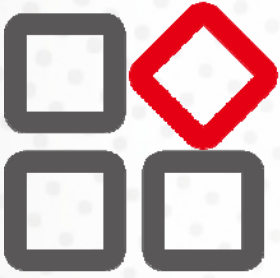
This page allows you to set the format of email and SMS. You have to enter the message for email and SMS by following the format suggested on this page.

The screenshot shows the 'Email&SMS Format' configuration page in the DrayTek VigorConnect interface. The page is divided into two tabs: 'Format' and 'Preview'. The 'Date Time Format' is set to '2006-01-02 15:04:05'. Below this is the 'VPN Access' section, which includes a list of keywords for use in templates: \$DATE_TIME (Event time), \$LAST_DATE (Last access time), \$PROFILE_ID (Profile ID), \$USERNAME (Username), \$ROUTER_NAME (Router name), \$IP (Virtual IP), \$PUBLIC_IP (Public IP), \$TYPE (connection type), \$VPN_TYPE (VPN type), and \$LOCATION (Location). The 'Email Subject' field contains the template '\$USERNAME(\$PROFILE_ID)@\$ROUTER_NAME VPN UP!'. The 'Email Message' field contains a template message: '\$DATE_TIME [\$ROUTER_NAME-\$USERNAME \$TYPE] is IP from \$PUBLIC_IP. If this is not your intent, please contact your system administrator immediately. Last VPN connection time is \$LAST_DATE.' A green 'Save' button is located at the bottom right of the page.

These parameters are explained as follows:

Item	Description
Format/Preview	Format - Click this tab for entering the content of SMS/email. Preview - Click this tab for viewing the content of SMS/email.
Date Time-Format	Displays the date time-format based on Golang (e.g., 2006-01-02 15:04:05).
VPN Access / Service Access	
Email Subject	Enter the subject of the email.
Email Message	Enter the message/content that the recipient will see by email.
SMS Message	Enter the message/content that the recipient will see by an SMS.
Save	Save the current settings.

Part V Device Menu for a CPE



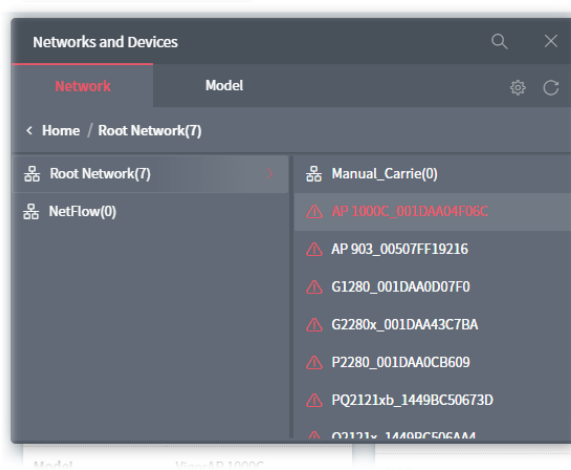
Chapter 9 Device Menu

On the dashboard for a specified CPE (AP/switch), the Device menu contains:



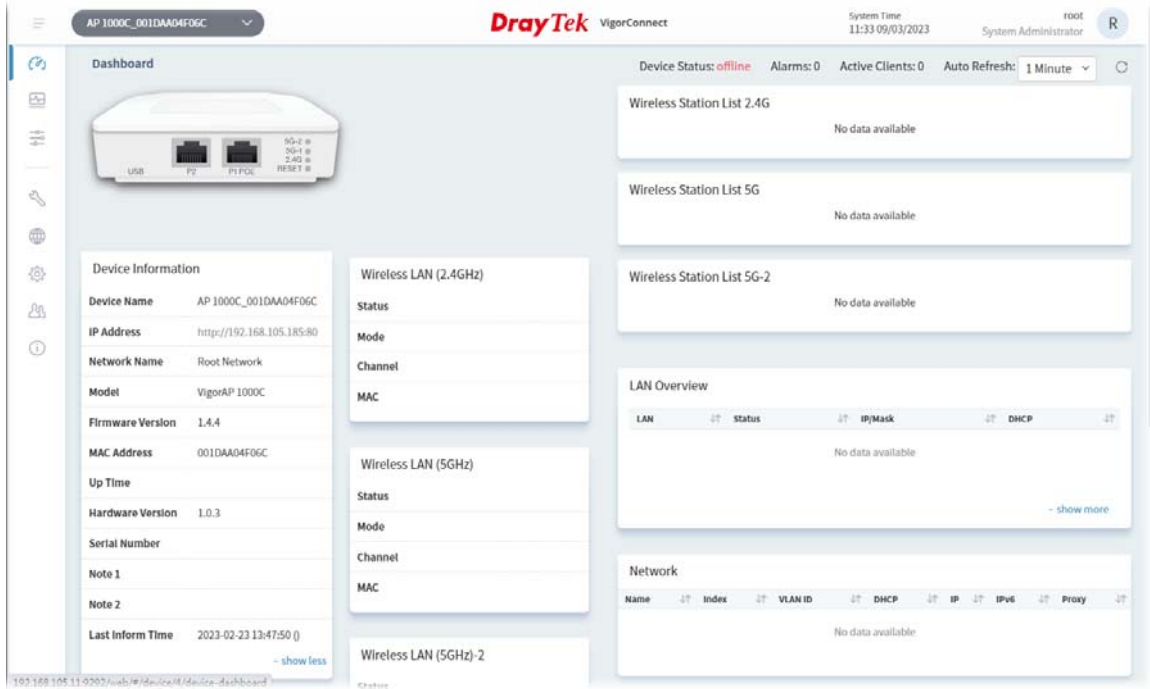
9.1 Dashboard for CPE

Use the drop-down menu on the top of the left side to select a CPE (e.g., AP 1000C).

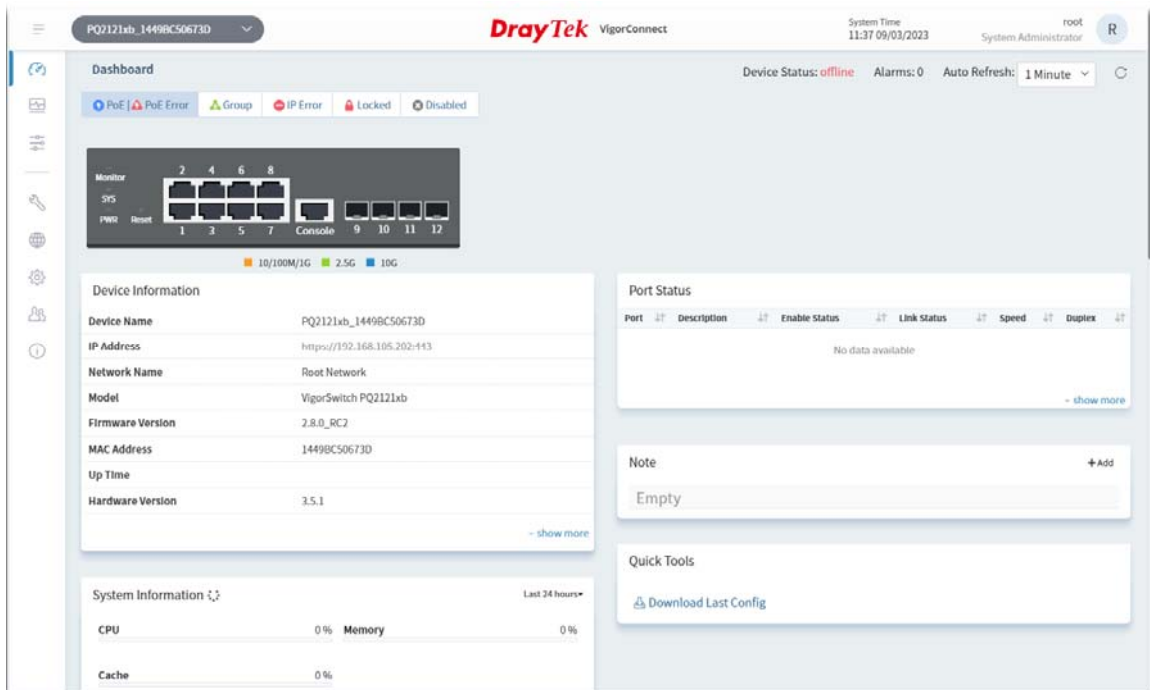


The dashboard will vary based on the selected CPE (access point/switch).

It will display device information, wireless LAN (2.4GHz/5GHz), wireless LAN(5GHz)-2, Wireless Station List 2.4G/5G/5G-2, LAN overview, network, note, quick tools, operation mode, connectivity and alerts for an access point.

