VigorACS 3

Unified Management System User's Guide

Manual Version: V2.0 Date: April 28, 2025 Software Version: 3.8.0 © All rights reserved.

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

Microsoft is a registered trademark of Microsoft Corp.
Windows 8, 10, 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.

VigorACS 3 License

© All rights reserved.

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

Limited Warranty

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

Customer Remedies

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

No Other Warranties

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

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

Table of Contents

Part I		1
	Chapter 1 Introduction	2
	1.1 Main Features and Benefit	2
	1.2 System Architecture	
	1.3 Web Service	
	Chapter 2 Install & Startup	5
	2.1 Platform for Windows 10, 11	5
	2.1.1 Installation for Java	
	2.1.2 Installation for MariaDB	8
	2.1.3 Installation for VigorACS 3	13
	2.1.4 StartMySQL/MariaDB Database	24
	2.1.5 Start VigorACS	25
	2.2 Platform for Linux	
	2.2.1 Installation for MariaDB, Java and VigorACS	
	2.2.2 StartMySQL/MariaDB Databse	
	2.2.3 Start InfluxDB	
	2.2.4 Start VigorACS	
	2.2.5 Start VigorACS Chatbot	
	2.2.6 Edit VigorACS IP	
	2.3 Registering VigorACS	
	2.3.1 Registration for VigorACS via Windows Platform	
	2.3.2 Troubleshooting for Unstable CPE Status	44
	Chapter 3 Getting Started	48
		40
	3.1 Accessing Web Page of VigorACS	
	3.2 Dashboard	
	3.2.1 Dashboard for Root Network	
	3.2.3 Dashboard for a Device	
	3.2.4 Menu Bar	
	3.2.5 Root Network, Group Network, and Selected CPE	
	3.2.6 Capture Packets	
	3.2.7 Set Password, Two-factor Authentication, Manage Notification, Change and Log Out	
	3.2.8 Auto Refresh, Manual Refresh, and Widget	
	3.2.9 Overviews	
	3.2.10 Icons Used in VigorACS 3	
	3.3 Operation Procedure	
	Applications	
	A.1 How to Register a CPE onto VigorACS 3?	
	A.2 How to Create a New Network?	
	A.3 How to Assign a New Added CPE to a Network?	
	A.4 How to Create a New User Group?	77
Part II .		
		0.0
	Chapter 4 SD-WAN Solution	80
	4.1 Topology of SD-WAN, Edge Router and ACS Server	80
	4.1.1 Enabling SD-WAN on VigorACS	
	4.1.2 Auto VPN	82
	4.1.3 VoIP WAN	83
	4.1.4 Full Traffic Control with the Route Policy	84
	4.2 Dashboard for SD-WAN Network Group	85
	4.3 Statistics for SD-WAN Network Group	87
	4.4 Monitoring for SD-WAN Network Group	
	4.4.1 WAN (SD-WAN)	88
	4.4.2 VPN (SD-WAN)	
	4.4.3 VoIP (SD-WAN)	
	4.4.4 Data Usage (SD-WAN)	97
	Chapter 5 SD-WAN CPE	90

5.2 Statistics for SD-WAN CPE 101 5.3 J Namron 102 5.3 J Alarron 102 5.3 J Alarron 102 5.3 J Logs 103 5.3 J Logs 104 5.3 J Logs 104 5.3 J Logs 104 5.3 J Logs 104 5.3 J May Devisite 109 5.3 J Starge 113 5.3 A WAN (SD-WAN) 114 5.3 Starge (SD-WAN) 114 5.3 Starge (SD-WAN) 114 5.3 Starge (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1.1 Scheduled Backup 121 6.1.2 Configuration Restore 138 6.1.3 Street Restore 138 6.1.4 Device Reboot 138 6.1.5 System Password Reset 136 6.1.6 Street Parameters 138 6.1.7 File Manager 139 6.1.8 Device Res Parameters 135 6.3 Provide In grameters 135		5.1 Dashboard for SD-WAN CPE	99
5.3 Monitoring for SD-WAN CPE 101 5.3.1 Alarm. 102 5.3.2 Logs 103 5.3.3 Flow 104 5.3.4 Diagnostics 103 5.3.5 GPS 113 5.3.6 WAN (SD-WAN) 114 5.3.8 Van (SD-WAN) 114 5.3.8 Van (SD-WAN) 116 5.4.7 Construction 117 5.3.8 Van (SD-WAN) 116 5.4.7 Construction 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 122 6.1.1 Scheduled Backup 123 6.1.1 Scheduled Backup 124 6.1.2 Configuration Restore 123 6.1.3 Firmware Uggrade 123 6.1.4 Scheduler Profile 138 6.1.7 Tile Manager 139 6.1.8 Scheduler Profile 138 6.1.7 Tile Manager 139 6.1.8 Scheduler Profile 138 6.1.9 Scheduler Profile 138 6.1.1 Scheduler Roter 139 6.1.8 Scheduler Profile 138 6.1.9 Scheduler Profile 138 <			
5.3.1 Alarm 102 5.3.2 Logs 103 5.3.3 Flow 104 5.3.4 Diagnostics 109 5.3.5 GPS 113 5.3.6 WAN (SD-WAN) 113 5.3.7 VPN (SD-WAN) 114 5.3.8 VAN (SD-WAN) 114 5.3.9 Data Usage (SD-WAN) 116 5.4.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 Maintenance 120 6.1.1 Schedule Backup 121 6.1.2 Schedule Backup 121 6.1.3 Stredule Backup 121 6.1.4 Device Reboot 133 6.1.5 Streten Ressourd Reset 136 6.1.5 Streten Ressourd Reset 136 6.1.6 Schedule Profile 138 6.1.7 File Manager 134 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3.3 CPE Keep Parameters 152 6.3.1 Global Parameters 152 6.3.2 CPE Arameters 152 6.3.3 Sterker Anangeme			
5.3.2 Logs 103 5.3.3 How 104 5.3.4 Diagnostics 109 5.3.5 GPS 113 5.3.5 GPS 113 5.3.5 GPS 114 5.3.5 WIN (SD-WAN) 114 5.3.5 Val Usger (SD WAN) 115 5.3.5 Val Usger (SD WAN) 116 5.4.5 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1.1 Scheduled Backup 121 6.1.2 Configuration Restore 122 6.1.3 Chedule Backup 123 6.1.5 Schedule Profile 133 6.1.5 Schedule Profile 133 6.1.5 Schedule Profile 134 6.2.1 Report Tasks 144 6.2.2 Legox Report Tasks (Deprecated) 151 6.3.2 CPE Sec Parameters 152 6.3.2 CPE Sec Parameters 153 6.3.3 CPE Sec Parameters 152 <		-	
5.3.3 Flow 104 5.3.4 Degnostics 109 5.3.5 GPS 113 5.3.6 VAN (SD-WAN) 113 5.3.7 VFN (SD-WAN) 114 5.3.8 VAN (SD-WAN) 115 5.3.8 Data Usage (SD-WAN) 115 5.3.9 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 Maintenance 120 6.1.1 Scheduled Backup 121 6.1.2 Schedule Portie 123 6.1.3 Schedule Portie 123 6.1.4 Schedule Rabot 123 6.1.5 System Password Restore 124 6.1.6 Schedule Portie 138 6.1.7 Schedule Portie 138 6.1.8 Schedule Portie 138 6.1.9 Schedule Portie 139 6.1.8 Schedule Portie 138 6.2.1 Report Task 144 6.2.2 Legort Task 152 6.3.1 Schedule Portie 152 6.3.2 C			
5.3.4 Dignostics 109 5.3.5 GPS 113 5.3.5 GPS 113 5.3.5 GPS 114 5.3.5 GPS 114 5.3.5 Avent (SD-WAN) 115 5.3.5 Data Usage (SD-WAN) 115 5.3.5 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1.1 Scheduled Backup 121 6.1.2 Configuration Restore 123 6.1.3 Configuration Restore 123 6.1.4 Device Reboot 133 6.1.5 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2 Report Task 145 6.2.1 Report Task 152 6.3.2 CPE Say Report Task (Deprecated) 151 6.3.2 CPE Say Report Tasks 152 6.3.2 CPE Set Parameters 152 6.3.2 CPE Set Parameters 152 6.3.2 CPE Set Parameters 152 6.3.4 Fimware Uggrade 163			
5.3.5 GPS 113 5.3.6 WAN (SD-WAN) 114 5.3.7 VPR (SD-WAN) 114 5.3.8 Poter (SD-WAN) 115 5.3.9 Data Usage (SD-WAN) 115 5.3.9 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1.1 Scheduled Backup 121 6.1.2 Schedule Pograde 122 6.1.3 Findure Rebot 123 6.1.5 System Password Reset 133 6.1.5 System Password Reset 136 6.1.7 File Manager 139 6.1.8 Schedule Profile 138 6.1.7 File Manager 155 6.3.8 Schedule Profile 155 6.3.1 Gibbal Parameters 156 6.3.2 CPE Keep Parameters 152 6.3.1 Gibbal Parameters 152 6.3.2 CPE Keep Parameters 152 6.3.1 Gibbal Parameters 156 6.3.2 CPE Keep Parameters 152 6.3.2 CPE Keep Parameters 152 6.3.3 Libbal Parameters 156			
5.3 6 WAN (SD-WAN) 111 5.3 7 VPR (SD-WAN) 115 5.3.3 9 Data Usage (SD-WAN) 115 5.3.9 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 A Configuration Restore 123 6.1.2 Configuration Restore 123 6.1.3 Schedule Backup 124 6.1.4 Device Rebotot 123 6.1.5 Schedule Poster 138 6.1.5 Schedule Profile 138 6.1.5 Schedule Profile 138 6.1.6 Schedule Profile 138 6.1.7 File Manager 135 6.2.1 Report Tasks (Deprecated) 151 6.3.2 (Peport Tasks (Deprecated) 151 6.3.2 (Peport Tasks (Deprecated) 152 6.3.1 Global Parameters 152 6.3.2 (Peport Tasks (Deprecated) 153 6.3.3 (Che Keep Parameters 152 6.3.4 (Network Management 166 6.4.4 Service Management 166 6.4.4 Service Management 164		0	
5.37 VPN (SD-WAN) 111 5.39 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 Maintenance 120 6.1 Maintenance 120 6.1 A Schedule Backup 121 6.1.2 Schedule Backup 121 6.1.3 Firmware Upgrade 123 6.1.4 Schedule Porlie 133 6.1.5 System Password Reset 133 6.1.5 System Password Reset 134 6.1.6 Schedule Prolie 138 6.1.7 File Manager 139 6.1.8 Activation 141 6.2 Report Tasks (Deprecated) 151 6.3 CPE Set Parameters 152 6.3 CPE Set Parameters 152 6.3.3 CPE Set Parameters 152 6.3 A Henwork Amagement 167			
5.33 VolP (SD-WAN) 115 5.34 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 A Incheduled Backup 121 6.1.1 Scheduled Backup 123 6.1.2 Configuration Restore 123 6.1.3 Scheduled Forfile 133 6.1.5 Schedule Forfile 133 6.1.6 Schedule Forfile 138 6.1.7 Schedule Torfile 138 6.1.8 Bach Activation 141 6.2 Report Tasks 145 6.2.1 Report Tasks (Deprecated) 151 6.3 Forkioning 152 6.3.3 CPE Keep Parameters 158 6.3.4 Detwork Management 166 6.4.2 Service Management 166 6.4.3 Scheup Darameters 163 6.4.4 Network & Service Management 166 6.5.4 Activation 164 6.5.3 Stystem Parameter 168 6.4.4 Network Management 166 6.4.2 Service Management 166 6.4.3 Evrice Management 167 6.5.4 Access Control			
5.3.9 Data Usage (SD-WAN) 116 5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 Maintenance 121 6.1.1 Schedlued Backup 121 6.1.2 Schedlued Backup 122 6.1.3 Firmware Upgrade 123 6.1.4 Schedlued Backup 123 6.1.5 System Password Reset 126 6.1.5 System Password Reset 128 6.1.7 Fire Marager 139 6.1.8 Batch Activation 141 6.2 Reports 145 6.2.1 Report Tasks 145 6.2.1 Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.2 CPE Set Parameters 152 6.3.2 CPE Set Parameters 158 6.3.2 CPE Set Parameters 158 6.3.4 Firmware Upgrade 163 6.4.1 Network Management 166 6.4.2 Service Management 166 6.5.3 External Monitoring Server 193 6.5.4 Creps Carinone 179 6.5.5 Storage Management <t< td=""><td></td><td></td><td></td></t<>			
5.4 Configuration Menu for SD-WAN CPE 117 Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 All Device Rebord 121 6.1.2 Configuration Restore 123 6.1.3 Extendued Backup 121 6.1.4 Device Rebord 123 6.1.5 System Password Reset 133 6.1.6 System Password Reset 136 6.1.6 System Password Reset 136 6.1.7 File Manager 139 6.1.8 Activation 141 6.2 Report Tasks 145 6.2.1 Report Tasks (Deprecated) 151 6.3.2 Legacy Report Tasks (Deprecated) 152 6.3.3 CPE Keep Parameters 152 6.3.4 Firmware Ugrade 163 6.4.1 Network Management 166 6.4.2 Service Management 177 6.5.3 System Parameter 138 6.5.1 System Parameter 139 6.5.4 Arrows of Management 160 6.5.2 Language 129 6.5.3 Storage Management 129 6.5.4 Storage Management 127 6.5.5 Storage M			
Part III 119 Chapter 6 System Menu 120 6.1 Maintenance 120 6.1 Maintenance 120 6.1.1 Schedüled Backup 121 6.1.2 Schedüled Backup 122 6.1.3 Firmware Upgrade 129 6.1.4 Device Reboot 133 6.1.5 System Password Reset 136 6.1.6 Schedüle Forlie 138 6.1.7 File Manager 139 6.1.8 Bach Activation 141 6.2 Reports 145 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 158 6.3.4 Firmware Upgrade 163 6.4 Network Management 167 6.4.1 Network Management 166 6.4.2 Service Management 168 6.5.1 System Parameter 199 6.5.3 CPE set Parameters 193 6.5.4 System Parameter 194 6.5.5 Storage Management 167 6.4.1 Network Management 166 <			
Chapter 6 System Menu 120 6.1 Maintenance 120 6.1.1 Schedule Backup. 121 6.1.2 Orifiguration Restore 125 6.1.3 Firmware Upgrade 129 6.1.4 Device Reboot 133 6.1.5 System Password Reset 136 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2 Report Tasks 145 6.2.1 Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.1 Origo Reset 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 152 6.3.4 Device Management 166 6.4.2 Service Management 166 6.4.2 Service Management 177 6.5 System Parameter 193 6.5.4 Centrol Monitoring Server 193 6.5.5 Upload Serial Number 200 6.5.6 Upload Serial Number 203 6.5.7 System 225 6.5.8 Gertificate 203 6.5.9 Backup Database 203 6.5.1 Sorge Management 219 </td <td></td> <td>5.4 Configuration Menu for SD-WAN CPE</td> <td>117</td>		5.4 Configuration Menu for SD-WAN CPE	117
6.1 Maintenance 120 6.1.1 Scheduled Backup. 121 6.1.2 Grüguration Restore 123 6.1.3 Firmware Upgrade. 129 6.1.4 Device Reboot 133 6.1.5 System Password Reset 136 6.1.6 Schedule Profile 138 6.1.7 Eine Manager 139 6.1.8 Eatch Activation 141 6.2 Report Tasks 145 6.2.1 Report Tasks (Deprecated). 151 6.3 Provisioning. 152 6.3 Provisioning. 152 6.3 A Provisioning. 152 6.3 CPE Keep Parameters. 156 6.3.3 CPE Set Parameters. 156 6.3.4 Deviork Management. 166 6.4.2 Service Management. 167 6.4.1 Network & Service Management. 177 6.5 System 138 6.5.1 System Parameter 139 6.5.4 Certral Monitoring Server. 139 6.5.5 Vorage Management. 177 6.5.5 Upload Serial Number. 200 6.5.6 Varie Management. 179 6.5.7 Sorage Management. 179 6.5.6 Upload Serial	Part III		119
6.1.1 Scheduled Backup. 121 6.1.2 Configuration Restore 125 6.1.3 Firmware Upgrade 129 6.1.4 Device Rebot. 133 6.1.5 System Password Reset 133 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation. 141 6.2 Reports 145 6.2.1 Report Tasks (Deprecated) 151 6.3.1 Global Parameters 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 156 6.3.3 CPE Keep Parameters 156 6.3.4 Firmware Upgrade 166 6.4.1 Network Management 166 6.4.2 Lenguage 176 6.5.1 System Parameter 178 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Actess Control 194 6.5.5 Storage Management 129 6.5.6 Language 220 6.5.7 API Key 220	Chapter	6 System Menu	120
6.1.1 Scheduled Backup. 121 6.1.2 Configuration Restore 125 6.1.3 Firmware Upgrade 129 6.1.4 Device Rebot. 133 6.1.5 System Password Reset 133 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation. 141 6.2 Reports 145 6.2.1 Report Tasks (Deprecated) 151 6.3.1 Global Parameters 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 156 6.3.3 CPE Keep Parameters 156 6.3.4 Firmware Upgrade 166 6.4.1 Network Management 166 6.4.2 Lenguage 176 6.5.1 System Parameter 178 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Actess Control 194 6.5.5 Storage Management 129 6.5.6 Language 220 6.5.7 API Key 220		6.1 Maintenance	120
6.1.2 Configuration Restore 125 6.1.3 Firmware Upgrade 129 6.1.4 Device Reboot 133 6.1.5 System Password Reset 136 6.1.5 System Password Reset 136 6.1.5 System Password Reset 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2 Reports 145 6.2.1 Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.3 CPE Keep Parameters 158 6.3.3 CPE Keep Parameters 168 6.3.4 Crimware Upgrade 163 6.4 Network & Service Management 167 6.4 Network Management 167 6.4.2 Service Management 177 6.5.5 Storage Management 178 6.5.4 Access Control 194 6.5.5 Storage Management 193 6.5.4 Access Control 194 6.5.5 Storage Management 200 6.5.7 API Key 200 6.5.7 API Key 202 6.5.6 Access Control 214 6.5.10 Login Bulletin 214 6.5.11 Login Bulletin <t< td=""><td></td><td></td><td></td></t<>			
6.1.3 Firmware Upgrade 129 6.1.4 Device Reboot 133 6.1.5 System Password Reset 136 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2 Report S 145 6.2.1 Report Tasks (Deprecated) 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 I Global Parameters 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 163 6.3.4 Firmware Upgrade 163 6.4.1 Network & Service Management 167 6.4.1 Network Management 177 6.5.5 Storage Management 178 6.5.5 Storage Management 199 6.5.5 Storage Management 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Storage Management 204 6.5.10 Login Bulletin 214 6.5.2 Language 223 6.5.3 External Monitoring Server 203 6.5.4 Certificate 203 6.5.5 I Delegit			
6.1.4 Device Reboot. 133 6.1.5 System Password Reset 136 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation. 141 6.2 Reports 145 6.2.1 Legary Report Tasks 145 6.2.2 Legary Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.3 CPE See Parameters 152 6.3.4 Firmware Upgrade 163 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 166 6.4.2 Service Management 177 6.5 System 188 6.5.1 System Parameter 189 6.5.1 System Parameter 193 6.5.4 Access Control 194 6.5.5 System Parameter 193 6.5.4 Access Control 194 6.5.5 Upload Serial Number 200 6.5.1 System Parameter 203 6.5.3 Packup Database 203 6.5.4 Access Control 194 6.5.5 Upload Serial Number 203 6.5.6 Upload Serial Number 203 6.5.11 Adverts Carousel		-	
6.1.5 System Password Reset 136 6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2.8 Ports 145 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3.1 Global Parameters 152 6.3.1 Global Parameters 152 6.3.2 CPE Ste Parameters 152 6.3.3 CPE Keep Parameters 152 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 166 6.4.2 Service Management 166 6.4.2 Service Management 177 6.5 System 193 6.5.1 System Parameter 193 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 193 6.5.6 Cupload Serial Number 200 6.5.7 API Key 202 6.5.8 Cupload Serial Number 203 6.5.9 Backup Database 209 6.5.11 Adverts Carousel 218 6.5.12 App Server 227 6.5.13 MMPP Profile <td></td> <td></td> <td></td>			
6.1.6 Schedule Profile 138 6.1.7 File Manager 139 6.1.8 Batch Activation 141 6.2 Report 145 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3 (Global Parameters 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 158 6.3.4 Firmware Upgrade 163 6.4.4 Network & Service Management 167 6.4.1 Network Management 167 6.4.1 Network Management 177 6.5.2 Language 193 6.5.1 System 193 6.5.2 Language 193 6.5.4 Access Control 194 6.5.5 Upload Serial Number 200 6.5.6 Upload Serial Number 203 6.5.7 API Key 203 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.11 Adverts Carousel 214 6.5.12 Logn Sultein 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 </td <td></td> <td></td> <td></td>			
6.17 File Manager 133 6.1.8 Batch Activation 141 6.2 Reports 145 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 158 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network Management 168 6.5.4 System 177 6.5 System 178 6.5.5 System Parameter 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server. 193 6.5.4 Storage Management 194 6.5.5 Storage Management 200 6.5.7 Storage Management 201 6.5.5 Storage Management 202 6.5.6 Upload Serial Number 203 6.5.6 Storage Management 203 6.5.7 Storage Management 204 6.5.8 Certificate 203 6.5.9 Backup Database 20			
6.1.8 Batch Activation 141 6.2 Reports 145 6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 152 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 166 6.4.2 Service Management 168 6.5.3 System 183 6.5.4 Access Control 194 6.5.3 Storage Management 199 6.5.4 Access Control 194 6.5.5 Storage Management 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 <			
6.2 Report Jasks 145 6.2.1 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 152 6.3.3 CPE Keep Parameters 156 6.3.3 CPE Keep Parameters 166 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network Management 166 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Corrol 194 6.5.5 Storage Management 199 6.5.6 Ordonal Server 203 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 203 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.13 XMPP Profile 225 6.5.13 AMPP Profile 225 6.5.14 Server 226 6.5.10 Logs Retings 226 <td></td> <td>5</td> <td></td>		5	
6.2.1 Report Tasks 145 6.2.2 Legacy Report Tasks (Deprecated) 151 6.3.2 CPE Set Parameters 152 6.3.3 CIObal Parameters 152 6.3.3 CPE Keep Parameters 158 6.3.3 CPE Keep Parameters 162 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network Management 168 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 193 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 200 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server			
6.2.2 Legacy Report Tasks (Deprecated) 151 6.3 Provisioning 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 162 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 166 6.4.2 Service Management 166 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 183 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server 226 6.5.13 XMPP Profile 225 6.5.14 Server 226 6.5.17 License Key Pools 228 6.6 User 225			
6.3 Provisioning 152 6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 162 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network Management 168 6.4.2 Service Management 177 6.5.5 System 188 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.17 API Key 227 6.5.17 License Key Pools 228 6.6 User 225 6.5.14 Server Support Settings 226 6.5.17 License Key Pools 228 6.6.2 Group Management 235			
6.3.1 Global Parameters 152 6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 152 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network & Service Management 167 6.4.1 Network & Service Management 168 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Storage Server 225 6.5.14 Server Support Settings 226 6.5.15 Detet Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6.1 User Management 235 6.6.2 Group			
6.3.2 CPE Set Parameters 158 6.3.3 CPE Keep Parameters 162 6.3.4 Firmware Upgrade 163 6.4 Network & Service Management 167 6.4.1 Network Management 168 6.4.2 Service Management 168 6.4.1 Network Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Login Bulletin 214 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 Delete Logs Actions 227 6.5.18 App Server 227 6.5.19 Augement 235			
6.3.3 CPE Keep Parameters. 162 6.3.4 Firmware Upgrade. 163 6.4 Network & Service Management. 167 6.4.1 Network Management. 168 6.4.2 Service Management. 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server. 193 6.5.4 Access Control. 194 6.5.5 Storage Management. 199 6.5.6 Upload Serial Number. 200 6.5.7 API Key. 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin. 214 6.5.12 Logs. 223 6.5.13 Super Scrupsel. 224 6.5.14 Server Support Settings. 225 6.5.14 Server Support Settings. 227 6.5.15 Delete Logs Actions 227 6.5.16 App Server. 228 6.6.1 User Management. 235 6.6.2 Group Management. 235 6.6.1 User Management. 235 6.6.2 Group Management. 235 6.6.3 Network Group. <td></td> <td>6.3.1 Global Parameters</td> <td>152</td>		6.3.1 Global Parameters	152
6.3.4 Firmware Upgrade. 163 6.4 Network & Service Management 167 6.4.1 Network Management 168 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 183 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Contol 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.3 Network Group. 243 6.6.4 User 235 6.6.5 User Management 235 6.6.6 User 235		6.3.2 CPE Set Parameters	158
6.4 Network & Service Management 167 6.4.1 Network Management 168 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Cupage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6.1 User Management 233 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 2		6.3.3 CPE Keep Parameters	162
6.4.1 Network Management 168 6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.17 License Key Pools 228 6.6.1 User Management 235 6.6.1 User Management 235 6.6.1 User Management 235 6.6.2 String Server 232 6.6.3 Network Group 243 6.6.4 External Authentication Server 243 6.6.4 External Authentication Server 243 6.6.4 SMS Server 252 6.6.6 Function Management 252		6.3.4 Firmware Upgrade	163
6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 KMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 249 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Wail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 252 6.6.8 SMS Server 262 </td <td></td> <td>6.4 Network & Service Management</td> <td>167</td>		6.4 Network & Service Management	167
6.4.2 Service Management 177 6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 KMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 249 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Wail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 252 6.6.8 SMS Server 262 </td <td></td> <td>6.4.1 Network Management</td> <td>168</td>		6.4.1 Network Management	168
6.5 System 183 6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 225 6.5.13 XMPP Profile 225 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.4 External Authentication Server 249 6.6.5 Kail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.1 System Parameter 184 6.5.2 Language 192 6.5.3 External Monitoring Server 193 6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.11 Adverts Carousel 214 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.15 Delete Logs Actions 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.6 Function Management 252 6.6.6 Function Management 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 25			
6.5.2 Language 192 6.5.3 External Monitoring Server. 193 6.5.4 Access Control 194 6.5.5 Storage Management. 199 6.5.6 Upload Serial Number. 200 6.5.7 API Key. 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 225 6.6.6 Function Management 255 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 258 6.6.8 SMS Server 258		-	
6.5.3 External Monitoring Server. 193 6.5.4 Access Control 194 6.5.5 Storage Management. 199 6.5.6 Upload Serial Number. 200 6.5.7 API Key. 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 225 6.5.13 Ever Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.3 Network Group. 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Mil Server 252 6.6.7 Wholesale Wizard. 258 6.6.8 SMS Server 258 6.6.8 SMS Server 258			
6.5.4 Access Control 194 6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 225 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.3 Network Group 249 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Nail Server 252 6.6.6 Noil Server 252 6.6.6 Twholesale Wizard 258 6.6.8 SMS Server 258 6.6.8 SMS Server 262			
6.5.5 Storage Management 199 6.5.6 Upload Serial Number 200 6.5.7 API Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 235 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 252 6.6.8 SMS Server 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.6 Upload Serial Number. 200 6.5.7 API Key. 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group. 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 258			
6.5.7 ÅP Key 202 6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 249 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 258			
6.5.8 Certificate 203 6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.9 Backup Database 209 6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 225 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.10 Login Bulletin 214 6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.11 Adverts Carousel 218 6.5.12 Logs 223 6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.12 Logs			
6.5.13 XMPP Profile 225 6.5.14 Server Support Settings 226 6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.14 Server Support Settings2266.5.15 Delete Logs Actions2276.5.16 App Server2276.5.17 License Key Pools2286.6 User2356.6.1 User Management2356.6.2 Group Management2436.6.3 Network Group2496.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.8 SMS Server262			
6.5.15 Delete Logs Actions 227 6.5.16 App Server 227 6.5.17 License Key Pools 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.16 App Server 227 6.5.17 License Key Pools. 228 6.6 User 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 252 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.5.17 License Key Pools. 228 6.6 User. 235 6.6.1 User Management 235 6.6.2 Group Management 243 6.6.3 Network Group. 249 6.6.4 External Authentication Server 249 6.6.5 Mail Server 252 6.6.6 Function Management 256 6.6.7 Wholesale Wizard. 258 6.6.8 SMS Server 262		-	
6.6 User2356.6.1 User Management2356.6.2 Group Management2436.6.3 Network Group2496.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.5.16 App Server	227
6.6.1 User Management2356.6.2 Group Management2436.6.3 Network Group2496.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.5.17 License Key Pools	228
6.6.2 Group Management2436.6.3 Network Group2496.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.6 User	235
6.6.3 Network Group2496.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.6.1 User Management	235
6.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.6.2 Group Management	243
6.6.4 External Authentication Server2496.6.5 Mail Server2526.6.6 Function Management2566.6.7 Wholesale Wizard2586.6.8 SMS Server262		6.6.3 Network Group	249
6.6.5 Mail Server 252 6.6.6 Function Management 256 6.6.7 Wholesale Wizard 258 6.6.8 SMS Server 262			
6.6.7 Wholesale Wizard			
6.6.7 Wholesale Wizard		6.6.6 Function Management	256
6.6.8 SMS Server			

6.6.11 Syslog Server	
6.6.12 Group Parameter	
6.6.13 Link with Router App	
6.7 About VigorACS	
6.7.1 Software Information	
6.7.2 License Information	
6.7.3 License Mail Notify	
6.7.4 License Agreements	
6.7.5 System Resource Notify	
Applications	
A.1 How to Create a Provision Profile with Global Parameters?	
A.2 How to Modify Provision Profile with Global Parameters?	
A.3 How to Create a Network for Managing Devices?	
A.4 How to Change the Network of a Device?	
A.5 How to Add a User?	
A.6 How to Add a Group?	
	200
Part IV	201
Falliv	
Chapter 7 Root Network Menu	
7.1 Dashboard for the Root Network	
7.2 Monitoring	
7.2.1 Alarm	
7.2.2 Logs	
7.2.3 Devices	
7.2.4 Cellular Data Usage	
7.2.5 Floor Plan	298
7.3 Configuration	
7.3.1 VPN Wizard	
7.3.2 AP Profile	
Chapter 8 Network Group Menu	300
8.1 Dashboard for the Network Group	300
o. i Dashbuaru fur the Network Group	
·	
8.2 Statistics for Network Group	
8.2 Statistics for Network Group 8.3 Monitoring for Network Group	
8.2 Statistics for Network Group 8.3 Monitoring for Network Group 8.3.1 Alarm	
8.2 Statistics for Network Group 8.3 Monitoring for Network Group 8.3.1 Alarm 8.3.2 Logs	
 8.2 Statistics for Network Group 8.3 Monitoring for Network Group 8.3.1 Alarm 8.3.2 Logs 8.3.3 Devices 	
8.2 Statistics for Network Group 8.3 Monitoring for Network Group 8.3.1 Alarm 8.3.2 Logs 8.3.3 Devices 8.3.4 Clients	
 8.2 Statistics for Network Group 8.3 Monitoring for Network Group 8.3.1 Alarm 8.3.2 Logs 8.3.3 Devices 8.3.4 Clients	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 328 329 320 321 322 323 324 325 326 327 330 331 336 337 339 339 348
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 328 329 320 321 322 323 324 325 326 327 330 331 336 337 339 348 350
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 328 329 320 321 322 323 324 325 326 327 320 321 322 323 324 325 326 327 328 329 348 350 351
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 320 321 322 323 325 326 327 330 331 336 337 339 348 350 351 355
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 336 337 339 348 350 351 355 356
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 336 337 339 348 350 351 355 356
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 330 331 336 337 339 348 350 351 356 356
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 330 331 336 337 339 348 350 351 356 356
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 336 337 339 348 350 351 356 356 357
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 330 331 336 337 339 348 350 351 356 356 357
 8.2 Statistics for Network Group	311 312 313 314 315 316 317 318 323 325 326 327 320 321 322 323 324 325 326 327 330 331 336 337 339 348 350 351 356 356 356 357 358

	9.2 Statistics for CPE	. 359
	9.3 Monitoring	. 360
	9.3.1 Alarm	. 360
	9.3.2 Logs	. 361
	9.4 Configuration	. 362
	9.4.1 WAN	. 364
	9.4.2 LAN	. 381
	9.4.3 Hotspot Web Portal	. 393
	9.4.4 Routing	. 408
	9.4.5 NAT	. 415
	9.4.6 Hardware Acceleration	. 421
	9.4.7 Firewall	. 422
	9.4.8 User Management	. 437
	9.4.9 Object Setting	
	9.4.10 QoS	. 460
	9.4.11 Applications	. 466
	9.4.12 VPN	. 487
	9.4.13 Mesh	. 505
	9.4.14 Wireless LAN	. 508
	9.4.15 Bandwidth Management	. 523
	9.4.16 USB Applications	. 528
	9.4.17 System	. 533
	9.4.18 Switch	. 551
	9.5 Advanced	. 562
	9.5.1 Parameter Tree	. 562
	9.5.2 Exclude Parameter	. 563
	9.5.3 Common UI Status	. 564
	9.5.4 Test Inform	. 564
Chapte	r 10 DrayTek Chatbot	. 567
	10.1 Installation	. 567
	10.2 Overview	



ACC?

Chapter 1 Introduction

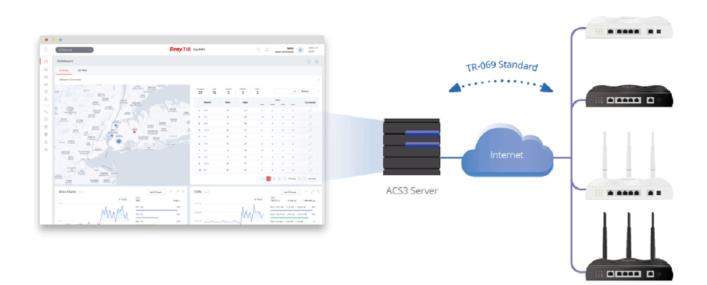
VigorACS 3 is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway, wireless AP and switch. VigorACS 3 has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore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

1.1 Main Features and Benefit

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

1.2 System Architecture

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



1.3 Web Service

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

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

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

Corresponding files are placed in -WebServices_TR069API.zip

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

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

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

This page is left blank.

Chapter 2 Install & Startup

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

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

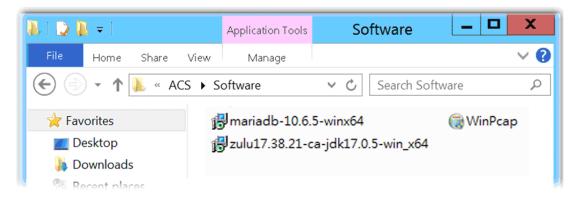
2.1 Platform for Windows 10, 11

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

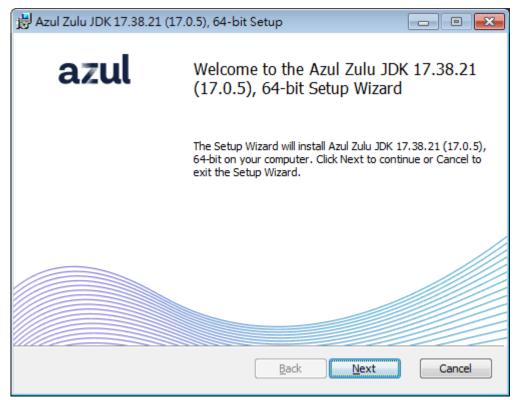
- (I) Installation for Java,
- (II) Installation for MariaDB
- (III) Installation for VigorACS 3
- (IV) Start MySQL/MariaDB Database.
- (V) Edit VigorACS ip.
- (VI) Start VigorACS.

2.1.1 Installation for Java

1. Install Java by clicking "zulu-17.38.21-ca-jdk-17.0.12-.win_x64" (or later) to execute the installation.



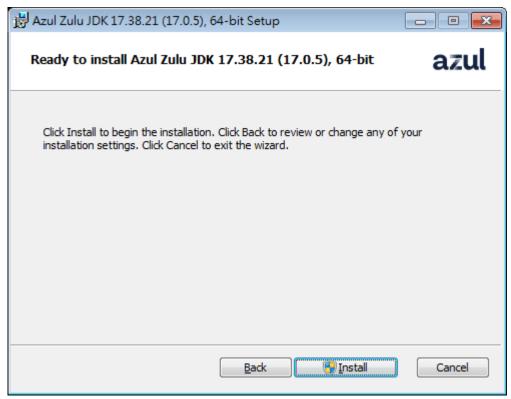
2. The first page will be shown as follows. Click Next to get into next page.