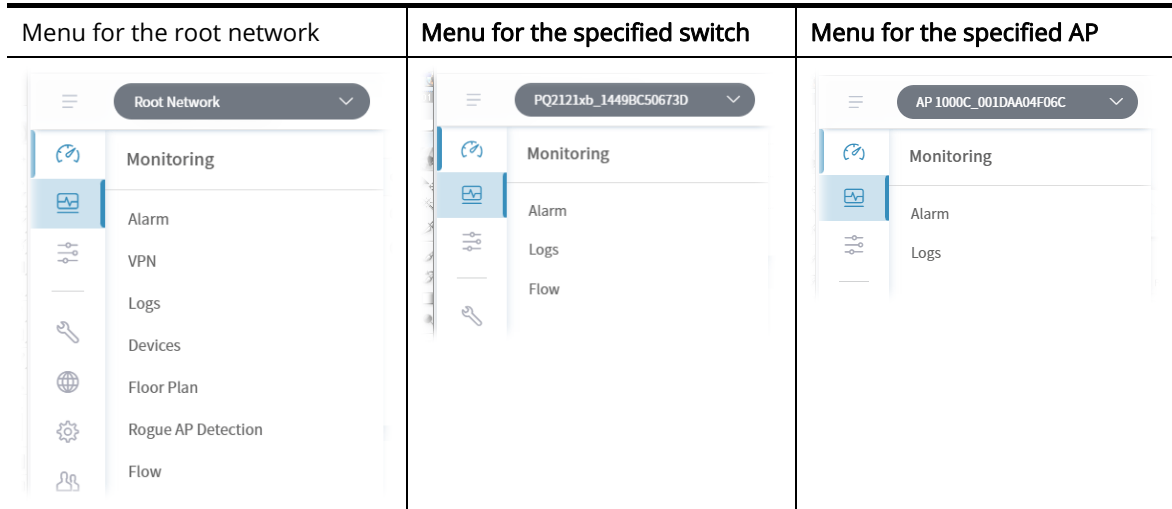


For a switch, it will display device information, system information, connectivity and alerts, last 10 SNMP events, port status, note and quick tools.



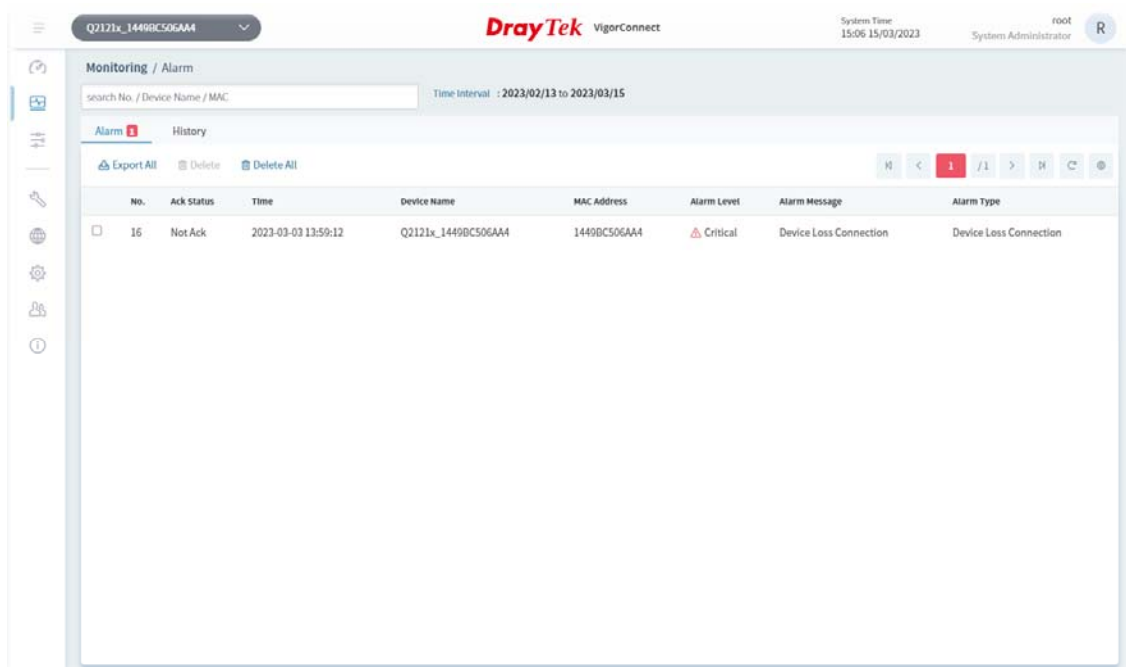
9.2 Monitoring Menu

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



9.2.1 Alarm for a Switch

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



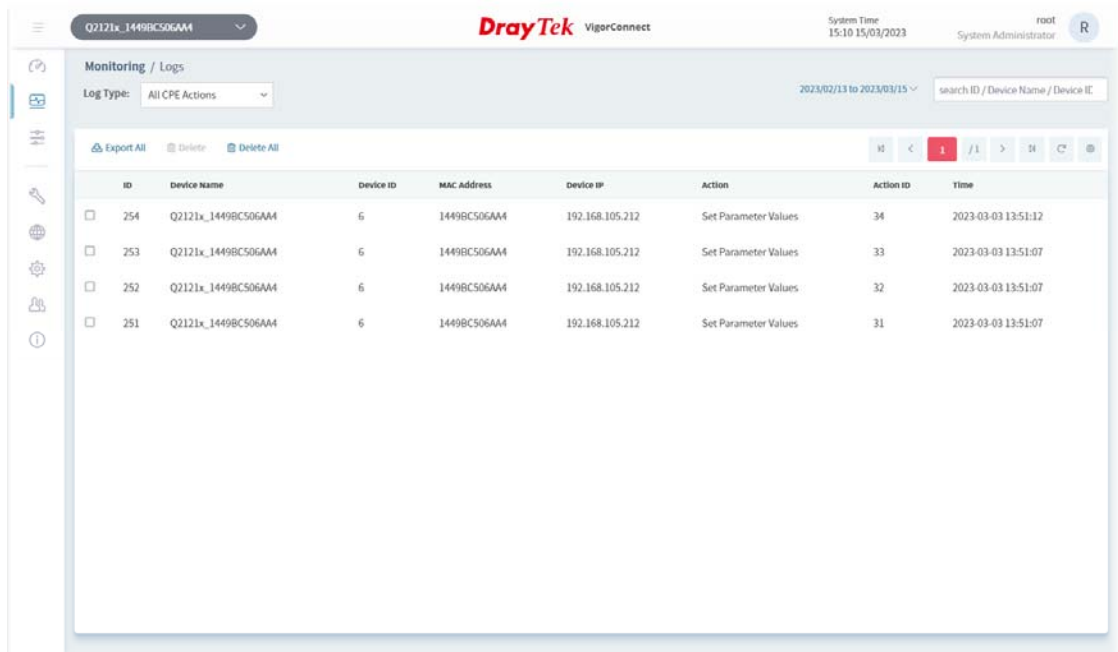
These parameters are explained as follows:

Item	Description
Alarm / History	Alarm – Display the alarm records recently. History – Display all the alarm records that have been solved and cleared.
Export All	Click to save alarm log as a XLS file.

Delete	Clear the alarm record which has been solved by VigorConnect.
Delete All	Clear all of the alarm records which have been solved by VigorConnect.
No.	Displays the index number of the alarm. It is offered by VigorConnect automatically.
Ack Status	Displays 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 VigorConnect automatically.
Alarm Type	Displays the alarm message with the type specified.

9.2.2 Logs for a Switch

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.



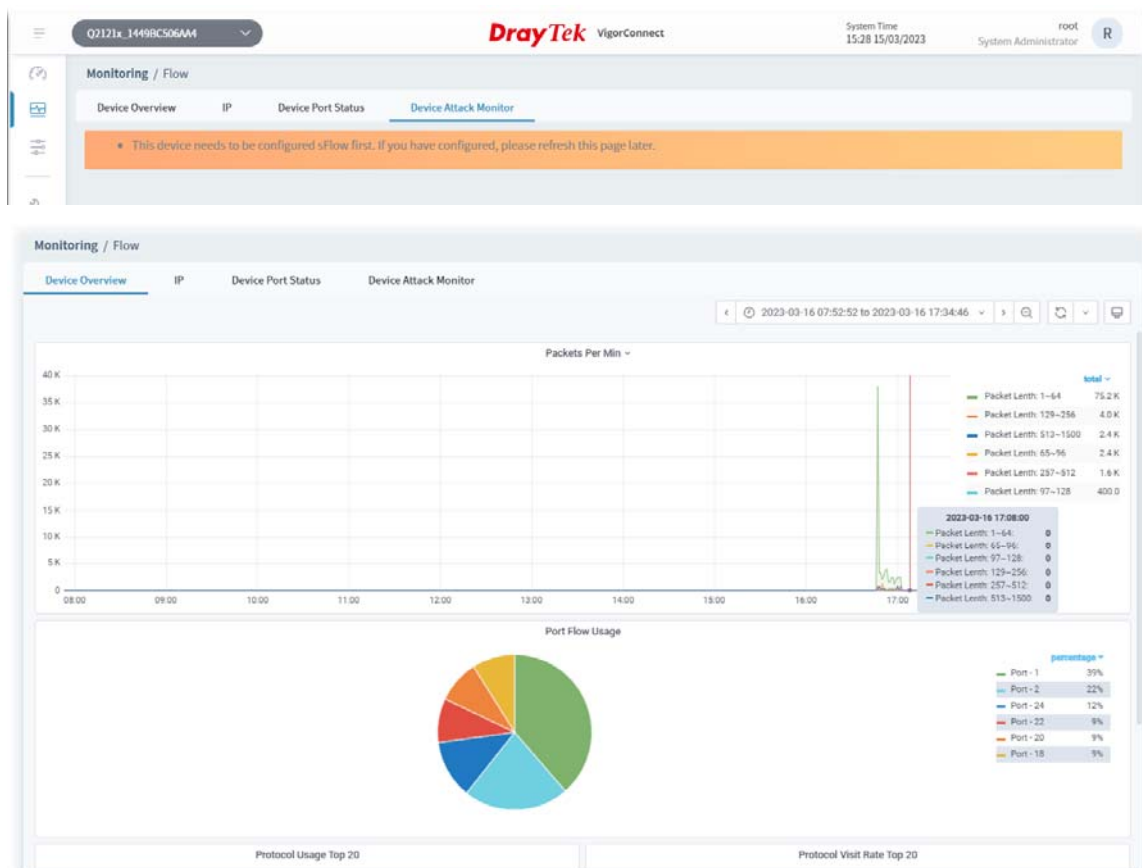
These parameters are explained as follows:

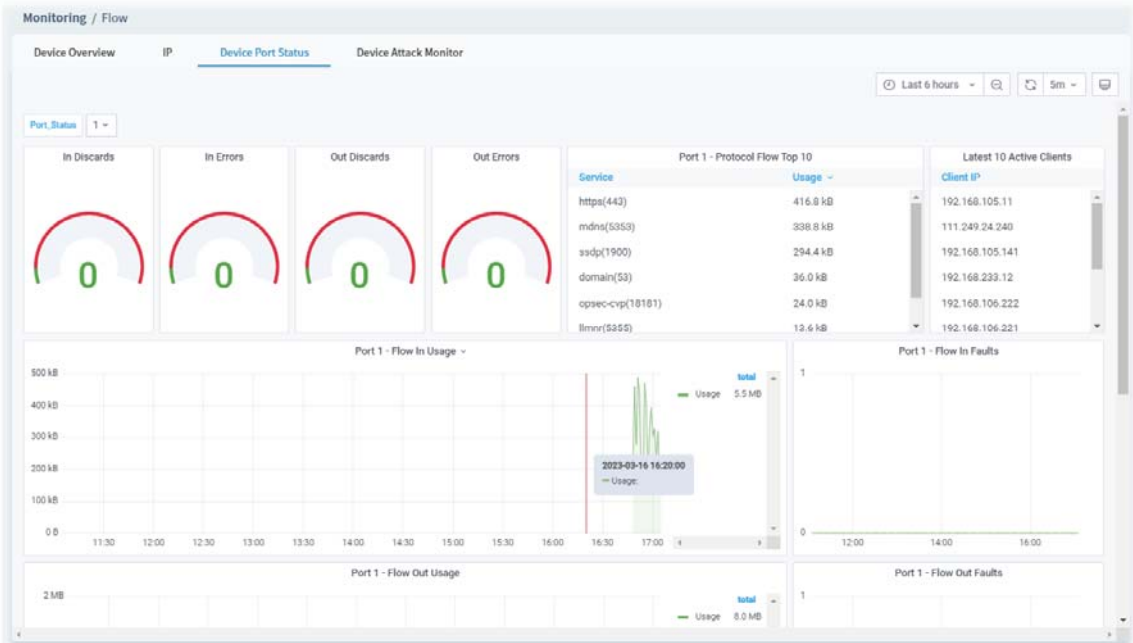
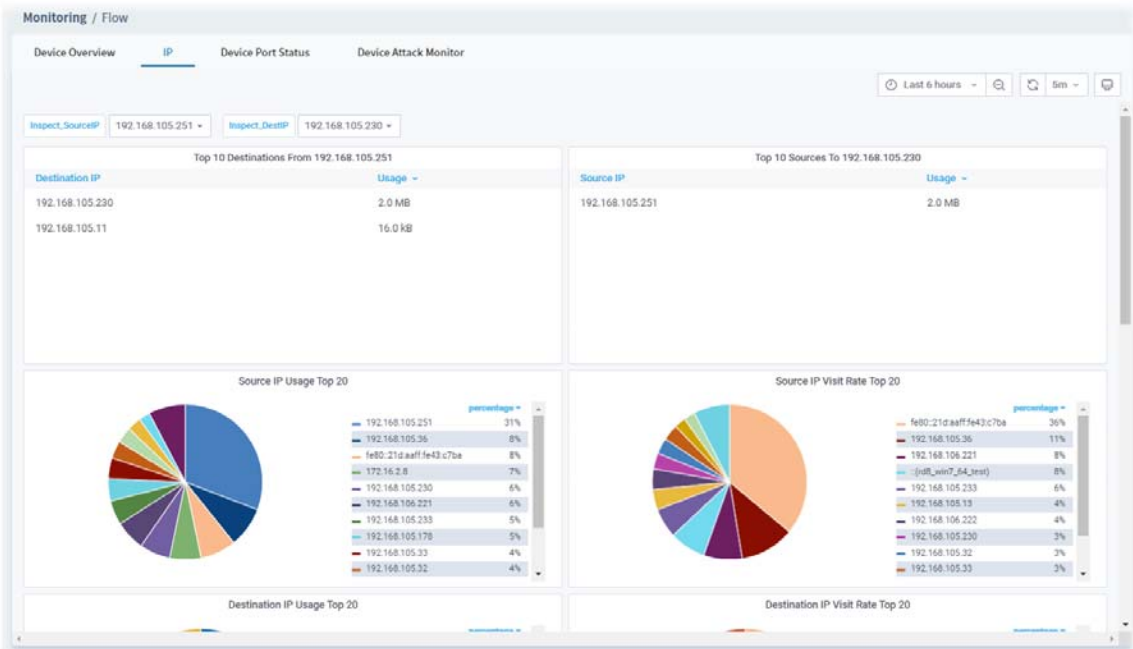
Item	Description
Log Type	Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate, Switch SNMP Alert and etc.) to display related log on this page.
<input type="text" value="search ID / Device Name / Device ID"/>	Enter the condition for VigorConnect to search and display relational information.
Export All	Click to save the log as an XLS file.

Delete	Clear the alarm record which has been solved by VigorConnect.
Delete All	Clear all of the alarm records which have been solved by VigorConnect.
ID	Displays the index number of the log. It is offered by VigorConnect automatically.
Device Name	Displays the name of the monitored device.
Device ID	Displays the identification number of monitored device.
MAC Address	Displays the MAC address of the monitored device.
Device IP	Displays the IP address of the monitored device.
Action	Displays the action performed by the monitored device.
Action ID	Displays the serial number for the action.
Time	Displays the time of the device to be monitored.

9.2.3 Flow for a Switch

This page displays the network traffic flow of certain switches which support the sFlow feature and enable the sFlow feature.