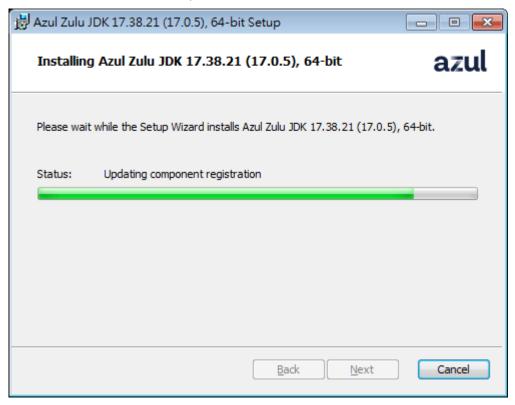
3. In this page, optional features will be listed for you to specify the destination folder for JAVA driver installation. Choose the one you need and click Next.

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

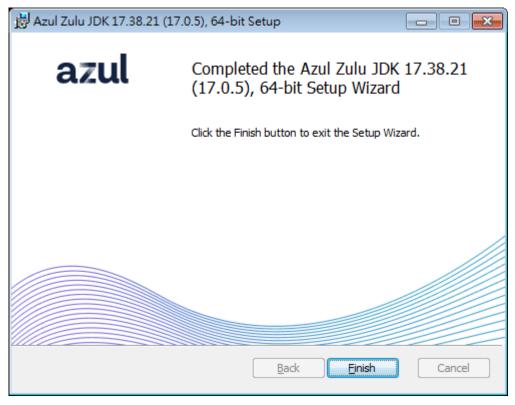
4. In the following page, just click Install.



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

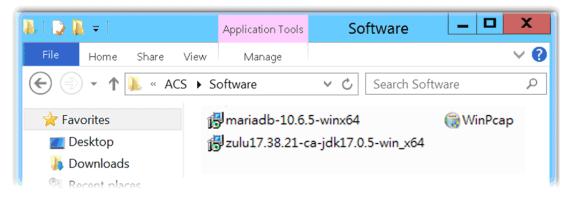


6. When the following page appears, the installation is completed. Click Finish to exit the installing program.

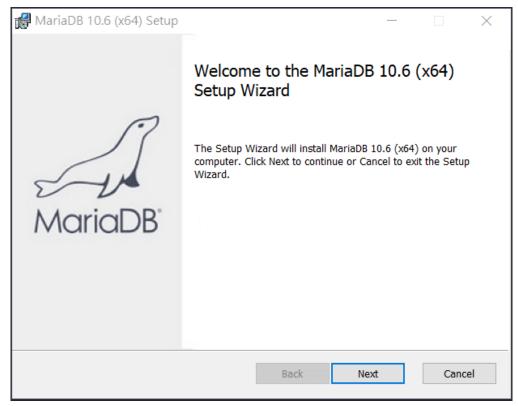


2.1.2 Installation for MariaDB

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



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



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

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

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

🖟 MariaDB 10.6 (x64) Setup	- 🗆 X		
Custom Setup Select the way you want features to be in:	stalled. MariaDB		
Click the icons in the tree below to change the way features will be installed.			
✓ MariaDB Server ✓ Database instance ✓ Client Programs ✓ Backup utilities ✓ Development Components ✓ Third party tools ✓ HeidiSQL	Install server This feature requires 143MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 72MB on your hard drive.		
Location: C:\Program Files\MariaDB 10.6\ Browse			
Reset Disk Usage	Back Next Cancel		

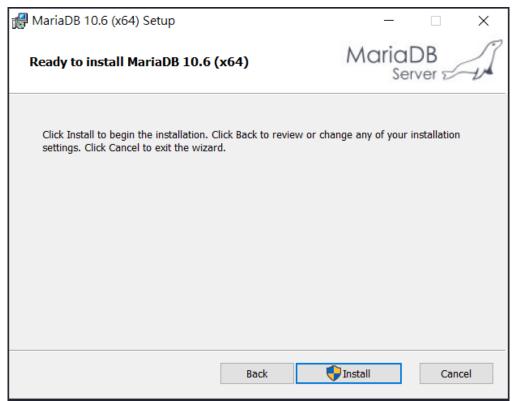
5. If you want to configure password for MariaDB server, please check Modify password... and enter the password. It depends on your request. Otherwise, simply click Next.

🖟 User settings	– 🗆 X
Default instance properties MariaDB 10.6 (x64) database configuration	MariaDB Server
Modify password for database user 'root' New root password:	7
Confirm:	Enter new root password Retype the password pr 'root'
User	
	Back Next Cancel

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

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

7. On this dialog box, click Install.



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

🕼 MariaDB 10.6 (x64) Setup	_		×
Installing MariaDB 10.6 (x64)	Maria Ser	DB ver 🗹	A
Please wait while the Setup Wizard installs MariaDB 10.6 (x64).			
Status: Updating component registration			
Back	Next	Can	cel
Duck	11070	Call	

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

🕷 MariaDB 10.6 (x64) Setup	- I X
	Completed the MariaDB 10.6 (x64) Setup Wizard
MariaDB'	Click the Finish button to exit the Setup Wizard.
	Back Finish Cancel

2.1.3 Installation for VigorACS 3

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

1. Click Setup to run VigorACS 3 setup wizard.

📜 ⊋ 🛄 =	ACS		_ D X
File Home Share	View		~ ?
🗲 🕘 🗸 🖡 🖌	CS > ACS	✓ Ċ Search	ACS \wp
쑫 Favorites	Name	•	Date modi
🗾 Desktop 퉩 Downloads	🕵 setup		6/17/201 6
🐉 Recent places			

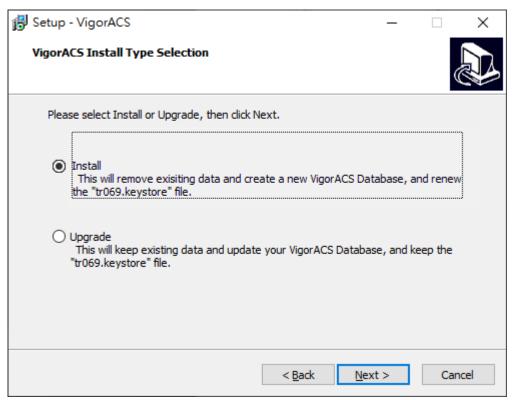
2. When the following dialog appears, choose Local Database / Remote Database and click Next.

🔂 Setup - VigorACS	_		×
Database Access Type Selection			Ð
Please select Local Database if you want to update or install the TF the local MySQL, or select Remote Database if the MySQL databas host. You will be asked for the connection details later.			
Choose the one you need, and click Next.			
Local Database			
 Remote Database * Connect to an existed database after finishing the installat 	ion proced	dure.	
Ne	xt >	Car	ncel

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

🔂 Setup - VigorACS	_		\times
Select MySQL/MariaDB Install Path		0	
Please specify the installation folder of MySQL/MariaDB and then did	Next	outton.	
C:\Program Files\MariaDB 10.6	B	owse	
5			
10			
< <u>B</u> ack <u>N</u> ext	>	Can	cel

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



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

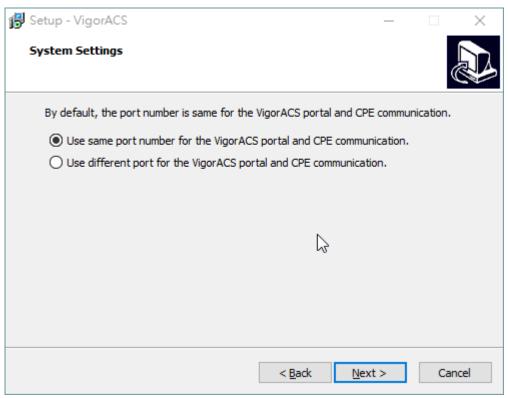
🔀 Setup - VigorACS	– 🗆 X
MySQL/MariaDB Account Setting	
<u>_</u>	
Please specify password of root of MySQL/ MySQL/MariaDB database has not been cor	MariaDB, this step can be ignored if nfigured.
root password	
••••	
confirm root password	
••••	
	_Check password
	< <u>B</u> ack <u>N</u> ext > Cancel
🔀 Setup - VigorACS	– 🗆 ×
The VigorServiceController Install Path	
	C
Folder	
C:\supervisord	Browse
	bjonse
	\searrow
	< Back Next > Cancel

6. Then select InfluxDB v1 or v2 and click Next.

🔂 Setup - VigorACS		-		×
Time-Series Database What Is Your Time-Series Database?				
Please select InfluxDB v1 or InfluxDB v2, t O InfluxDB v1	hen dick Next.			
○ InfluxDB v2				
	< Back	Next >	Ca	ncel
😽 Setup - VigorACS		-		×
The InfluxDB Install Path as below			Q	
dick Next button.				
<mark>C:\influxdb</mark>			Browse	
	< Back	Next >	Can	icel

the Inf	
	luxDB Install Path as below
dick 1	Next button.
etup	
4	If you upgrade the ACS (from the version before 2.4.0) for the first time, please remember to run the rrd2influxdb tool to convert the existed/old data after ACS upgrade. It will on the Your_VigorACS\convert_rrd2_Influxdb\ path.For more explanation, you may refer the Your_VigorACS\bin\acs_util\convert_rrd2_Influxdb\readme.txt document.
	確定
	< <u>B</u> ack <u>N</u> ext > Cancel
Setup -	VigorACS —
	3
	is your maximum and minimum memory?
What	m And Minimum Memory
What Please Maxim	is your maximum and minimum memory?
What Please Maxim	Im And Minimum Memory is your maximum and minimum memory?
What Please Maxim (Defai 1024 Minimu	Im And Minimum Memory is your maximum and minimum memory?
What Please Maxim (Defai 1024 Minimu (Defai	Im And Minimum Memory is your maximum and minimum memory? e specify your maximum and minimum memory, then click Next. num Memory: ult maximum memory is 1024MB) um Memory:
What Please Maxim (Defai 1024 Minimu (Defai	Im And Minimum Memory is your maximum and minimum memory? e specify your maximum and minimum memory, then click Next. num Memory: ult maximum memory is 1024MB) um Memory:
What Please Maxim (Defai 1024 Minimu (Defai	Im And Minimum Memory is your maximum and minimum memory? e specify your maximum and minimum memory, then click Next. num Memory: ult maximum memory is 1024MB) um Memory:
What Please Maxim (Defai 1024 Minimu (Defai	Im And Minimum Memory is your maximum and minimum memory? e specify your maximum and minimum memory, then click Next. num Memory: ult maximum memory is 1024MB) um Memory:

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



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

🔀 Setup - VigorACS		
HTTP And HTTPS Port What is your HTTP and HTTPS port?		
Please specify your HTTP and HTTPS port, then click Next.		
HTTP Port:		
80		
HTTPS Port:		
443		
HTTPS Chatbot Port:		
18443		
< <u>B</u> ack	<u>N</u> ext >	Cancel

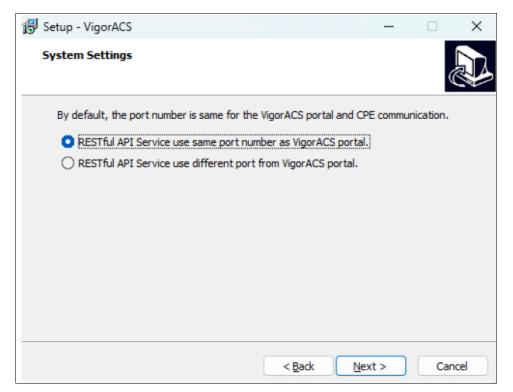
9. Click Next to enter the STUN Port, Syslog Port and the Netflow Port. Default values are 3478, 514 and 20314.

🛃 Setup - VigorACS	_	
Netflow, STUN And Syslog Port What is your Netflow, STUN and Syslog port?		
Please specify your Netflow, STUN and Syslog port, then click Next.		
STUN Port:		
3478		
Syslog Port:		
514		
Netflow Port:		
T.		
< <u>B</u> ack <u>N</u> ext	:>	Cancel

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

10. Specify the server domain.

🛃 Setup - VigorACS		_	
Server Domain What is your server domain?			
Please specify your server domain.			
Server Domain:			
acs.draytek.com			
	5		
	< <u>B</u> ack <u>N</u> ex	t >	Cancel



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

🛃 Setup - VigorACS	_		\times
JBoss Configuration Selection The JBoss configuration which VigorACS used for Web and CPE co	ommunicatio	on.	
For enhanced security select TLS 1.3 (standalone-secure.xml) For security and compatibility with existing CPEs we recommend T (standalone.xml) For compatibility with older legacy CPEs use TLS 1.0 (standalone- Choose the one you need, then click Next.		.xml)	
 standalone-secure.xml * Supported Protocols: TLS 1.3 only standalone.xml (Recommended) * Supported Protocols: TLS 1.2 only standalone-compatible.xml * Supported Protocols: TLS 1.0 or above 			
< <u>B</u> ack	lext >	Ca	ancel

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

🛃 Setup - VigorACS	_	
Select Vigoracs user home path		
Please specify the installation folder of Vigoracs user home and then This folder is for storing the statistics and configurations	click Ne	ext button.
C: \Users\User\AppData\Roaming	В	rowse
2		
< <u>B</u> ack <u>N</u> ext	>	Cancel

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

🔀 Setup - VigorACS	_		\times
Select Destination Location Where should VigorACS be installed?		(
Setup will install VigorACS into the following folder.			
To continue, click Next. If you would like to select a different folder, cl	ick Bro	wse.	_
C:\Program Files\VigorACS	Br	owse	
5			
At least 998.0 MB of free disk space is required.			
< <u>B</u> ack <u>N</u> ext :	>	Car	ncel

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

🛃 Setup - VigorACS	_		×
Select Start Menu Folder Where should Setup place the program's shortcuts?			
Setup will create the program's shortcuts in the following St	art Mer	nu folder.	
To continue, click Next. If you would like to select a different folder,	click Br	owse.	
VigorACS	B	rowse	
2			
< <u>B</u> ack <u>N</u> ext	t >	Ca	ncel

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

🔀 Setup - VigorACS	_	
Select Additional Tasks Which additional tasks should be performed?		
Select the additional tasks you would like Setup to perform while insta then dick Next.	lling Vigo	orACS,
Additional shortcuts:		
Create a <u>d</u> esktop shortcut		
Other tasks:		
Allow VigorACS access through Windows Firewall (Recommended)	
Allow VigorACSChatbot access through Windows Firewall (Recom	mended)
\searrow		
< <u>B</u> ack <u>N</u> ext	>	Cancel

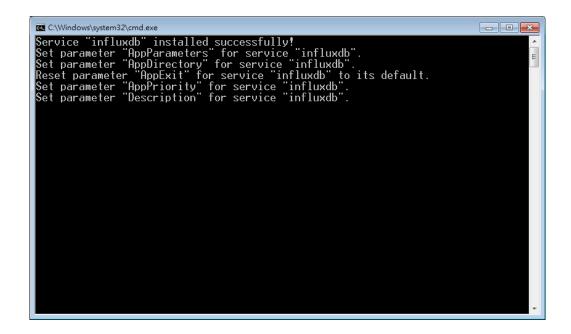
16. Now, the program is ready to install necessary features and files to your computer. Please click Install to start.

🔂 Setup - VigorACS	_		×
Ready to Install Setup is now ready to begin installing VigorACS on your computer.		¢	
Click Install to continue with the installation, or click Back if you want change any settings.	to revie	w or	
Destination location: C: \Program Files\VigorACS		^	
Start Menu folder: VigorACS			
Additional tasks: Additional shortcuts: Create a desktop shortcut Other tasks: Allow VigorACS access through Windows Firewall (Recommend	ded)		
<		>	
< <u>B</u> ack <u>I</u> nst	all	Can	icel

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

🔂 Setup - VigorACS	_		×
Installing Please wait while Setup installs VigorACS on your computer.			
Extracting files C:\Users\User\AppData\Local\Temp\is-G3GP2.tmp\supervisord\supe	rvisord.	exe	
N			
G			
		Ca	ncel

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



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



2.1.4 StartMySQL/MariaDB Database

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

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

2.1.5 Start VigorACS

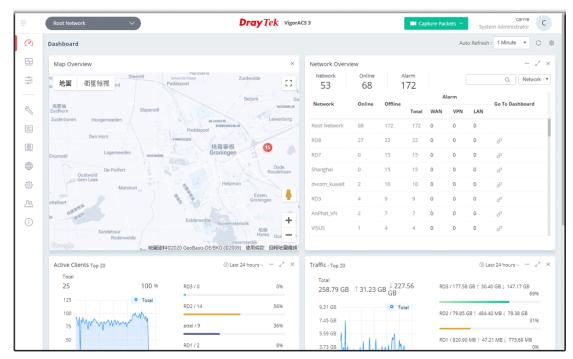
- 1. Login VigorACS. Use a web browser and enter "localhost:portnumber". Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be "localhost:8011".
- 2. The login page of VigorACS will be shown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

	@ EN
	VigorACS
	User Name root
	Password •••••••
Dray Tek	Validation Code 5817
	Remember me 5817
	Login

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

	# restriction	_	K Close Adv	ens
			\$160 T	
Warning : Your	ACS is still set to the default r	oassword. Please d	hange it ASAP	
and a second second second second second			an Se ici ai i	
root is still using the default	ACS is still set to the default p password. For security reasons, changing it is st	trongly recommended.	Change password	Cancel
root is still using the default	password. For security reasons, changing it is s	trongly recommended.	-	Cancel

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



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

2.2 Platform for Linux

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

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

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

2.2.1 Installation for MariaDB, Java and VigorACS

Follow the steps listed below to install VigorACS under Linux:

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

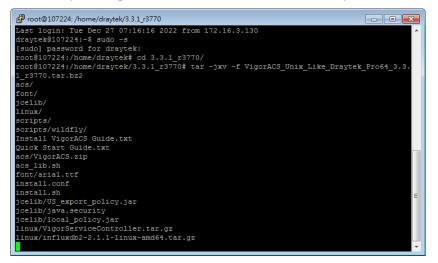
#bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2 | tar xvf -

or

#tar -jxv -f VigorACS_Unix_Like_xxxxxx_xxxx.tar.bz2

3. Decompress the setup packages

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

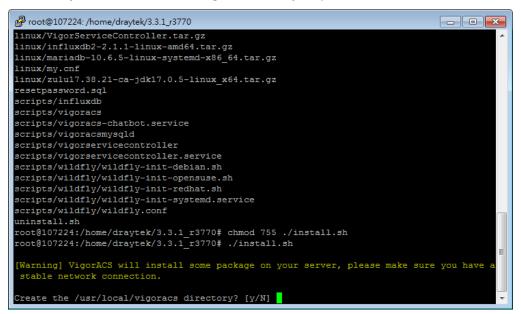


4. Change the permissions mode of install.sh and uninstall.sh.

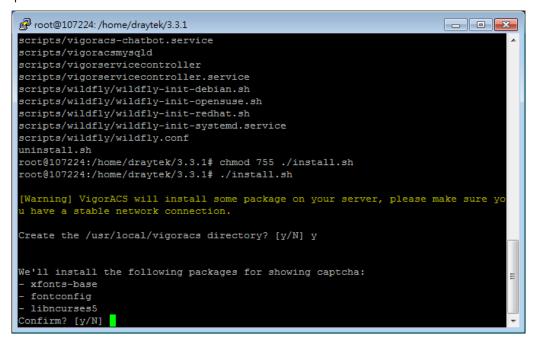
chmod 755 ./install.sh

chmod 755 ./uninstall.sh

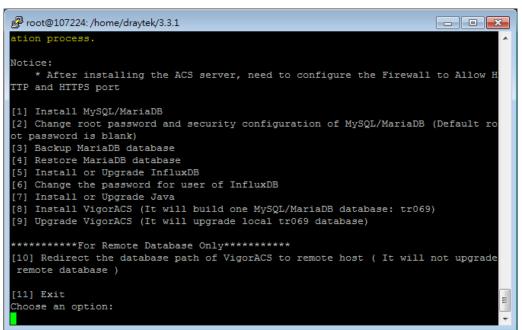
- 5. Enter "y" to execute ./install.sh installation file.
- 6. Later, the system will ask to create vigoracs, enter "y" to proceed.



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



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



- (1) Install MySQLI/MariaDB
- (2) Change root password and security configuration of MySQL/MariaDB
- (3) Backup MariaDB database
- (4) Restore MariaDB database
- (5) Install or Upgrade InfluxDB
- (6) Change the password for user of InfluxDB
- (7) Install or Upgrade Java
- (8) Install VigorACS
- (9) Upgrade VigorACS
- (10) Redirect the database path of VigorACS to remote host
- (11) Exit
- Choose an option :
- (i) If your computer has installed MariaDB and java previously, ignore the installation of them. Otherwise, install all the required items (MariaDB, Java and VigorACS) for your system. Item number 6 is used to upgrade VigorACS, so it is not necessary for you to execute for the first time of installation.
- 9. Input 1 to install MariaDB first. Notice that it will setup blank as default password. You can change the password by using the following command.

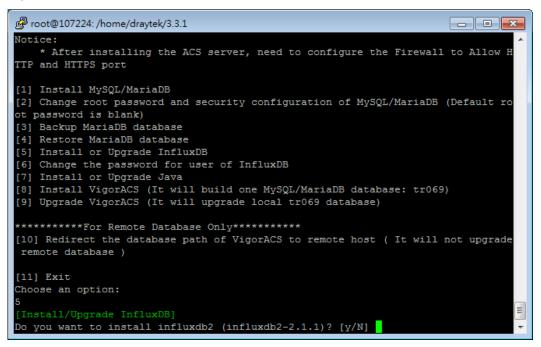
#/usr/local/mysql/bin/mysqladmin --defaults-file=/usr/local/mysql/my.cnf -u root password 'new password'

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

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

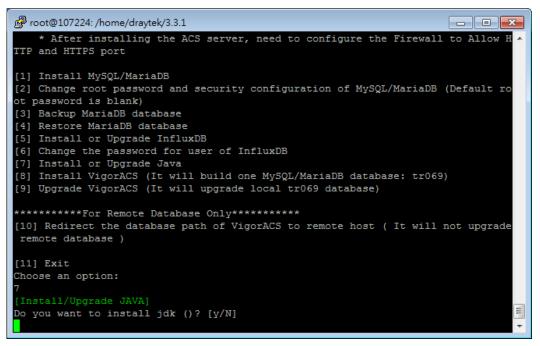
Follow the instructions on the screen to finish the MariaDB installation.

10. Input 5 to install InfluxDB.



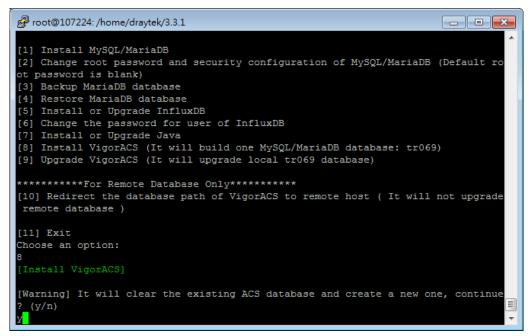
Follow the instructions on the screen to finish the InfluxDB installation.

11. Input 7 to install Java.

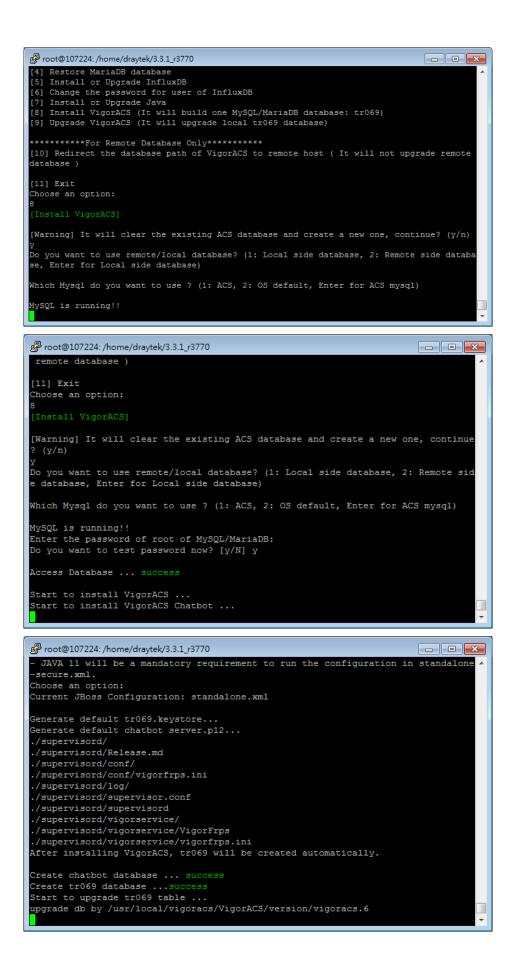


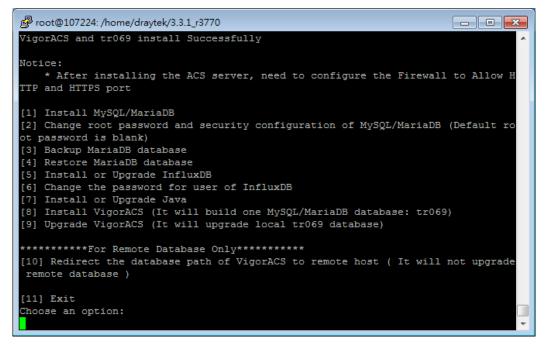
Follow the instructions on the screen to finish the Java installation.

12. Input 8 to install VigorACS. It is suggested to use ACS customized MariaDB database. When asked to enter MariaDB password, press "Enter" if you haven't changed the password via the command. Then, confirm that TR-069 database has been installed successfully.



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



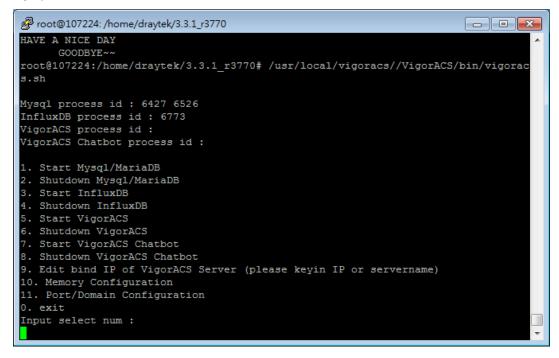


- 13. Input 11 to finish and exit the installation.
 - (i) Step 14 is required for establishing remote database only. You can ignore it while building local database.

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

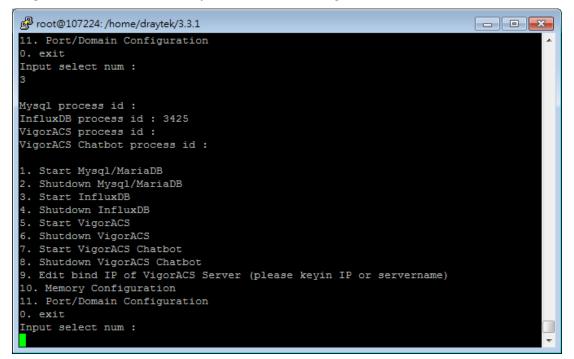
2.2.2 StartMySQL/MariaDB Databse

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



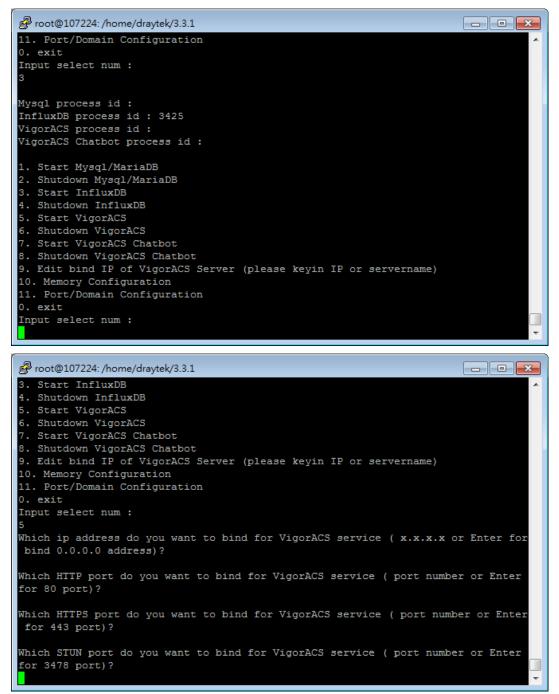
2.2.3 Start InfluxDB

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

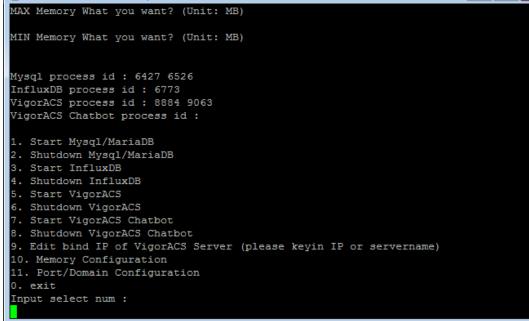


2.2.4 Start VigorACS

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



📴 root@107224: /home/draytek/3.3.1_r3770 📃 💌
bind 0.0.0.0 address)?
Which HTTP port do you want to bind for VigorACS service (port number or Enter for 80 port)?
Which HTTPS port do you want to bind for VigorACS service (port number or Enter for 443 port)?
Which STUN port do you want to bind for VigorACS service (port number or Enter for 3478 port)?
Which syslog port do you want to bind for VigorACS service (port number or Ente r for 514 port)?
Which Netflow port do you want to bind for VigorACS service (port number or Ent er for 20314 port)?
How many memory do you want to set for VigorACS service? (Enter for default MAX Memory is 1024, MIN Memory is 900 MB) MAX Memory What you want? (Unit: MB)
MIN Memory What you want? (Unit: MB)
Proot@107224: /home/draytek/3.3.1_r3770
MAX Memory What you want? (Unit: MB)

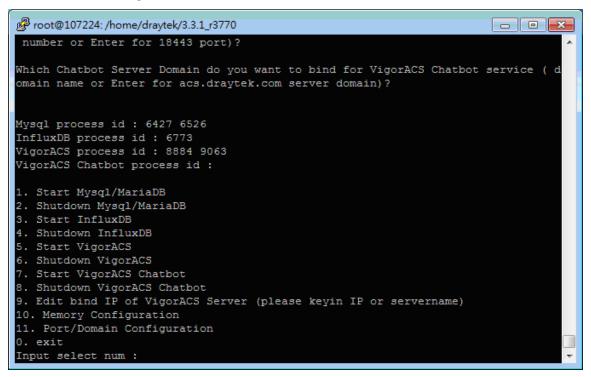


If you ever reboot the machine after installing VigorACS, just select item 1 to start mysql/mariadb first. Then, select item 5 to start VigorACS.

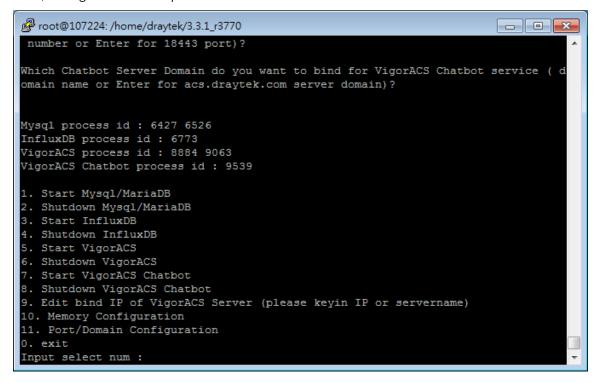
2.2.5 Start VigorACS Chatbot

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

Select item 7 to start VigorACS Chatbot.



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



2.2.6 Edit VigorACS IP

When starting the VigorACS at first time on Solaris or Linux, startup program will ask you input Server IP or input Enter key by using the IP address of the host. Once you input the IP address, VigorACS will keep it on startway.txt. Next time, if you want to change it, you can select item 9 to edit startway.txt using vi editor.