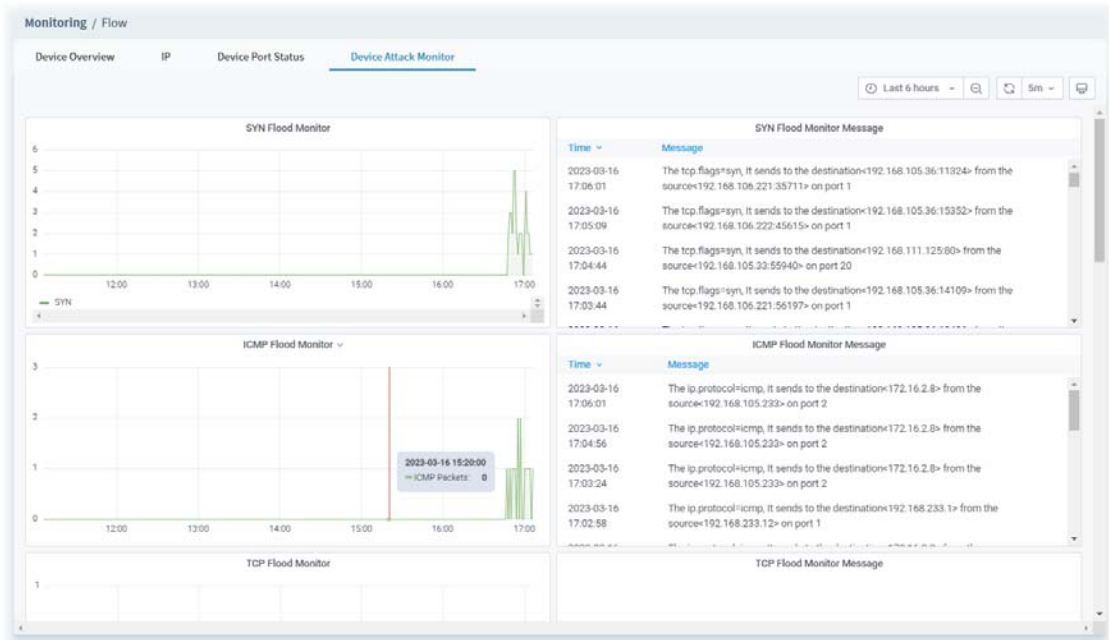


Port 1 - Flow In Usage -

Port 1 - Flow In Faults

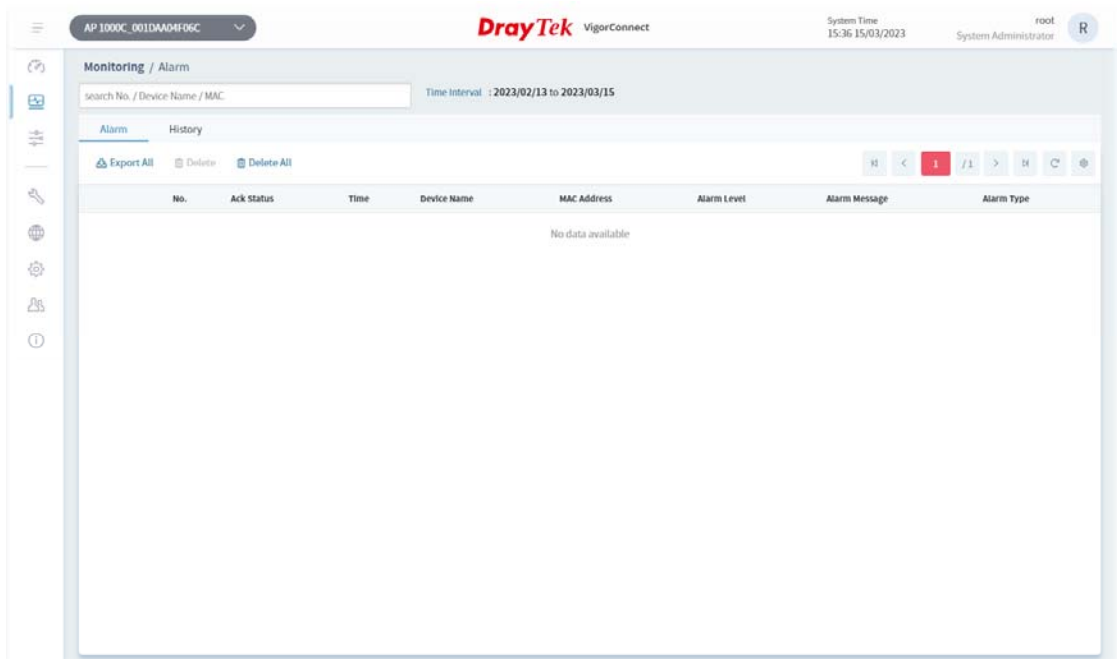
Port 1 - Flow Out Usage

Port 1 - Flow Out Faults



9.2.4 Alarm for an AP

Alarm message will be recorded on VigorConnect server when there is a trouble happened to the device (AP).



These parameters are explained as follows:

Item	Description
Alarm / History	Alarm – Display the alarm records recently. History – Display all the alarm records that have been solved and cleared.
Export All	Click to save alarm log as a XLS file.
Delete	Clear the alarm record which has been solved by VigorConnect.
Delete All	Clear all of the alarm records which have been solved by VigorConnect.

No.	Displays the index number of the alarm. It is offered by VigorConnect automatically.
Ack Status	Displays 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 VigorConnect automatically.
Alarm Type	Displays the alarm message with the type specified.

9.2.5 Logs for an AP


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.

ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
598	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Inform	---	2023-03-13 15:41:21
582	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	65	2023-03-13 13:52:58
580	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	63	2023-03-13 12:51:02
579	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	62	2023-03-13 13:50:50
578	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	61	2023-03-13 13:50:39
577	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Inform	---	2023-03-13 13:50:22
575	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	60	2023-03-13 13:49:14
573	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	59	2023-03-13 13:47:04
572	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	58	2023-03-13 13:46:32
571	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	57	2023-03-13 13:46:09
570	AP 1000C_001DAA04F06C	4	001DAA04F06C	192.168.105.185	Set Parameter Values	56	2023-03-13 13:45:44

These parameters are explained as follows:

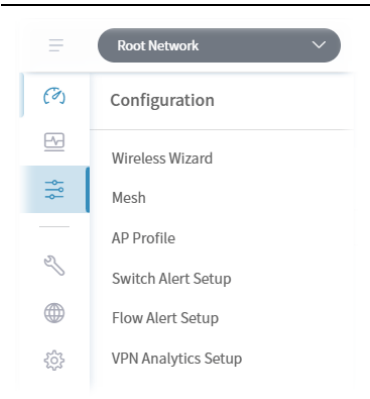
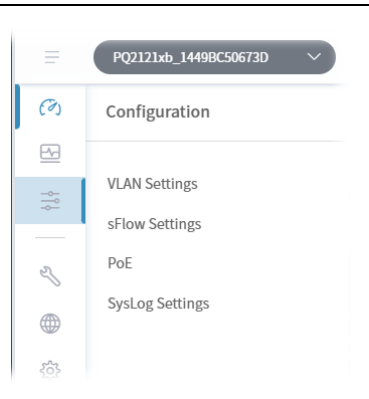
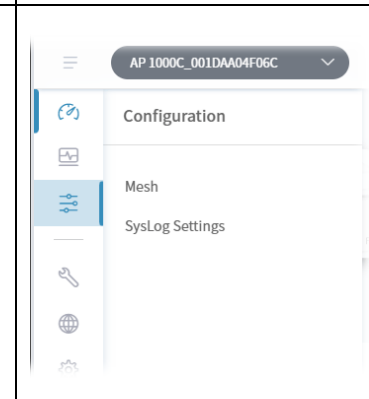
Item	Description
Log Type	Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate, Switch SNMP Alert and etc.) to display related log on this page.
<input type="text" value="search ID / Device Name / Dr"/>	Enter the condition for VigorConnect to search and display relational information.
Export All	Click to save the log as an XLS file.
Delete	Clear the alarm record which has been solved by VigorConnect.
Delete All	Clear all of the alarm records which have been solved by VigorConnect.
ID	Displays the index number of the log. It is offered by VigorConnect automatically.
Device Name	Displays the name of the monitored device.
Device ID	Displays the identification number of monitored device.
MAC Address	Displays the MAC address of the monitored device.
Device IP	Displays the IP address of the monitored device.
Action	Displays the action performed by the monitored device.
Action ID	Displays the serial number for the action.
Time	Displays the time of the device to be monitored.

9.3 Configuration

 This section introduces the menu item used for the selected CPE (AP or switch) briefly. For more detailed information on each menu item, refer to User's Guide of the selected CPE device.

Configuration menu will vary for root network, user-defined network and specified CPE (AP/switch).

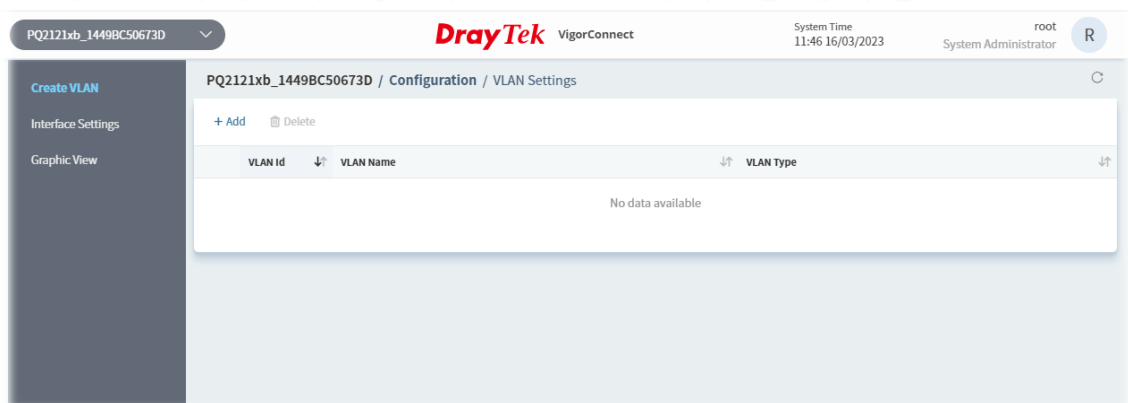
This section offers Configuration menu items for the specified CPE (AP/switch).

Menu for the root network	Menu for the specified switch	Menu for the specified AP
 <p>Root Network</p> <ul style="list-style-type: none"> Configuration Wireless Wizard Mesh AP Profile Switch Alert Setup Flow Alert Setup VPN Analytics Setup 	 <p>PQ2121xb_1449BC50673D</p> <ul style="list-style-type: none"> Configuration VLAN Settings sFlow Settings PoE SysLog Settings 	 <p>AP 1000C_001DAA04F06C</p> <ul style="list-style-type: none"> Configuration Mesh SysLog Settings

9.3.1 VLAN Settings for a Switch

The VLAN configuration is available for Vigor switch only.

9.3.1.1 Create VLAN



These parameters are explained as follows:

Item	Description
+Add	Click to create a VPN profile.
Delete	Click to remove the selected VPN file.
VLAN Id	Displays the VLAN ID number used by the VPN file.
VLAN Name	Displays the name of the VPN file.

VLAN Type	Displays the VLAN type of the VPN file.
------------------	---

To create a VLAN profile,

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

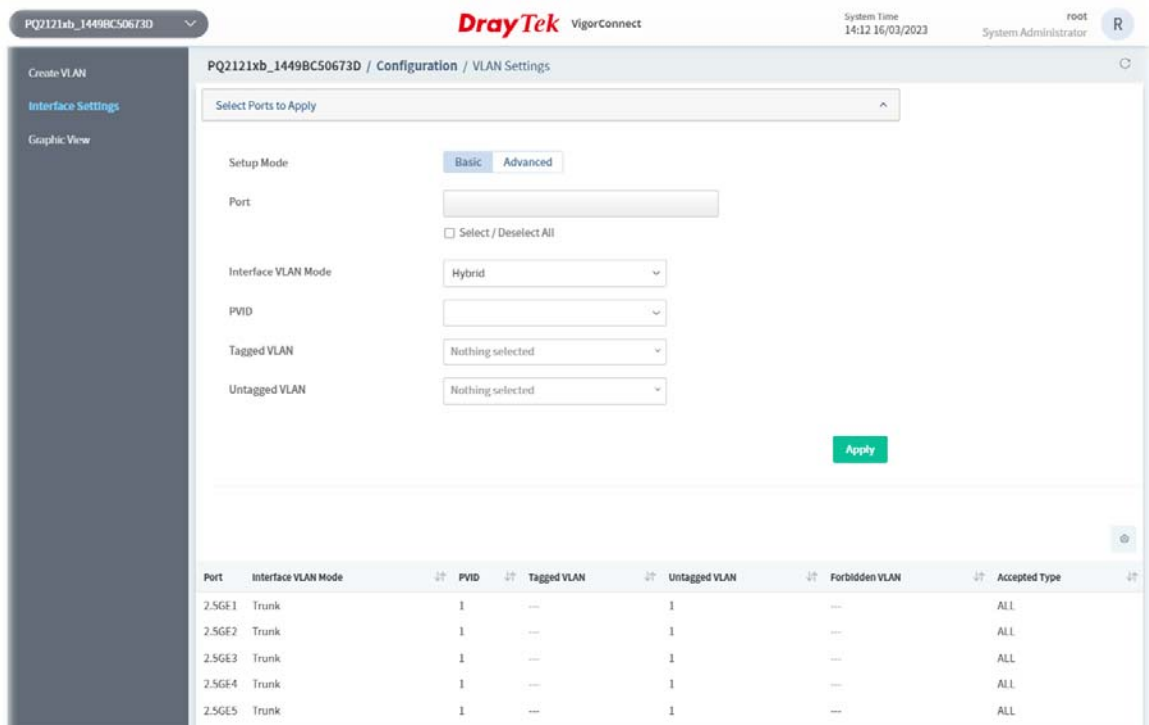
These parameters are explained as follows:

Item	Description
VLAN Id	Enter a number.
VLAN Name	Enter a name of the VPN file.
Cancel	Discard current modification and return to the previous page.
+Add	Save the current settings and return to the previous page.

2. After entering the ID number and name of the profile, click the **+Add** button. A new VLAN profile will be added to the page.

9.3.1.2 Interface Settings

This page allows a user to configure interface (GE) settings related to VLAN.



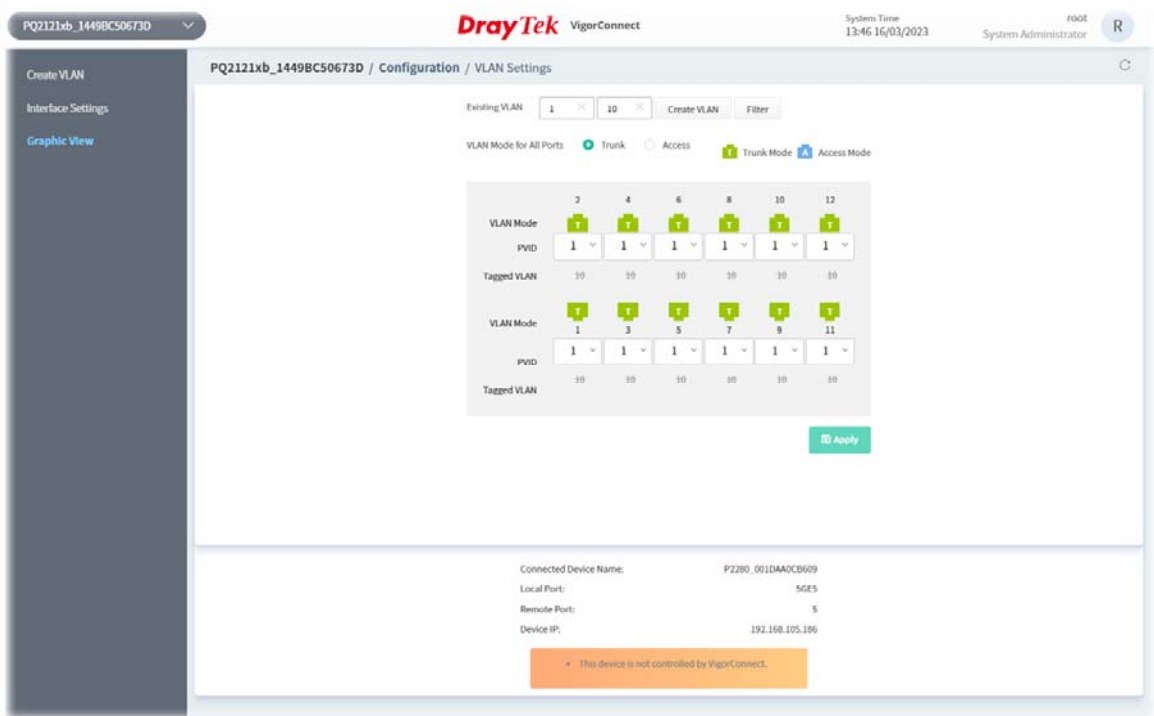
These parameters are explained as follows:

Item	Description
Setup Mode	Click to choose basic or advanced settings.
Port	Select the interface (GE, LAG) to apply the settings configured on this page.
Interface VLAN Mode	Select the VLAN mode of the interface. Hybrid – Support all functions as defined in IEEE 802.1Q specification. Access – Accepts only untagged frames and join an untagged VLAN. Trunk - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. Tunnel - Support all functions as defined in IEEE 802.1Q tunneling specification.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. For port under Access Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.
Accepted Type	It is available in the Advanced mode. Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode. All - Accept frames regardless it's tagged with 802.1q or not. Tag Only - Accept frames only with 802.1q tagged. Untag Only - Accept frames untagged.
Enable Ingress Filtering	It is available in the Advanced mode. Enable the ingress filtering to filter out any packets not belong to any VLAN members of this port. It is enabled automatically while operating in Access and Trunk mode.
Tagged VLAN	Specify the VLAN profile tagged in the VLAN.

Untagged VLAN	Specify the VLAN profile untagged in the VLAN.
Forbidden VLAN	It is available in the Advanced mode. The selected GE port only allows default VLAN packet to pass through.
Enable Uplink	Switch the toggle to enable/disable the function. It is available when Trunk is selected as Interface VLAN mode. Click the toggle to enable the function and specify the TPID type. TPID - Use the drop-down list to set the TPID type.
Apply	Save the current settings.

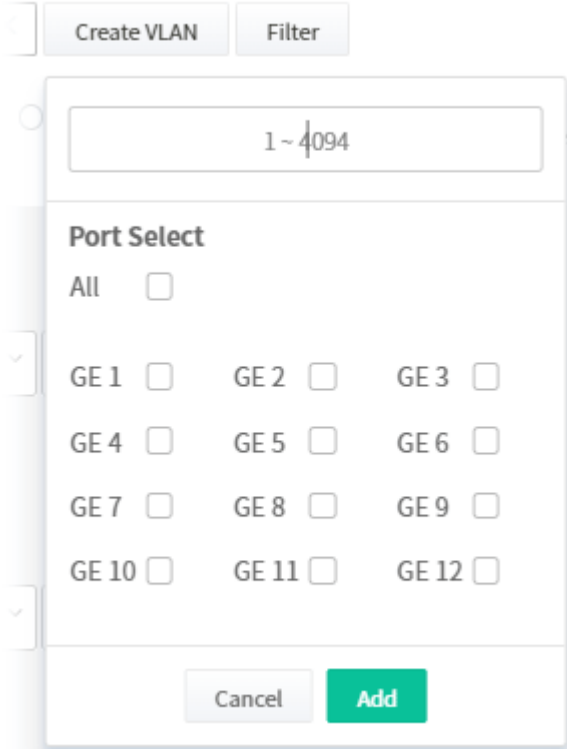
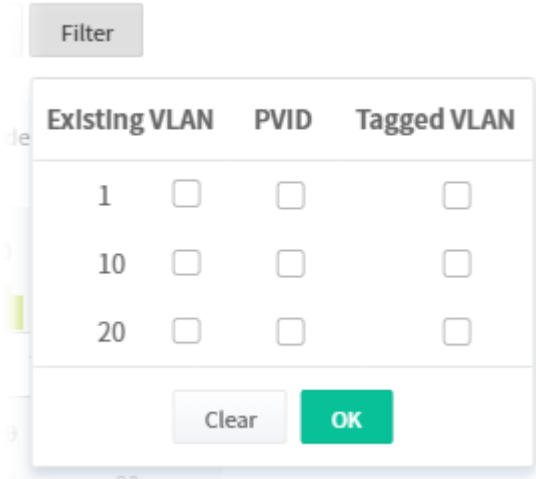
9.3.1.3 Graphic View

This page can display the PVID and VLAN ID number of each port in real time.