2.3 Registering VigorACS

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

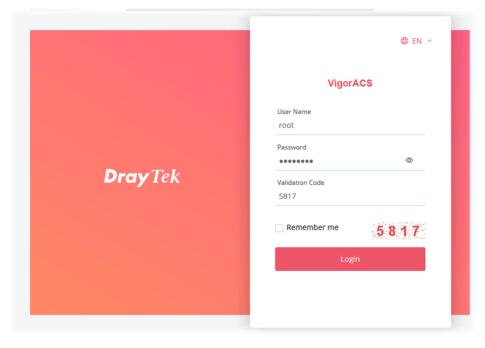
(i) While installing VigorACS, install program will register MySQL/MariaDB to Windows Service. MySQL/MariaDB will startup automatically after installing VigorACS or rebooting system. Normally, you don't need to worry about this step on Windows. But if you find any problems on VigorACS, you should check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

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

2.3.1 Registration for VigorACS via Windows Platform

Below shows the steps to register VigorACS:

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



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

	⊕ EN ∽ VigorACS
License Warning : Your license is invalid or ex Please go to license server to activate your license.	pired. root Password execute the Activate
Dray lek	Validation Code 7354 Remember me Login ()

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

Dray Tek MyVigor	ENCLURA Menturne Zarneni Password Logen Greate Account / Grit Help Greate Account / Grit Help
d Provension	Terms of Service / Protecy

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

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

		Product register (Add Device)	
	Device Name	VigorACS3_carrie	
lel	Model	VigorACS3	Ser
	MAC	ACS3200100013	
	Serial Number	AC\$3200100013	
		Cancel Submit	

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

ACS	
License Status License Action License Action Force Sync	
License History	
Today cost-or-et	
Product Registration	

7. When the following page appears, click Accept.

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

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

		A	ctiv	/ate	Lice	ense	of A	ACS 3		
> Service Status	License				Trial					
	Activate Date			202	0-01	1-31				
				Janu	ıary	2020		»		
		Su	Мо	Tu	We	Th	Fr	Sa		
								4		
			6							
				14						
							31			
					Rese	t				
	C	ancel							Next	

9. Confirm the content and click Activate.

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

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

DrayT	ek 🔤	
VigorACS License I		Þ
OPERATION 1000 : Lic	ense Key OK	ν¢
LICENSE ID 0002b097		
START DATE 2020-01-3	D	
EXPIRE DATE 2021-02-2	9	
MAX NODE 00000020		
TRIAL LICENSE No		
Login to ACS		
 Login to ACS		

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

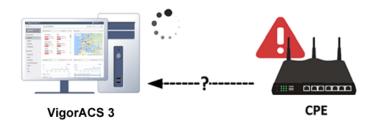
	⊕ EN ~
	VigorACS
	User Name root
	Password @
Dray Tek	Validation Code 5817
	Remember me 5.8.1.7
	Login

	1								Auto Ref	fresh : 1	Minute ~ (
Map Ove	rview		×	Network Overview							Map Overvies
	1000	Onarso	1 1	Sub Network Online 123 6	Alarm 100136						New Devices
1 - 1	J.F.	1 Ab		© Root Network	100150						Reset to deta
		(18.94)	1	Network Members	Online	Offine			area		Go To Dashboard
			- 010				Total	WAN	VPN	LAN	
3		and the second second	T: 27	0 directly-under-Root Network	0	13	13	0	0	0	
	1			F D AutoTestNetwork	1	0	2	2	0	0	0
	and monthly	and and a set of the s		@ AutoTest_Dev	1	7	7	0	0	0	P.
3-	1 9	NY IT	- mart	1 AutoTest_SB-WAN	0	2	2	0	0	0	e.
and the second				@ Autolest_VPN	1	10	0	0	0	0	0
and the second second											
USA			an man and	1 Hotspot_Web_Portal	0	2	2	0	0	0	0
UI BA UI FU GK 11	Tuisa			 Hotspot_Web_Portal Router_App_Network 	o o	2	2	0 0	0	0	1
States States	A				0 0 0	2 2 1	2 2 0	0 0 0	0	0 0 0	1.5.9
New Dev	XIX		-/*	♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0 0 0	2 2 0	2 2 0	0 0	0	0 0	1
	XIX	Decis Rama	- · · ×	♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0 0 0	2 0	2 2 9	0	0	0	1.5.9
New Dev	ices	Erke Kana J220: SJIGATEDAI Stor		♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0	2 0	7 2 0	0 0	0	0	1.5.
New Dev Action	ices IP Adress		Device Type	♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0	2 2 0	7 2 0	0	0	0	1.5.5
New Dev Action	ices IP Adress ISZLIGE LALIDER	2120rt 001DAA71F2A4_sturn	Device Type Vigor2120n+	♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0	2 0	7 2 0	0	0	0	***
New Dev Action	rces. PAdres: 192.168.143.10.87 192.168.145.10.87 192.168.145.104.80	2120H 001DAA71F2A4 stud 2855Lac 14498C307A08	Device Type Vigor2120n* Vigor2865Lac	♥ Roules: App. Network ♥ T_2024-07-22_Wholesue_GA_D	0	2 0	7	0	0	0	***

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

2.3.2 Troubleshooting for Unstable CPE Status

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



Allow TR-069 server access from the Internet

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

IPv4 Management Setup	IPv6 Ma	nagement Setup	LAN Access Setup		
Router Name DrayTek					
Default:Disable Auto-Logout		Management Port Se	etup		
Enable Validation Code in Internet/LAN	Access	User Define Ports	s 🔿 Default Ports		
Note: IE8 and below version does NOT sup	port DrayOS	Telnet Port	23 ((Default: 23)	
CAPTCHA auth code.		HTTP Port	80 ((Default: 80)	
Internet Access Control		HTTPS Port	443 ((Default: 443)	
Allow management from the Internet		FTP Port	21 ((Default: 21)	
Domain name allowed		TR069 Port	8069 ((Default: 8069)	
FTP Server		SSH Port	22	(Default: 22)	
HTTP Server Enforce HTTPS Acc	ess	Note:			
HTTPS Server		Ports 8001 and 8043	are used for Hotspot We	eb Portal.	
Telnet Server		Brute Force Protecti	ion		
✓ TR069 Server		Enable brute force			
SSH Server			rogin protection		

System Maintenance >> Management

Enable Periodic Inform

2

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

Protocol	<pre>●HTTP ○HTTPS</pre>	
URL		
Port	8069	
Jsername	vigor	
Password		
Note: Please page.	se enable TR-069 server to allow access from Internet on <u>System Maintenance >> Manageme</u> e.	<u>nt</u>
page. Periodic Infor Enable	e. Dorm Settings Je O Disable	<u>1t</u>
page. Periodic Infor © Enable Time I	e. orm Settings le O Disable Interval 900 second(s)	<u>nt</u>
page. Periodic Infor © Enable Time I	e. Dorm Settings Je O Disable	<u>1t</u>
Page. Periodic Infor © Enable Time I Npply Setting © Enable	e. orm Settings ile O Disable Interval 900 second(s) gs to APs/Switches ile Disable	<u>nt</u>
Page. Periodic Infor Enable Time I Time I C Enable	e. porm Settings ile O Disable Interval 900 second(s) gs to APs/Switches	<u>nt</u>

Check TR-069 authentication

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

- Register to the network of VigorACS 3

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

			Register ACS Netv		
furtheast *	Vi DrayTek Verses	gorACS3		CPE System Mainteauce >> 18.009 Setting	0
Network Management					-
Careb by Descert Parent Mania (Mar. 19 (2020))	e Map			ACS and CPE Settings Reporting Configuration Export Parameters TR.665 Disable Exuble	
● EDA GRANNEN • \$ ¹ for an annual (Teal liss bound	General 40 Fonesi 111000	-	Primary ACS Server On Costant and primary Access Control User Access On Acces	

- Get CPE information

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

		Get CPE In 	oformation
			System Maintenance >> TR-069 Setting
y Omer Holfman, Albony Anthy & Address Boot Network(2) () 822055 (D01DAASSA4758	C Serie Map Roter This Device Ja Change factories		ACS and CPE Settings Reporting Configuration Export Parameters
	General Settings Status Backs Backs Security 1	Issue bers Report Insecution Insecution I	Primary ACS Server ACS Server On Internet > 2 Enable TR069 Server on System Maintenance >> Management >> Internet Access Control URL Witzers
	Malat Kime Mgad225m mag L	stoom Same stoom CostonASSe135 Mate 2	CPE Client
	Senti mindee 201909090412601	464 Address 001594354758	Podocol HITP CHITPS URL Pod 1909 Usertaine Vogor
	licalle Rise 61	CH (Start) P 132 LIN, 105 52 CH C Clark Flor Not	Passood Note: Plass endors IK-(Kr) server to allow access from Minnel on System Maintenance.22 Management gage. Periodic Inform Settings.
	Dennist Kind Hanggenet Tyming (1): solars prove Hanggenet Freq AS	Of Canti Ne Voers Schloen Of Canti Ver Name Pate Pate	Chudie Duadrie Time Interval
on OpenLan		7 ton	

Check STUN setting

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

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

Check the ACL setting

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

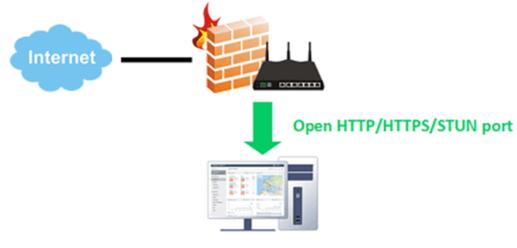
1.4

Acc	ess List from	the Internet		CVM Access Control	
	Apply Access	List to PING Index	Description	CVM Port	8000 (Default: 8000)
1		1-acs 🗸	11.22.33.44/255.255.255.255	CVM SSL Port	8443 (Default: 8443)
2	IP Object 🗸	None 🗸		AP Management	
3	IP Object 🗸	None 🗸		Enable AP Management	
4	IP Object 🗸	None 🗸]	_	
5	IP Object 🗸	None 🗸		Device Management	
6	IP Object 🗸	None 🗸		Respond to external dev	ice
7	IP Object 🗸	None 🗸]]		
8	IP Object 🗸	None 🗸]]		
9	IP Object 🗸	None 🗸			
10	IP Object 🗸	None 🗸]		

• Check the firewall on ACS server

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

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

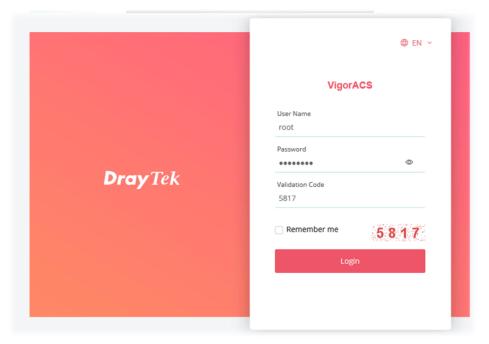


VigorACS 3

Chapter 3 Getting Started

3.1 Accessing Web Page of VigorACS

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



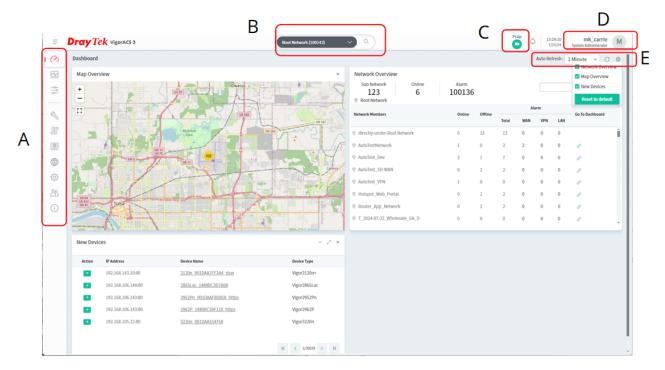
2. After clicking Login, main screen of VigorACS 3 will be shown as below.

Map Over	l			Network Overview					Auto Ref	fresh: 1	Minute ~ C Network Over	M
*	E	A Sector Comp		Sub Network Online 123 6 Boot Network	Alarm 100136						New Devices	
		C - C - WW	1	Network Members	Online	Office		Ala	in a		Go To Dashboard	
		Sal It	- 0.10				Total	WAN	VPN	LAN		
3		-1791	am 7:27	directly under Root Network	0	13	13	0	0	0		
	+ 2			F 0 AutoTestNetwork	1	6	2	2	0	0	0	
1120	and the second	Parel Parel		@ AutoTest_Dev	2	7	7	0	0	0	.p	
	1		the the	1 AutoTest_SD-WAN	0	2	2	0	0	0	0	
Parent I				U AutoTest_VPN	1	-	0	0	0	0	0	
		a mandanter	di nor and	0 Hotspot_Web_Portal	0	2	2	0	0	0	11	
	Turs			1) Hotspot_Web_Portal 12 Router_App_Network	0	2	2	0 0	0	0	1	
VIAU	A A				0 0 0	4 2 2	2 2 0	0 0 0	0	0 0 0		
-	XIX		-7.	♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	4 2 2	2 2 0	0 0 0	0	0	4	
	XIX	Decks Rame		♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	2 4	7 2 0	0	0	0	4	
New Devi	ices	Device Reme 21201: SSIDAR-112244. store		♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	2 0	2 2 0	0	0	0	4	
New Devi	ices IP Address		Device Type	♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	4 2	2	0	0	0	4	
New Devi	ices IP Adress 192.168.143.10:89	2120H S01DAA71F2AH sturt	Device Type Vigor2120n+	♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	1	7 2 0	0	0	0	4	
New Devi	rces P Adress 192.168.143.10:80 192.168.144.10:80 192.168.144.10:80	2120H 001DAA71F2AH stum 2855Lac 14490C307A08	Device Type Wgor2120n+ Wgor2865Lac	♥ Router, App, Network ♥ T_2024-07-22_Wholesate_GA_D	D	1 2 6	2	0	0	0	4	

3.2 Dashboard

3.2.1 Dashboard for Root Network

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



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

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

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

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

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

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

3.2.2 Dashboard for a Network Group

Pcap

=	Dray Tek VigorAcs 3		В	utoTest_SD-WAN (2)				С		14:08:22 7/22/24	mk_carrie)
10	Dashboard		C						-	Auto Refresh : 1 M	linute → () @
	Summary SD-WAN											
	Map Overview			×	Device Overview							×
114	•	Canada		Ч.	Routers 2	APs O	Switch				Q. Device	*
		S. Carl			Device Name	Model	MAC	Status	UP Time	Firmware Version	Active Clients	VPN
			1000		2865Vac 1449BC34F5D0	Vigor2865Vac	14:49:BC:34:F5:D0	Offline	0 days 00:00:00	4.4.1_STD	0	0
Z			A. 4.		2865Vac 1449BC34FE08	Vigor2865Vac	14:49:BC:34:FE:08	Offline	0 days 00:00:00	4.4.1_STD	0	0
F		1 × 1 2								ы	< 1/1 >	ы
\$		United 2										
-	Sec. 19	Mexico										
¢		A CONTRACT										
쓰			Colombia - C									
(j)			25 Sint									
-	Active Clients- Top 20			©Last24hours _ ∠ ×	Traffic- Top 20					© Las	st 24 hours	×
	Total				Total							
	0	0 %	2865Vac_14498C34F5D0/0	0%	0 Byte	¹ 0 Byte	0 Byte		2865Vac_14	∟/0Byteî0Byte⊥0	Byte 0	6
	1	• Total	2865Vac_14498C34FE08/0	0%	1 Byte			• Total	2865Vac_14	L_/0Byte↑0Byte↓0	Byte 0	6
			•						-			
					0 Byte							
	08.0	8				0	1.00					

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

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

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

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

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

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

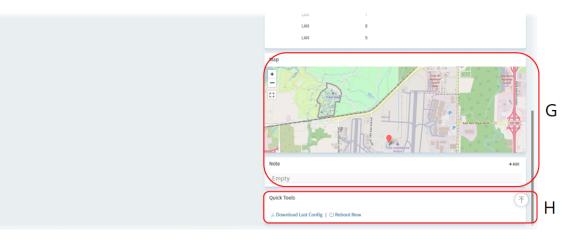
Overview - There are five types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview for the Network Group.

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

3.2.3 Dashboard for a Device

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

2865Vac_1449BC34FE08		Device Status: ① Offline Alarms: 1 A	ctive Clients: 0 Auto Refresh: 1 Minute 🗸
Port Status		WAN Overview	© Last 24 hou
ACT WANZ GOS	Vigor2865Vac	1 Byte	o Tota
USB DSL Phone1			
	1946 1957 Pri P2 P3 P4 P5 Pased Pased		
Device Information		0 Byte 08:00	
Device Name	2865Vac_1449BC34FE08	Total († 0 Byte 4 0 Byte)	0
IP Address	http://192.168.106.148:80	WANI (↑ 0 Byte ↓ 0 Byte)	(
Network Name	AutoTest_SD-WAN	WAN2 (↑0 Byte ↓0 Byte)	0
Model	Vigor2865Vac	WAN3 (↑0 Byte ∔0 Byte) e	0
Firmware Version	4.4.1_STD	WAN4 (↑0 Byte ↓0 Byte)	(
MAC ADDress	14:49:BC:34:FE:08	WANS (↑0Byte ↓0Byte) «	(
Up Time		WANG (↑0 Byte ↓0 Byte)	(
J		- show more	© Last 24 hou
Connectivity and Alerts		DAN OVER NEW	
ld ↓↑ Start Time	3↑ ClearTime 3↑ Type 3↑ Message	47 1	 Active Clients
374651330 2024/07/22 05:26:04	- Device Lost Connection Device Loss Connec	lon	
		0 08:00	



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

B: Display Tab - Displays current selected item, e.g., root network, group network and CPE model. In this page, a CPE device (e.g., Vigor2865 series) is selected.

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

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

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

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

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

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

3.2.4 Menu Bar

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

Menu Bar for Root Network.		Menu Bar for Network Group.	Menu Bar for Selected CPE.
 Dashboard Monitoring Configuration Configuration Maintenance Reports Provisioning Network & Service Management System User About 		 Dashboard Statistics Monitoring Configuration Hotspot Web Portal Maintenance Reports Provisioning Network & Service Management System User About 	 Dashboard Statistics Monitoring Configuration Advanced Advanced Maintenance Reports Provisioning Network & Service Management System User About
RD8 V Configuration VPN AP Profile Load Balance Route Policy (SD-WAN) VoIP WAN (SD-WAN)	icon to open to list. Select the me	use cursor to each the drop down menu enu item and access guration web page.	

3.2.5 Root Network, Group Network, and Selected CPE

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

3.2.5.1 The Display Tab, Root Network

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

Root Network(267)	
Romanio	Model	
읊 R03(14)		
옳 ROS(9)		
옮 RD6(3)		
& R07(15)		
5 RD8(58)		
옲 KD8-1(1)		
& RD999(1)		

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

3.2.5.2 The Display Tab, Network Group

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



3.2.5.3 The Display Tab, CPE Device

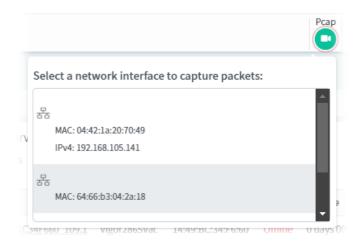
Click the Model Tab. Next, click the > button to list other CPE devices with the same model as the selected device. Select the device you want, then the selected CPE will be shown on the Display Tab.



3.2.6 Capture Packets

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

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



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

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

Pcap A No network device detected, please check if libpcap/WinPcap is installed. 3

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

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

Capture Set	0	
Selected Ne	twork Interface	

MAC: 04	:42:1a:20:70:49	
IPv4: 19	2.168.105.141	
Filter Examples	i	
(None)		
	e filter normally, for more expression syn <u>PCAP-FILTER</u>	ntax
	PCAP-FILTER	ntax
please visit:	PCAP-FILTER	ntax
please visit: Custom Filt	PCAP-FILTER	ntax

These parameters are explained as follows:

ltem	Description
Capture Settings	Filter Examples – Choose a filter for filtering the packet corresponding to the type selected.
	For example, when TCP Only is selected, only TCP packets will be captured and recorded. When IPv4 address 127.0.0.1 is selected, then only the packets coming from/sending to that IP address will be captured and recorded.
	Custom Filter – Variation of Filter Examples will change the setting in Custom Filter. However, the system administrator can define the filter by entering correct syntax (e.g., host 172.16.2.222) if required. Packet capturing will be executed according to Custom Filter setting.
Timer	Switch the toggle to enable/disable the setting. If enabled, VigorACS server will capture the packets within the time limit defined below. Timer (1-15 Minutes) – Enter a value as a time limit.
Start Capturing	Click to start packets capturing.
	 After clicking it, VigorACS server will continuously capture the packets until time up or manual stop. While capturing, the system administrator can perform any job on VigorACS still. The status will be shown as the following figure. If Time Limit is disabled, the status bar will not show the timer information.

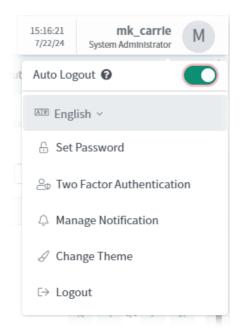
© Pcap (4:45
 When the time is up or stop the job manually, the status of Pcap will be stored as a file on the hard disk. Later, use the tool of Wireshark to check the content of the file.
 In considering the network security, when someone performs the packet capturing on VigorACS server, other users are not permitted to use Capture Packets until the one finishes or stops the job. Only the one who performs the packets capturing can download the packet capture file.
f A Pcap is now in use by "root", please wait for current capturing finished. $m C$
Click the Refresh button on the right side of Pcap status bar to check if someone else uses Pcap or not.

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

	_1514856095133_20)18-10-23.175419.pcap					- 🗆	2
e <u>E</u> d	lit <u>V</u> iew <u>G</u> o <u>C</u> a	apture <u>A</u> nalyze <u>S</u> tatistics	Telephony Wireless	<u>T</u> ools <u>H</u> elp				
	🤊 🛞 📙 🛅 🗙	🗳 । ९. 👄 🔿 🕾 🚺	📃 🗏 @, Q, Q, I	E				
Apply :	a display filter … «Ctrl-/	l>					Expression	····
	Time	Source	Destination	Protocol	Length Info			
	1 0.000000	192.168.50.10	192.168.105.59	TCP	66 64750 → 8069	[SYN] Seq=0 Win=64240 Len=0	MSS=1460 WS=256	S
	2 0.001467	192.168.105.59	192.168.50.10	TCP	60 8069 → 64750	[SYN, ACK] Seq=0 Ack=1 Win=2	25600 Len=0 MSS=1	4
	3 0.001608	192.168.50.10	192.168.105.59	TCP	54 64750 → 8069	<pre>[ACK] Seq=1 Ack=1 Win=64240</pre>	Len=0	
	4 0.001821	192.168.50.10	192.168.105.59	HTTP	155 GET /cwm/CRN			
	5 0.004302	192.168.105.59	192.168.50.10	HTTP		Authentication Failed		
	6 0.004673	192.168.50.10	192.168.105.59	TCP		[FIN, ACK] Seq=102 Ack=209 N		F
	7 0.005244	192.168.50.10	192.168.105.59	ТСР		[SYN] Seq=0 Win=64240 Len=0		S
	8 0.005541	192.168.105.59	192.168.50.10	TCP		[ACK] Seq=209 Ack=103 Win=2		
	9 0.005630	192.168.105.59	192.168.50.10	TCP		[FIN, ACK] Seq=209 Ack=103 N		
	10 0 005600	107 168 50 10	103 168 105 50	тор	51 61750 - ROCO	[ACK] Soc-103 Ack-210 Win-6	1032 Lon-0	
Inte Tran	rnet Protocol V	AsustekC_56:f7:99 (8 Version 4, Src: 192.: ol Protocol, Src Port Protocol	168.50.10, Dst: 19	2.168.105.59		.09:44:00)		
Inte Tran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		09:44:00)		
Inte Tran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		09:44:eo)		
[nte [ran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		09:44:20 <i>)</i>		
[nte [ran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		07:44:60)	_	
nte ran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		07:44:60)		
nte ran	rnet Protocol smission Contro	Version 4, Src: 192. ol Protocol, Src Port	168.50.10, Dst: 19	2.168.105.59		.07:44:60)		
inte Tran lype	rnet Protocol v smission Contro rtext Transfer	Version 4, Src: 192.: ol Protocol, Src Port Protocol	168.50.10, Dst: 19: t: 64750, Dst Port	2.168.105.59 : 8069, Seq: 1	, Ack: 1, Len: 101	.07:44:60)		
inte Tran lype	rnet Protocol v smission Contro rtext Transfer 00 1d aa 69 4a	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7	168.50.10, Dst: 19 t: 64750, Dst Port	2.168.105.59 : 8069, Seq: 1	, Ack: 1, Len: 101	.07:44:60)		
Inte Iran Hype	rnet Protocol v smission Contro rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 co	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 a8 32 0a c0 a8 -	2.168.105.59 : 8069, Seq: 1	, Ack: 1, Len: 101	.07:44:60)		
Inte Iran Hype	rnet Protocol V smission Contr rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 a8 32 0a c0 a8 a 36 64 50 18 i	2.168.105.59 : 8069, Seq: 1	, Ack: 1, Len: 101	.07:44:60)		
Inte Fran Hype 10 20 30	rnet Protocol smission Contr rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f a f0 1d 16 00	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 66 00 00 c0 85 3c 14 c0 8e e5	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 88 32 0a c0 a8 83 a5 64 50 18 i 3 77 6d 2F 43	2.168.105.59 : 8069, Seq: 1	, Ack: 1, Len: 101	.07:44:60)		
[nte [ran Hype 00 10 20 30 40	rnet Protocol 1 mission Contr. ntext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 25 4e 2e 68 74	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e 65 00 47 45 54 20 2f	168.50.10, Dst: 193 t: 64750, Dst Port 99 08 00 45 00 a8 32 0a c0 a8 a8 35 64 50 18 i 63 77 6d 2f 43 50 2f 31 2e 31 R	2.168.105.59 : 8069, Seq: 1	<pre>, Ack: 1, Len: 101 E P/C1</pre>	.07:44:60)		
Inte Iran Hype 00 10 20 30 40 50 60	rnet Protocol smission Contr rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ce 1f fa f0 1d 16 60 52 4e 2e 68 74 0d 0a 55 73 65 66 61 72 74 61	Version 4, Src: 192. ol Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e 65 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 88 32 0a c0 a8 33 564 50 18 i 377 60 27 43 50 27 31 2e 31 R 74 3a 20 4a 61 57 32 04 874 k	2.168.105.59 : 8069, Seq: 1 : 8069, Seq: 1 :	E. 	.07:44:60)		
Inte Tran Hype 00 10 20 30 40 50 60 70	rnet Protocol smission Contr. rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 8d 20 73 65 6b 61 72 74 61 74 70 43 66 69	version 4, Src: 192. ol Protocol, Src Port Protocol 88 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5 04 42 c0 48 45 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 83 32 0a c0 a8 83 a5 64 50 18 i 63 77 6d 2f 43 83 a5 02 43 74 74 3a 20 4a 61 66 73 2d 48 74 k 31 0d 0a 48 6f t	2.168.105.59 : 8069, Seq: 1 	E. 	.07:44:60)		
Inte Fran Hype 00 10 20 30 40 50 60 70 80	rnet Protocol smission Contr rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 00 3b fc ce 1f fa f0 1d 16 00 52 4e 26 88 74 04 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 69 73 74 3a 20 31	Version 4, Src: 192. cl Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 06 00 cl 85 3c 14 c0 8e e5 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e 39 32 2e 31 36 38	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 8 32 0a c0 a8 a8 32 0a c0 a8 a5 64 59 18 i 63 77 6d 2f 43 50 2f 31 2e 31 R 14 3a 20 4a 61 t 56 73 2d 48 74 k 31 0d 0a 48 6f t 2e 31 30 35 2e s	2.168.105.59 : 8069, Seq: 1 : 8069, Seq: 1 :	E. 	.07:44:60)		
Inte Iran Iype 00 10 20 30 40 50 50 70 80	rnet Protocol smission Contr rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 00 3b fc ce 1f fa f0 1d 16 00 52 4e 26 88 74 04 0a 55 73 65 6b 61 72 74 61 74 70 43 6c 69 73 74 3a 20 31	version 4, Src: 192. ol Protocol, Src Port Protocol 88 88 d7 f6 56 f7 00 80 06 00 00 c0 85 3c 14 c0 8e e5 04 42 c0 48 45 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 8 32 0a c0 a8 a8 32 0a c0 a8 a5 64 59 18 i 63 77 6d 2f 43 50 2f 31 2e 31 R 14 3a 20 4a 61 t 56 73 2d 48 74 k 31 0d 0a 48 6f t 2e 31 30 35 2e s	2.168.105.59 : 8069, Seq: 1 	E. 	.07:44:60)		
Inte Tran Hype 00 10 20 30 40 50 60 70 80 90	rnet Protocol smission Contr. rtext Transfer 00 1d aa 69 4a 00 8d 10 fa 40 69 3b fc ee 1f fa f0 1d 16 00 60 55 73 65 65 61 72 74 65 74 70 43 6c 69 73 74 3a 20 31 35 39 3a 38 30	Version 4, Src: 192. cl Protocol, Src Port Protocol e8 88 d7 f6 56 f7 00 80 06 00 cl 85 3c 14 c0 8e e5 00 47 45 54 20 2f 6d 6c 20 48 54 54 72 2d 41 67 65 6e 20 43 6f 6d 6d 6f 65 6e 74 2f 33 2e 39 32 2e 31 36 38	168.50.10, Dst: 19; t: 64750, Dst Port 99 08 00 45 00 8 32 0a c0 a8 a8 32 0a c0 a8 a5 64 59 18 i 63 77 6d 2f 43 50 2f 31 2e 31 R 14 3a 20 4a 61 t 56 73 2d 48 74 k 31 0d 0a 48 6f t 2e 31 30 35 2e s	2.168.105.59 : 8069, Seq: 1 : 8069, Seq: 1 :	E. 	D7:+4:E0)	Profile: D	

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

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



3.2.7.1 Change Language

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

1	Auto Logout 🕼	
	[™] English ∨	
	中文 (简体)	Change language
	Deutsch	
	English	
	Nederlands	
	中文 (正體)	

3.2.7.2 Set Password

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

Set Password	
Account :	
New Password	0
Confirm Password	٢
	Save

3.2.7.3 Two-factor Authentication

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

For using two-factor authentication for accessing VigorACS;

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

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

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

Two-factor authentication	
Enable two-factor authenticati	on C
Choose 'Default' mes Get and install Googl Scan the QR-Code or Click the save button	uthentication please follow the instructions below. ans Two Factor Authentication is based on TOTF Authenticator. e Authenticator (OS Android) manual input secret key to verify the code generated from APPs ou should backup the secret key or QR-Code
Description	mk_carrie@VigorACS
QR-Code	
Manual Input	3HKBRJLHI6LR03GM
Verification Code	
	Cancel Save

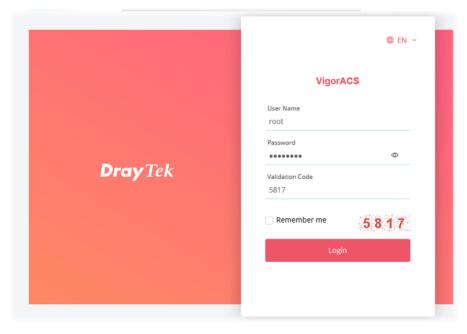
4. Use your cell phone to scan the QR-Code shown on the Two-factor Authentication page.



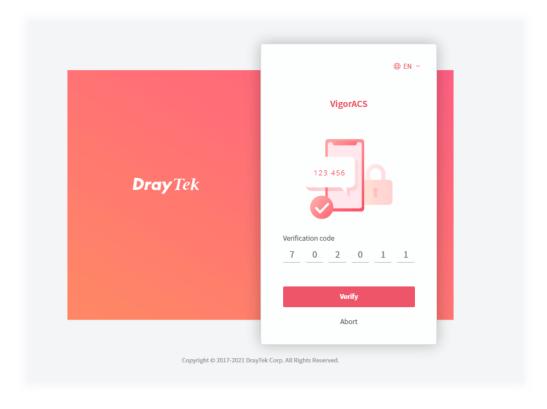
5. A key will be created randomly on the cell phone. Enter that key on the box of Verification Code and click the Save button.

Enable two-factor authenticat	on 💽	
Notes		
	kathentication picose follow the instructions prove. ans two Factor Authentication is based on 1017 Authenticates	
	white-encoder (#15 Action)	
	minut light front key	
· Click line save builter	its verify the code generated from ADPs	
 Hospitalities adulties of W 	w denote bodrup the secret Key or QR Cede	
Description	mil_cume@VigorAc5	
	Display in App: VigorACSYnik, coming/VigorA241	
QB-Code		
Maessal Imput	SHKERJCHIGLRÖJGM	
Verification Code	278808	

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



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



3.2.7.4 Manage Notification

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

These parameters are explained as follows:

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

3.2.7.5 Change Theme

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

 Automatically detect 	t system or browser theme (Detec	ted: Light Them	e)									
Light Theme						Darl	k Theme					
Beef Barlands	DrayTek ver				R		Red Network	Dray	Tek voruss			-
_			10	area dalarana dalar				Undy			50000 L.	
Roat Network(74)			Auto Server?	1 Minute		198	Boot Network(74)			Auto Bala	ab 1 Minute	
150 Kasara	••••	twork Overview			1.2.8	55			C work Dverview			
3		12 2 72			5:503 ~	- 12			12 2	72		
A 410			-	Arr		~	ă +00		-			-
A +851				na was u	TN LAN	8	a +800				-	-
		erilyceshe dont Metsenk, 1		4.4		1000			willy under Real Nation			
(E) & en 20		and straining of	1.1.1	6 9	0		& 100 200		steers - the second			
G & H M M		and in the		4 0		•	A resign		-			
S CALLANTE		along term (4 4	4		A students		chating carrie			- A.I.
	· · · · ·	L YORKY		1.1.1	0	19			(FADBAR			
28		100mil(120		4 4	0	25			T AMAMAN (127)			
()	+ **		1. 11. 1	4 4	0	0			+ 940			
the second se					0			- Jak	748	7 40		

3.2.7.6 Logout VigorACS

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

Auto Logout 😧
Image: Anglish ∨
🔒 Set Password
$\stackrel{_{\odot}}{_{\oplus}}$ Two Factor Authentication
Manage Notification
🖉 Change Theme
[→ Logout

3.2.8 Auto Refresh, Manual Refresh, and Widget

Auto Refresh : 1 Min	nute ~ C 쒛
ltem	Description
Auto Refresh	Select the time interval for refresh the web page automatically. Auto Refresh: 1 Minute 5 Minute 10 Minute Disable
Manual Refresh	Click to refresh the web page immediately.
Widget	There are six display views to select, including Network Overview, Map Overview, Clients, Traffic, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard. Auto Refresh: 1 Minute
	Available quick overviews on the dashboard will vary according to the root network, selected group network and selected CPE.

3.2.9 Overviews

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

ctive Clien	its Top 20			()) Last 24 hours 🗸 🚽 🦯 🗙	Traffic - Top 20	③ Last 24 hours
Total 27 125 100 75 50 25 20:		100 % Total	RD3 / 0 RD2 / 13 attel / 11 RD1 / 3 RD8 / 0	0% 48% 41% 0%	Total 251.28 GB 1 30.38 GB GB 9.31 GB 7.45 GB 3.73 GB 1.86 GB 0 Byte 20:0000:0004:0008:00 12:0016:00	RD3 / 172.67 GB 29.52 GB 143.15 GB RD2 / 77.24 GB 518.84 MB 76.74 GB RD1 / 818.54 MB 47.23 MB 771.31 M attel / 453.14 MB 245.69 MB 207.461
lew Device	IP Address	Device N	lame	— 之 🗙		• • • •
+	172.17.5.151:4433	3910_00	1DAA18E740	Vigor3910		
+	14.161.2.165:443	2912Fn_	001DAA8C0F0C	Vigor2912Fn		
+	123.20.123.2:443	2912_00	1DAA87FAE4	Vigor2912		
+	14.167.99.211:443	2912_00	1DAA88040C	Vigor2912		
+	192.168.11.5:443	AP 810_0	001DAA0F3320	VigorAP 810		
				KI < 1/45 > DI		

3.2.9.1 Network Overview / Device Overview

This area displays the Network Overview or the Device Overview.

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

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

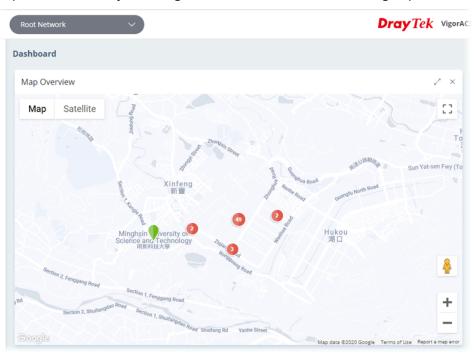
					Auto Ref	resh : [Disable 🗸	Cğ
Network Overview Sub Network 0nline 123 8 Root Network	Alarm 100138						ے Net	∠ × work ∨
Network Members	Online	Offline	Alarm				C. T. Dashhard	
Network members	Onune		Total	WAN	VPN	LAN	Go To Dashboard	ira
Irectly-under-Root Network	0	13	13	0	0	0		i
AutoTestNetwork	0	1	3	2	0	0	8	
AutoTest_Dev	2	7	7	0	0	0	8	
AutoTest_SD-WAN	0	2	2	0	0	0	в	
AutoTest_VPN	1	0	0	0	0	0	8	
Hotspot_Web_Portal	0	2	2	0	0	0	8	
Router_App_Network	0	2	2	0	0	0	8	
T_2024-07-22_Wholesale_GA_D	0	0	0	0	0	0	8	

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

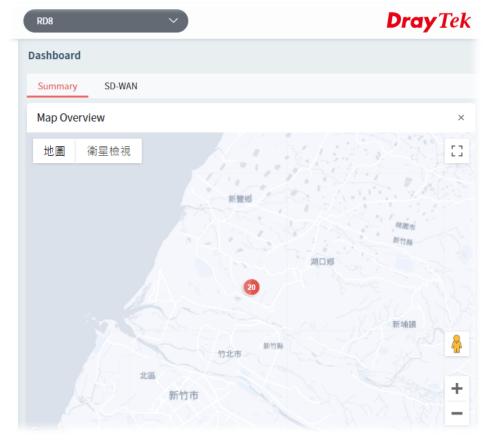
141 9	APs 9995	Switch 6				Q Device	~
Device Name	Model	MAC	Status	UP Time	Firmware Version	Active Clients	VP
927Lac 1449BC023768	Vigor2927Lac	14:49:BC:02:37:68	Online	0 days 02:50:16	4.4.2.3	0	1
120n 001DAA7FF2A4 stun	Vigor2120n+	00:1D:AA:7F:F2:A4	Online	41 days 20:00:29	3.8.10	0	0
865Lac 1449BC3D7A08	Vigor2865Lac	14:49:BC:3D:7A:08	Offline	0 days 00:00:00	4.4.5_STD	0	0
952Pn 001DAAF8D818 https	Vigor2952Pn	00:1D:AA:F8:D8:18	Offline	0 days 00:00:00	3.9.7.2	0	0
962P 1449BC39F110 https	Vigor2962P	14:49:BC:39:F1:10	Online	46 days 19:57:10	4.3.2.6	0	1
220n 001DAA554758	Vigor3220n	00:1D:AA:55:47:58	Offline	0 days 00:00:00	3.9.7.4	0	0
P 810 001DAA7C2B50	VigorAP 810	00:1D:AA:7C:2B:50	Offline	0 days 00:00:00	1.3.4	0	0
P 902 001DAA3F150E stun	VigorAP 902	00:1D:AA:3F:15:0E	Offline	0 days 00:00:00	1.3.4	0	0

3.2.9.2 Map Overview

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



Map Overview will vary according to the root network or the network group selected.



3.2.9.3 Active Clients

It is available for Group Network and CPE Device selected.

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



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

3.2.9.4 Traffic

It is available for Group Network and CPE Device selected.