These parameters are explained as follows:

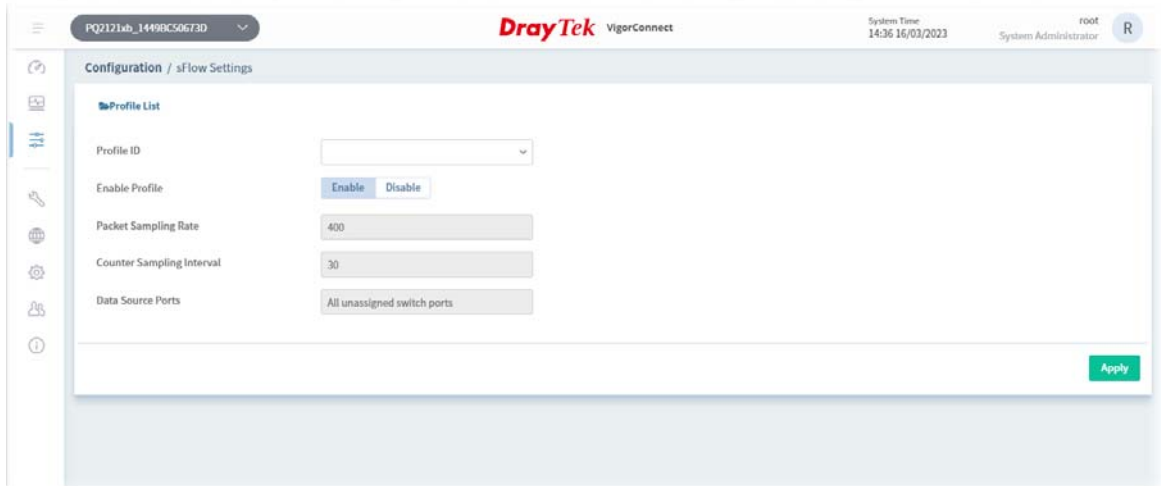
Item	Description
Existing VLAN	Displays the existing VLAN profiles. Use the drop-down list to select an existing profile.
Create VLAN	A quick method to create a VLAN profile. Enter the VLAN ID number (1 to 4094), and select the port number (GE1 to GE12, or All) as the VLAN member. Then click Add .

	
<p>Filter</p>	<p>VLAN - Select to enable PVID and Tagged VLAN at the same time.</p> <p>PVID - A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.</p> <p>For port under Access Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.</p> <p>Tagged VLAN - Specify the VLAN profile tagged in the VLAN.</p> 
<p>VLAN Mode for All Ports</p>	<p>Trunk - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.</p> <p>Access - Accepts only untagged frames and join an untagged VLAN.</p>
<p>Apply</p>	<p>Save the current settings.</p>

9.3.2 sFlow Settings for a Switch

The sFlow configuration is available for Vigor switch only.

sFlow (Sampled Flow) is a method which uses sampling to get the network packets information for the system administrator understanding the network operation and the network congestion.



These parameters are explained as follows:

Item	Description
Profile List / sFlow Config	Click Profile List to display the table of sFlow profiles. The link will be changed into sFlow Config for you to click again to return to the configuration page.
Profile ID	The number 1 to 8 represents the profile 1 to 8.
Enable Profile	Click Enable / Disable to enable or disable this function.
Packet Sampling Rate	Displays the sampling rate of the packets for the server to capture.
Counter Sampling Interval	Displays the time (sec.) for the sFlow server to obtain the traffic on the interface (LAN port) periodically.
Data Source Ports	Displays the LAN interface (10GE1 to 10GE4) of the data source port.
Apply	Save the current settings.

Click **Profile List** to list the following table.

Profile ID	Enable Profile	Packet Sampling Rate	Counter Sampling Interval	Collector Address Type	Collector Address	Collector Port	Data
<input type="checkbox"/> 1	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 2	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 3	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 4	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 5	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 6	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 7	Disable	400	30	Hostname		6343	
<input type="checkbox"/> 8	Disable	400	30	Hostname		6343	

9.3.3 PoE

The PoE configuration is available for Vigor switch (with PoE feature) only.

9.3.3.1 Properties

This page allows a user to configure general settings for supplying PoE power for all PoE ports.

The screenshot displays the PoE configuration interface. At the top, it shows the device ID 'PQ2121xb_1449BC50673D' and the 'DrayTek VigorConnect' logo. The system time is 14:53 16/03/2023, and the user is 'root System Administrator'. The main configuration area includes:

- PoE Mode:** Radio buttons for Auto, Manual, and Disable.
- Power Budget(W):** Input field with value 140.
- Consuming Power(W):** Input field with value 7.8.
- Advertised Power(W):** Input field with value 0.
- Remaining Power(W):** Input field with value 132.2.
- SW Version:** Input field with value 1.
- Port:** A drop-down menu and a checkbox for 'Select / Deselect All'.
- Enable:** A toggle switch currently turned on.
- Priority:** Radio buttons for Low, High, and Critical.
- Apply:** A green button to save settings.

Below the configuration area is a table with the following data:

Port	Enable	Status	PD Class	Priority	Power Used (W)	Power Limit (W)	Port Cycle
GE1	Enabled	No PD	---	Low	0	AT (30)	Apply
GE2	Enabled	No PD	---	Low	0	AT (30)	Apply
GE3	Enabled	ON	4	Low	3.9	AT (30)	Apply
GE4	Enabled	No PD	---	Low	0	AT (30)	Apply

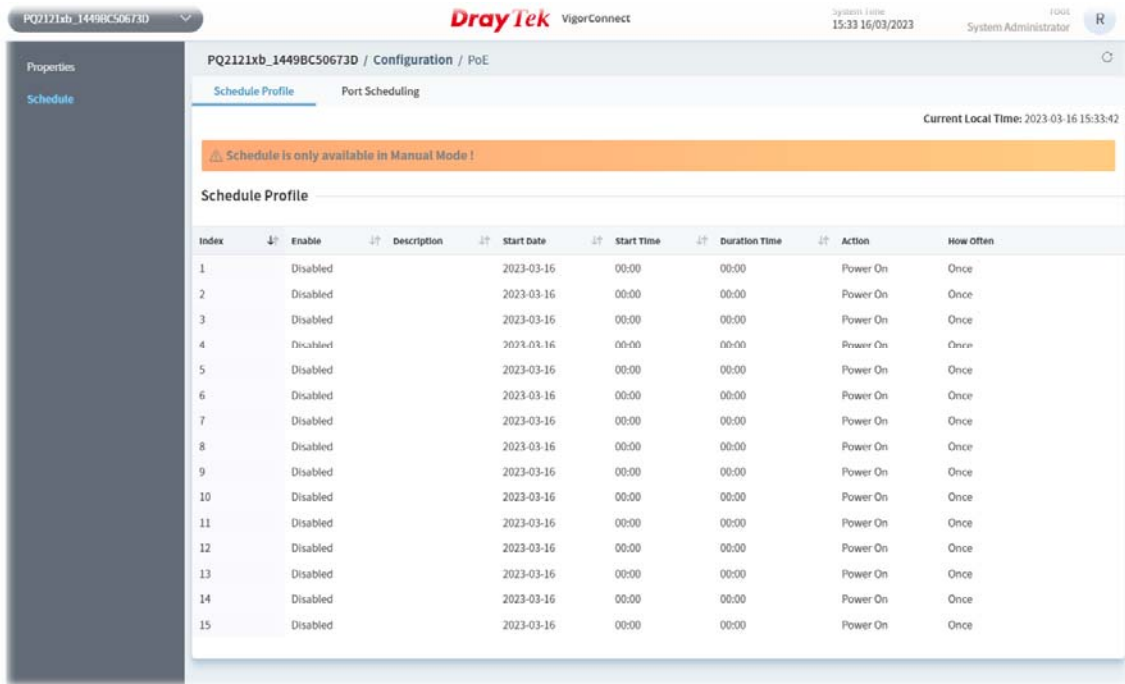
These parameters are explained as follows:

Item	Description
PoE Mode	<p>Auto – Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode.</p> <p>Manual – Before using scheduled PoE, set Manual as PoE mode.</p> <p>Disable - Disable the PoE function.</p>
Port	<p>Use the drop-down list to select the GE port for applying the settings configured above.</p> <p>Select/Deselect All - Check to select or deselect all the GE ports.</p>
Enable	Switch the toggle to enable/disable settings configured on this page.
Priority	Specify the priority of the GE port.
Power Limit	Select the power limit (AT or AF).
Apply	Save the current settings.