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

5.54 GB	$^{\uparrow}$ 101.25 MB $^{\downarrow}$ 5.44 GB	RD2 / 5.54 GB $\uparrow~$ 101.25 MB $\downarrow~$ 5.44 GB	100%
3.26 GB	• Total		
2.79 GB		ALANWEN / 0 Byte ↑ 0 Byte ↓ 0 Byte	0%
2.33 GB		-	
1.86 GB		Alvaco / 0 Byte↑ 0 Byte↓ 0 Byte	0%
1.40 GB		-	
953.67 MB		AnPhat_VN / 0 Byte↑ 0 Byte↓ 0 Byte	0%
476.84 MB		-	
0 Byte 🗕		Angela / 0 Byte ↑ 0 Byte ↓ 0 Byte	0%

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

3.2.9.5 New Devices

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

Action	IP Address	Device Name	Device Type	
+	192.168.105.143:443	2862Vac_001DAAEA38C0	Vigor2862Vac	
+	192.168.11.12:443	2920LVac_1449BCFFF9A8	Vigor2926LVac	
+	192.168.15.10:443	2926Vac_001DAA5DCAF0	Vigor2926Vac	
+	192.168.105.81:443	810_001DAA7D6514	2862Vac_001. A38C0	
+	192.168.105.89:8442	902_001DAA3D4F16		
			Port Status	Vigor2862Vac Visita Security Forwards
			Device Information	2862Vac_001DAAEA38C0
			IP Address	https://192.168.105.143:443
			in Address	1100110111011101110111011101110

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

3.2.9.6 Reset to Default

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

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

3.2.10 Icons Used in VigorACS 3

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

3.3 Operation Procedure

Follow the instruction listed below to operate VigorACS 3:

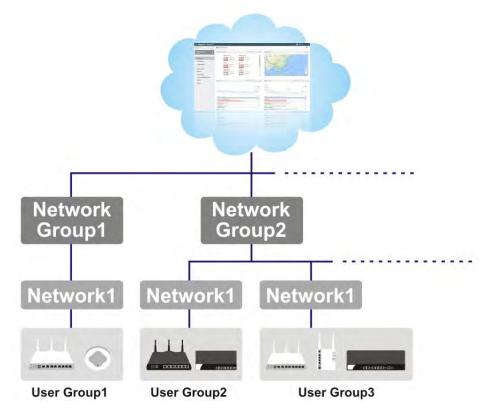
- Create networks.
- Create users and user groups.

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

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

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

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



Applications

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

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

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

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

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

System Maintenance >> Management

IPv4 Management Setup IPv6 N		Management Setup	
Router Name	DrayTek		
Default:Disable Auto-Logout Enable Validation Code in Internet/LAN Access		Management Port Setup User Define Ports De Telnet Port	
Domain name al	Enforce HTTPS Access	HTTP Port HTTPS Port FTP Port TR069 Port SSH Port Note: Ports 8001 and 8043 are used	
 SSH Server SNMP Server Disable PING fr 	om the Internet	Brute Force Protection Enable brute force login pr FTP Server	

- Allow management from the Internet – Enabled.

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

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

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

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

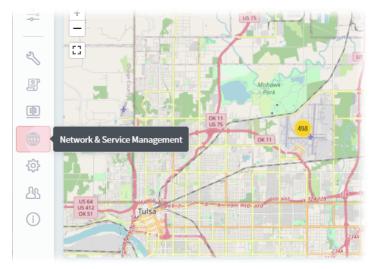
- 5. Open the homepage of VigorACS 3.
- 6. Now, Vigor2927Vac has been registered onto VigorACS 3 and displayed on the homepage.

lew Devi	ces		- 2
Action	IP Address	Device Name	Device Type
+	172.17.5.151:4433	3910_001DAA18E740	Vigor3910
+	14.161.2.165:443	2912Fn_001DAA8C0F0C	Vigor2912Fn
+	123.20.123.2:443	2912_001DAA87FAE4	Vigor2912
+	14.167.99.211:443	2926_001DAA88040C	Vigor2926Vac
			⋈ < 1/1 > ⋈

A.2 How to Create a New Network?

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

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



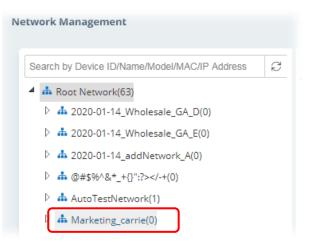
3. Select Network Management. When the following page appears, click the link of +Add New Network.

Setting Map	ר	
+Add New Network		
General Settings		
Network ID		
2		
Name		
Root Network		
Location		

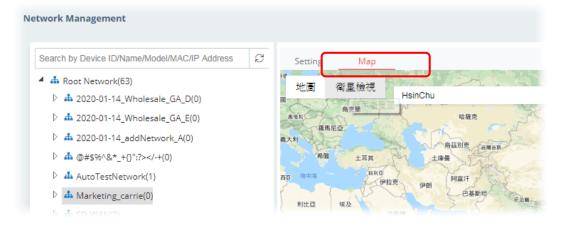
4. A pop-up window appears. Type the required information.

Parent Network	
Root Network	
Name	
Marketing_carrie	~
Location	
HsinCHu	
User Name	
carrie	×
Password	
	✓ ⊚

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



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



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

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

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

	5 Top 20		©Last 24 hours - / ×	Traffic Top 20			() Last 24 hours ~	-
Total 27	100 *	R02/14	52%	Total	1479.24	1.00.00	R02734.04 G8 1 369.37 M8 1 33.68 G8	.9
				35.96 GB	MB	1 35.49 GB		_
30 25	MMIN	attel / 10	37%	3.26 GB		O Total	RD1 / 1.80 G8 + 46.13 M8 1 1.76 G8	
20	M. M.			2.79 GB		0.1	-	
15		RD1/3	11%	2.33 GB			attel / \$0.99 MB 1 -45.91 MB 1 35.08 MB	
				1.85 GR		M M.	·	
10.		1111/0	0%	1.40 G8		- Mun	RDS / 30.77 MB 1 17.82 MB 1 12.95 MB	
5				953.67 MB				
		ALANWEN / O	- 0%	476.84 MB			1111/0 Byte 1 0 Byte 1 0 Byte	
12:00 18	6:00 20:00 00:00 04:00 08:00			0 Byte	0 16:00 20:00 00:		-	
New Devices			- / ×					
		ice Name	Device Type					
Action	IP Address Devi	ee raame	accurate the					
		0_001DAA18E740	Vigor3910					
•	172,17.5.151:4433 391							
	172.17.5.151:0433 391 14.161.2.165:043 291	0_001DAA18E740	Vigor3910					
0	172,17,5,151,8433 391 14,161,2,165,9443 291 123,20,123,29443 291	0_001DAA18E740 2Fri_001DAA8C0F0C	Vigor3910 Vigor2912Fn					

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

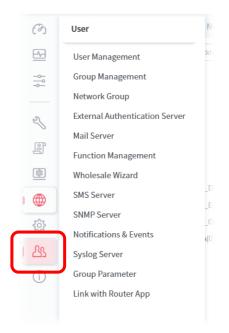
+ Add New Device			
Add to Network	Root Network		Q
Device name:	3910_001DAA18E740		
Location:			
Emergency phone:			
Set to known device:			
		Cancel	🗸 Apply

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

A.4 How to Create a New User Group?

Only the administrator can create a new user group.

1. From MENU bar, open the User menu.



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

User / Group	o Management				
Setting	Management	UI CustomIzation			
+Add 🗐					
+Add 🗎	Group ID ↓↑	Delete with wholesate Group Name	↓↑ Max Nodes	↓↑ Used Nodes	$\downarrow\uparrow$ Enable Expire Date

RootGroup is a default setting.

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

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

- Group name – Enter a new name.

- Nodes – Use \blacktriangle or \blacktriangledown to add or decrease the number of nodes.

- Enable Global Mail Server Click to enable or disable the service.
- Enable Global SNMP Server Click to enable or disable the service.
- Enable Expire Date Click to enable the Expire Date mechanism.
- Expire Date If it is enabled, click the entry box to choose the date.
- 4. Click Save to save the settings and exit the dialog. The new network group has been created and displayed on the screen.

User / Group	Management								
Setting	Management	UI CustomIzation							
+Add ₪D									
	Group ID ↓↑	Group Name	$\downarrow\uparrow$	Max Nodes	¢↑	Used Nodes	$\downarrow\uparrow$	Enable Expire Date	↓ ↑
	1	RootGroup		200		120.5		Disabled	
	2	Marketing2024		No Limit Nodes		12		Disabled	

Part II

SD-WAN



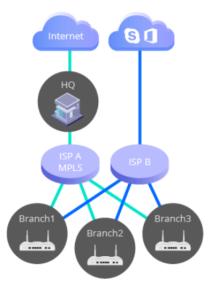
Chapter 4 SD-WAN Solution

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

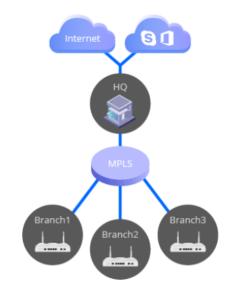
However, with adopting more and more SaaS and private/public cloud applications, we need new technologies that can efficiently and dynamically route different traffics either to the central site or to the cloud directly.

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

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



Direct Internet Access with lower cost



Tunneled via Central Site with higher cost

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

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



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

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

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

4.1.1 Enabling SD-WAN on VigorACS

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

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

5	Network & Service Management / Network Ma	nagement				
	Scouth by Device III/Name/Model/MAL/IP Addr Q 韋	Setting Map Alarm Setting				
	 Root Network(165) Alan(13) 	+Add New Network ElDelete This Network	Change Network			
	D fac(0)					
	[/	General Settings				
	() the mis(0)	Authork (D		Osername		
	b A pp(3)	10		rd8network		
	0 A pqc(3)	Name		Passmert		
	 tra1(7) 	rdä	~			
	b an rd2(29)	Location				
	5 m rd3(11)					
	D A rd5(8)					
	0 A rd6(60)	Advanced Settings				
	p 👬 rd7(20)					
	b 35 rd8(11)	Enable SD-WAN				
	(* 22.103(0)					
	(r 👫 (yrone(i))					Say
	(r 🚓 tyrone(0)					Sav
						Sav
						Sav
	Til Delete Devices	Alivanced Settings				Sav
	Dente Devices					Sav
	IDenteta Devicas IP #1 rd5(8) IP #1 rd5(6) IP #1 rd5(70) IP #1 rd5(1)	Alivanced Settings Ender 50-WAN				Sav
	Понита рекисак 0 ф. (65(8) 1) ф. (66(60) 2) ф. (67(20))	Enable SD-WAN				Sav
	IDenteta Devicas IP #1 rd5(8) IP #1 rd5(6) IP #1 rd5(70) IP #1 rd5(11)	Enable SD-WAN				Sav
	IDenteta Devocas IP #1, rd5(8) IP #1, rd6(60) IP #1, rd7(20) IP #1, rd9(0)	Endle So-WAN	innifrais. You can hreefn selec	at the dilla you want to cover	if, use drags and drop to place exe	Sav ch category in the
	IDenteta Devocas IP #1, rd5(8) IP #1, rd6(60) IP #1, rd7(20) IP #1, rd9(0)	Endle SD-WAN.				
	IDenteta Devocas IP #1, rd5(8) IP #1, rd6(60) IP #1, rd7(20) IP #1, rd9(0)	Encle SD-WAN Bulk Data Settings Set the category of data to be collected for statistical a corresponding profile and specify the report interval a operation.	at which the profile returns I		lisable bulk data categories, it w	ill affect the SD-WAI
	IDenteta Devocas IP #1, rd5(8) IP #1, rd6(60) IP #1, rd7(20) IP #1, rd9(0)	Endle SD-WAN.				ill affect the SD-WAI
	Detects Devices 0 #a rd5(8) 0 0 #a rd6(60) 0 #a rd6(60) 0 #a rd7(20) 0 #a rd9(9) 0 #a rd9(9) 0 #a tyrone(0)	EVEN BO-WAN EVEN Data Settings Bulk Data Settings Set the category of data to be collected for statistical a goresponding profile and specify the report interval a goreation Profile E1 reason second mennal (sec)	Profile #2 Report Internal (sec)	bulk data to the ACS. If you d	Isable bulk data categories, if w Available / Disabled Bulk Da	all affect the SD-WAI
	Detects Devices 0 #a rd5(8) 0 0 #a rd6(60) 0 #a rd6(60) 0 #a rd7(20) 0 #a rd9(9) 0 #a rd9(9) 0 #a tyrone(0)	Encle SD-WAN.	et which the profile returns I	bulk data to the ACS. If you d	Ibable bulk data categories, if w Available / Disabled Bulk Da	oll affect the SD-WAI ata Categories Size 8
	Detects Devices 0 #a rd5(8) 0 0 #a rd6(60) 0 #a rd6(60) 0 #a rd7(20) 0 #a rd9(9) 0 #a rd9(9) 0 #a tyrone(0)	EVEN BO-WAN EVEN Data Settings Bulk Data Settings Set the category of data to be collected for statistical a goresponding profile and specify the report interval a goreation Profile E1 reason second mennal (sec)	Profile #2 Report Internal (sec)	bulk data in the ACS. If you d	Isable bulk data categories, if w Available / Disabled Bulk Da	all affect the SD-WAI
	Detects Devices 0 #a rd5(8) 0 0 #a rd6(60) 0 #a rd6(60) 0 #a rd7(20) 0 #a rd9(9) 0 #a rd9(9) 0 #a tyrone(0)	Bulk Data Settings Bulk Data Settings Set the category of data to be collected for statistical a corresponding profile and specify the report interval a specifient. Profile El pairs Report menval (sec) 120	Profile #2 Roport Interval (sec) 300	bulk data in the ACS. If you d	Ibable bulk data categories, if w Available / Disabled Bulk Da	sill affect the SD-WAI ata Categories Size 8

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

- Auto VPN
- VoIP WAN, and

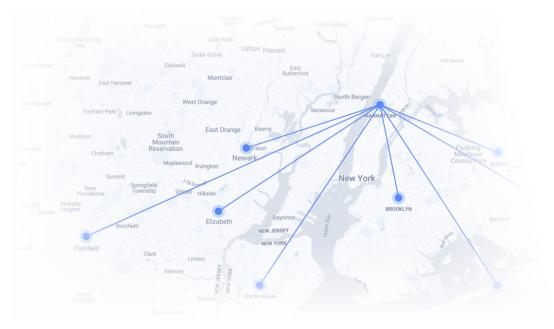
• Full Traffic Control with SD-WAN Route Policy

4.1.2 Auto VPN

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

• For Hub and Spoke(s)

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



For Full Mesh

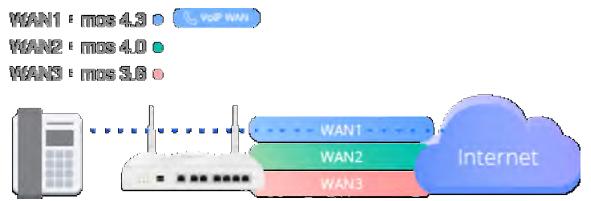
VigorACS server will create tunnels between each router automatically. If a subnet conflict occurs, VigorACS server is capable to design and suggest LAN subnets for all devices.



4.1.3 VoIP WAN

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

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



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

Real-time Call Quality Monitoring

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

Live Failover when Having Poor Call Quality

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

Live Failover Scenarios

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

4.1.4 Full Traffic Control with the Route Policy

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

Please select a network, but do not select the Root Network.

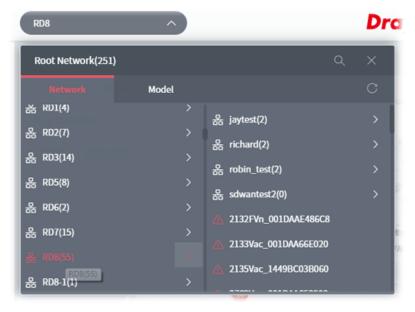
			RD8 (1)		<u> </u>	
	Ro	ot Netwo	ork (1)			×
			Model			C ~
a>	<	Root Ne	etwork > RD8			
				>	₽ 2927Vac_1449BC22C588	

Then open Configuration>>Route Policy>>+Add New Route Policy.

Enable		
Comment	For_MKT_education	
Source	Апу	~
Destination	App Services	~
App Service Profile	Create a new profile From an existing profile	
Selected App Service	WhatsApp 🛞	
Send via Interface O Note If you want to send via VPN First. Go to SD, WAN VPN Set	WAN 1 (to the Hub), please dial VPN Hub and Spoke connection	~
① Note If you want to send via VPN first. Go to SD-WAN VPN Set	(to the Hub), please dial VPN Hub and Spoke connection tings	
() Note If you want to send via VPN	(to the Hub), please dial VPN Hub and Spoke connection	
① Note If you want to send via VPN first. Go to SD-WAN VPN Set	(to the Hub), please dial VPN Hub and Spoke connection tings	
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway	(to the Hub), please dial VPN Hub and Spoke connection tings Default Gateway Specific Gateway	
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway Packet Forwarding to WAN/LAN	(to the Hub), please dial VPN Hub and Spoke connection tings Default Gateway Specific Gateway	
Note If you want to send via VPN first. Go to SD-WAN VPN Set Send via Gateway Packet Forwarding to WAN/LAN via	(to the Hub), please dial VPN Hub and Spoke connection tings Default Gateway Specific Gateway	

4.2 Dashboard for SD-WAN Network Group

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



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

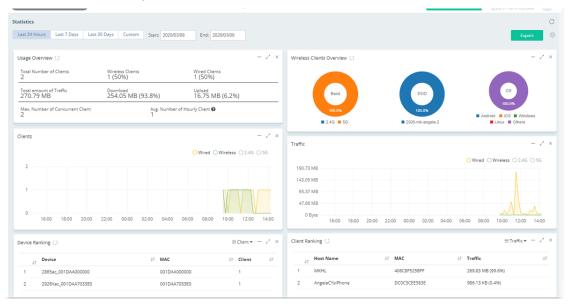
Ô	Dashboard					\bigcirc Auto Refresh: 5 minutes \checkmark
61	Summary SD-WAN					
62	Wirele	ss WAN	IPsec VPN () 24 hrs	Other VPN (3 24 hrs)	VolP	🔘 7 days
=						
2	Average MOS MOS Compliancy	No Data	Average MOS MOS Compliancy	No Data	Average MOS 3.9	MOS Compliancy 33 $\% \ge 4.0$
	3.2 26 % ≥ 4.0		3.4 31 % ≥ 4.0		~ 3.9	~ 33%
2	~ 3.2 ~ 26%		~* 3.4 ~* 31%			
	Active Physical WAN		Active VPN		Active VoIP Call	etected 67117 - Failovered 33451
_			ALL COMPANY			t1hour
	• Wired			IPSec 9	80	٨
	10 WAN Online LTE	ess 2.4G / 5G 0	9	SSL 0 L2TP 0	40	
(3)	WAN Online USB	0	VPN Online	• PPTP 0	20	////
85					2.25 pm 2.35 pm 2.45 pm	2.65 pm 3.05 pm 3.16 pm
()						
0	Active Physical WAN Quality		Active VPN Quality		Active Call Quality	
	Great 4.3-5.0	2	Great 4.3~5.0	3	Great 4.3~5.0 +	
	Good 4.0~4.2		Good 4.0~4.2		Good 4.0~4.2	30098
	Okay 3.6~3.9		Okay 3.6~3.9		Okay 3.6~3.9	
	Poor 3.1~3.5 Bad 1.0~3.0	2	Poor 3.1~3.5 Bad 1.0~3.0		Poor 3.1~3.5 Bad 1.0~3.0	
	Bad 1.0~3.0	5	Bad 1.0~3.0		Bad 1.0~3.0	0
	2 Routers are Having Poor Active Physical WAN Qual	lity.	4 Tunnels are Having Bad Active VPN Q		10 Routers are Having Poor Active Cal	
	2952Pn_001DAA000001, 2952Pn_001DAA000007 5 Routers are Having Bad Active Physical WAN Quali	ty.	2952Pn_001DAA000009, 2952Pn_001D/	A000008, 2952Pn_00	2952Pn_001DAA000009, 2952Pn_0010	DAA000008, 2952Pn_00…
	2952Pn_001DAA000009, 2952Pn_001DAA000008, 29					
		More		More		More

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

	are not counted at the moment).
	VigorACS only captures the signals from the SD-WAN CPE with VoIP feature.
More	Click to access the Monitoring>>WAN, VPN, or VoIP web page to get more detailed information.

4.3 Statistics for SD-WAN Network Group

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



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

4.4 Monitoring for SD-WAN Network Group

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

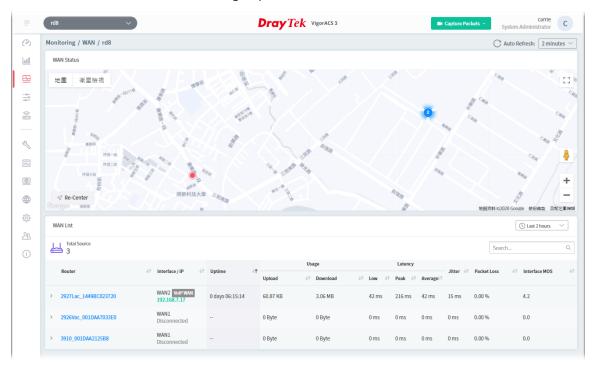
(7)	Monitoring	
1 600	Alarm	
I 🗠	Logs	
	Devices	e
-0-	Clients	
	Cellular Data Usage	w B
	Floor Plan	
Z	Rogue AP Detection	
F	WAN (SD-WAN)	
(章)	VPN (SD-WAN)	
	VoIP (SD-WAN)	
	Data Usage (SD-WAN)	

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

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

4.4.1 WAN (SD-WAN)

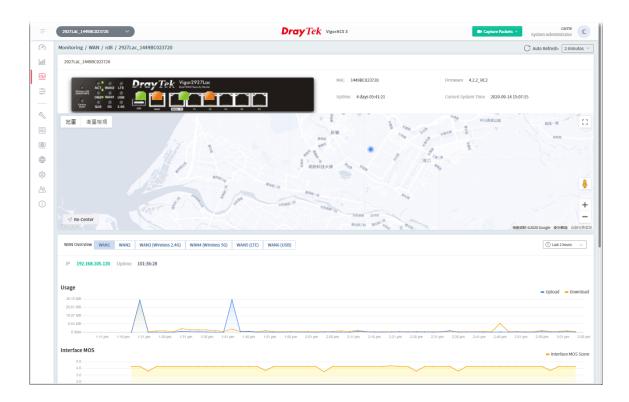
This page displays the location, name, interface/IP, uptime, usage, latency, jitter, packet loss and interface MOS of the routers within the group.



These parameters are explained as follows:

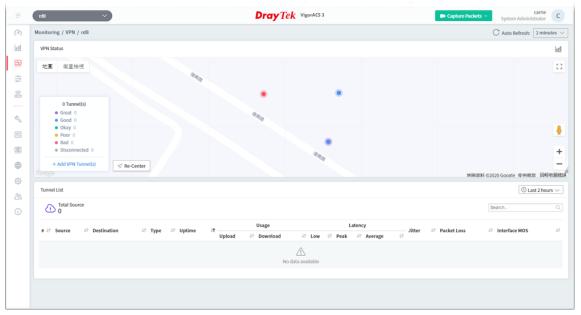
ltem	Description
WAN Status	Displays the location of the network group.
WAN List	Displays the total number of CPEs within the selected group.

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



4.4.2 VPN (SD-WAN)

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



4.4.2.1 AutoVPN Establishment

As a Hub-and-Spoke network,

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

4.4.2.2 Creating VPN with Basic Mode

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

VPN Setup	×
Туре	Hub and Spoke Full Mesh
Enter Server Hostname	
Server Hostname	Max : 128 characters
Hub Devices	2865L_1449BC37E740 (Vigor2865L) ⊗ 2927Vac_1449BC22C588 (Vigor2927Vac) ⊗
Support spokes count	32
	+ Advanced Mode
	× Cancel B Save and set to CPEs

These parameters for Basic Mode are explained as follows:

ltem	Description
Туре	Hub and Spoke - Simply select a router as the hub router, the rests would be spokes automatically.
	VPN Setup ×
	Type Hub and Spoke Full Mesh
	Enter Server Hostname
	Server Hostname Max: 128 characters
	Hub Devices 2865L_1449BC37E740 (Vigor2865L) ③ 2927Vac_1449BC22C588 (Vigor2927Vac) ③
	Full Mesh - It is effective only when there are more than three CPEs on the group.
	VPN Setup
	Type Hub and Spoke Full Meety
	Full Mesh Devices 2865L 14498C37E740 (Vigor2865L) ③ 2927/Vac_14498C23C588 (Vigor2927/Vac) ④
	+ Advanced Mode
	x Cancel (B) Save and set to CPEs
Enter Server	Switch the toggle to enable/disable the function.
Hostname	Server Hostname – Enter the hostname, URL of the server to establish the VPN connection.
Hub Devices / Full Mesh Devices	Lists the name of the hub device or full mesh device. Select one device as the hub device.
Support spokes count	Displays the total number of devices, excluding the main device.

+Advanced Mode	Click to open the configuration page with more options.
Save and Set to CPEs	Save the above configuration and set to CPE devices.

2. Click Save and set to CPEs.

ett ~	Dray Tek VigorACS 3	Bit Capture Packets - Cyliner Advisoritation
	Creating VPN Hub and Spoke Connections One Please wait for a while.	
	 Succeed: 0 Processing: 0 Waiting: 0 Failed: 0 To Succeed: 0 	

3. The VPN tunnel has been set successfully.

4.4.2.3 Creating VPN with Advanced Mode

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

VPN Setup	×
Туре	Hub and Spoke Full Mesh
Enter Server Hostname	
Server Hostname	Max: 128 characters
Hub Devices	2865L_1449BC37E740 (Vigor2865L)
Support spokes count	32
	+ Advanced Mode
	× Cancel Save and set to CPEs

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

ype	Hub and Spoke Full Mesh	
nter Server Hostname	đ	
ub Devices	2927Vac_1449BC22C588 (Vigor2927Vac) 🛞	
	2865L_1449BC37E740 (Vigor2865L) ③	
support spokes count	32	
Spoke Devices	Select spoke devices	
VPN Connection Through	WAN1 First ~	
Dial Type	IPsec Tunnel PPTP L2TP SSL	
IPsec		
Customize IKE Pre-Shared Ke	у 💽	
IKE Pre-Shared Key	Required, Please input IKE Pre-Shared Key	
IPsec Security Method	AES	~

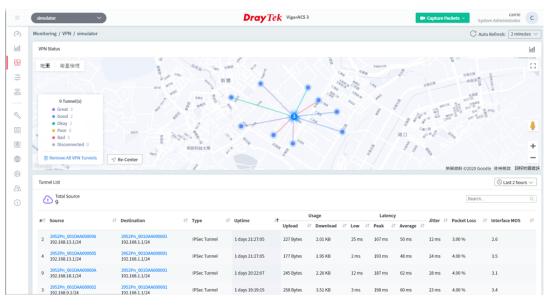
These parameters for Advanced Mode are explained as follows:

ltem	Description
Spoke Devices	Lists the name of the devices. Select one device as the spoke device.
VPN Connection Through	Select a WAN interface. WANx First - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the router will use another WAN interface instead. WANx Only - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the connection will be off.
Dial Type	Select one of the tunnels for this VPN profile.IPsec TunnelPPTPL2TPSSL
IPsec - IPsec Tunne	el is selected as Dial Type
IPsec	Customize IKE Pre-Shared Key - Click to enable or disable the IKE PSK setting. IKE Pre-Shared Key - Enter a string as PSK.
	IPsec Security Method - Authentication Header (AH) means data will be authenticated, but not be encrypted. The Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security. DES_NO_AUTH, 3DES_NO_AUTH and AES_NO_AUTH means the packets will be encrypted with no authentication.

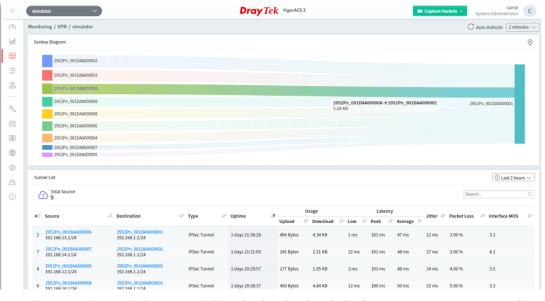
	AES ~
	AH
	DES_NO_AUTH
	DES
	3DES_NO_AUTH
	3DES -
	AES_NO_AUTH
	AES
PPTP - PPTP is	s selected as Dial Type
РРТР	Username - Enter a username for establishing VPN connection.
	Customize Password - Click to enable the password configuration.
	 Password - Enter a username for establishing VPN connection.
	PPP Authentications - Authenticate dial-in users using the PAP protocol
	only or PAP/CHAP/MS-CHAP/MS-CHAPv2.
	VJ Compression - Click to enable Van Jacobson (VJ) header compression
	to improve throughput on slow connections.
	Dial Type IPsec Tunnel PPTP L2TP SSL
	PPTP
	Username Generate automatically
	Customize Password
	PPP Authentications PAP/CHAP/MS-CHAP/MS-CHAPv2 v
	VJ Compression
	colorted as Dial Type
	selected as Dial Type
L2TP	L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:
	 None - Do not apply the IPsec policy. Accordingly, the VPN
	connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.
	 Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one
	pure L2TP connection.
	 Must - Specify the IPsec policy to be definitely applied on the L2TP connection.
	Username - Enter a username for establishing VPN connection.
	Customize Password - Click to enable the password configuration.
	 Password - Enter a username for establishing VPN connection.
	PPP Authentications - Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.
	VJ Compression - Click to enable Van Jacobson (VJ) header compression
	to improve throughput on slow connections.

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

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



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



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

v	PN Overview												(© La	st 2 hours 🗸
	earch VPN Tunnel List Q	To 2952Pn_001DAA0	000003 IP	192.168.105.52										
	Total													
1	To 2952Pn_001DAA000002 192.168.105.52	COD Bytes											Upload 🗕	Download
2	To 2952Pn_001DAA000003 192.168.105.52	400 Bytes 200 Bytes												
3	To 2952Pn_001DAA000004	0 Byte	1:26 pm	1:30 pm	1:40 pm	1:50 pm	2:00 pm	2:10 pm	2:28 pm	2.30 pm	2:40 pm	2:50 pm	3.00 pm	3:10 pm
4	To 2952Pn_001DAA000005	Interface MOS											 Interface I 	MOS Score
5	To 2952Pn_001DAA000006	3.0 2.0 1.0											L	
6	To 2952Pn_001DAA000007	0.0	1:26 pm	1:36 pm	1:48 pm	1:58 pm	2:08 pm	2:18 pm	2:28 pm	2:38 pm	2:48 pm	2:50 pm	3.06 pm	3:16 pm
7	To 2952Pn_001DAA000008	200 ms 150 ms										-	Low – Averag	e – Peak
-	To 2952Pn 001DAA000009	100 ms												

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

4.4.3 VoIP (SD-WAN)

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

110	ring / Vo	P1/ simulator														.(
nik (CATLIN													0	🕚 Last Z hou	in i
1	-	11	991 4	08	4	0										
1	1414	Great				Bad										
5	Tocal	5.0 - 4.3	4.2 - 4.0 3.9	- 3.6	3.5 - 3.1 3.0	= 1.0										
	-													_		
		a	AU/15981 Acov	re (758)	Finished (810)						Rows	10 •	10 ×	1	160 1	(4)
											Latency					
	Status	LAN IP	Peer IP	Call ID	Via Interface	Start Time	19	Failovered Interface	Up Time	Low 17	Peak 1	Average	Jim.	ir Pi	ecket Loss	Mos
	8	192.168.120.118	40.197.130.34	8850	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:37 PM		-	00.00.53	15 ms	484 ms	220 ms	12)	ms 0	9E	4
	C	192.168.120.119	281.242.7.112	8849	WANE	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:26 PM		~	00:01:04	7 mi	467 mi	240 mi	14	ni .1	n	4
	ß	192,168,120,120	140,51,54,84	8848	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:57 PM			00:00:33	18 ms	478 ms	279 ms	12-	ms 0		4
	S	192,168.120.116	98,108,133,232	8846	WAN1	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:46 PM		5	00:00:44	10 ms	493 ms	252 ms	(2)	ns D	¥.	3.8
	6	192,168.120,117	147.116.111.78	8845	WANT	2020/03/19 03:53:30 PM Local Time: 2020/03/19 03:52:41 PM		ie i	00:00:49	7 ms	4.61 ms	237 ms	14.	ms ú	4	4
						2020/03/19 03:53:30 PM										

These parameters are explained as follows

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

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

4.4.4 Data Usage (SD-WAN)

nd8 🗸	Dray Tek VigorACS 3	📾 Capture Packets –	System Administration C
Monitoring / Data Usage / rd8			C Auto Refresh: 5 minutes
Source Map			
地面 美星模块			0
4		-	
Re-Center App Source Overview	200 0 1200 100 1200 200 200 200 500		() Last 2 hoes
			(i) i ant upstain at 2000/11/11 01:40 p
7 Teta Source	Sort By Device Name Traffic 4		Sowidt_
2927Lac_1449BC023720 Wgsr207Lac_(14486C029778)	2865as, 001DAA000000 Way-2005-c (0010A000000)	2865ac_14498C05F1A8 'Veger/INSec (1460AC8571A9)	
	Desertional Upload Download 111.02 MB 469.23 KB 115.56 KB	Upload 0 Byte	Download 0 Byte
		2927Lac 1449BC0237E8	

4.4.4.1 Data Usage of Selected CPE

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

292/Lac_14498C023720 V	Dray Tek VigorACS 3		In Capture	Packets - System Administrator C
Monitoring / Data Usage / rd8 / 2927Lac_14498C023720				C Auto Refresh: 5 minutes
2927Lac_14498C023720				1
Usage Sorting by Application Client Device				🕃 Last 2 hours 🔍
Total Search Calegory or Rep III				
	Protocol	211.43 440	Others	51.65 MI
	Instant Message	34.18 MI	· Vol	7.13 100
Total	Apple Services	2.17 407	Google Services	2.17 %
301.89	Streem	1.44 //10	 Turneting. 	928.10 m
	 Web HD. 	195.62 etc.	 Remote Control 	3.45 (3)
Traffic Line Chart Uppost/Download By Interface				
				- Upicad - Download
1000. 10010		A		
117M				
EDOIN		~ _		
New other follow total inter the other total	the one the the one one	5-00pm (00pm (00pm 1)	ten i fine i fine i file	e Silve (See 14)e 14)e
Usage List by Application Client Device				

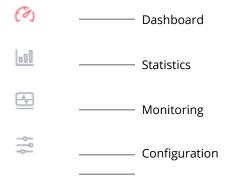
These parameters are explained as follows:

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

	Application - Clic					isage.
	Client Device - C	lick to disp	lay a pie ch	hart for the	selected CPE.	
Traffic Line Chart	Displays a line ch interface. Upload/Downloa By Interface - Cli interface.	ad - Click to	display da	ata upload/o	download.	
Usage List by	Displays the data	usage for	common A	ons or for c	onnected clien	+
	Application - Clic applications, inclu download usage.			ation, numb		
	(7) Monitoring / Bata Usage / elli / 2027Lac_144000	078720	Druy lek	- Andrew - A	0	Auto Belivede Stematole -
	Image: Source of the second state of the second s	iter 3.74 ter	 Apple Service Postcal Cogis Servic Web ND 		0.2140 8 000er 30100 8 Davidg 12140 8 07 3244	Quer M Days
	Tuells Line Duel Type=Thomson (types)	500				- Uylaad - Oywythaat
	s 4: App Name	Users		Upload	Unage	
	3 Faorbook/Instagram	6 0		0 Byte 0 Byte	0 Byte 0 Byte	
	Client Device - C including host na system, upload an	me, IP add	ress, MAC			
	Usage List by Application Classic Days					
	Visige Litt by Appleances Comp Davis	a MAC Address	🗧 Connection Type	- 05 -	Dauge	
	9 2 Host Name - 19 Address 1 adam MBP 192,156,124,12	MC#8980205462	T Winniess (SG)	C 208 Bytes	Daage Download 132 Bytes	
	F 2 Mod Name IP Address 1 adam 9800 100.256.126.12 2 2 Universe 102.166.126.12 3 3 F2000175 182.166.124.10	80/80/922 6/42 0050/9398883 840/745947799	7 Winniess (SG) 전 Word 회 Wind		tosage Download E32 liptes 2,34 KB 4,44 KB	
	2 Nort Name P Address 1 adam MBP 892.104.124.12 7 Unknown (NV.104.124.20	8C80962C6662 00507F398882	ाण Winniess (SG) की Winni	 201 Bytes 3.92 HB 	2.14 KB	

Chapter 5 SD-WAN CPE

The menu items related to a CPE:



5.1 Dashboard for SD-WAN CPE

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



In this case, we choose Vigor2865 series (e.g., Vigor2865Vac) as an example.	
--	--

Dray Tek vi	gorACS 3	2865Vac_1449	BC34FE98	~		P	ap 🗘	11:47:29 7/23/24	mk_carrie System Administrator	
2865Vac_1449BC3	4FE98			Device Status: 🥝	Online A	arms: 0 Active	Clients: 0	Auto Refre	sh: Disable ~	
Port Status				WAN Overview					③ Last 24 hou	urs-
	Phone 2 UNIX		Part 03	781.25 KB 585.94 KB 390.63 KB 195.31 KB	M	~				~
Device Informati	on	DSL Information		0 Byte 12:00	16:00	20:00	00:00	04:00	08:00	
Device Name	2865Vac_1449BC34FE98	DSL Status	TRAINING	Total (↑2.69	MB ↓22.10 M	IB)			1	.00 %
IP Address	http://192.168.106.141:80	DSL Type	VDSL2	WAN1 (↑0 By	rte ↓0 Byte)					0%
Network Name	AutoTest_VPN	Download Speed(kbps)	0	WAN2 (↑2.69	MB ↓22.10	MB)			1	.00 %
Model	Vigor2865Vac 🥏	Upload Speed(kbps)	0	WAN3 (↑0 By ⊄	rte ↓0 Byte)					0%
Firmware Version	4.4.2_STD 🤣	SNR Margin	0	WAN4 (↑0 By	rte ↓0 Byte)					0%
MAC Address	14:49:BC:34:FE:98	Loop Attenuation(0.1dB)	0	WAN5 (↑0By ≪	rte ↓0 Byte)					0%
Up Time	95 days 18:42:09	CRC Errors	0	WAN6 (↑0 By	rte ↓0 Byte)					0%
	~ show more		~ show more	WAN ↓↑ Line/Mo	ode	↓† IP	ψŤ	Uptime	$\downarrow\uparrow$ Active Mode	$\downarrow\uparrow$
System Resource	2		③ Last 24 hours-	WAN1 VDSL2	/			0d 00h 00m	Always On	
CPU	1%	Memory	83 %	WAN2 Ethern	et / Static IP	192.168.106	.141	41d 20h 53m	Always On	
15%		100%		WAN3 Wireles	ss_2.4G /			0d 00h 00m	Always On	
10%		75% 50% 25%		WAN4 Wireles	ss_5G /			0d 00h 00m	Always On	
0%	20:40 02:00 07:20	0%	07:20	WAN5 USB/-	-			0d 00h 00m	Always On	
Connectivity and	l Alerts			WANG USB/-				0d 00h 00m	Always On	
ld ↓↑ Start Ti	me ↓↑ Clear Time	↓↑ Type ↓↑ Messag	je ↓↑	LAN Overview					③ Last 24 ho	urs-
	No data	available		1					 Active Clients 	

5.2 Statistics for SD-WAN CPE

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

rd8 ~		DrayTek VigorAC	S 3	Capture	Packets Y System Administrator C
Statistics					C
Last 24 Hours Last 7 Days Last 30 Da	sys Custom Start: 2020/03/08 Er	nd: 2020/03/09			Export
Usage Overview (.)		- 2 ×	Wireless Clients Overview (,)		- 2 ×
Total Number of Clients V 2	Nireless Clients Wire 1 (50%) 1 (5	d Clients 0%)			
Total amount of Traffic 270.79 MB	Download Uplo 254.05 MB (93.8%) 16.7	^{ad} 75 MB (6.2%)	Band	SSID	os
Max. Number of Concurrent Client 2	Avg. Number of Hourly Cliv 1	ent 🛛	100.0% 2.4G 5G	100.0%	Android IOS Windows
Clients		- 2 ×			
	O Wit	red OWireless O 2.4G O 5G	Traffic		^ × ○Wired ○Wireless ○2.46 ○56
2			190.73 MB		
1			143.05 MB 95.37 MB		
		W V V	47.68 MB		
0 16:00 18:00 20:00 22:0	00 00:00 02:00 04:00 06:00 0	8:00 10:00 12:00 14:00	0 Byte 16:00 18:00	20:00 22:00 00:00 02:00 04:00	06:00 08:00 10:00 12:00 14:00
Device Ranking (.)		\equiv Client \bullet - e^{*} \times	Client Ranking 4.3		≡Traffic• - <⁄ ×
 ↓↑ Device	↓† MAC	.↓↑ Client .↓↑	↓↑ Host Name	J↑ MAC	J↑ Traffic J↑
1 2865ac_001DAA000000	001DAA000000	1	1 MKHL	406C8F525BFF	269.83 MB (99.6%)
2 2926Vac_001DAA7033E0	001 DAA7033E0	1	2 AngelaCYsiPhone	DC0C5CEE583E	986.13 KB (0.4%)

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

5.3 Monitoring for SD-WAN CPE

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

In this section, we choose Vigor2927Vac/Vigor2865ac series as an example.

(7)	Monitoring	
1 600	Alarm	:3
🗠	Logs	
	WAN (SD-WAN)	re
~	VPN (SD-WAN)	10
E.	VoIP (SD-WAN)	w B
	Data Usage (SD-WAN)	_

5.3.1 Alarm

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

ray	Tek vi	gorACS 3		2927Vac_1449BC	22C438_101.1	✓ Q		Pcap	¢ P	11:59:38 7/23/24 Syste	mk_cari m Administra	
Monitoring / Alarm							2024/06/23 to 2024/07/23 V Search No. / Device Name / MA					/MAC C
Alarm	0 н	istory										
	te 🖶 Dele	te All	ownload						И	< 1 /1	> 1	Я C'
	No.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Ty	ype	Ack Time	Ack Us
	37554252	Not Ack	2024/07/23 05:29:34	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	🛦 Critical	Device Loss Connection	Device	Lost Connection		

ray	Tek vig	orACS 3	2927Vac_14498	iC22C438_101.1 V	Q	Po	ap 🗘	12:01:14 7/23/24	mk_carrie	
Ionit	oring / Alarn	n				2024/06/23 to 20	Search No. / Device Name / MAC Q			
Alarr	n 🚺 🛛 His	story								
	iete 🕮 Delet	e All 🕹 Download					м <	1 /2	> N C	٢
	No.	Time	Device Name	Network Name	MAC Address	Clear Time	Alarm Lev	el Alarm P	Message	
	37465460	2024/07/22 05:26:06	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/23 05:03:49	\Lambda Critica	l Device	Loss Connection	
	37364051	2024/07/21 05:26:03	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/22 05:03:48	\Lambda Critica	l Device	Loss Connection	
	37252574	2024/07/20 05:28:51	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/21 05:03:42	🛦 Critica	l Device	Loss Connection	
	37215739	2024/07/19 05:36:55	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/20 05:04:08	🛦 Critica	l Device	Loss Connection	
	37052935	2024/07/18 05:28:57	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/19 05:03:47	🛦 Critica	l Device	Loss Connection	
	36953229	2024/07/17 05:28:53	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/18 05:03:43	🛦 Critica	l Device	Loss Connection	
	36915323	2024/07/16 17:16:51	2927Vac_1449BC22C438_101.1	U_2927_5	14:49:BC:22:C4:38	2024/07/17 05:04:13	\land Critica	l Device	Loss Connection	

These parameters are explained as follows:

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

5.3.2 Logs

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

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

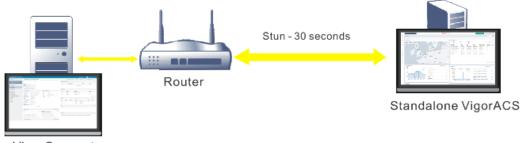
₹	Ľ	Dray	Tek v	igorACS 3		2865Vac_1449BC34FE98	~ ~		Pcap	13:11: 7/23		М
(7)		Monit	oring / Log	iz				203	4/06/23 to 2024/0	7/23 ~ sea	rch ID / Device Name / Device 🔍	۶.
				Device Reboot Reboot By CPE	Reset System Pass	word Set Parameter	File Transfer Setting Pro	ofile Device Syslog	CPE Notify	Device Registe	r Device Operate	
			ete 🛱 Del	ete All 🕹 Download					к	I < 1	/17 > ▷ Ĉ 🛞	
],			ID	Device Name	Device ID	MAC Address	Current IP	Logged IP	Action	Action ID	Time	
-83-			212081	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 12:36:41	
Z			212080	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 10:51:39	
			212041	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:21:33	
\$			212038	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:06:31	
			212035	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/23 05:00:13	
ŝ			212034	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 16:36:19	
ß			212023	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 14:21:17	
j)			212000	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 08:51:13	
			211998	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 08:36:13	
			211965	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 05:06:09	
			211962	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/22 05:00:15	
			211955	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/21 20:36:00	
			211938	2865Vac_1449BC34FE98	104956	14:49:BC:34:FE:98	192.168.106.141	192.168.106.141	Inform		2024/07/21 16:35:57	

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

5.3.3 Flow

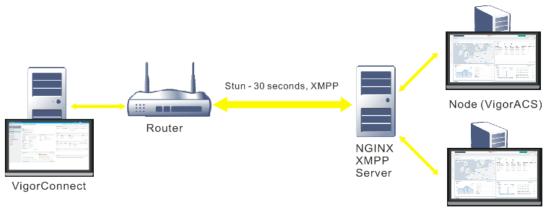
Vigor router adopts the function of NetFlow to collect the quantity and data of incoming and outgoing packets. With analysis of the collected data, the network administrator can get the source and destination IPs of the packets, type of network service, and the reason for network congestion.

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



VigorConnect

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



Node (VigorACS)

Dray Tek VigorACS 3 0 7175~ 1445 AFRE V R 0 ng / Flor 11 --0-1 3 R Ð . 0 28

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

Click Login Device to display the advanced page.

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

5.3.3.1 Device Overview

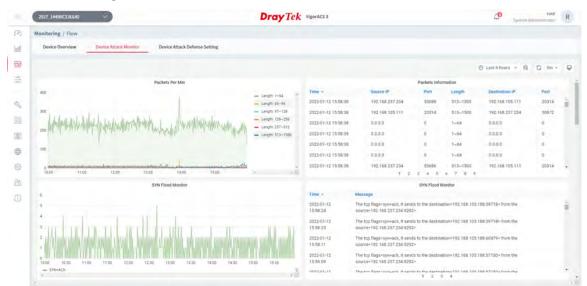
NetFlow uses several types of data to identify the data flow, for example, source IP address, destination IP address, source port number, destination port number, IP protocol, interface, and so on.

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

		Setting		
				⊙Lastóhours - Q Q Sm -
Inspect_SourceP 192	168 237 234 + Inspect_Dent/P 192 168 237 234 +			
	Top 10 Destinations From 192.168.237.	234		Top 10 Sources To 192.168.237.234
Destination IP		Usage ~	Source IP	Usage ~
192.168.105.111		947.7 kB	192 168 105 180	1.7 MB
192.168.105.180		842.0 kB	192.168.105.111	1.4 MB
192.168.105.238		139.3 kB	192.168.105.188	296.6 kB
192.168,105,188		125.3 kB	192.168.105.238	73.0 kB
192 168 105 235		8.3 kB	192.168.105.235	08
8.6.8.8		6.6 kB	192.168.105.234	0.8
192.168.105.234		4.1 MB	8.8.8.8	0.8
224.0.0.251		0 R.	274.0.0.251	nR
	Flow Usage			L3 Protocol Visit Rate
		- DownStream 3.5 MB		- LOP 72.8
		- upStream 3 t MB		- LOP 72.8 TOP 27.2
				- Others D.O

5.3.3.2 Device Attack Monitor

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



5.3.3.3 Device Attack Defense Setting

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

	2007_14498C13E640 ~		Dray Tek VigorACS 3	Dynam Administrator
en.	Monitoring / Flow			
hel.	Device Overview Device Attack Monitor	Davion Attack Delansa Setting		
E	Device Upstream Flow			
	Enable	0		
2	Fraquency	30 min	¥1	
	Volume	1	GB -	
(30)				
	Device Downstream Flow			
Ō	Enable	0		
<u>B</u> \$	Frequency	30 min	(w)	
Q	Volume	1	68 -	
	Inspect Source Flow			
	Enable	100.		
	Frequency	30 min	<i>3</i> 1	
				Saw

ltem	Description
Device Upstream	Flow / Device Downstream Flow
Enable	Switch the toggle to enable the function of monitoring all upstream flow / downstream flow via this router. - means "Enable". - means "Disable".
Frequency	Set the timeout value.
Volume	Set the threshold value.
1046 7.50 km 8.46 3.30 km 9.70 to 37 11.00	1128 1220 1230 1230 1230 1230 1230 1230 1469 14.03 1508 1508 1508 1649
35.44B	Top 10 UpStream Usage
20146 20146 20146 11106 100 5 00 0 0 1000	100 12.05 13.00 13.05 14.00 14.05 14.00 100 12.05 13.00 13.05 14.00 14.05 14.00
Increase Source El	aw / Inspect Destination Flow
Inspect Source Fi	ow / Inspect Destination Flow
Enable	Switch the toggle to enable the function of monitoring the data flow for specified source IP / destination IP.

Frequency	Set the timeout v	alue.				
Volume	Set the threshold	l value.				
See the following e	example figure					
Monitoring / Flow Device Attack Monitor	Device Attack Defense Setting					
			⊙Last6haurs - Q, C, tm - Q			
Impett, Sourcell 192,108,237,234 - Inspect, Dentif	192.168.237.234 -		O Leité Nours - El C Im - U			
	Top 10 Destinations From 192.168.237.234		Top 10 Sources To 192.168.237.234			
192.168.105.111	Usage ~ 34 T MB	192.168.105.230	Ullage - 227.5 MS			
192.168.105.230	32.1 MB 935.0 kB	192.168.105.111	2.6 MB 2.2 MB			
192.168.105.238	90.0 18	192.168.105.238	69.6 kB			
192.168.105.235	8.7k8 6.618	192.168.105.235	08 08			
192 168 105 234	4.758	1.8.8.8	08			
224.0.0.251	0 R	2240.0.281	08			
APP Flow						
Enable		to enable the function ous APPs via the rou	on of monitoring the data flow ter.			
Frequency	Set the timeout v	alue.				
Volume	Set the threshold	l value.				
SYN Flood						
Enable	Switch the toggle	to enable the function	on of monitoring SYN flood defense.			
	 When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources. The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively. 					
Frequency	Set the timeout v	alue.				
Volume	Set the threshold	l value.				
ICMP Flood						
Enable	When the arrival router will start to as defined in Tim The default value	rate of ICMP packets o randomly discard T eout. s of threshold and ti	on of monitoring ICMP flood defense exceeds the Threshold value, the CP SYN packets for a period of time meout are 250 packets per second			
Frequency	and 10 seconds,					
Frequency Volume	Set the timeout v					
UDP Flood		ו ימועכ.				
	Constants all and the	to operate the first				
Enable	When the arrival router will start t as defined in Tim	rate of UDP packets o randomly discard T eout.	on of monitoring UDP flood defense. exceeds the Threshold value, the CP SYN packets for a period of time			
	The default value and 10 seconds,		meout are 2000 packets per second			
Frequency	Set the timeout v	alue.				
Volume	Set the threshold	l value.				
volume	Set the threshold	value.				

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

5.3.4 Diagnostics

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

5.3.4.1 Ping

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

These parameters are explained as follows:

ltem	Description
Protocol	Select the protocol (IPv4 or IPv6) to perform the ping operation.
Ping Though	Select a WAN interface from drop down list to through which you want to perform the ping operation, or choose Auto to be let the router select the WAN interface.
Ping To	Select the type of target (Host/IP, DNS, Gateway) to which you wish to ping. DNS-8.8.8.8 ~ Host/IP DNS-8.8.8.8 Gateway2-192.168.105.1 ~
Source IP	Select a WAN IP as the source IP. If Auto is selected, the source IP will be specified according to the interface chosen for ping through.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Run	Click to perform the job.

5.3.4.2 Trace Route

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

← Configuration	2865ac_001DAA000000 / Monitoring / Diag	nostics	С
Ping	Туре	IPV4 IPV6	
Trace Route	Trace through	WAN1 ~ ~	
Routing Table	Protocol	ICMP UDP	
ARP Table DHCP Table	IP Address / Domain		
Sessions Table			
			un
			-

These parameters are explained as follows:

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

5.3.4.3 Routing Table

This page displays the IPv4/IPv6 routing information.

Configuration	2865ac_001	DAA000000 / Monitoring / Dia	gnostics					C
Ping	IPv4 Rout	ting Table						
Trace Route	Index	Destination	Subnet Mask		Gateway		Key	Iface
	1	0.0.0.0	0.0.00		192.168.105.1		•	WAN2
	2	192.168.105.0	255.255.255.0		directly connected		с	WAN2
ARP Table	3	192.168.10.0	255.255.255.255		192.168.1.2		S~	LAN1
DHCP Table	4	192.168.1.0	255.255.255.0		directly connected		C~	LAN1
Sessions Table	5	211.100.88.0	255.255.255.255		192.168.1.3		S~	LAN1
	IPv6 Rout	-	D					
	Destination	Prefix Le	ngth	Interface	Flags	Metric	Next Hop	P
	FE80::	64		LAN1	U	256	:	
	FE80::	64		LAN2	U	256		
	FE80::	64		LAN3	U	256		
	FE80::	64		LAN4	U	256		
	FE80::	64		LAN5	U	256	=	
	FE80::	64		LANG	U	256	=	
	FE80::	64		LAN7	U	256	=	
	FE80::	64		LAN8	U	256		
	FE80::	64		DMZ	U	256		
	FF00::	8		LAN1	U	256		
	FF00::	8		LAN2	U	256	2	

5.3.4.4 ARP Table

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

- Configuration	2865ac	_001DAA00000	0 / Monitoring / Diag	nostics							(
ling	🖯 Clea	r									
race Route	LAN	WAN									
Routing Table	Show L	AN		ALL LANS	~						
HCP Table	Show	LAN		ALL VLANS	~						
	Index	IP	MAC Address	HOST ID	Interface	VLAN	Port	Device	Description	Comment	
	15	192.168.1.10	18-D6-C7-01-A2-34	R1000675	LAN1		P3				
- Configuration Ping frace Route Routing Table 100 Table	2865ac © Cles LAN Show	wan	0 / Monitoring / Diag	gnostics ALL WANS	v						
ing race Route buting Table RP Table	Clea	wan	0 / Monitoring / Diag MAC Address		~ Interface	VLAN	Port	Device	Description	Comment	
race Route buting Table RP Table HCP Table	Clea LAN Show 1	wan	MAC Address	ALL WANS		VLAN	Port	Device	Description	Comment	
race Route buting Table RP Table HCP Table	Cles LAN Show1	WAN	MAC Address 00-1D-AA-F8-D8-19	ALL WANS	Interface	VLAN 	Port 	Device	Description	Comment	
² ing Irace Route	Cless LAN Show I Index 1	WAN WAN IP 192.168.105.52	MAC Address 00-1D-AA-F8-08-19 00-1D-AA-66-E0-21	ALL WANS	Interface WAN2	VLAN 	Port 	Device	Description	Comment	
ing race Route bouting Table IRO Table HCP Table	Clear LAN Show 1 Index 1 2	WAN 192.168.105.52 192.168.105.59	MAC Address 00-1D-AA-F8-D8-19 00-1D-AA-66-E0-21 00-1D-AA-F7-C0-E2	ALL WANS	Interface WAN2 WAN2	VLAN 	Port 	Device	Description	Comment	
ing race Route bouting Table IRO Table HCP Table	Clear LAN Show's Index 1 2 3 4 5	WAN IP 192.168.105.52 192.168.105.52	MAC Address 00-1D-AA-F8-D8-19 00-1D-AA-66-E0-21 00-1D-AA-F7-C0-E2 00-50-7F-F1-00-16	ALL WANS	Interface WAN2 WAN2 WAN2 WAN2 WAN2 WAN2	VLAN 	Port 	Device	Description	Comment	
ng ace Route suting Table RP Table HCP Table	Clear LAN Show 1 Index 1 2 3 4	 WAN WAN IP 192.168.105.52 192.168.105.52 192.168.105.62 192.168.105.62 192.168.105.81 192.168.105.81 192.168.105.81 192.168.105.84 	MAC Address 00-1D-AA-F8-D8-19 00-1D-AA-66-E0-21 00-1D-AA-F7-C0-E2 00-50-7F-F1-00-16 00-1D-AA-7D-65-14	ALL WANS	Interface WAN2 WAN2 WAN2 WAN2	VLAN	Port 	Device	Description	Comment	

These parameters are explained as follows:

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

5.3.4.5 DHCP Table

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

← Configuration	2865ac_001DAA	000000 / Monitoring / Diagn	ostics			C
Ping	IPv4 Address	Assignment Table				
Trace Route	Name	IP	Mask	Start IP	End IP	DHCP Server
Routing Table	LAN1	192.168.1.1	255.255.255.0	192.168.1.10	192.168.1.209	On
ARP Table	① Note:					
DHCP Table		ick on a specific LAN to display	the detailed information of	the DHCP client.		
Sessions Table	IPv6 Address	Assignment Table				
	Interface	IPv6 Address	IAID	Link-Layer Address	Leased Time	DUID
				No data available		

5.3.4.6 Sessions Table

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

Index Physite P Physite P Pased Pa								
B 121.68.110 6425 2827 8.8.4 53 WA2 c Rode 2 12.168.110 6425 2837 8.8.8 53 WA2 Ing Table 3 12.168.110 65156 2837 8.8.8 53 WA2 Place 4 12.168.110 65156 3308 2.229.06.30 43 WA2 Place 5 19.168.110 65196 3301 409.18152 43 WA2 Place 12.168.110 65196 3301 20.169.1912 43 WA2 Place 12.168.110 65196 3301 20.169.1912 43 WA2 Place 12.168.110 6519 3301 409.1912 43 WA2 Place 12.168.110 6519 5050 21.061.1210 609 WA2 Place 12.168.110 4930 5054 12.061.121 609 WA2 Place 12.168.110 4930 5054 12.061.211 609 WA2 Place 12.061.110 4930 5064 01.061	← Configuration	2865ac_001D	AA000000 / Monitoring / Dia	gnostics				(
1 12 <th< th=""><th></th><th>Index</th><th>Private IP</th><th>Private Port</th><th>Pseudo Port</th><th>Peer IP</th><th>Peer Port</th><th>Interface</th></th<>		Index	Private IP	Private Port	Pseudo Port	Peer IP	Peer Port	Interface
Image: Control (Control (Contro) (Contro) (Control (Contro) (Control (Contro) (Contro) (Contro) (Ping	1	192.168.1.10	64325	32837	8.8.4.4	53	WAN2
Number Number Plack 4 92.168.1.10 65196 33708 52.29.26.530 443 WAN2 Plack 5 92.168.1.10 65299 33801 40.90.189.152 43 WAN2 OP Table 6 192.168.1.00 65433 33945 204.19.197.219 43 WAN2 Attempt Fibbe 7 19.168.1.01 4907 5059 21.06.142.105 30513 WAN2 Attempt Fibbe 9 19.21.68.1.10 4907 5059 21.06.142.105 30513 WAN2 Attempt Fibbe 9 19.21.68.1.10 4904 5054 121.68.1.10 8069 WAN2 10 19.21.68.1.10 4934 5064 21.06.1.21.63 8069 WAN2 12 19.21.68.1.10 49364 5064 21.06.1.142.105 30513 WAN2 12 19.21.68.1.10 49364 5064 20.16.1.12.105 3069 WAN2 12 19.21.68.1.10 49364 5064	Trace Route	2	192.168.1.10	64325	32837	8.8.8.8	53	WAN2
Plade 5 92.168.1.10 55.299 339.1 4.90.189.152 443 WAV2 CP Table 6 192.168.1.10 65433 33945 204.79.197.219 443 WAV2 Singer Table 7 192.168.1.00 492.70 50550 210.61.142.105 30513 WAV2 Singer Table 7 192.168.1.01 49304 50580 192.168.121 3069 WAV2 10 192.168.1.01 49304 50580 192.168.1.01 8069 WAV2 11 192.168.1.01 49304 50580 192.168.1.01 8069 WAV2 12 192.168.1.01 49304 50580 192.168.1.01 8069 WAV2 12 192.168.1.01 49364 50640 20.168.1.21.51 8059 WAV2 12 192.168.1.01 49364 50648 192.168.1.04 8069 WAV2 14 192.168.1.01 49399 50678 192.168.1.04 8069 WAV2 14 192	Routing Table	3	192.168.1.10	65186	33698	216.58.200.227	443	WAN2
5 192.168.1.0 65289 3301 40.90.189.152 443 WAV2 CP Table 6 192.168.1.0 65433 33945 204.79.197.210 443 WAV2 status 7 141 7 192.168.1.0 65433 33945 204.79.197.210 443 WAV2 status 7 141 92.168.1.0 49270 5050 201.61.12.105 3051 WAV2 10 192.168.1.10 49304 5054 121.63.136 6069 WAV2 11 192.168.1.0 49324 50662 20.51.12 6069 WAV2 12 192.168.1.0 49364 50646 20.164.2.105 3051 WAV2 13 192.168.1.0 49364 50646 20.51.12.10 8069 WAV2 14 192.168.1.0 4938 50663 192.168.12.15 8069 WAV2 15 192.168.1.0 4939 50679 192.168.12.15 8069 WAV2 16 192.168.1.10 49497 50717	ADD Table	4	192.168.1.10	65196	33708	52.229.206.30	443	WAN2
6 19.1 hs.1.10 59.43 39.95 20.4.9.59/L19 443 MM2 2 datas Table 7 192.168.1.10 49270 5050 120.61.142.105 3051 MM2 8 192.168.1.10 49300 50580 120.61.12.105 8069 MM2 9 192.168.1.10 49304 50584 172.163.136 8069 MM2 10 192.168.1.01 49322 50602 192.168.2.1 8069 WA12 11 192.168.1.00 49364 50640 20.184.57.167 443 WA12 12 192.168.1.10 49364 50646 20.184.57.167 493 WA12 13 192.168.1.01 49380 50663 192.168.124.15 8069 WA12 14 192.168.1.01 49380 506679 192.168.124.11 8069 WA12 15 192.168.1.01 49437 50717 192.168.017 8069 WA12 16 192.168.1.01 49449 50728 192.168.01	Avo, table	5	192.168.1.10	65289	33801	40.90.189.152	443	WAN2
Number 8 192.168.1.10 4930 50580 152.168.1.10 8069 WAN2 9 192.168.1.10 4930 50580 152.168.2.1 8069 WAN2 10 192.168.1.10 4932 50602 192.168.2.1 8069 WAN2 11 192.168.1.10 49364 50640 20.184.57.167 443 WAN2 12 192.168.1.10 49364 50664 20.05.1142.105 30513 WAN2 13 192.168.1.10 4938 50668 192.168.124.115 8069 WAN2 14 192.168.1.10 49497 50717 192.168.017 8069 WAN2 15 192.168.1.10 4948 50728 192.168.0101 8069 WAN2 16 192.168.1.10 49499 50749 192.168.011 8069 WAN2	DHCP Table	6	192.168.1.10	65433	33945	204.79.197.219	443	WAN2
9 192.168.1.10 49304 50594 172.16.3.136 8069 WAV2 10 192.168.1.10 49322 50602 192.168.2.1 8069 WAV2 11 192.168.1.10 49364 50640 20.184.5.1.67 443 WAV2 12 192.168.1.0 49364 50646 21.05.1142.105 30513 WAV2 13 192.168.1.0 4938 50664 192.168.124.15 8069 WAV2 14 192.168.1.0 4938 50667 192.168.124.11 8069 WAV2 15 192.168.1.0 49437 50174 192.168.104 8069 WAV2 16 192.168.1.10 49448 50728 192.168.101 8069 WAV2 17 192.168.1.10 49459 50749 192.168.20.11 8069 WAV2		7	192.168.1.10	49270	50550	210.61.142.105	30513	WAN2
10 192.168.1.10 49364 50602 192.168.2.1 8069 WAN2 11 192.168.1.0 49364 50644 20.184.57.167 443 WAN2 12 192.168.1.0 49366 50646 21.06.1.42.105 30513 WAN2 13 192.168.1.0 49384 50688 192.168.1.2.1 8069 WAN2 14 192.168.1.10 49399 50679 192.168.1.2.1 8069 WAN2 15 192.168.1.10 49437 50717 192.168.50.17 8069 WAN2 16 192.168.1.10 49449 50728 192.168.20.11 8069 WAN2 17 192.168.1.10 49469 50749 192.168.20.1 8069 WAN2		8	192.168.1.10	49300	50580	192.168.121.1	8069	WAN2
11 192.168.1.10 49364 50644 20.184.57.167 443 WM2 12 192.168.1.00 49366 50646 20.05.1142.105 30513 WM2 13 192.168.1.00 49388 50668 192.168.1.24.15 8069 WM2 14 192.168.1.10 49399 50679 192.168.124.11 8069 WM2 15 192.168.1.10 49437 50717 192.168.0.17 8069 WM2 16 192.168.1.10 49488 50728 192.168.0.101 8069 WM2 17 192.168.1.10 49469 50749 192.168.0.1 8069 WM2		9	192.168.1.10	49304	50584	172.16.3.136	8069	WAN2
12 192.168.1.10 49366 50646 210.61.142.105 30513 WAN2 13 192.168.1.0 49388 50668 192.168.1.42.105 8069 WAN2 14 192.168.1.10 49399 50679 192.168.124.11 8069 WAN2 15 192.168.1.10 49437 50717 192.168.0.17 8069 WAN2 16 192.168.1.10 4948 50728 192.168.0.101 8069 WAN2 17 192.168.1.10 49469 50749 192.168.0.1 8069 WAN2		10	192.168.1.10	49322	50602	192.168.2.1	8069	WAN2
13 192.168.1.10 49388 50668 192.168.124.15 8069 WAN2 14 192.168.1.0 49399 50679 192.168.124.11 8069 WAN2 15 192.168.1.0 49437 50717 192.168.0.17 8069 WAN2 16 192.168.1.10 49448 50728 192.168.0.101 8069 WAN2 17 192.168.1.10 49469 50749 192.168.0.11 8069 WAN2		11	192.168.1.10	49364	50644	20.184.57.167	443	WAN2
14 192.168.1.10 49399 50679 192.168.124.11 8069 WAN2 15 192.168.1.10 49437 50717 192.168.0.17 8069 WAN2 16 192.168.1.10 49448 50728 192.168.0.101 8069 WAN2 17 192.168.1.10 49469 50749 192.168.0.11 8069 WAN2		12	192.168.1.10	49366	50646	210.61.142.105	30513	WAN2
15 192.168.1.10 49437 50717 192.168.50.17 8069 WAN2 16 192.168.1.10 49448 50728 192.168.50.101 8069 WAN2 17 192.168.1.10 49459 50749 192.168.20.1 8069 WAN2		13	192.168.1.10	49388	50668	192.168.124.15	8069	WAN2
16 192.168.1.10 49448 50728 192.168.50.101 8069 WAN2 17 192.168.1.10 49469 50749 192.168.20.1 8069 WAN2		14	192.168.1.10	49399	50679	192.168.124.11	8069	WAN2
17 192.168.1.10 49469 50749 192.168.20.1 8069 WAN2		15	192.168.1.10	49437	50717	192.168.50.17	8069	WAN2
		16	192.168.1.10	49448	50728	192.168.50.101	8069	WAN2
18 192.168.1.10 50192 51472 52.229.206.30 443 WAN2		17	192.168.1.10	49469	50749	192.168.20.1	8069	WAN2
		18	192.168.1.10	50192	51472	52.229.206.30	443	WAN2

5.3.4.7 DNS Cache Table

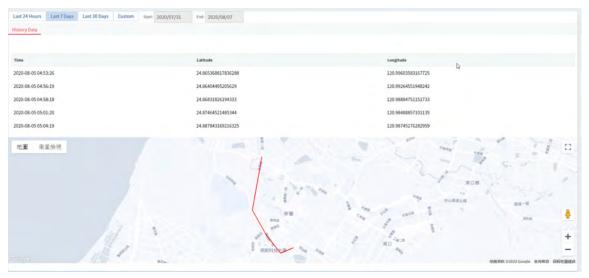
This screen shows the cache information related to DNS.

H.	Dray Tek VigorACS 3		vzeznac v Q	Pca	10-38-48 AM 10/14/34	rachel System Administration	
0	Ping	RClear TLOIG	2001:67C-4E&F004-9youtabe-uiLl.google.com	70			
	Trace Boute	JAN MART MAY BOOST - COM	2404:6800:4012;4::20youtube-uil.googts.com	70			
1400	Rossing Table	youtube-uil.google.com	2404-6800-4012:5=20youttube-ui.l.googie.com	70			
69	ARP Table	youtube-ull.google.com	2404:6800:4012:6:20youtube ull.google.com	70			
	DHCP Table	youtube-uil.google.com	2404-6800-4012-2::20c.tile.openstreetmap.org	70			
2	Sessions Table	c.tlle.openstreetmap.org	2A04.4E42.48::347	30			
-0	Sessor Land	www.youtuba.com	2404:6800:4012:5ct20www.youtube.com	189			
2	CRO Lance Caller	www.youtube.com	2404:6800:4012:2::20www.youtube.com	189			
		www.youtube.com	2404:6800:4012:4::20www.youtube.com	189			
98		www.youtube.com	2404:6800:4012:5::20pki-goog.i.googiv.com	189			
₽		pki-goog_i.googie.com	2404:6800:4012:2::20content-signature-2.cdn.mozilla.net	.35			
£		content-signature-2.cdn.mozilia.net	2600-1901-0-9249-	203			
(å)		b.tile.openstreetmap.org	2A04.4E42:48::347	.30			
		safebrowsing.googleapls.com	2404;6800;4012;4::200A	10			
28		_		_			
0		③ Note: An intry of which T11 shows "Static" is	a domain plants cristical in Applications, so LAN DHS				
		Deleto when an entry's TTL is larger than	Y1L must be between 5 and 214/483647, or 8 for				
			animid				$\overline{\Upsilon}$
						Cancel	ave.

5.3.5 GPS

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

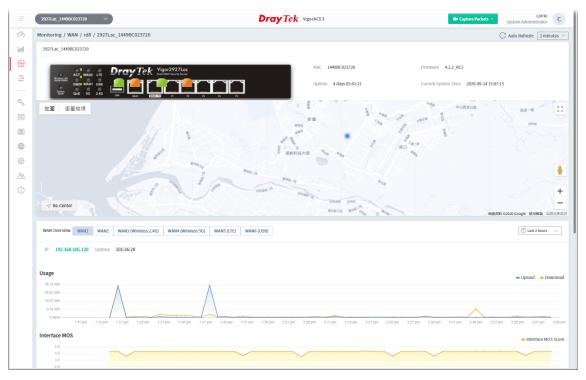
The GPS page will display the moving path (including time and coordinate position, latitude, and longitude) of the Vigor device.