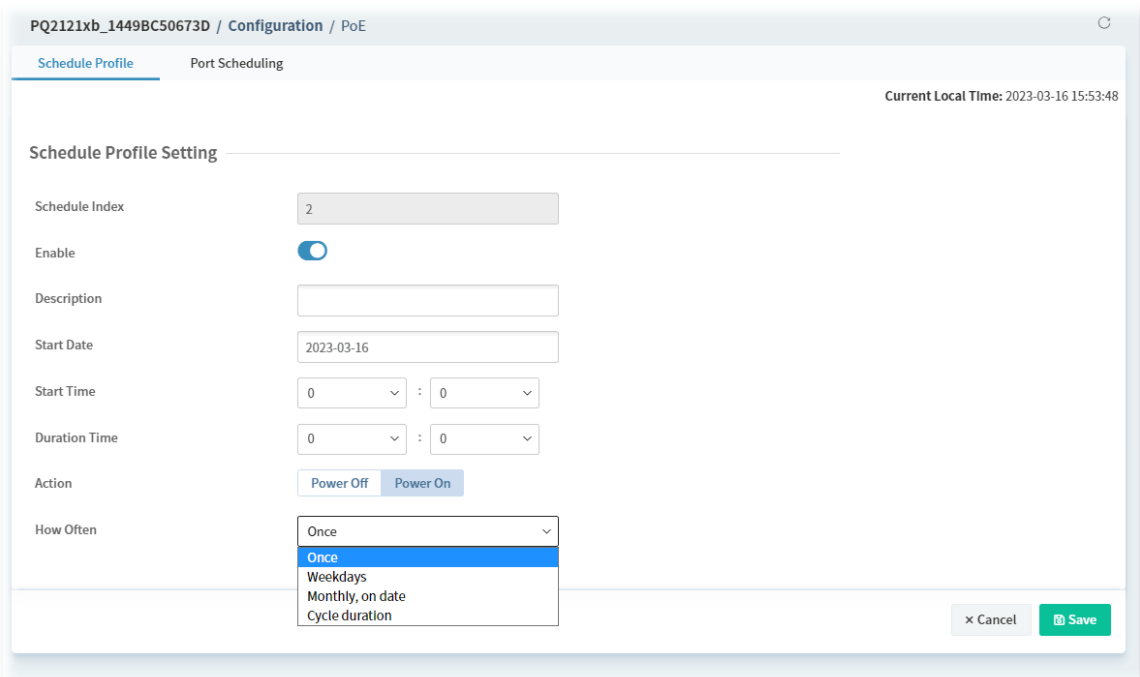
9.3.3.2 Schedule

Schedule Profile

This page displays the schedule profiles (1 to 15), with related settings. It is available when **Manual** is set as **PoE Mode**.



To configure the schedule profile, move the mouse cursor on the index number of the profile you want to change and click it. The configuration page will be shown as the following.



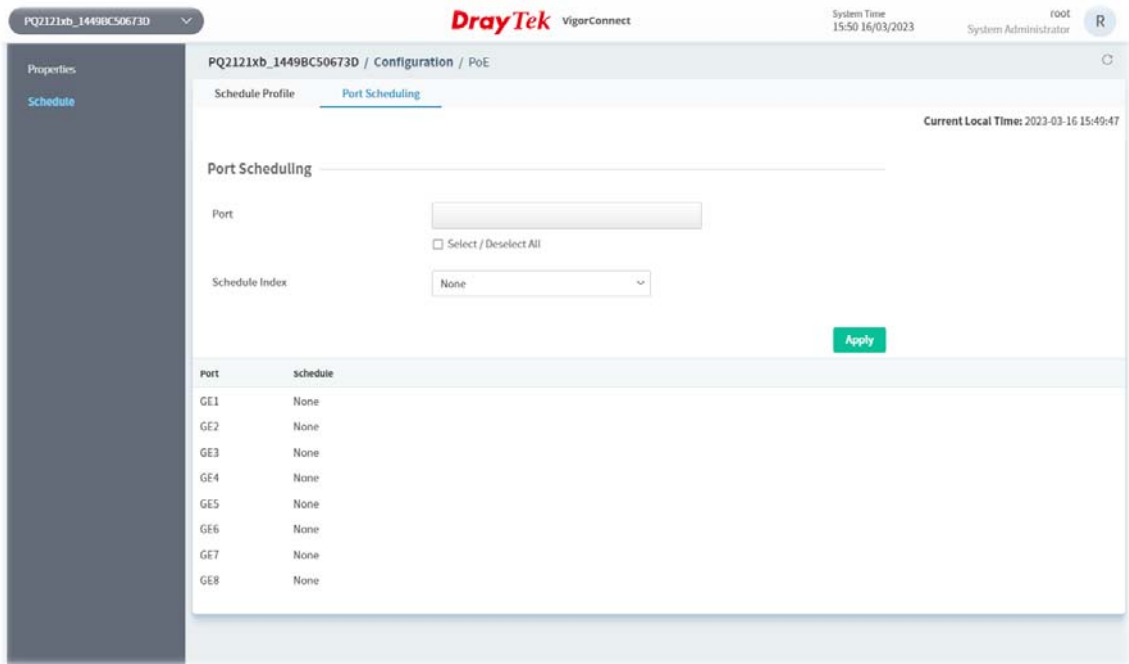
These parameters are explained as follows:

Item	Description
PoE Mode	<p>Auto – Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode.</p> <p>Manual – Before using scheduled PoE, set Manual as PoE mode.</p> <p>Disable - Disable the PoE function.</p>
Port	Use the drop-down list to select the GE port for applying the settings configured above.

	Select/Deselect All - Check to select or deselect all the GE ports.
Enable	Switch the toggle to enable/disable settings configured on this page.
Priority	Specify the priority of the GE port.
Power Limit	Select the power limit (AT or AF).
Apply	Save the current settings.

Port Scheduling

This page allows you to specify a schedule for each GE port.

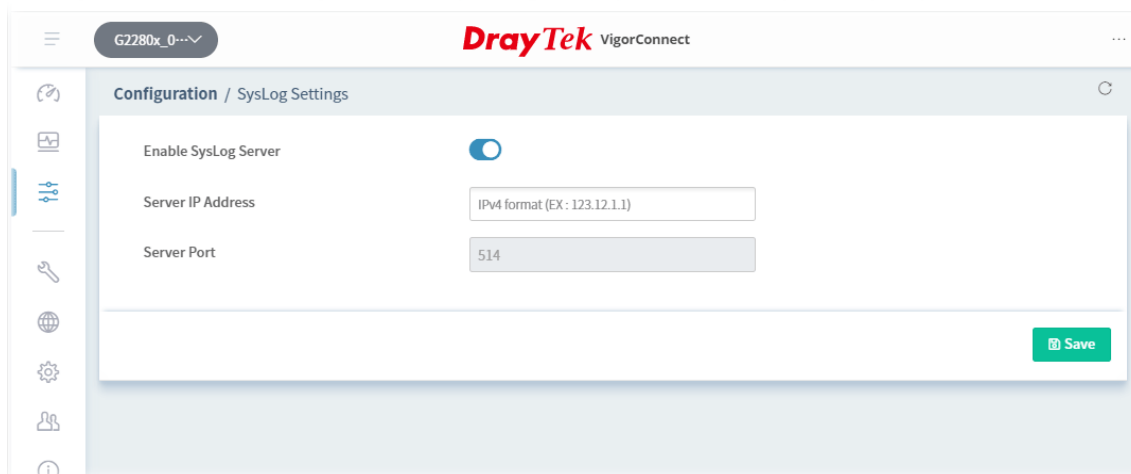


These parameters are explained as follows:

Item	Description
Port	Use the drop-down list to select the GE port for applying the settings configured below. Select/Deselect All - Check to select or deselect all the GE ports.
Schedule Index	Select the index number of the schedule profile to apply to the GE port.
Apply	Save the current settings.

9.3.4 SysLog Settings for a Switch

SysLog is provided for users to monitor a switch. There is no bother to directly get into the Web user interface of the switch or borrow debug equipment. This page allows you to specify the IP address, and port number for the SysLog server.

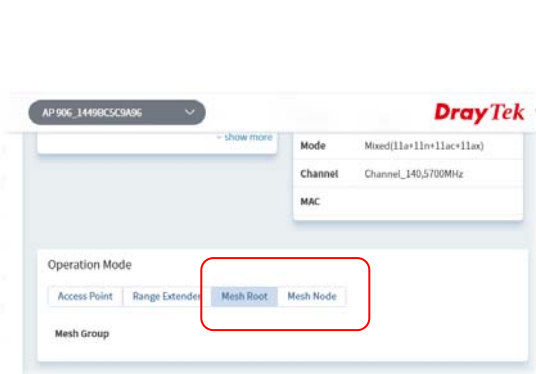


These parameters are explained as follows:

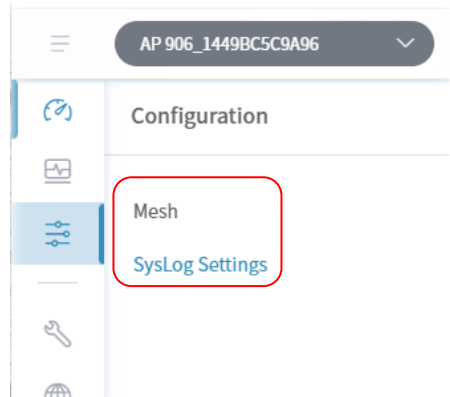
Item	Description
Enable SysLog Server	Switch the toggle to enable/disable the SysLog Server settings.
Server IP Address	Enter the IPv4 address of the server.
Server Port	Displays the port number used by the server.
Save	Save the current settings.