5.3.6 WAN (SD-WAN)

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

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



These parameters are explained as follows:

-

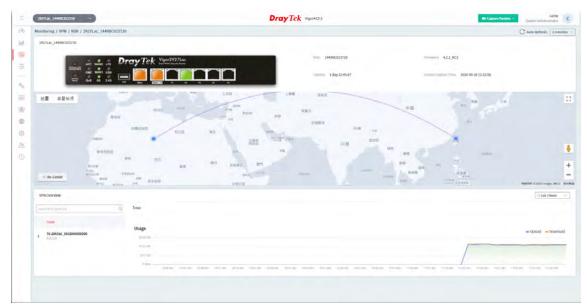
Description

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

5.3.7 VPN (SD-WAN)

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

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



5.3.8 VoIP (SD-WAN)

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

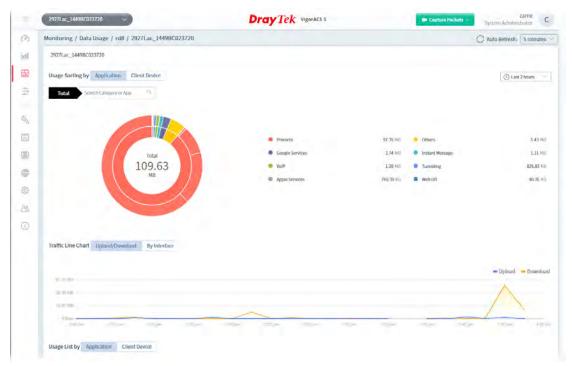
HP (CATLINE												C Last 2 ho	Nia 🤟
	~													
٢		11	991	408	4	0								
	1414	@ Great	. Good	Dkay.	· Poor	Bad								
	Total	5.0 - 4.3	4.Z = 4.0 3.	9 - 3.6	3.5 - 3.1 3.0	1 = 1.0								
	~													
		Q.	All /1598) Act	Dvp (738)	Finished (a10)					Rows	10 •	31 ×	7 7841 2	(4
										Latency				
	Status	LAN IP	Peer IP	Call ID	Via Interface	Start Time	Failovered Interface	Up Time				jitter	Packet Loss	MO
									Low 17	Peak	Average	149		
	3	192.168.120.118	40.197.130.34	8850	WANT	2020/03/19 03:53:30 PM		00.00.53	15 ms	484 ms	220 ms	12 ms	0.16	4
						Local Time: 2020/03/19 03:52:37 PM								
	C	192.168.120.119	281.242.7.112	8849	WANS	2020/03/19 03:53:30 PM		00:01:04	7 mi	467 mi	240 mi	14 mi	1.54	4
	0					Local Time: 2020/03/19 03:52:26 PM								
	8	192.168/120/120	140.51.54.84	8848	WAN1	2020/03/19 03:53:30 PM		00:00:33	18 ms	478 ms	279 ms	12 ms	0.16	4
		(sector) entire	Contenter		diam'r	Local Time: 2023/03/19 03:52:57 PM					are me	12 (12		
	3	192.168.120.116	98.108.133.232	8846	WANT	2020/03/19 03:53:30 PM		00:00:44	10 ms	495 ms	252 ms	12 ms	0.%	3.8
		1.1.1.1.1.1.1.1.1.1.1.1.1				Local Time: 2020/03/19 03:52:46 PM	10				100	12110		3.4
	6	192.168.120.117	147.116.111.78	8845	WANT	2020/03/19 03:53:30 PM		00:00:49	7 ms	461 ms	237 ms	14.ms	ú%	. 4
						Local Time: 2020/03/19 03:52:41 PM								
						2020/03/19 03:53:30 PM								

These parameters are explained as follows:

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

5.3.9 Data Usage (SD-WAN)

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



ltem	Description				
Usage Sorting by	Displays a pie cl	hart related to variou	us application	usage.	
	Application - C	lick to display a pie c	hart for vario	us application ι	usage.
	Client Device -	Click to display a pie	chart for the	selected CPE.	
Traffic Line Chart	Displays a line c interface.	hart related to data	upload/down	load, or traffic	via the V
	Upload/Downlo	oad - Click to display	data upload/	download.	
	By Interface - C interface.	lick to display a line	chart related	to traffic via th	e WAN
Usage List by	Application - Cl	a usage for commor lick to display the da luding name of appl	ta informatio	n related to var	ious
Usage List by	Application - Cl	lick to display the da cluding name of appl	ta informatio	n related to var	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e.	ta informatio	n related to var per of users, up	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e.	ta informatio	n related to var per of users, up	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e. PrayTck vertex	ta informatio	n related to var per of users, up	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e. PrayTck vertex	ta informatio	n related to var per of users, up	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e. PrayTck vertex	ta informatio	n related to var per of users, up	ious
Usage List by	Application - Cl applications, inc download usage	lick to display the da cluding name of appl e. PrayTck vertex	ta informatio	n related to var per of users, up	ious

	-			ad usage.			ection type, o	
syste	eni, upioa	au anu	uowinoa	au usage.				
Fighte Lines	Charle, represent/insernant	The Property lies of						
								-WAR - WVD
							~	
								~
	the other time of			the set of a	1.14			and the local
							and the second	
Usurger Link b	by Application CamerDay	-		-				
1000			- Mar Andrews	in Consultion Tura	- 05		Dage	
1000		Matrice and a second	MAC Address	🐑 Connection Type	- 05	Uptood	Disage Download	
* 2 **	soit Name 🦟 IP		 MAC Address MAR98255662 	 Connection Type Winning ISG 	- os ©			
¥ 2 m X m	Gost Name - 19 dam MBP - 19	Address				Upload	Download	
1 2 10 1 10 2 10	Soit Name P dam MBP 135 mknown (35	Addines	808590206662	T Winniess (SG)		Upload 208 Bytes	Download 132 Bytes	
9 al 10 1. da 2. 00 3. 50	dam MBP IN dam MBP IN Inknown IN 1000675 IN	* Address 92.158.124.12 92.168.124.29	8C81902C6642 00507F7981E82	ক Winniess ISGI শ্রী Winned	0.0	tipload 108 Bytes 3.52 #8	Download E32 Bytes 2.14 KB	
¥ 12 m 31 m 7 m 3 m 3 m 3 m 3 m 3 m	Sout Name P BP dam MEP BS minnown (%) 2000675 BS SCalifform (%)	• Address 92.168.124.12 92.168.124.29 92.168.124.29	8C80902C6462 0050773938382 880776067799	77 Winniess, 1961 라 Word 라 Wind	0.0	Nyload 208 Bytes 3.32 HB 20.01 MB	Download E32 Bytes 2.14 KB 4.64 MB	

5.4 Configuration Menu for SD-WAN CPE

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

This page is left blank.

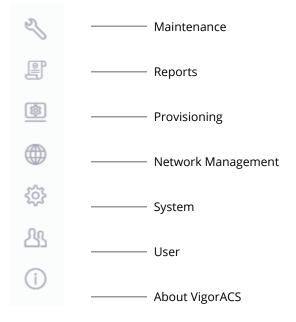


System Menu



Chapter 6 System Menu

System menu contains:



6.1 Maintenance

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

10	Maintenance
<u></u>	Scheduled Backup
	Configuration Restore
	Firmware Upgrade
2	Device Reboot
(Inclusion)	System Password Reset
ſ	Schedule Profile
\$	File Manager
	Batch Activation
ŝ	
<u>4</u> 3	
(j)	

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

6.1.1 Scheduled Backup

6.1.1.1 Networks & Devices

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

Maintenance / Scheduled Ba	ckup			
User Group RootGroup				
Vetworks & Devices Backup Se	ttings Profile			
Name	File Type	Backup Setting		
Root Network(123)	Tinaliguation File	Emply		
ji 😨 AutoTest_SD-WAN(2)	Contrgoration File	As Parent	sh.	
1 @ U 2133 100(100)	Costligaci/Iosi File	As Parent	~	
1. 🐼 VigorSwitch(2)	Configuration File	As Parent		
7: 🐨 aia(5)	Contiguation File	As Parent		
) 🌚 tssue6925(0)	Configuration Elie	As Parent	+	
/ 🐼 Jason_test(1)	Configuration File	As Parent	1.46	
@ 2133Vac_001DAA66E02	Konggagood File	As Parent	w.	
@ 2762Vac. 001DAA65330	Contraction Ene	As Parent	-	
@ 2765Vik_1449BC2C42E	Configuration Die	As Parent	4	
@ 7850V 001DAA7D9CC8	Contraction File	As Parent		
@ 2865ac_0010AA4ACFB	ConfigurationThe	As Parent	*	
@ 7865ac_14498C143DAG	Configuration File	As Parent	- 9	
@ 2952 14498C0D2040	Linut/pontiest Eller	As Parent	- 44	
@ 3910_14498C1CA218	1. matry paragoont File.	As Parent	-4	
@ 3910_1449BC6B9178	1. Deal/guard/Loci #Be	As Parent	*	
@ 39125_1449BC3072A0	Contrapozities File-	As Parent		
@ P1280_0010AA4E6C33	Configuration Tile	As Parent	- 4	
@ P1282_14498C43C019	X pertupophics File	As Parent	. ¢.	

These parameters	are explained	as follows:

ltem	Description				
User Group	Specify a user group for applying the backup settings profile. Each user group can be configured with different backup settings profiles.				
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 Empty Default As Parent - The backup setting for the selected network / device is the same as the top setting.				

	Empty - No backup setting for the selected network / device.
	Default - Use the default backup setting for the selected network / device.
	Others - In addition to As Parent, Disable and Default, profiles defined in Backup Settings Profile also will be listed in this drop-down list.
Save	Save the current settings.

6.1.1.2 Backup Settings Profile

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

ietworks & Devic	es Backup Settings Profile				
Add					
- Add fame	Period(Days)	Туре	7 ime Interval	Action	
elault tt1	1	The Last 20	Neiw	🖉 Edit. 🕼 taoloto	
tt.L.	1	The Last 20	Now	🖉 Edit 🗇 Delete	

These parameters are explained as follows:

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

The following setting page appears when +Add is clicked.

Intenance / Scheduled Backup ser Group : RootGroup		
works & Devices Backup Settings	Profile	
Name		
Backup Period(days)	Ĩ	
Keep Files	The Last 20 All	
Backup Time	Now Scheduled Schedule Profile	
Schedule Profile	reset_password_wizard \sim	
		Cancel

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

	files.	o keep al	ll of th	e files (r	outer's d	onfigu	iration	files) o	r the last 2
Backup Time	 Set a time interval for executing the backup work for networks and devices. Now - The backup work will be executed immediately after clicking 								
	the Save button.								
		eduled - date aft					ecuted	at the	specified 1
	• Sch		rofile	The ba	ckup wc	ork wil			according ıtton.
Scheduled	Start Tim and minu							a clock	. Set the h
	50 45 40 Select tir	01:0 55 00 35 30	05 10	25 Pro					
	Specify S Date – Cli	tart Dat	:e – Cli	ck to er calend	ar to cho		-		arting dat
	Date – Cli	tart Dat ck to po	e – Cli p up a	ck to er calend	able the ar to cho	ose a	-		arting dat
	Date – Cli	tart Dat ck to po Jan	e – Cli p up a	ck to er calend	able the ar to cho	oose a	-		arting dat
	Date – Cli	tart Dat ck to po Jan	e – Cli p up a	ck to er calend	able the ar to cho P P Fr	sa	-		arting dat
	Date – Cli	tart Dat ck to po Jan Mo 3	e – Cli p up a Tu	ck to en calend 2022 Ne Ti	able the ar to cho Fr 7	sose a solution of the solutio	-		arting dat
	Date – Cli K Su	tart Dat ck to po Jan Mo 3 10	te – Cli p up a Tu 4 11	ck to er calend 2022 Ne Tl 5 6	able the ar to cho Fr Fr 3 14	oose a > Sa 1 8	-		arting dat
	Date – Cli K Su 2 9	tart Dat ck to po Jan Mo 3 10 17	e – Cli p up a Tu 4 11 18	ck to er calend 2022 We Tl 5 6 12 13	able the ar to cho Fr Fr 3 14 21	> Sa 1 8 15	-		arting dat
	Date – Cli Su 2 9 16	tart Dat ck to po Jan Mo 3 10 17	e – Cli p up a Tu 4 11 18	ck to en calend 2022 We Tl 5 6 12 1: 19 2(able the ar to cho Fr Fr 3 14 21	Sa 1 8 15 22	-		arting dat

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

6.1.2 Configuration Restore

6.1.2.1 Apply to Devices

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

Maintenance / Configuration Resto	re		
User Group : RootGroup	× .		
Apply to Devices Restore Settings Prof	file		
PQuick Setting			
Name	Apply File List	Restore Profile	
Root Network(91)			
ALANWEN(3)			
@ 2952n_001DAAE061E8		Empty	
 2960_00507FFF3900 3910_001DAA18E740 AnPhat_VN(8) AnPhat_VN(8) AnPhat_VN(8) AnisTest(0) Cshih(2) Dsvid_Test_n1(3) FAE(3) FAE(3) Anketing_carrie(0) OCTOBER(1) RD1(3) SEG1(1) 		Engly restore, witzard Default *ROSTestTestTest 1111 222 3.333	
h 🔊 ScanAccess(3)			Save

ltem	Description
User Group	Specify a user group for applying the restore settings profile. Each user group can be configured with different restore settings profiles.
Quick Setting	This wizard offers a series of steps to specify configuration file which can be applied to multiple APs / Switches at one time.
	Quick Setting Common Config File AP903_20190715.dg
	7. Notice: To apply ACL CEG file to APs, please make sure the firmware version is 1.2.5 or newer. With old formware, your AP regists for each to factory settings, so the selected AP with old firmware will be ignored automatically.
	Common Restore Profile Device Filter APs: Switches
	Select Devices
	Name Model Name Firmware Version Image: Control C
	× Close Next->

	In which, click the Common Config File to select a "cfg" file. Then select a restore profile and specify the device filter (AP or switch). From the Select Devices list, select one or more APs/Switches required to apply the configuration file. Click Next to get the following page.
	♥ Quick Setting ×
	Common Config File /AP903_20190715.cfg
	▲ Notice: To apply ACL CFG file to APs, please make sure the firmware version is 1.2.5 or newer. With old firmware, your AP might be reset to factory settings, so the selected AP with old firmware will be ignored automatically.
	Common Restore Profile Default
	Device ID Device Name Model Firmware Version User Group 2 136288 AP 903_00507FF19216 VigorAP 903 1.3.5RC7 RootGroup
Apply	Check if the selected devices are correct or not. If yes, click Apply. The selected configuration file will apply to all of the selected devices. Click the icon to enable configuration restoration for the selected CPE.
File List	Open a dialog to choose one of the files for the file restoration of the selected CPE.
	S Select a config file
	Filename J↑ Property J↑ Size Last Modified J↑ File Path J↑
	▷ Directory 0 Byte 02/19/2020 13:10:11 .
	AP1000C_20190604.cfg cfg file 9.41 KB 06/04/2019 14:09:13 /RootGroup AP910C_acl_20181206.cfg cfg file 210 Byte 06/04/2019 11:22:24 /RootGroup
	▲ Notice: To restore a CFG file from a different model, please make sure the firmware on both devices is up to date. To apply ACL CFG file to APs, please make sure the firmware version is 1.2.5 or newer. With old firmware, your AP might be reset to factory settings, so the selected AP with old firmware will be ignored automatically.
Restore Profile	Choose a profile defined in Restore Settings Profile for applying onto the selected CPE.

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

6.1.2.2 Restore Settings Profile

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

Apply to Devices Re	istore Settings Profile				
÷Add					
Name	Trigger Profile	Time Interval	Action		
Default	default	Now	🧷 Edit	Delete	
befault vinkless		04chwy		© Delete	
ACL.		Now	/ Edit	© Delete	

These parameters are explained as follows:

ltem	Description
User Group	Specify a user group for applying the configuration restore settings profile. Each user group can be configured with different configuration restore settings profiles.
+Add	Click to create a new profile.
Name	Displays the name of the restore setting profile.
Trigger Profile	Displays the time schedule selected for the restore setting profile.
Time Interval	Displays the time period to trigger the setting restoration.
Action	Edit - Click to modify, change the selected profile. Delete - Click to delete the selected profile.

The following setting page appears when +Add is clicked.

Maintenance / Configuration Restor		
pply to Devices Restore Settings Profi		
Name		
Restore Time	Now Scheduled Schedule Profile	
Start Time	Selectime	
End Time	Select time	
Specify Start Date	O	
		Cancel Save

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

	_1						
	<	Jan		~ 2	022	~	>
	Su	Мо	Tu	We	Th	Fr	Sa
							1
	2	3	4	5	6	7	8
	9	10	11	12	13	14	15
	16	17	18	19	20	21	22
	23	24	25	26	27	28	29
	30	31					
Schedule Profile	rese rebo resto	gorACS t_passwo t_passwo ot_wiza ore_wiza kup_wiz ult	offer ord_wi vord_v ord_v ord ard	s defai zard			
Save	Save the	curren	t setti	ngs.			

6.1.3 Firmware Upgrade

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

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

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

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

User Group :	RootGroup -						
Irmware Up	grade Job List						
	Delete Al Complete Jots					A.4.1	
+ Add in Name	Deleter All Complete Johns	11 School	Sola 🥼 Device Count	if Status it	Result (1	Action	

These parameters are explained as follows:

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

The following setting page appears when +Add is clicked.

aintenance / Firmware Upgrade			
ser Group : Routidroup			
rmware Upgrade Job Settings			
Name			
Status	Disable Enoble		
Upgrade Time	Now Scheduled		
Date	Science as denter		
Start Time	Solod timin		
End Time	Solid Simp		
Apply Firmware			
Protocol Options	Odiki HTTP		
Send Report by Email			
Recipients (User)	Nothing selected		
Recipients (Email)	TAdd	Recipients Email Limit: 0/5	
	# Email	Action	

These parameters are explained as follows:

ltem	Description
Name	Enter a name of the job profile.
Status	Click Enable to activate the firmware upgrade profile.
Upgrade Time	Set a time interval for executing the firmware upgrade job for networks and devices.
	 Now - The firmware upgrade job will be executed immediately after clicking the Save button.

								clicking the S	ll be executed Save button.	
Scheduled								ct time to di r on the cloc	splay a clock. k.	Set the hour
		22	01 23 11	00 12	13					
			10 9 8 7 19	6 5 18	2 3 19 4 16 17	5				
		01:14		Ü	∕Select t	ime	Ü			
	Date	– Click	to p	op up	o a ca	lenc	lar to	o choose a da	ate as the sta	rting date.
	<	Jan		~ 2	022	~	>			
	SI	u Mo	Tu	We	Th	Fr	Sa	le		
	2		4	5	6	7	8	-		
	9		11 18	12 19	13 20	14 21	15 22			
	23		25	26	27	28	29			
Apply Firmware		o opei ed CPI						mware file. V	igorACS will ເ	pgrade the
	Select	a firmware								×
	File	name			Prope		Size 0 Byte	Last Modified	↓↑ File Path ↓↑	
	D 9	SharedFirmware			Directi		0 Byte	02/19/2020 13:10:11	./RootGroup	
		Vigor2960_001D PublicArea	AA694AE8		Direct		0 Byte 0 Byte	06/04/2019 13:55:45	./RootGroup	
	~4									
	(0)								X Close	
Brotocol Options	Coloct	them	och	nicm	for	oorf	ormi	ng firmwara	upgrada	
Protocol Options) – This						ng firmware	upgi due.	
	1 11005		rACS	will a	authe	entic	ate t		PE by router n ade for the CF	
		ord ar	iu tri							
	passw •	Route	r Us	ernai				e name (e.g., he router.	admin) of the	e router as
	passw	Route the us	r Uso erna r Pas	ernai me fo sswo	or aco rd – I	cess Ente	ng t	he router.	admin) of the e.g., admin) of	

	• Recipients (User) – Select the user from the drop-down list.
	 Recipients (Email) – Click +Add to enter the email address which will receive the report email.
Device to Upgrade	Click the Filter icon to set the filtering conditions.
	Device to Upgrade 🛛 🖓
	Filter
	Device Name
	MAC Address
	Model All ~
	Firmware Version All ~
	Modem Version All ~
	Cancel Q Apply
	Model – Select a model of CPE. Firmware Version – Select a firmware version. CPE with the selected firmware will be shown on the table. Modem Version - Select a modem version. CPE with the selected modem will be shown on the table. Apply - After clicking Apply, the table below will show the devices according to filter conditions.
Table	Select one device or more devices to apply the firmware upgrade provision.
	Device to Upgrade 🛛 🖓
	Name MAC Address Model Name Firmware Version Modem Version
	C 0 001DAAE061E8 V01DAAE061E8 Vigor2952n 3.9.1.1_RC3 No DSL D 2960_00507FFF3900 00507FFF3900 Vigor2960 1.3.0_Beta undefined
	3910_001DAA18E740 001DAA18E740 Vigor3910 3.9.2_Beta r1064_84359 No DSL
	⊳ 🐼 AnPhat_VN(8)
	b S AriesTest(0)
	Model Name – Display the model name for identification.
	Firmware Version – Display the firmware version that the model used currently.
Cancel	Discard current settings and return to previous page.
Save	Save the current settings and exit the page.
	The firmware upgrade job will be performed based on the above
	conditions automatically.

6.1.4 Device Reboot

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

6.1.4.1 Networks & Devices

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

er Group : RootGroup ~	
work& Devices Reboot Settings Profile	
ame Model Name Firmware Version Modem	Version Reboot Setting
🔹 🐼 Root Network(90)	Empty ~
p 🐼 ALANWEN(3)	As Parent 🛩
j. 🐼 AnPhat_VN(8)	As Panerit 😽
p 🐼 ArtesTest(0)	As Parent 😔
p 💿 Cshih(2)	As Parent 🗢
1) 🐼 FAE(3)	As Parent
p 🐼 Marketing_carrie(0)	As Parent 😪
D OCTOBER(I)	As Parent ~
J @ R01(3)	As Parent *
↓ SEG1(1)	As Parent ~
p 😨 ScanAccess(3)	As Parent 😪
p 💿 TreeDepthTest(0)	As Parent 🛩
p 🕲 USA(1)	As Parent 👻
p 🐼 cole6666(0)	As Parent 🗸
(b) ⊗ cole71111111111111111(0)	As Parent
ji 🐼 mamie(2)	As Parent ~
b o robintest2(0)	As Parent.
p (Tiwerwe(0)	As Parent Y
▶ ⊕ test(0)	As Parent ~
) 💿 test666666(0)	As Parent 👻

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

6.1.4.2 Reboot Settings Profile

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

MaIntenance / Device Reboot				
User Group : RootGroup				
Networks & Devices Reboot Settings P	rolle			
+Add				
÷Add Name	Period(Days)	Time Interval	Action	
reboot_wizard	365	00:00-23:59	🖉 Edit 🕅 Delete	
Default	1	00:00-00:00	/ Edit // Delete	
11	1	Now	P Edit IP Detete	
m	365	01:05-03:15	de Edit 🖷 Delete	
shih_test	1	13:15-17:05	@ Edit 🕅 Delete	

These parameters are explained as follows:

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

The following setting page appears when +Add is clicked.

aintenance / Device Reboot:		
Iner Group : RootGroup		
Hworks & Devices Reboot Settings Profile		
Name		
Period (days)	1	
Reboot Time	Now Scheduled Schedule Profile	
Start Time	Signal form	
Ind Time	Solid One	
Specify Start Date	0	
Date	Saloci actaiz	
		Cancel 5-r

ltem	Description
Name	Enter the name of the profile.
Period(days)	Determine the frequency for the CPE reboot by VigorACS. The default value is 1 day.
Reboot Time	 Set a time interval for executing the device reboot. Now Scheduled - The device reboot will be executed at the specified time and date after clicking the Save button. Schedule Profile - The device reboot will be executed according to the selected schedule profile after clicking the Save button.
Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.

	03:10 Specify S	20 7 6 5 16 ule Profile 19 18 17 2							starting
	<	Jan		v 2	2022	~	>		
	Su	Мо	Tu	We	Th	Fr	Sa		
							1	le	
	2	3	4	5	6	7	8		
	9	10	11	12	13	14	15		
	16	17	18	19	20	21	22		
	23	24	25	26	27	28	29		
	30	31							
								J	
Schedule Profile	Trigger P which, Vig							om the drop e.	down lis
		oassword					~		
	reboot restore	passwoi :_wizard e_wizard p_wizard t	I	ird					
Cancel	Discard c	urrent	settin	igs and	d retur	n to pi	reviou	ıs page.	
Save	Save the o	urren	t setti	ngs.					

6.1.5 System Password Reset

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

Reset Time	Now Scheduler:			
Start tíme	00:00			
ind time	23:59			
Start Date	01/07/2022			
ielect devices				
Name	Model Name	Firmware Version	Modem Version	
A @ Root Network(2)				
O 111111(0) O				
() @ 22222(0)				
6 🐼 Manual Carrie(1)				
AP 903 005077 F1918C	VigorAP 903	1.4.2	No DSL	

ltem	Description
Reset Time	 Now – Reset the password for the selected device(s) immediately. Scheduled – To specify a certain time to perform the job, choose this one and specify start day, start time and end time respectively. VigorACS will perform the job for the selected CPE (s) according to the schedule set here. Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.
	 O3:10 23 00 13 22 11 12 1 14 21 9 3 15 20 7 6 5 16 19 18 17 20 Select time Date - Click to pop up a calendar to choose a date as the starting date.

	_1	1						
		<	Jan		~ 2	022	~	>
		Su	Мо	Tu	We	Th	Fr	Sa
								1
		2	3	4	5	6	7	8
		9	10	11	12	13	14	15
		16	17	18	19	20	21	22
	:	23	24	25	26	27	28	29
		30	31					
Select devices	Choose	the	device	that y	you wa	nt to	do dev	vice pa
Save	Save the	e cur	rent se	etting	s.			

6.1.6 Schedule Profile

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

1403					
Name	Start Day	End Day	Start Time	End Time	Action
reset_password_wizard	2017-04-27		07:08	07:13	P Edit 19 Delete
eboot_wtzard	2017-06-20		08:21	20:11	ef Edit III Deleti
estore_wtzard	2016-12-14		05:12	05:17	🖉 Edit 🗇 Deteor
ackup_wtzard	2016-12-07		03:05	.03:25	d Edit 🗐 Delete
default	2016-10-08	2016-10-09	00:00	00:00	🖉 Edit. 🗐 Delete
estl	2017-04-19	2017-04-11	00:00	00:00	P Edit 🕮 Deleta
est2					P Edit 🕀 Delate
est3					S Edit III Delete
est4					FEDR IT Delete
est5					d Edit 🗐 Delete
est6					2 Edit 🕅 Deleta
est7					2 Edit. 11 Delete
11			00.00	23:59	P Edit I Delete

These parameters are explained as follows:

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

The following setting page appears when +Add is clicked.

Profile Name			
ste Type	Scheduled	~	
art Date	Sector date-		
heck End Date	•		
nd Date	Sielect a date		
ime Type	Scheduled	- +	
start Time	Select time.		
End Time	Scientime		

These parameters are explained as follows:

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

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

6.1.7 File Manager

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

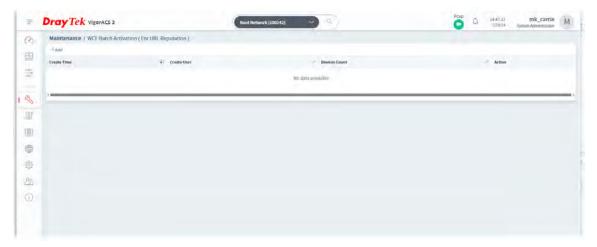
User Group RootGroup									
🖞 Upload 🕹 Download 🖹 Delete 🖼 New Folder 🗠 DrayTek FTP									
	Filename	U↑ Device Name U1	Property 4	Size ↓↑	Last Modified	$\downarrow\uparrow$ File Path			
	SharedFirmware		Directory		07/30/2020 09:16:40	./RootGroup			
	🗅 test555		Directory		06/06/2019 14:22:59	./RootGroup			
	🗅 ttl		Directory		03/04/2019 14:39:56	./RootGroup			
	D Vigor2925Vac_001DAAF06DF0		Directory		10/08/2019 11:23:27	./RootGroup			
	D VigorAP 902_001DAA3D9808		Directory		10/08/2019 13:25:36	./RootGroup			
	UigorAP 960C_1449BC775566		Directory		07/09/2020 10:24:02	./RootGroup			
	🗋 11@22.txt		txt file		03/04/2019 15:46:09	./RootGroup			
	🗅 test2.txt		txt file		05/22/2019 14:03:32	./RootGroup			
	🗋 docker.txt		txt file	1.98 KB	06/19/2019 09:22:04	./RootGroup			
	C certificate.cfg		cfg file	5.92 KB	03/04/2019 14:40:01	./RootGroup			
	AP903_20190715.cfg		cfg file	7.58 KB	09/21/2020 14:57:52	./RootGroup			
	acs2_url.txt		txt file	19.38 KB	03/04/2019 14:39:51	./RootGroup			
]	ap810_r9031_125.all		all file	5.17 MB	06/19/2019 09:22:35	./RootGroup			
]	ap910c_r10090_128.all		all file	6.76 MB	06/19/2019 09:20:01	./RootGroup			
	ap920_r9469_125.all		all file	15.88 MB	06/19/2019 09:16:57	./RootGroup			

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

	The PublicArea is designed for sharing firmware files. It allows users to upload and delete files. Therefore, if PublicArea is selected as the User Group, then information listed on this page can be downloaded, uploade and used by any other user.							
Upload	Click to upload a file to VigorACS 3 server.							
	⊥ Upload File ×							
	Target: ./RootGroup Browse							
	▲ The file must be less than 50MB.							
	× Cancel ✓ Apply							
Download	Download a driver (*.all, *.rst and etc.) related to CPE device from VigorACS 3 server.							
Delete	Click to delete the selected profile.							
New Folder	Create folders for files classification/management.							
	+ New Folder							
	Folder Name:							
	Cancel + Add							
DrayTek FTP	After clicking the link, the following page will appear for you to download file from DrayTek FTP directly.							
	Maintenance / Druyfek 177: + Beck to Local Titles Deventing for : norm/crea							
	Resented Paperty Tats Lat Headly Etimology AS33 Berschary 2021-04-0812.231 Etimology 2022-04-0812.231 AS433 Berschary 2022-06-0812.331 Etimology 2022-06-0812.331 AS43 Berschary 2024-06-0812.04 Etimology 2024-06-0812.04 AVM Berschary 2024-06-0812.04 Etimology 2024-06-0812.04 AVM Berschary 2024-06-0812.02 Etimology 2024-06-0812.04 Constances Berschary 2024-06-0812.06 Etimology 2024-06-0812.06 Distances Directory 2024-06-0812.06 Etimology 2024-06-0812.07 Distances Directory 2024-06-0812.06 Etimology 2024-06-0812.07 Distances Directory 2024-06-0812.06 Etimology 2024-06-0812.07							

6.1.8 Batch Activation

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



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

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

Maintenance / WCF Batch	Activation (For Cyren)		
Login MyVigor First			
with the distr	on is the feature which provided to the distributor on butor privilege account. e requirement of batch activation, please contact you nce.		
Username Password	·····	Φ	•
↑ Back to profile list			Login

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

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

Import WCF batch activation	ı data						
Upload file	Browse						
	🕭 Download entry sample file						
↑ Back to profile list		ر Upload کې ا					
ltem	Description						
Upload file	Click Browse to locate the CSV file with name of import-batch-activation-file.						
	Maintenance / WCF Batch Activation (For Cyren)						
	Import WCF batch activation data						
	Upload file	import-batch-activation-file.csv Browse					
		🛃 Download entry sample file					
	↑ Back to profile list						
	If there is no file existed, clie download one file.	ck "Download entry sample file" link to					
Download entry Click to download an entry sample file (import-batch-activation-file.csv							
sample file	Open the CSB file and enter device.	r the "MAC address" and "WCF KEY" for each					
Back to profile list	Return to the previous prof	ile list page.					
Login	Access into next page.						

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

Maintenar	ce / WCF Batch Activation (For Cyre	en)						
Upload Result								
🖧 Export								
	L↑ Device Name	↓↑ Device MAC	↓↑ Network	↓↑ License Key	↓↑ ACS Check Status	41		
~	2865Lac_1449BC0D8F00	1449BC0D8F00	MKT_manual	6F6CD-CF2A6-EE7CE-6C5D2	Check OK			
↑ Back to pr	ofile list							
					Previous	Next		

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



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

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

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

							heck	or Devices & License Ch	MyVigo
								rt	ය Expor
MyVigor Check Status	$\dot{\gamma} \dot{\tau}$	License Key	AT.	Network	÷t	Device MAC	-41	Device Name	ψt
Check OK		6F6CD-CF2A6-EE7CE-6C5D2		MKT_manual		1449BC0D8F00		2865Lac_1449BC0D8F00	~
								profile list	↑ Back to p
Previous Activat									
								profile list	↑ Back to p

7. Click Activate. Wait for a minute.

Root Net… >>	Dray Tek VigorACS 3		
Maintenance Save OK Result		×	

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

Root Net… ~	L	Dray Tek VigorACS 3		
Maintenance / WCF Bate	h Activation (For Cyren)			
+Add				
Create Time	↓ Create User	Devices Count	⊥⊤ Action	
2021-02-26 06:27:12	root	1	Q, View Log 💼 Delete	
ltem	Description			
+Add	Click to create	a new batch activati	on profile.	

Click to view the records of the WCF batch activation.

Click to remove the selected record.

View Log

Delete

Click View Log to see current processing status.

example 1

Root Network		~			1	DrayTek vigor	ACS 3			Capture Packe	ts + System Administrator	R
Maintenance / WCF Ba	atch A	ctivation (For C)	ren)								
All Processing C	omple	te Fail 1349	inch (ieven Norrie / MAC. / Koy								
Device Name	4	MAC	i.	License Key Number	av.	License Date	Network	- 1	Last Update Time	Status	Result	
2865Lac_1449BC0D8F00		1449BC0D8F00		B3072-A595A-FE7C3-F7CEF		2021-02-26+2021-03-28	MKT_manual		2021-02-26 06:27:14	Processing	MyVigor added license successfully	

example 2

Device Name	7+	MAC	License Key Number	License Date	Nel	work -	Last Update Time	Status -	Result
850n+_001DAAD1E290		001DAAD1E290	03F10-D6468-280A1-40DA5	2019-02-13-2019-03-15	RD	5	2019-04-02 11:30:41	Complete	CPE sync license successfully
925Ln_001DAADD7580		0010AADD75B0	671C8-8222F-55F4E-907C8	2019-02-13-2019-03-15	RD	6-1	2019-04-02 11:32:40	Fan	Cannot connect to CPE (timeout)
* Back to profile list									

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

6.2 Reports

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

(7)	Reports
<u></u>	Report Tasks
¦ 	Legacy Report Tasks
Z	
I 🖉 🗸	Reports
-	
ŝ	
23	
I (j)	

6.2.1 Report Tasks

6.2.1.1 Report Tasks

Open Reports>Reports Tasks to get the following page.

Barried & Barriel and				Pran D. 1450-10 7/28/24	mk_carrie
Report / Report Jasks					
User Group : RootGroup					
User Group : RockGroup Report Tables Add Generated Repo	rts				
+ Add				P	Profile Number Limit: 1/20
Profile Name	- Report Type	Report Range	Recurrence	Action	
2024-1-82-5-11-SCPEs	Statistic Report	Device(s)	Once	🖉 Edit 🗏 Delete	

ltem	Description
User Group	Use the drop down list to choose a group (e.g., RootGroup).
	Only the report task profiles defined for the selected user group will be shown on this page. If there is "no" profile displayed for the selected group, you may click the link of +Add to create a new one.

+Add	Click to create a new report task for specified CPE.
Action	Edit – Click to modify an existing report task.
	Delete – Click to remove the selected report task.
	Download - Click to download the report task as a "*.pdf" file for reference.

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

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

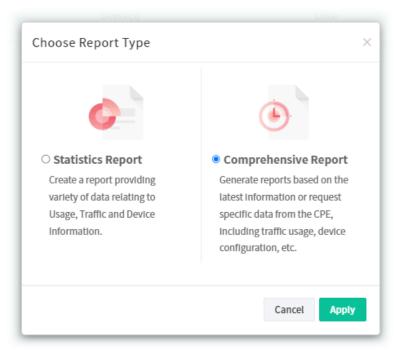
If Statistics Report is selected, the following setting page will appear.

eport / Report Tasks			
User Group : RootGroup			
Statistic Report Settings			
General			
Profile Name			
Report Range	Network Device(s)		
Network	Nothing selected		
Timeframe	Lasi 24 bours 🔍		
Send Report by Email			
Recipients and Logo			
Report Recurrence	Every Week 🛷 1 st =		
Report file Logo	Phone with the bases Browsee The this must be less than Juli 88.		
Customized Widgets			
Network Wide	🖂 Usage Overview	🗇 Elleri Muruber	
	U Wireless Client Overview	Client Traffic	
Device/ Client Ranking	Tup Destce Banking by Olent Number	Top Client Rimking by Traffic	
	Top Device Ranking by Traffic	D Top Device Ranking by Uptime	
			Cancel Sale

These parameters are explained as follows:

ltem	Description
	•

General							
Profile Name	Enter a name for such report task profile.						
Report Range	Determine the content range (network or devices) of the report.						
Network	Select one or more networks for generating the statistics report.						
Timeframe	Display the report related to the CPE detected within 24 hours, 7 days, 3 days or user defined days.						
Send Report by Email	 Switch the toggle to enable/disable this function. If enabled, Recipients (User) – Specify the subject for the email. Recipients (Email) - Enter the email address of the recipient. +Add - If there is more than one recipient for adding, click the link to have more entry box(es) for adding more recipients. 						
Recipients and Logo							
Report Recurrence	Once – The report will be made just for one time. Every Day/Every Week/Every Month – The report will be made repeatedly. Set the day, starting date and starting time based on the selection.						
Report file Logo	Click to put a logo on the report. Select the logo file (with the file size less than 100KB).						
Customized Widgets							
ltems	Select the items related to Network Wide, Device/Client Ranking, Monitoring, and Hotspot Web Portal. Corresponding information will be shown on the statistics report.						
Report Device(s)	If Devices(s) is selected as Report Range, this option will appear. Only the CPEs under the selected User Group (e.g., RootGroup in this case) will be shown in this field. Check the box to the left of the network group to select the device(s) you want to make report.						
Save	Save the settings and return to previous page.						