9.3.5 Mesh for an AP

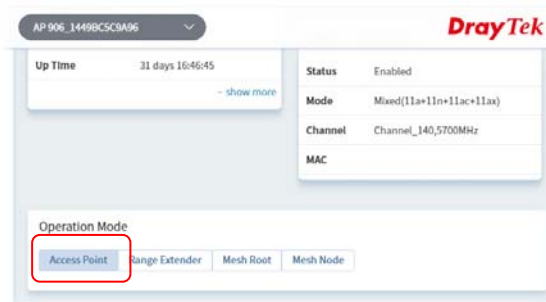
The mesh item is available for the Vigor access point only when the device set with the Mesh Root/Mesh Node operation mode.



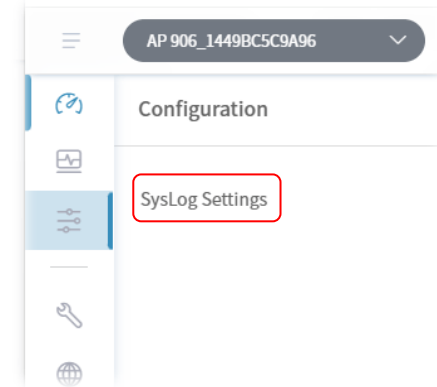
If the AP is set with the **Mesh Root** or **Mesh Node**



The Mesh menu item will be shown on Configuration.



If the AP is set with the Access Point

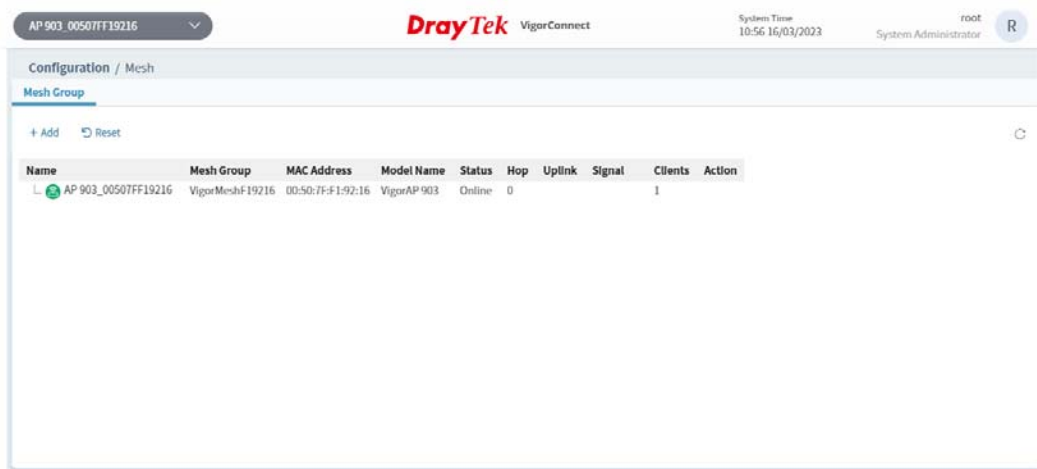


No Mesh menu item appears

Open **Configuration>>Mesh**.

This page allows you select mesh node(s) to be grouped under an existing mesh root (in this case, AP903).

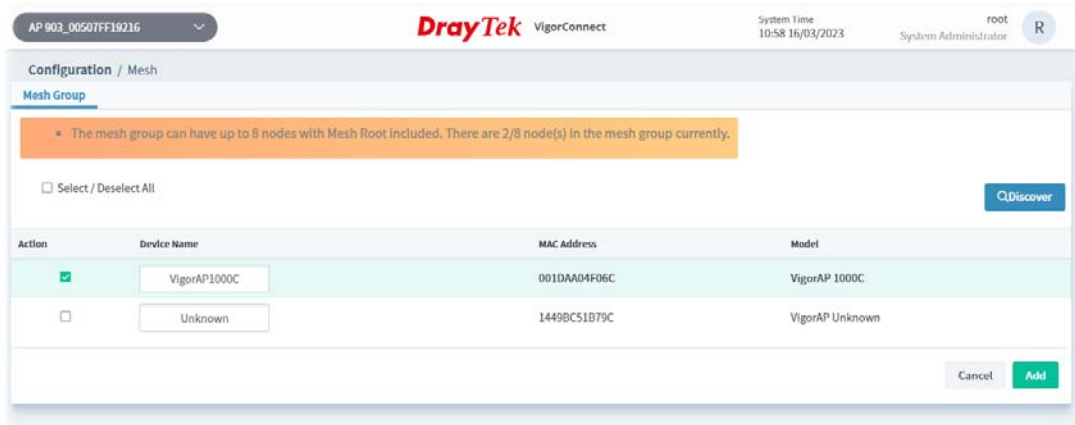
1. Click **+Add**.



These parameters are explained as follows:

Item	Description
+Add	Create a new mesh group.
Reset	Reset current page.

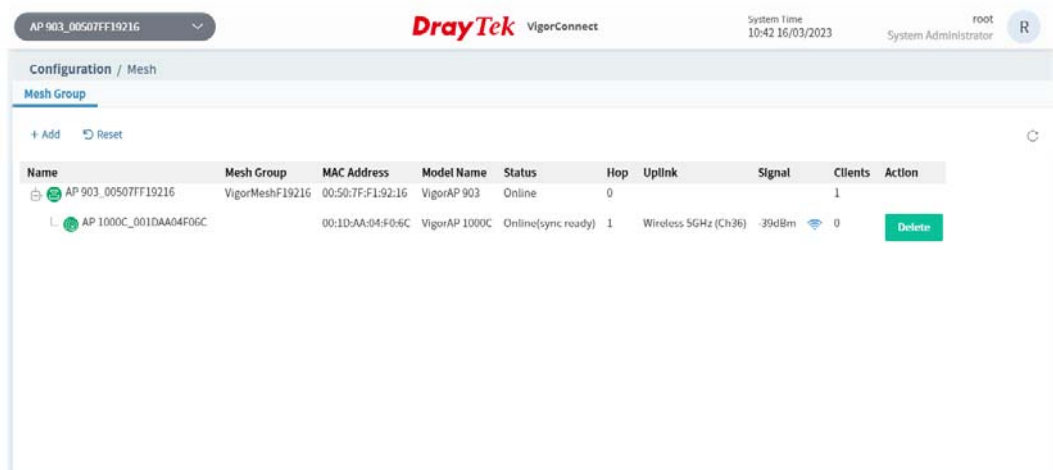
- Click **+Add**. The system will search for available mesh nodes near the mesh root, then display them on the page.



These parameters are explained as follows:

Item	Description
Select/Deselect All	Check the box to select all the devices listed on this page.
Discover	Click to search more mesh nodes.
Action	Check the box to select the device.
Device Name	Displays the name of the device for identification if there is more than one of the same model.
MAC Address	Displays the MAC address of the device.
Model	Displays the model of the device.
Cancel	Discards current settings.
Add	Make the selected device group under the mesh root.

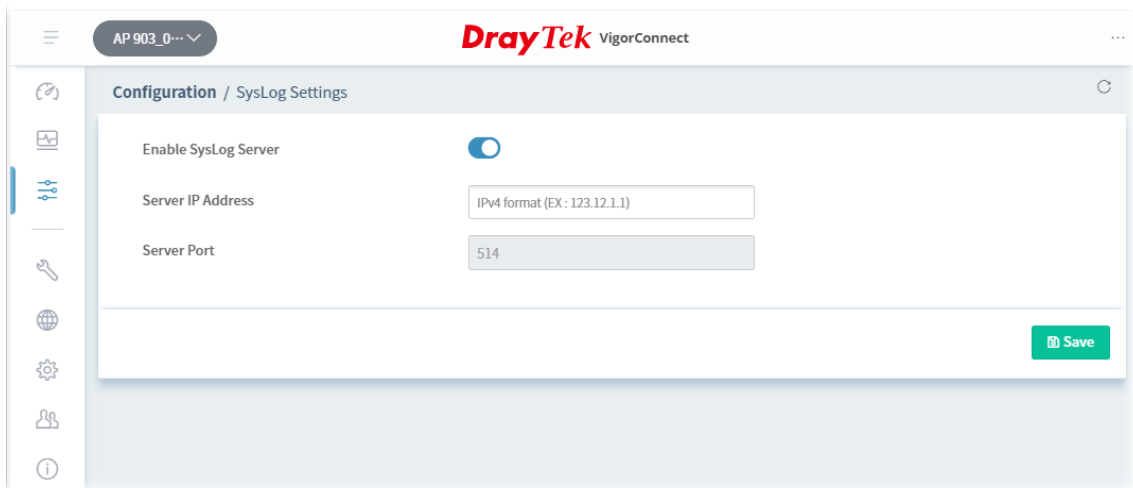
- Select the mesh node you want and click **Add** to make the new device grouped under the mesh root.



Click **Delete** to remove the unnecessary mesh node.

9.3.6 SysLog Settings for an AP

SysLog is provided for users to monitor AP. There is no bother to directly get into the Web user interface of the AP or borrow debug equipment. This page allows you to specify the IP address, and port number for the SysLog server.



These parameters are explained as follows:

Item	Description
Enable SysLog Server	Switch the toggle to enable/disable the SysLog Server settings.
Server IP Address	Enter the IPv4 address of the server.
Server Port	Displays the port number used by the server.
Save	Save the current settings.