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

epert / Report Tasks		
ser Group: PhonGroup		
Comprehensive Report Settings		
General		
Profile Name		
Report Type	Traffic.	
Report Content	LAN Statistic 🗢	
File Type	PDF Word CSV Excel	
Report Range	Merjannik Devlorist	
Network	Nothing selected -	
Send Report by Email		
Recipients and Logo		
Report Recurrence	Every Wrek - 1 #	
Report file Lago	Place small an image	
	The file must be less than 100KB.	
		Cancel Save

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

Report Content Select the way (statistic or graph) to show the report. The content will vary
LAN Statistic ~ select an option LAN Statistic WAN Statistic WAN Statistic NAT Statistic LAN Graph WAN Graph NAT Graph
File Type Choose PDF, Word, CSV, or Excel as the file format for device configuration report.
Report Range Determine the content range (network or devices) of the report.
Network Select one or more networks for generating the statistics report.
Send Report by EmailSwitch the toggle to enable/disable this function. If enabled, Recipients (User) - Specify the subject for the email. Recipients (Email) - Enter the email address of the recipient. +Add - If there is more than one recipient for adding, click the link to have more entry box(es) for adding more recipients.
Recipients and Logo
Report RecurrenceOnce - The report will be made just for one time.Every Day/Every Week/Every Month - The report will be made repeatedly. Set the day, starting date and starting time based on the selection.
Report file LogoClick to put a logo on the report. Select the logo file (with the file size less than 100KB).
Save Save the settings and return to previous page.

6.2.1.2 Generated Reports

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

=	Dray Tek VigorACS 3		Root Network (100142)	-		Pap 0	15:51:13 7/28/24	mk_carele System Administration	M
0	Report / Report Tasks								G
-83	User Group : RootGroup ~								
ŝ	Report Tasks Generated Reports								
9	Show 20 V entries						Dealithe		
围	C Time	Profile Name	Hoport Type		Action				
<u>100</u>	2024/01/08 13:53:08	2024-1-42-5-41-SEPEs	Statistic Repo	4	@ Download				
0	Showing 1 to 1 of Lestries								-
Ø									
<u>н</u>									

6.2.2 Legacy Report Tasks (Deprecated)

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

Ŧ	Dray Tek VigorACS 3	6	ool Network (190142)	× 4			Co D	15:55:49 7/23/24	mk_carrie System Administration	М
(S) (B)	Reports / Legacy Report Tasks (Deprecated) User Gröup : BootGroup ~									
2								Search	Tide/Type-	9,
4 B	Title Device Information Report from 141,8080 Report Task 666	Root Network	Report Content Information Device Configuration	Report Delivery Email Download	ScheduleyPeriod Now	Last implemented 2018-09-12 10:32	Action de Edit	T Doleta	- Download	
9 9			and a second	FIGHTS						
御山										

Click Edit to review the detailed settings.

Device Information Report from 141:80
Information ~
Device Information ~
Send By Email Download File
PDF CSV Excel Word
root / Internal
Once Repeat
Now ~

6.3 Provisioning

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

(7)	Provisioning	ir.
<u></u>	Global Parameters	~
	CPE Set Parameters	
	CPE Keep Parameters	
Z	Firmware Upgrade) (i
I		

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

6.3.1 Global Parameters

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

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

6.3.1.1 Global Profile

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

Provis	sioning / Global Parameters								
User	Group: RootGroup ~								
Gibb	A Profile Network & Devices								
Profile	Edit Mode : All Web UI View XMI, File	Parameter List CSV File							
	+ Add .4. XML Template .4. C	SV Template							
	Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action		
.0	Global_parameter_Example	XML File		No	2	2024/03/14 04:24:07 PM	Ø Edit	С Сору То	El View Log
	TEST NETWORK global params	XML File		NO	2	2024/06/28 11:34:33 AM	Ø Edit	C Copy To	A view Log
	0729vtvtantest	Web Ut View	Vigor2927Lac	No	26	2024/07/29 02:08:55 PM	27 Edm	COPY TO	A View Log
9	0729vivlantest_Parameter_List.	Parameler List	Vigor2927Lac	No	3	2024/07/29 01:58:53 PM	2 Edit	С Сору То	New Log
	0729vrvlantest_Parameter_List(1)	Parameter List.	Vigor2927Lac	No	0	2024/07/29 02:08:55 PM	Ø Edit	С Сору То	4 View Log
	RebootCLi 3day 1432	XML File		No	16	2024/09/06 04:59:40 PM	/ Eds	С Сору То	₽ View Log
	cpecilent	Parameter List		No	2	2024/12/03 10:16:26 AM	Ø Edit	CI Copy To	Wew Log
	LTE Custom R55i	XML File		No	1	2024/12/19 02-14-11 PM	17 540	CODY TO	S Maw Line

ltem	Description
Profile Edit Mode	 All - Displays all of the profiles. Web UI View - Displays the profiles related to web UI view. XML File - Displays the profiles with the file format of "XML". Parameter List - Displays the profiles related to parameter settings for different CPEs. CSV File - Displays the profiles with the file format of "CSV".
Delete	Click to remove the selected profile.
+Add	Click to create a new provision profile.
XML Template	Click to store current global parameter configuration as a file (*.xml). XML Template The XML is separated into two parts, you may edit it based on your requirement: • Profile: Specify the unique "item id" for each TR-059 parameter that you want to configure • Profile: Specify the parameter value for each TR-059 parameter that you want to configure • Profile: Specify the parameter value for each TR-059 parameter that you want to configure • Profile Name: The profile name will display in the global parameter page. • Sixep: We could decide whether to keep the value of this parameter. Setup true then ACS will detect and change it back if someone edits the value. • ord: ACS will apply the setting based on the order of parameters. Close Download XML
CSV Template	Click to store current global parameter configuration as a file (*.CSV).

	CSV Template × The following messages outline the conditions and elements for importing a CSV file. You may edit them based on your requirements. • Domain requirement: • •<							
Profile Name	Displays the name of the profile.							
Profile Edit Mode	Displays the edit mode.							
Model	Display the model name of the device.							
Always Keep	Yes – Such profile is kept always. No – Such profile is not kept always.							
Revision	Displays the time for last modification.							
Last Modification At	Displays the time and date of the last modification of the provision.							
Action	Edit – Click to configure settings for the selected profile. Copy To – If the administrator wants to apply the provision to certain user group, such action shall be used.							
	2. Copy the profile to ×							
	Copy To: Pick some user group RootGroup SDWAN rd8							
	View Log – Click to review detailed information for the selected profile.							

User Group :	; / Global Paramet RootGroup Network & Devic	¥					
Profile Info Profile ID Profile N Profile Ec Model Always K Revision Last Mod Reboot a	ime it Mode sep	Web UI Vie General Yes 559	o_always_keep ww 0 05-49:56 PM		Status Overview	Status nitibele e Not yet applied 1	Concilete E Failed
Device ID	Device Name		↓↑ MAC Address	↓↑ Network (ID)	↓↑ Time	↓↑ Result	J† Status
293	2952n_001DAAE061E	В	001DAAE061E8	ALANWEN (82)	2019/09/27 12:00:46 A	м	Complete.
295	2960_00507FFF3900		00507FFF3900	ALANWEN (82)			Not yet applied.
141243	3910_001DAA18E740		001DAA18E740	ALANWEN (82)			Not yet applied.

The following setting page appears when +Add is clicked.

ltem	Description	Description							
Create Profile by	There are three methods (Sampling from an Online Device, Sampling from an XML file, Sampling from an CSV file, Creating a New Parameter List) to create a profile.								
For Sampling from an Online Device,		ameter List is spec e parameter profi							
	A the Root Network		Firmware version						
For Sampling from an XML file,	Select XML file - Click Browse to choose a file.								
For Sampling from an CSV file,	Select CSV file - Click Browse to choose a file.								
For Creating a New Parameter List,	Profile Name - Ente	er a name to creat	e a new profile.						

	Some ISPs do not wish CPE client changing the parameters of CPE device, therefore make the profile being kept is required.								
Reboot after Provisioning	Enable it t	o rebo	oot the	e CPE a	after t	he pro	visio	ing is applied by certain	CPE.
Provisioning Time	devices. Nov Sch Sch	v edulec edule	d Profil	e			-	ork for networks and display a clock. Set the h	
	and minu	03 23 11 10 9 8 7 19	: 10	3 2 ¹⁴ 2 15 4 16	ule Pr		the cl	ock.	
	date.						o cho	setting. ose a date as the starting	g
	Start dat			oop up				-	g
	Start dat date.	e – Clic		oop up	a cale		o cho	ose a date as the starting	g
	Start date.	e – Clic Jan	k to p	v 2	a cale	endar t	o cho	-	g
	Start date.	e – Clic Jan	k to p	v 2	a cale	endar t	sa	ose a date as the starting	g
	Start date.	e – Clic Jan Mo	to p	v 2 We	a cale 2022 Th	endar t V Fr	sa	ose a date as the starting	gg
	Start date.	e – Clic Jan Mo 3	tk to p	v 2 We	a cale 2022 Th 6	endar t v Fr 7	sa 1	ose a date as the starting	g
	Start date.	e – Clic Jan Mo 3 10	t to p Tu 4 11	• 2 We 5 12	a cale 2022 Th 6 13	Fr 7 14	o cho > Sa 1 8 15	ose a date as the starting	g
	Start date.	e – Clic Jan Mo 3 10 17	t to p Tu 4 11 18	 2 We 5 12 19 	a cale 2022 Th 6 13 20	endar t F r 7 14 21	 Sa 1 8 15 22 	ose a date as the starting	g

	Now Scheduled Schedule Profile			
	~			
	reset_password_wizard			
	reboot_wizard			
	restore_wizard			
	backup_wizard			
	default			
	test1			
	test2			
	test3			
Cancel	Discard current settings and restore the default settings.			
Add	Save and create the new profile.			

6.3.1.2 Network & Devices

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

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

er Group : RootGroup ~		
sbat Profile Network & Devices		
ame	Profile Id	
Root Network(90)	Empty	~
ALANWEN(3)	root group always keep	~
(AnPhat_VN(8)	(As Parent)	R.
1) S ArkesTest(0)	(As Parent)	9
) 🐼 Cshih(2)	Manoj	14 M
5 S FAE(3)	(As Parent)	~
1 S Marketing_carrie(0)	(As Parent)	~
() OCTOBER(1)	(As Parent)	
) 🐼 RD1(3)	(As Parent)	
)/ 🐼 SEG1(1)	(As Parent)	*
🐼 ScanAccess(3)	(As Parent)	4
/ 🐼 TreeDepthTest(0)	(As Parient)	~
1 🐼 USA(I)	(As Parent)	~
(· 📀 cole6666(0)	(As Parent)	*
1) 🙆 coleittittittittittittiin	(As Parent)	*
🐼 mamte(2)	Empty	
i do intest2(0)	(As Parent)	*
(b) (0) (7) (0) (0) (0) (0) (0) (0) (0) (0) (0) (0	(As Parent)	Ψ.
(r 🐼 (test.)0)	(As Parent)	~
test666666(0)	(As Parint)	*
(r 💿 wholesaletest(0)	(As Parent)	×
1- 🐼 xxxxxxxx(0)	(As Parent)	v
1 (YYYYYIO)	(As Parent)	*
2762Wac_001DAA653308	(As Parent)	
@ 2860/m+_001DAAD83D80	(As Parent)	×

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

6.3.2 CPE Set Parameters

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

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

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

ser Gro	RootGroup	w.												
Add	Dimport XMI Dimp	ort CSV (J.XML Template J.CSV Template							423	ech Pro	file Narr	e/Dev	ce Na	59
									10:	0	Ĩ.	/1	÷	t
	File Id / Profile Id	Profile Name / Device Name			Complete	Action								
~	15	ct2233.xml				2 Donoto								
	15	14;49;80;3E:30;99	Hodel: General Renew Count, 2	Rebeat: 1 Retry: 0	No Set.	e ⁰ .Edir	(i) Deploy	M. View Log	R:					
2	31	Individual-14498C3FFF78-Batch1_1.6k-240219024713.xmt				10 Delete								
9 -	54	SSID_TEST_2.xml				III Delete								
21	87	v2865_4453_RC4a_FAE4151_1-2.xml				音 Delete								
5	110	haven5.xml				m Delete								

ltem	Description					
User Group	Specify a user group. The devices under that group will be displayed on this page.					
+Add	Click to create a file saved with the file format of XML.					
Import XML	Click to upload a file to VigorACS 3 server.					
	Upload File × Browse Cancel Apply					
Import CSV	Click to upload a file to VigorACS 3 server.					

XML Template	Click to store current global parameter configuration as a file (*.xml).
	XML Template ×
	The XML is separated into two parts, you may edit it based on your requirement: I tem: Specify the unique "item id" for each TR-069 parameter that you want to configure Profile: Specify the parameter value for each "parameter id", ACS will check the parameter id(mapping to item id) with the parameter name. Profile Name: The profile name will display in the global parameter page. I skeep: We could decide whether to keep the value of this parameter. Setup true then ACS will detect and change it back if someone edits the value: ord: ACS will apply the setting based on the order of parameters.
	Close Download XML
CSV Template	Click to store current global parameter configuration as a file (*.xml).
	CSV Template × The following messages outline the conditions and elements for importing a CSV file. You may edit them based on your requirements.
	 Format requirement : There should be no blank lines between two rows. Make sure that parameters with the same profile name are placed in the same section. Device Serial Number: Define the MAC address of CPE. ACS will apply the settings if the MAC address matches the device. IsReboot: ACS will check the CPE responses and ask the CPE to reboot if needed after applying the parameters.: Device Name: Change the device name of CPE which is displayed on the ACS. Iskeps: We could decide whether to keep the value of this parameter. Setup true then ACS will detect and change it back if someone edits the value. You can keep all the parameters in the profile, or only keep specific parameters
	Close Download CSV
File Id / Profile Id	Displays the number of parameter file or the ID number of the profile.
Profile Name / Device Name	Displays the profile name or the device name.
Action	Delete – Click to delete the profile. View Parameters – Click to display parameter settings for the selected profile.
	View Log – Click to review detailed information for the selected profile.

The following setting page appears when +Add is clicked.

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

These parameters are explained as follows:

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

The following web page (varies according to the device selected) appears after clicking Continue.

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

ltem	Description
Device	Display the name of the device which will be applied with the parameters configured in this page.
Web UI View	Parameters (including WAN, LAN, NAT, Object Settings, QoS, Firewall, System, Routing, Wireless, Applications and etc.) ready for each CPE

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

6.3.3 CPE Keep Parameters

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

rovisioning / CPE Keep Parameters			
ser Group : RootGroup	~		
Device	Parameters Count	Action	
 Root Network(123) 			
AutoTest_SD-WAN(2)			
V_2133_100(100)			
VigorSwitch(2)			
> 📀 aaa(5)			
Sissue6925(0)			
b Sason_test(1)			
2133Vac_001DAA66E020	0	🖉 Edit 🛛 🗎 View Log	
2762Vac_001DAA653308	0	🖉 Edit 🛛 🗟 View Log	
2765Vac_1449BC2C42E8	0	🖉 Edit 🛛 🗎 View Log	
2850V_001DAA7D9CC8	0	🖉 Edit 🛛 🗎 View Log	
2865ac_001DAA4ACFB0	0	🖉 Edit 🛛 🗎 View Log	
2865ac_1449BC143DA0	0	🖉 Edit 🛛 🖴 View Log	
2962_1449BC0D2040	0	🖉 Edit 🛛 🗟 View Log	
3910_1449BC1CA218	0	🖉 Edit 🛛 🖴 View Log	
3910_1449BC6B9178	0	🖉 Edit 🛛 🗎 View Log	
3912S_1449BC3072A0	0	🖉 Edit 🛛 🗟 View Log	
P1280_001DAA4E6C33	0	🖉 Edit 🛛 🖴 View Log	
P1282_1449BC43CD19	0	🖉 Edit 🛛 🗟 View Log	
Q2121x_1449BC506AA4	0	🖉 Edit 🛛 🖴 View Log	

ltem	Description
Edit	Click to open the configuration page.
	Device: 3910_001DA18E740 Web UI View Parameter List Reboot Reboot After Provisioning Image: Compared and the CPE to reboot if needed. A Note: • After applying the parameters. ACS will check the CPE responses and ask the CPE to reboot if needed. Enable Compared and the CPE to reboot if needed.
	The menu list to the left will show available parameters regarded to the device.

6.3.4 Firmware Upgrade

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

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

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

6.3.4.1 Firmware Upgrade Job List

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

Provisioning / Firmware Upgrade User Group: RootGroup ~			
Firmware Upgrade Job List			
+Add			
Name ↓↑ Status ↓↑ Model	$\downarrow\uparrow$ FW Version	↓↑ FW File	$\downarrow\uparrow$ Schedule $\downarrow\uparrow$ Start Date $\downarrow\uparrow$ Action
sample Disabled Vigor2700 Series	3.1.1.1_RC6	v2k7v_a_3.1.1.1_RC6.all	Now N/A 🖉 Edit 🖲 Delete 📾 View Log
Exclude Devices			
+Add ∥Edit @Delete			
□↓↑ MAC Address		¢τ	
No data available			

ltem	Description		
User Group	Specify a user group. The job list under that group will be displayed on this page.		
Firmware Upgrade Job	List		
+Add	Click to create a new job profile.		
Edit	Click to modify, change the selected profile.		
Delete	Click to delete the selected profile.		
View Log	Click to view the record related to the firmware upgrade of the CPE.		
Exclude Devices			
+Add	Specify the device that the firmware upgrade job configured and displayed on the job list will not perform for it.		

	Click to display an entry box. Enter the MAC address of the device.
Edit	Click to modify the MAC address of the devices one by one.
Delete	Click to delete the selected device.
Check box	Check the box to specify a device. Later, the selected one can be deleted if required.
MAC Address	Displays the MAC address of the device.
Cancel	Discard current settings and return to previous page.
Save	Save the current settings and exit the page.

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

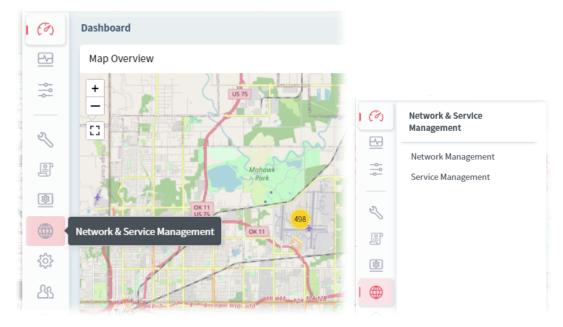
Provisioning / Firmware Upg User Group : RootGroup	rade			
Firmware Upgrade Job Se	ettings			
Name				
Status		Disable Enable	2	
Upgrade Time		Now Schedule	d Schedule Pro	file
Job Type		Normal Auth K	ey Check	
Protocol Options		TR069 HTTP		
Device Criteria		Vigor167*	~]
Upgrade Type 🛛		Target Current		
Device does not match the firmw	are version	1.2.3RC4	~]
Modem Version		No DSL	~]
Firmware Upgrade & Net	work selecti	on		
Apply Firmware				
Name	Model Name	Firmware Version	Modem Version	Apply
 Root Network(123) 				NO ~
AutoTest_SD-WAN(2)				As Parent ~
U_2133_100(100)				As Parent∨
VigorSwitch(2)				As Parent \sim

ltem	Description		
Firmware Upgrade Job	Settings		
Name	Enter a name of the job profile.		
Status	Disable – Firmware upgrade is not allowed for such job profile. Enable – Firmware upgrade is allowed for such job profile.		
Upgrade Time	 Set a time interval for executing the backup work for networks and devices. Now Scheduled Schedule Profile 		
Job Type	Normal – VigorACS 3 performs firmware upgrade without using any authentication key. Auth Key Check – To avoid hacker's attack via Vigor device (router or AP), special authentication key is used for communication between Vigor device and VigorACS 3. That is, VigorACS 3 will verify all of the Vigor devices		

	via authentication key issued by DrayTek to ensure the network security.				
Protocol Options	Select the mechanism for performing firmware upgrade.				
	TR069 – This is the default setting.				
	HTTP – VigorACS will authenticate the router/CPE by router name and the password and then perform the firmware upgrade for the CPE.				
	 Router Username – Enter the name (e.g., admin) of the router as the username for accessing the router. 				
	• Router Password – Enter the password (e.g., admin) of the router for accessing the router.				
Scheduled	Start Time / End Time – Click Select time to display a clock. Set the hour and minutes by clicking the number on the clock.				
	$\begin{array}{c} 03:10\\ \begin{array}{c} 23 & 00 & 13\\ 22 & 11 & 12 & 1\\ 21 & 9 & & 2 & 15\\ 20 & 7 & 6 & 5 & 16\\ 19 & 18 & 17 & & \\ \end{array}$				
	Specify Start Date – Click to enable the time setting. Date – Click to pop up a calendar to choose a date as the starting date.				
Schedule Profile	Trigger Profile – Choosing a trigger profile from the drop down list. In which, VigorACS 3 offers default schedule profile.				
	reset_password_wizard ~				
	reset_password_wizard				
	reboot_wizard				
	restore_wizard				
	backup_wizard				
	default				
	test1				
	test2 test3				
Device Criteria					
Model	Choose a model for firmware upgrade.				
Upgrade Type	Select Target or Current.				
	Target - If the firmware version of the CPE is different from the one listed in "Device matches firmware version", the firmware upgrade job will be performed immediately.				
	 Device does not match firmware version - Displays current firmware version recorded on VigorACS server. 				
	Current - If the firmware version of the CPE is the same as the one listed in "Device matches firmware version", the firmware upgrade job will be performed immediately.				
	 Device matches firmware version - Displays current firmware version recorded on VigorACS server. 				

	Choose the correct n and etc.	nodem ve	ersior	n of the device	e, e.g., Annex	x A, Annex B
	Before performing firmware upgrade for the CPE, VigorACS 3 will check if the received model name, modem firmware version, and software version match with the information recorded in VigorACS 3 server or not. If you type "*" in this filed, the modem version will not be regarded as a comparison condition in the process of firmware upgrade. It will be ignored.					
Firmware Upgrade 8	Network selection					
Apply Firmware	Click to open a dialog	д.				
	Select a firmware				×	
	Filename	Property ↓↑	Size	Last Modified	↓↑ File Path ↓↑	
	8.	Directory	0 Byte	11/19/2019 17:07:11		
	□ SharedFirmware	Directory	0 Byte	05/08/2019 08:36:52	./RootGroup	
	test555	Directory	0 Byte	06/06/2019 14:22:59	./RootGroup	
	🗅 #1	Directory	0 Byte	03/04/2019 14:39:56	./RootGroup	
	Vigor2925Vac_001DAAF06DF0	Directory	0 Byte	10/08/2019 11:23:27	./RootGroup	
	VigorAP 902_001DAA3D9808	Directory	0 Byte	10/08/2019 13:25:36	./RootGroup	
	🗅 PublicArea	Directory	0 Byte			
					× Close	
	Available versions fro Select the firmware v	-				d in this field.
Apply	As Parent - The setting for the selected network / device is the same as the top setting.					
	NO - No setting for the selected network / device.					
	YES - Use the firmwa					ce.
Cancel	Discard current setti	Discard current settings and return to previous page.				
Save	Save the current settings and exit the page.					

6.4 Network & Service Management



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

lt can

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

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

6.4.1 Network Management

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

6.4.1.1 Settings for Root Network

Network & Service Management / Network Manage	ment		
Search by Dovice IU/Namo/Hode/MAC/PAddress	Serring Map		
Rhot Network(100142) AutoTestNetwork(1)	- Add New Network		
 AutoTest_Dev(9) AutoTest_SD-WAN(2) 	General Settings		
AutoTest, VPN(1)	Network (D	Voename	
p 🚠 Hotspot_Web_Portal(2)	1	205	
Abuter_App_Network(2)	Name	Passance	
p 🚓 T_2024-07-30_Wholesale_GA_D(0)	Root Network		-
5 🚓 T_2024-07-30_Wholesate_GA_E(0)	Exercises		
p 🚠 T_2024-07-30_Wholesale_GA_OOBE(0)	American		
b # 7 2024-07-30 addNetWork Al0)			
p .1. 0. 2133 100(100)			Sm
D === U_2865_5(2)			
b 🚠 U 2866 5(4)			
D			
p 🚠 Vigorswitch(2)			
p 🚓 aaa(5)			
D A ExpiraLicense_A(0)			
p 🚠 fullLicense_A(1)			
1) 🚠 Issue6925(0)			
(L) test (nocel 🚠 d			
1)			
D 21 UII4(2)	-		
Bi Datana Davisan			

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

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

Add Network	
Parent Network	
Root Network	
Name	
Marketing_carrie	
Location	
HsinChu	
Username	
carrie	×
Password	
	✓ ©

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

6.4.1.2 Settings for Network Group

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

sanch by Device 13/Hame/Model/MAK./IP Address	Setting Map Alar	m Setting			
Ritrol Network(100142)	Add New Network	es Network de Change Ne	twork		
b AutoTestNetwork(1)	and the second s				
pAutoTest_Dev(9)	General Settings				
6 AutoTest_SD-WAN(2)					
5 AutoTest VPN(I)	Servera D			semame.	
Hotspot_Web_Portal(2)	4424			U_2866_5	
B A Router App Network(2)	Name			asserved	
0 🚓 T_2074-07-30_Whotesate_GA_0(0)	10_2866_5				
t 👬 7_2024-07-30_Wholesale_GA_E(0)	Location				
5 A T 2024-07-30 Wholesale GA_006E(0)					
0					
0_2133_100(100)	Advanced Settings				
0 🚓 U 2865 5(2)					
p 🚠 U. 2866 5(4)	Enable SD-WAN				
p 🚮 U_2977_5(5)					
	Bulk Data Settings				
0 👬 VigorSwitch(2)	Bulk Data Settings				
 p AL 0_2827_5(s) p AL vigorSwitch(2) p AL viaa(5) p AL viaa(5) p AL viaa(6) 	Set the category of data to be collect				d drop to place such category in the corresponding profile
0 🚓 VigorSwitch(2) 2 🚓 444(5) 6 🚓 expireLicense, A(0)					
0 🚓 VigorSwitch(2) 5 🚓 eaa(5) 6 🚓 expireLicense, A(0) 5 🚓 tuilLicense, A(1)	Set the category of data to be collect	the profile returns buik data t			
0 -#, VigorSwitch(2) 0 -#, asa(5) 5 -#, expires(Kense, A(0)) 5 -#, full.itense, A(1) 0 -#, issue6925(0)	Set the category of data to be collect apearty the report interval at which t	the profile returns buik data t	o the ACS, If you disable bulk d	lata categories, it will affect	the SD-WAN operation.
A VigorSwitch(2) A A aaa(5) A A failLicense_A(0) A A failLicense_A(1) A A issue66925(0) A A issue66925(1) A	Set the category of data to be collect specify the report interval at which t Profile 61	the profile returns buik data t reader	o the ACS, If you disable bulk d	lata categories, it will affect	the SD-WAN operation.
0 A. Vigorswitch(2) 0 A. Aus(5) 0 A. Superscription (A. (0)) 0 A. Superscription (A. (0)) 0 A. Superscription (A. (1)) 0 A. Superscription (A. (1))	Set the conservery of data to be collect upecify the roport intervial at which t Profile a1 Report Numerical Sect. [120]	the profile returns built data to	o the ACS, If you disable buik d Profile #2 Internations J00	Lata categories, it will affect	the SD-WAN operation.
P 🚓 VigorSwitch(2) P 🚓 aaa(5)	Sel the category of data to be collect specify the report interval at which t Profile s1 Report Interval (set)	the profile returns built data t Readle	o the ACS, If you disable bulk d Profile #2 Internal Ises	Lata categories, it will affect	the SD-WAN operation.

ltem	Description
Search by Device ID/Name/Model/MAC /IP Address	Enter the ID, name, model or MAC/IP address of the device you want to locate.
+Add New Network	Click to add a new network. New created network will be the sub-network of current selected network.
Delete This Network	Remove current network group.
Change Network	Click to change the network / group for the selected CPE.
General Settings	
Network ID	Display a number which is given by VigorACS randomly for the selected network.

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

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

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

These parameters are explained as follows:

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

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

Network Management

Search by Device ID/Name/Model/MAC/IP Address	C
A 👬 Root Network(70)	
▷ 👬 @#\$%^&*_+{]":?> -+(0)</td <td>- 11</td>	- 11
Layer2(0)	- H
Marketing_carrie(0)	- 11
▷ 👬 SD-WAN(2)	- 11
aaaaaa(123)(0)	- 11
⊳ 👬 rd7(0)	- 11
⊿ 👬 rd8(52)	- U
▷ 👬 MKT(0)	Ĭ
902_001DAA3D4F16	
130_001DAA8411C8	
130_001DAA854204	

6.4.1.3 Settings for Device

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

Open Network Management. This web page allows to:

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

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

ich fig Neuker (D)Namie/Mindel/MAC/IP Address 🛛 😁	Setting Map Alarm Setting		
 0 m (_2024-07-30_Wholesale_GA_E(0))	Delete This Device As Change Network		
1_2024-07-30_Wholesale_CA_OOBE(0)	General Settings		
and the second sec			
p 👬 U 2133 100(100)	Shatas	Known Devise	
	Disable Enable	Known Unknown	
≥ 👬 U 2866 5(4)	Device III	Network III	
✓ ♣ U_2927_5(5)	104532	4422	
6 2927Vac 1449BC22C2C0 104.1	Mindet Kurne	Device Name	
292TVac_1449BC22C400_103.1	Vigor292/Vac	292/Var_14498C22C620_102.1	
292TVac 1449BC22C438 101.1	Nos 1	Note 3	
2927Vac_1449BC22C588_106.1	Hom 1	Note 2	
2927VRc_1449BC22C630_102.1	Settal inerteer	MAC Address	
VigorSwitch(2)	Securitority.	1449.BC.22.C6.30	
0 5 aaa(5)			
A expireLicense A(0)			
TullLicense_A(1)	Location	CPE Client (P	
:		192 168 103 10	
	Plane No.	CPE Client Port	
ason_test(1)		8069	
5 A. 00.03)	Dunain Name	CPE Clives (UR)	
(·		/cwm/CBN.html	
- A tttt5(2)	Nanagement Protocol	CPE Client User Name	
0 A 222 test 003(998)	CPE default (http) http: https	vigor	
Tekete Devizes	Management Fort	//Edit	
	60	CPE Client Password	

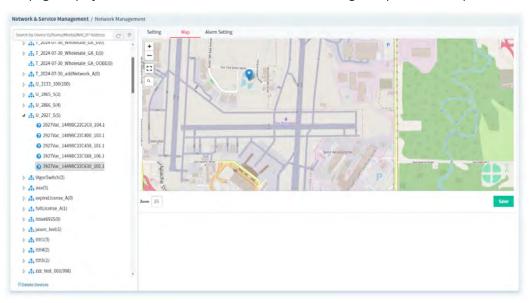
These parameters are explained as follows:

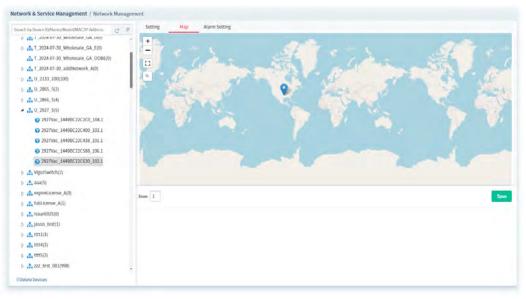
ltem	Description
Delete This Device	Click to remove the selected CPE from current group.
Change Network	Click to change the network / group for the selected CPE.

	+ Change Network
	Name 22020-2013A492652E
	Add to nessori
	Ib Root terbionis d. 1111 d. ALANYSTI d. ANTIN d. ANTIN d. ANTIN d. ANTIN d. ANTIN d. ANTIN d. Conin d. Displat/hima d. Faig d. Antinevani
	**
	🕷 Cancel 🥠 Apply
	Move the mouse cursor on the network you want and click Apply.
General Settings	
Status	Disable – The selected device will be hidden on the tree view.
	Enable – The selected device can be displayed on the tree view.
Known Device	Known – The selected CPE is known(😃) to VigorACS 3.
	Unknown – If the selected CPE is new added device, it will be identified as Unknown (?).
Device ID / Network ID	Device ID – Display the number of that device which is given by VigorACS 3 randomly.
	Network ID- Display the ID number of the network that selected device is grouped under.
Model Name / Device Name	Model Name – Display the model name of the selected device. Model name cannot be changed.
	Device Name – Display the name of the device for identification. It can be changed if required.
Note 1 / Note 2	Note 1 – Display brief description for the selected device. Note 2 – Display brief description for the network.
Serial number / MAC	Serial number – Enter a number for identification of the device.
Address	MAC Address – Display the MAC address of the device.
Location	Display the position of the device.
Phone No.	It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device.
Domain Name	Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE.
Management Port	Enter a port number which will be used for accessing into web user interface of the CPE.
Management Protocol	Choose HTTPS or HTTP.
CPE Client IP / Port / URI	Display the IP address, port number and URI.
CPE Client User Name / Password	Display the username and password that VigorACS 3 can use to access into the CPE.
	Edit - Click to change the username and password.

6.4.1.4 Map

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





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

6.4.1.5 Alarm Setting

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

arch by Device (D/Hame/Model/MAIC/RP Adc. 🦿 🗵	Setting Map Alarm Sutting	
0 11 1 2029-01-90 Wholesale 0A U(0)	Atams setting as parent rotwork	
5 T_2024-07-30_Wholesale_GA_E(0)		
T_2024-07-30_Wholesale_GA_OOBE(0)		
P # T_2024.07.30_addNetwork_A(0)	WAN Alarm Settings	
b U_2133_100(100)	was disconnection alarm interface	
p 🔥 U_2865_5(2)	L	
1 AU_2865_5(4)	Interface:	
a 🚓 U_2927_5(5)	WAN2	_
2927Var_1449BC22C2C0_104.1	WAN3	
2927Var 1449BC22C400 103.1	WAN4	
2927Var 1449BC22C438 101.1	WAN5	
2927Vac_1449BC22C588_106,1	WAN6	
7927Vac_1449BC22C630_107.1		
1 👬 Vigor Switch(2)		
() 🚓 asa(5)		
expireLicense A(0)		
fullLicense_A(1)		
p- 📇 issue5925(0)		
(r 👬 jason_test(1)		
1) tttt1(3)		
b 🚓 tttt4(2)		
p 🚓 uu5(2)		
b 1 222 test 001(998)		

These parameters are explained as follows:

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

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

6.4.2 Service Management

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

6.4.2.1 Service Subscription

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

(%) E4	Network & Service Management	Network & Service Management / Service Management User Group: ReotGroup	C
	Network Management	Service Subscription History	
	Service Management		
		Bind with MyVigor Account	
Z		Status Login with MyVigor	
P			
-			

Click Login with MyVigor to get the following dialog.

Dray	Tek
MyVig	
Username draytek_rd8	
Password	
*****	0
Login	

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

The following web page will appear.

P	Dray Tek VigorACS 3	Re	ot Network (100342)	v e.		Co 🕫		k_carrie N
ð.	Network & Service Management / S	ervice Management						C
3	User Group : RootGroup 😒							
	Service Subscription History							
5.	Bind with MyVigor Account							
2	Status d	draytek rd8 Log out Unb	ind					
1	User Group Device Service S	ubscription @						
							Militage 5	discription
	Service	status	Purchased	used	Nodes			
				1-1			Total : 0 Node	
	URL Reputation - D Card	Unsubscribed					10001-014000	
	URL Reputation - D Card URL Reputation - A Card	Unsubscribed	-	-			Total : 0 Node	
			-	- 1	_			
	URL Reputation - A Card	Unsubscribed	-				Total : 0 Node	
	URL Reputation - A Card URL Reputation - Silver Card	Unsubscribed	4		_		Total : 0 Node	
	URL Reputation - A Card URL Reputation - Silver Card Network Device Inventory Seleni Network	Unsubscribed Subscribid	-		_		Total : 0 Node	
)	URL Reputation - A Card URL Reputation - Silver Card Network Device Inventory Selend Network	Unsubscrited SetsEnbed Root Network (13)	4		_		Total : 0 Node	Q.

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

Manage Subscription	Bind the selected license keys to specified device. Click to open the following page.
	Manage Subscription × 1 2 3 Select Service Select Device Confirm
	Select Service
	Service Purchased Keys Keys Currently Available
	URL Reputation - B Card 3 3
	URL Reputation - A Card 8 4
	URL Reputation - Silver Card 5 2
	Auto Danaya
	Auto Renew
	Previous Next
	Enable Auto Denous to renow the licenses for all energified devices
	Enable Auto Renew to renew the licenses for all specified devices automatically.
	After selecting the service card (s), click Next.
	Manage Subscription
	Select Service Select Device Confirm
	Selected Service URL Reputation - Silver Card Available Keys : 2
	Select Networks or Devices
	Name Model Name MAC Address
	 ▲ Boot Network(3) ▶ ▲ O Evis(0)
	> •
	2 0 2962_14498C38ECC8 Vigor2962 14:49:8C:38:EC:C8
	① 3910_14498C689178 Vigor/3910 14:49:BC:6B:91:78 ① 39125_14498C3DC6F8 Vigor/3912S 14:49:BC:3D:C6F8
	Previous Next
	Select the CPE(s) to apply the service card. Then click Next.
	Select the Cric(s) to apply the service card. Then thick wext.

	Manage Subscription ×
	Select Service Select Device Confirm
	Confirm
	Selected Service Available Keys Selected Devices Remaining Keys
	URL Reputation - Silver Card 2 1 1
	Auto Renew Enable
	Previous Apply
	Click Apply.
	Manage Subscription
	Enable List
	Device Name Model MAC Address Status Message
	2962_1449BC38ECC8 Vigor2962 1449BC38ECC8 1 Success
	Selected Service Available Keys Success Devices Remaining Keys
	URL Reputation - Silver Card 2 1 1
	Auto Renew Enable
	✓ Finish
	The page with brief summary will be shown as above. Click Finish to exit this page.
Service	Display the name of the service (e.g., URL Reputation).
Status	Display current status (Unsubscribed or Subscribed) of the service.
Purchased	Display the quantity of the service card purchased.
Used	Display the quantity of the service card used.
Nodes	Display the number of nodes that have used this service card.
Network Device Invent	tory
Select Network	To view the status of keys bound of CPE devices under some group, use the drop-down list to select the network you want.
Network ID	Display the index number of the current network, randomly assigned by VigorACS for identification.
Edit	Click the button to activate and enable the Auto Renew, Cancel, and Save buttons for editing.
Device Name	Display the name (composed by model and MAC address) of the device.

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

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

6.4.2.2 History

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

Bind	ling Log			lation of a	E. Seléct à date	🗇 - Select	Ladate 🖸 Greene Jype	All	 ✓ Search- 	
Liser G	Sroup Net	work	Device MAC	License Key	Activated Date	Expired Date	License Type	Action	Status	Operator
RootG	roup Roo	t Network	00:1D:AA:65:33:08	-	-	-	URL Reputation - D Card	Bind	Device is not exist.	
RootG	iroup Roe	t Network	00:10:AA:66:F0:20	-	-	-	URL Reputation – R Cant	Rind	Device is not exist	
RootGi	iroup Roc	t Network	14:49:8C:30:72:A0	1656A-80691-787E4-39021	2924/01/22	2024/02/21	URL Reputation - Silver Card	Bind	Success	
RootG	roup Aut	aTest_SD-WAN	14:49:80:34:55:00		-	-	URL Reputation - A Card	Bind	Dinoce is not out?	
RootG	roup Aut	Test_SD-WAN	14:49:80:34:5:00	-			URL Reputation - A Card	Bind	Device In not exist.	
RootG	icaup Roo	t Network	00:10:AA4A:CF:80	-	-	-	URL Reputation - A Card	Bind	Device is not exist	root
									Show 10 × e	ntries n 1
-										

6.5 System

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

(7)	System
000	System Parameter
<u></u>	Language
- 	External Monitoring Server
	Access Control
Ê	Storage Management
	Upload Serial Number
Z	API Keys
P	Certificate
\$	Backup Database
	Login Bulletin
I 🌐	Adverts Carousel
र्छ	Logs
出	XMPP Profile
	Server Support Settings
(j)	Delete Logs Actions
	App Server
	License Key Pools

6.5.1 System Parameter

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

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

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

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

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

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

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

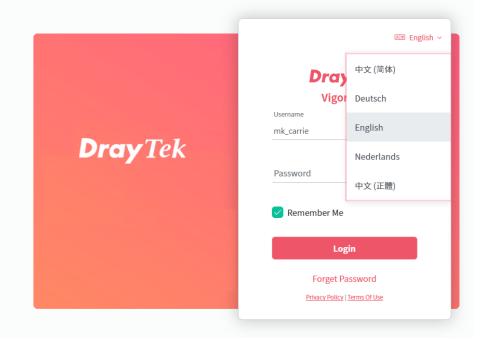
	Set how many devices will be shown on the home device tree. Default value is 100.
74	
71	EnableSendCPENotify True - When the value of parameters for CPE is changed, a notification of 'IntenetGatewayDevice.X_00507F_Notify' will be sent to VigorACS. VigorACS will send the message to the specified user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

82	ClientRecordAliveTimeInDays
	Set the number of days for reserving the record (about client traffic). When exceeding the day limit, VigorACS will delete the record.
	Default value is 30(days).
83	IsDeleteExpiredClientTrafficByTimestamp
	True – Enable the function of ClientRecordAliveTimeInDays.
	False – Default setting.
84	EnableClientRecord
	True – Default value. Enable the function of recording client traffic and displaying related information on NETWORK MENU >> Monitoring >>Clients.
85	NotifyServerProcessCountPerMinute
	It can be set with -1, 100 to 100000. This parameter determines how many Emails, SMS, and
	health parameters notification items the notification server can process per minute. -1 means unlimited.
86	ForceWUIRedirectHttps True - Force ACS WUI to HTTPS only. If you encounter login failed error after changing this
	parameter, please clear the browser's cache then try again. If the
	EnableSecureCookieSessions parameter is set to "true", this parameter will be automatically enabled and disallow set to false.
07	
87	JbossConfigForStandaloneMode The Default Configuration for standalone Mode is "standalone.xml" (default). The
	standalone-secure.xml will enhance the security protections of your ACS website with
	plugins that prevent hacking.
88	EnableSecureCookieSessions
	True - Secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. If the value set to true, the
	ForceWUIRedirectHttps parameter will be automatically enabled and the cookie will only be
	sent in a secure manner (i.e. Https).
	False - Default setting.
89	LogRotationHandlerType - Select one of the following types for log.
	• Size
	PeriodicPeriodic-size
91	MapServiceProvider There are two mechanisms to display maps on VigorACS, Google and Leaflet.
92	EnableUsermailValidation
92	true - If it is enabled, the user will receive an e-mail first and be guided to pass the
	authentication when he tries to log in to VigorACS.
	After switching the toggle to enable this function, the VigorACS system will open the
	User>>Mail Server page. You have to check if the mail server is enabled and other options have been configured correctly.
	false - Default setting.
93	NetflowSetPortConfig
	The function in "Monitoring>>Flow" requires VigorConnect servers, which are installed in
	remote networks, to collect NetFlow data from routers in the background.
	When browsing "Monitoring>>Flow" on VigorACS, the corresponding VigorConnect servers will establish connections to VigorACS. Thus, VigorACS can retrieve the relevant data. The

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

6.5.2 Language

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



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

Open System >> Language.

.Tu	pload					н	-8	1	/1	3	11	Ģ
	Filename	(4)	Size	-31	Last Modified							4
3	lang_CN.bx		218722		2024/07/20 05:06:31							
1	lang_DE.txt		564595		2024/05/29 05:06:35							
1	lang, EN.txt		443410		2024/05/29 05:06:35							
1	lang_NLtxt		570735		2024/07/20 05:06:31							
2	lang_TW.txt		438027		2024/07/20 05:06:31							

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

6.5.3 External Monitoring Server

6.5.3.1 Health Server

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

Scott Garge	System / External Monitoring Server		
Winles Client Information Server	Enable Server		
	URL	apt.tptechvlew.com	
	Usemanie	acs.drayddos.còm	
	Password	**** (D	
	API	Health_Default_GLOBAL ~	
			Cancel Save

These parameters are explained as follows:

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

6.5.3.2 Wireless Client Information Server

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

Health Server	System / External Monitoring Ser	ver	0
	User Group	RootGroup	
	Enable Server		
	Authentication	N2YCcCGM23NS2sW2rGp/UC6apQLsE48tZkqD86Var	
	1181.	http://www.draytek.co.uk/torms/json.php	
	API	Wireless_Client_Default_GLOBAL ~	
			Save

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

6.5.4 Access Control

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

6.5.4.1 General Setting

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

neral Setting Blacklist	Whitelist Blo	ck Device List		
WUI Login	None	Blacklist	Whitelist	
CPE Service	Noné	Bläcklist	Whitelist	
API WebService	None	Blacklist	Whitelist	

These parameters are explained as follows:

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

6.5.4.2 Blacklist

This page is used for creating blacklist profiles.

						Search IP / Description
+ Add 🗇	Delete All					Limit: 3/2
p id	Description	47 WUI Login	17 CPE Service	API WebService	- 00	
1.1.1.1	ui		D		🖉 Edit	1 Delete
	tt2	•			Ø Edit	@ Delete
192,168,105,210	ti5	5	D		🖉 Edit	查 Delete

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

The following setting page appears when +Add is clicked.

+ IP Address For	m ×
Description	Marketing_CAN
Address Type	Single IP Address ~
Start IP Address	123.12.1.1 🗸
Service Enable	☑ WUI Login 🔽 CPE Service
	API WebService
	× Cancel 🚯 Save

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

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

6.5.4.3 Whitelist

This page is used for creating whitelist profiles.

					Search IP / Description	Q
+ Add 🖻 Delete All					and a foreigned	Limit: 1/256
P 57	Description	↓* WUI Login	CPE Service	L* API WebService	de.	
192.168.105.140 - 192.168.105.145	192.168.105.141				🖉 Edit 🖷 Delete	
						Save

These parameters are explained as follows:

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

The following setting page appears when +Add is clicked.

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

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

6.5.4.4 Block Device List

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

eneral Se	tting Blacklist	Whitelist Block Device List			
Id	Name	Model Name	Firmware Version	IP Address	Network
			No data avaitable		

6.5.5 Storage Management

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

System / Storage Management		
Clearlogs		
Delete Time	Alt	*
Delete Type 🖗	Alarm Log Device Sysiog	
Auto Clear		
Duration	Every Day Every Week Every Month	
Periodic(days)	1	
Clear Now		Sava
E Clear Now		Sa

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

6.5.6 Upload Serial Number

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

LUpio	ad J.Download Template J.Exp	bba. I mo		3	Search		8	Rows 10 ~	ы <	1	/1 >	61	C
	Mac Address	Serial Number	17 D	evice Name	17	Network	e.	Model 17	WAN IP	ġ.	LAN IP	ht.	FW I
0	001DAA9FD698	1234657987											
0	001DAAB0BB78	999999999999999											
	001DAAE5CFA8	6543213212											
1	001DAAFEF9D0	זזדודודודו											
	001DAAFEF9F0	888888888											

ltem	Description
Upload	Click to upload a ".CSV" file (located on host) to VigorACS. After comparing the MAC address listed on the file with the information of device(s) managed by VigorACS, the result (device name with serial number) will be shown on this page immediately.
Download Template	Click to download a template from the VigorACS server to your local host. This template is convenient for the system administrator to enter the required information for lots of devices at one time. Later, the template can be uploaded to VigorACS server. Please open the template with a software which can read and write ".CSV" file. Fill the MAC address and serial number (printed on the rear side / bottom) of a device.
Export	Click to export the current serial number table as a file.
Add	Click to add a CPE or VigorAP onto this table.

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

6.5.7 API Key

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

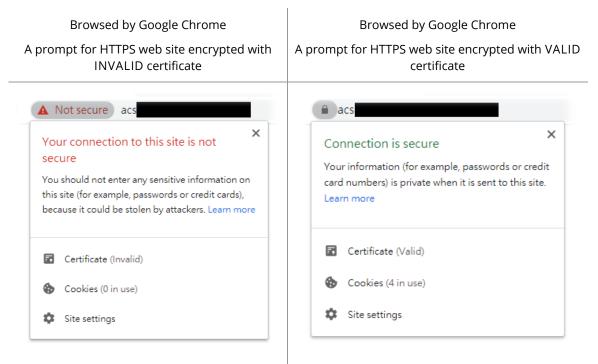
oogle Maps API Key 😡	AlzaSyDnoAWeTGDlzdnkBPnjHGZv44ekxrePCdg	
	Please go to the function management to assign user roles to access the map.	Function Management
	Or go to the System Parameter page to select another map service.	System Parameter
ioogle Ánalytics API Key 🛛		
		El Sav

ltem	Description										
Google Maps API Key	Enter the key you obtained from Google.										
	• Function Management - Click this button to open the setting page. Determine which user role can view the map and switch the toggle to enable the map display for the user.										
	User / Function Management	Shire Unknown Davies	Minutesa In Minister	Deep About Hame	New Version Number	Show Maps	Can Roboot Device	Managa Public Area Film	Can Delete Logs		
	System Administrator	•	•	•	•	•					
	Group Administrator	•	•	۲	•	•	•	•	٠		
	Advatentitutor	۰	۰	۲	•	۰	۲	۰	۰		
	Commissioning	۰	۰	۰	۲	•	۲	۲			
	Operator			۰	•	۰					
	Duttomand Operation		•	•		•	•				
	Wew Only Operator	O		•	•	•					
	Continuanced View Only Operator			•	•	•					
		•			•	•					
									See		
	 System I VigorACS 							play ma	ps on		
	N1 40 Bather D0 40 Exather D0 0 Exather D0 0 Exather D1 0 Exather D2 0 Exather D3 0 Exather D4 0 Exather D5 0 Exather								X		
Google Analytics API Key	Enter the an	alytics	API key f	for track	ing the c	lata.					
Save	Save and act	tivate tł	ne curre	nt settin	gs.						

6.5.8 Certificate

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

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



6.5.8.1 Certificate

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

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

tificate Certificate with private key	PKCS #12 Let's Encrypt
. Create a local Certificate Signing Reques	:t(CSR) :
Generate a CSR	
① Note:	
Please submit the "certreq.csr" file	e to the Certificate Authority then do the next step.
Import Certificate :	
loot CA Certificate (.cer, .crt)	Browse
ntermediate CA Certificate (.cer, .crt)	Browse Delete
	+Add
rusted Certificate (.cer, .crt)	Browse
	_
	Save

These parameters are explained as follows:

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

6.5.8.2 Certificate with Private Key

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

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

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

(.cer, .crt)	content of the certificate from the clipboard.
When One PEM File is s	elected
PEM File (.pem)	Click the Browse button to select one PEM file.
Save	Save current settings and uploading/pasting the certificate.

Example

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

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

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

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

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

MIIEkjC....

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIGDjCCBPag....

-----END CERTIFICATE-----

6.5.8.3 PKCS #12

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

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

System / Certificate		
Certificate Certificate with private key PKCS #12	Let's Encrypt	
Import PKCS #12 file	Browse	
PKCS #12 Password	Φ	
③ Note: Please use the "tr069" as the entry name for yo	ur PKCS #12 certificate file.	
	Save	

These parameters are explained as follows:

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

6.5.8.4 Let's Encrypt

This page will help to

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

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

and

stem / Certificate			
Certificate Certificate with private key PKCS #12 Let's E	ncrypt		
Register Domain	allentestapp.ddns.net		
Auto Renew			
Challenge Type	HTTP-01 Challenge DNS-01 Challenge		
API			~
Function Data			
Export Data	Key	Value	Action
	DuckDNS_Token	aaaaaaa-bbbb-cccc-dddd-eeeeeeeee	
	+Add		
Note: ACME Let's Encrypt will do the following things: Creating a Printe Key & Account from Let's Encry Creating a Cetificate sign by Let's Encrypt Account Automatically change your keystore file from your	it.		
(i) Note:	age by as many people as possible. For more informal	tion please visit ACME website.	
 Let's Encrypt provides rate limits to ensure fair us 			
Let's Encrypt provides rate limits to ensure fair us Note: "HTTP-01 Challenge" can only be done on port 80			

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

6.5.9 Backup Database

6.5.9.1 Backup Tasks

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

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

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

+Add a Task					Auto Refresh: 30 Seconds ~	0 9	urch Prolile, Name/Cre - G
Task Name	Schedule/Period	Last Implemented Status	Last Implemented Date	Created By	Authentication	Action	
testBckAllNow	Now	E Completed	2018-04-11 09:25	yrctw	internal	er eda	IB Delete
lestBckDally	Now	Completed	2019-03-21 14:17	yrctw	Internal	🦉 Edit	If Delete
testBckDailyPM	Daily	Completed	2020-11-02 20:00	yrctw	internal	e" Eda	11 Delete
taskBckNowEaclude	Now	Completed	2020-10-29 15:55	yrctw	internal	er Edil	IT Delete
aackup	Now	Completed	2020-03-03-09:20	artes	Internal	SP Eðil	f) Delete
(i) Note							

These parameters are explained as follows:

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

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

🛢 Backup Database Task		×
Task Settings		_
Enable This Task		
Task Name		
Scheduling		-
Run Backup	Once Repeat	
	Later ~ 11/03/2020 00:00	
Backup Options		-
Backup Type	Backup all tables v	
Ignore License Tables		
Compress Backup File		
After backup delete log tables	Yes No	
Email Notification		-
Enable Email Notification		
Email Subject	Backup Database Task	
Email From	example1@gmail.com	
Email Contant		
	Cancel 🛛 🗟 Sav	ve

ltem	Description
Task Settings	Enable This Task - Click to enable the task. Task Name - Enter a name for the new task.
Scheduling	 Run Backup - Choose Once to perform the backup immediately or at certain time. Choose Repeat to perform the backup periodically. Later / Now - It is available when Once is selected as Run Backup. Starts on xxxxx - It is available when Repeat is selected as Run Backup. Click Edit to open the following web page for modifying the time setting.

	Repeat	×	
	Repeats	Weekly	
	Repeat on	☑ Sun Mon Tue Wed	
	Starts on	02/25/2020	
	Starts time	00.00	
	Summary	Weekly on Sunday	
	e		
		Cancel Done	
Backup Options	Backup Type – Choose	an option to perform the backup.	
	Backup all tables	~	
	Backup all tables		
	Exclude syslog table	s	
	Exclude syslog and log tables Ignore License Tables – VigorACS system performs the database backup by ignoring the tables concerning of backup and license (such as syscd, syssn, dslpmid, dslpmshow and etc.,) to prevent from license error while transferring VigorACS server. The default value is "Enabled". Compress Backup File - The backup file will be compressed.		
	After backup delete lo VigorACS server finishes	g tables – Delete the log tables immediately when s the backup job	
Email Notification	Enable Email Notificat	ion – If enabled, VigorACS server will send a	
		t database backup to the recipient.	
		nter the subject for the email.	
		er the email address of the sender/agent/registrar. Enter the content of the email.	
		he email address of the recipient.	
		Add more recipients to receive the email from	
	VigorACS server.		
Cancel	Discard current modifica	ation.	
Save	Save the current setting	s and exit the page.	

6.5.9.2 Backup Files

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

Backup Tasks	Backup Files Error Logs		
Delete (LDownload		K < 1 /44 > K C
	Filename	$\downarrow\uparrow$ Size $\downarrow\uparrow$	Last Modified 4
	backup_ACS_Trunk AutoBuild 13635_ExcludeSyslogAndLogVer_2020-02-24.2000.sql	11.88 MB	02/24/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13635_ExcludeSyslogAndLogVer_2020-02-22.2000.sql	11.85 MB	02/22/2020 20:00:03
	backup_ACS_Trunk AutoBuild 13622_ExcludeSyslogAndLogVer_2020-02-21.2000.sql	11.86 MB	02/21/2020 20:00:03
	backup_ACS_Trunk AutoBuild 13584_ExcludeSyslogAndLogVer_2020-02-19.2000.sql	11.86 MB	02/19/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13569_ExcludeSyslogAndLogVer_2020-02-18.2000.sql	11.86 MB	02/18/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13548_ExcludeSyslogAndLogVer_2020-02-15.2000.sql	11.87 MB	02/15/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13546_ExcludeSyslogAndLogVer_2020-02-14.2000.sql	11.86 MB	02/14/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13532_ExcludeSyslogAndLogVer_2020-02-13.2000.sql	11.85 MB	02/13/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13508_ExcludeSyslogAndLogVer_2020-02-12.2000.sql	11.85 MB	02/12/2020 20:00:02
	backup_ACS_Trunk AutoBuild 13451_ExcludeSyslogAndLogVer_2020-02-10.2000.sql	11.85 MB	02/10/2020 20:00:01
	backup_ACS_Trunk AutoBuild 13427_ExcludeSyslogAndLogVer_2020-02-08.2000.sql	11.83 MB	02/08/2020 20:00:03

ltem	Description			
Delete	Click to remove the selected filename.			
Download	Click to download the file from the hard disk of VigorACS server located for restoration or transferring.			
	System / Backup Database Backup Tosks - Backup / Mas E Dette - J.Demilaud	ar Star 19 Dat Mutthed		
	tackup ACS. Trunk AutoBuild 2016. ExcludeSystogAndLogVer. 2020-11-02.2000 sqLttp	1.09 MB 11/07/2020 20:00:04		
	backup, ACS, Trunk AutoBuild 2016. ExcludeSyslogAndLogVer, 2020-11-01.2000.sqLnp	1.09 MB 11/01/2020 20:00:02		
	backup, ACS_Trunk AutoBuild 2016_ExcludeSystogAndLogVer_2020-10-31.2000.sqLmp	L09 MB 10/31/2020 20:00:07		
	backup: ACS_Trunk AutoBuild 2016; ExcludeSystegAndLegVer_2020-10-90-2000.sqLtpp	1.09 MB 10/30/2020 20:00:07		
Filename	Display the name of the backup file.			
Size	Display the size of the backup file.			
Last Modified	Display the last modified time.			

6.5.9.3 Error Logs

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

ickup Ta	iks Backup Files Entor Logic							
				<i>u</i> <	Т.	1 2	21	đ
	Filename	en Size an	Last Modified					
0	backup_ACS_Trunk AutoBuild 1024_ExcludeSyslogAndLogVer_2020-07-15.2000_error.log	0 Byte	07/15/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 996_ExctudeSyslogAndLogVer_2020-07-14.2000_error.log	0 Byte	07/14/2020 20:00:00					
D	backup_ACS_Trunk AutoBuild 992_ExcludeSyslogAndLogVer_2020-07-13.2000_error.log	0 Byte	07/13/2020 20:00:00					
п	backup_ACS_Trunk AutoBuild 944. ExcludeSystogAndLogVer_2020-07-09.2000_error.log	0 Byte	07/09/2020 20:00:00					
	backup_ACS_Trunk AutoBuild 852_ExcludeSyslogAndLogVer_2020-07-04.2000_error.log	0 Byte	07/04/2020 20:00:00					
D.	backup_ACS_Trunk AutoBuild 842_ExcludeSyslogAndLogVer_2020-07-03.2000_error.log	0 Byte	07/03/2020 20:00:00					
D.	backup_ACS_Trunk AutoBuild 802_ExcludeSystogAndLogVer_2020-07-01.2000_error.log	0 Byte	07/01/2020 20:00:00					
	backup_AC5_Trunk AutoBuild 780_ExcludeSyslopAndLogVer_2020-06-29.2000_error.log	ù Byte	06/29/2020 20:00:00					
	backup_AC5_Trunk AutoBuild 761_ExcludeSyslogAndLogVer_2020-06-24.2000_error log	0 Byte	06/24/2020 20:00:00					
0	backup_ACS_Trunk AutoBuild 159_ExcludeSystogAndLogVer_2020-06-23.2000_error.log	0 Byte	06/23/2020 20:00:00					
	backup_AC5_Trunk AutoBuild 12732_ExcludeSyslogAndLogVer_2020-06-19.2000_error.log	0 Byte	06/19/2020 20:00:00					
0	backup_AC5_Trunk AutoBuild 722_ExcludeSyslogAndLogVer_2020-06-18.2000_error log	0 Byte	06/18/2020 20:00:00					
1	backup. ACS, Trunk AutoBuild 12732, ExcludeSyslogAndLogVer_2020-06-17.2000, error.log	0 Byte	06/17/2020 20:00:00					
0	backup_ACS_Trunk AutoBuild 664_ExcludeSyslogAndLogVer_2020-06-12.2000_error.log	0 Byte	06/12/2020 20:00:00					

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

6.5.10 Login Bulletin

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

6.5.10.1 Preview

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

Ŧ	Dray Tek VigorACS 3	Root Network (100142)	COP
(3)	System / Login Bulletin		
	_		Preview General Settings Builletin Items
E # # E			
-			etiv DemozTali
S.			DrayTek
ø			VigorACS
1		Dray Tek	
			Usemama
10			Freemand
M (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			Ramember me
0			Login
			Color Color

6.5.10.2 General Settings

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

Ŧ	Dray Tek VigorACS 3	Root Network (100142)	Q Pcap A 15:54:08 mk_carrie M.
	Dray Tek VigorACS 3 System / Login Bulletin	Root Network (100342) DrayTek	15:5438 mk_carrie M
0			Show Carpusel Indicators Stuffle Message Sover

These parameters are explained as follows:
--

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

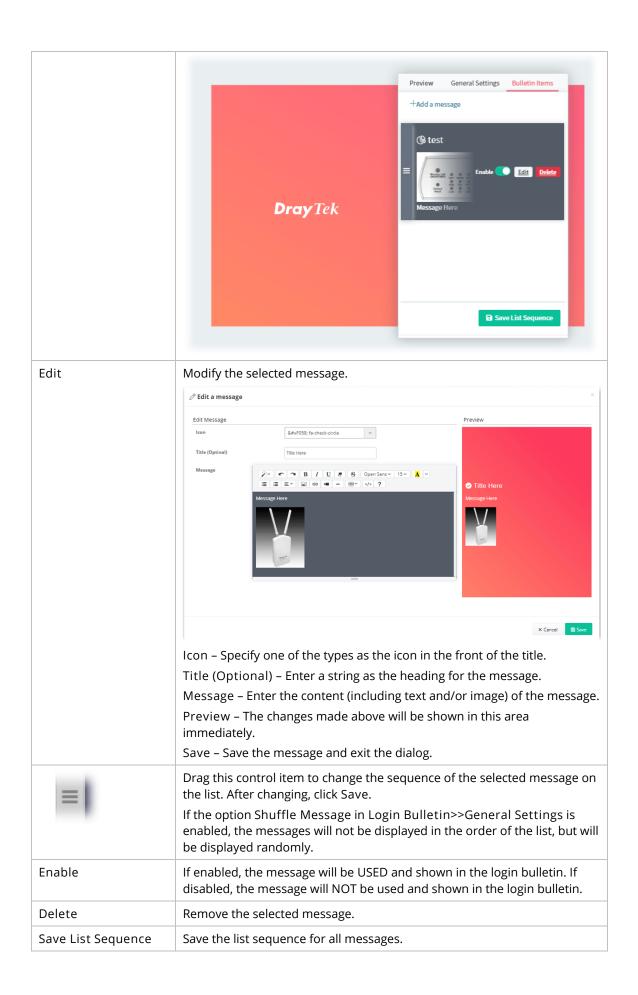
6.5.10.3 Bulletin Items

Peap A 15:54:08 mk_carrie M = Dray Tek VigorACS 3 9 Root Network (100142) ~ System / Login Bulletin Eas Preview General Settings Bulletin Items +Add a message A Notice: Option "Shuffle Message" in general settings has been enabled. The messages will not show in the following order but in random. B 圕 1 **Dray**Tek 1 🕸 23 0 Save List Se

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

Item	Description	
+Add a message	Create a new message.	
	+ Add a message	×
	Edit Message	Preview
	Icon  fa-check-oircle >	
	Trite (Optinal) Title Here Message	
	Message Here	Title Here
		Message Here
		X Cancel Save
	Icon – Specify one of the types as the icon in the	front of the title.
	Title (Optional) – Enter a string as the heading for	or the message.
	Message – Enter the content of the message.	
	Preview – The changes made above will be show immediately.	n in this area
	Save – Save the message and exit the dialog. Ref result.	er to the following setting

These parameters are explained as follows:



6.5.11 Adverts Carousel

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

6.5.11.1 General Settings

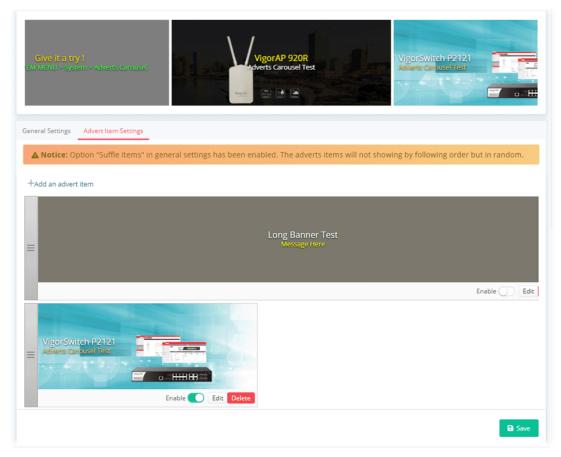
This page determines if displaying the adverts on the login page or not, enabling the auto play carousel function, selecting cycling delay time and using the shuffle items.

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

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

6.5.11.2 Advert Item Settings

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



These parameters are explained as follows:

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

To add an advert item, do the following steps.

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

+ Add an item		×
Upload Image	Please select an image. Browse	
	🕹 Upload	
ONote:Height will automatically addressed	ljust to 180px.	
 Notice: Image width needs to be g 	eater than or equal to height.	
Preview		
	Upload an Advert Image Please upload an image first.	
	Cancel 🔀 Sav	/e

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

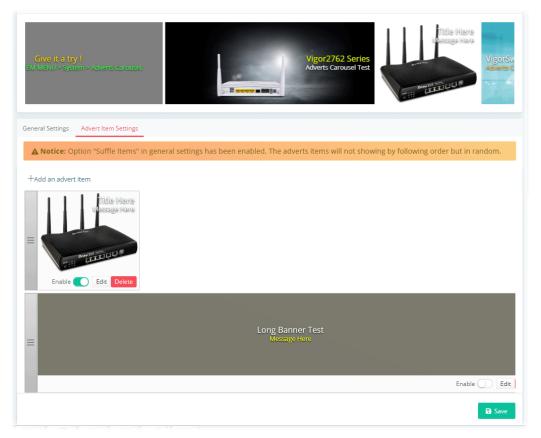
2. After specifying an image file, click the Upload button. Later, a page with detailed settings will appear as follows:

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

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

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

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



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

	A mistake is only an er it becomes a mista when you fail to correct Enable You make me w to be a better m	Enable C Edd Dedes
Enable	If enabled, the advector carousel.	ert item will be USED and shown in the adverts
		ert item will NOT be used and shown in the adverts
Edit	Click to modify sett	ings for the selected image.
	🕑 Edit an item	×
	Upload Image	Please select an image. Browse
		💩 Upload
	Title (Optinal)	Give it a try ! (Max. 60 characters)
	Title Color	##fde00
	Message (Optinal)	Change it on SYSTEM MENU > System > A (Max_250 characters)
Delete	Delete the selected	advert item.
Save	Save the current se	ttings.

6.5.12 Logs

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

	stem Loe	System Lo	e Lozin Loz	Access Con	TRALLOW	Device Reject Log Server Log				
					troi Log	Device Heject Log Server Log				
elect b			/ Calegory / Result							
Critts	cal Majór	Minor	Warring Non	mal M	antenance	Reports Provisioning Netw	ork System User Apply Succeeded Apply Fal	(c)		
	2 Date	in Ali)c	
		User	Authentication	Severity	Interface	Category	Overview	Result	Login IP	Titte
	2445	1001	unternal	e Normal	WEB	User > Function Management	Configuration has been updated.	succeeded	111.251.202.14	2025/01/17 12:03:05
0	2448	1001	ovternal	 Normal 	WUI	Hotspot Web Portal > Pyome	Configuration has been added,	Falled	111.251.202.34	2025/01/16 10:56:12
2	2441	root	Internal	a Normal	WUI	Horspot Web Portal > Profile	Configuration has been added.	Tailed	111.251.202.14	2025/01/16 10:58:47
3	2442	root	Internal	A Critical	Wei	User > User Management	User root's Profile has been updated.	Succeeded	1.169.228.62	2025/01/14 18:32:18
3	2441	root	internal	🔥 Critical	WUI	USer > Group Management	User allentest has been removed from coll's group	Succeided	1.169.208.116	2025/03/14 18:04:44
2	2440	1005	Internal	a Critical	WDF	User > Group Management	User allentest has been removed from trimpp's group	Succeided	1.169.208.110	2025/01/14 18:04:40
2	24,39	root	Internal	A Critical	(U.S.I)	User - Group Management	User allentest has been removed from RochGoup's group	Succended	1.169.208.116	2025/01/14 18-04:30
a,	2011	3001	Internal	O Normal	WU	Configuration	Configuration of VPN_LAN2LAN_Profiles(14490C055378)	Succeeded	1.169.208.116	2025/01/14 18:00:48
2	2437	1001	internal	/fs. Critical	wu	User > User Management	User alientest's Profile has been updated.	Succeeded	1.169.208.116	2025/01/14 18:00:27
з.	2436	1001	internal	A Critical	WUI	User > User Management	User allentest's Prome has been updated.	Succeeded	1169.208.116	2025/01/14 17:50:11

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

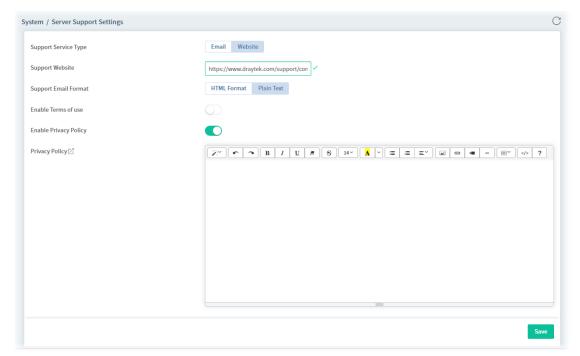
6.5.13 XMPP Profile

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

Status	Disconnected		
Enable	Gal		
Server IP/Domain	192.168.105.1		
Server Port (default : 5222)	9090		
Username	admin		
Password		•	
Password		0	

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

6.5.14 Server Support Settings



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

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

6.5.15 Delete Logs Actions

Information displayed here shall be deleted.

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

Category filter:	ACS Users Vigor	Devices Network Client					303A/33/38 to 2025/0	ujii s	5034	th ID / op	erator		. 0
							kd.	¢	10	/1 2	D.	e	
D	† Category	Log Table	Operator	Authentication	Login IP	Overview	17	Time					
				,	io data available								

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

6.5.16 App Server

To use the push notification function, the App Server must be enabled first.

Enable App Server		
App API Key		
	Send App Notification Test	
() Note:	nd to use the week antiBentian functions. Binned for in 1000000, and then slide then	
	ed to use the push notification functions. Please log in $$ MyVIII01 $$ and then click App Pl Key.	
An API key is require		

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

6.5.17 License Key Pools

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

From the following page, click Login with MyVigor.

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

Later, a login page appears.

	>
Dray T	ek
MyVigor	
Username	
draytek_rd8	
Password	
*********	¢
Login	

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

6.5.17.1 Bind to User Group

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

	Dray1	ek vigoracs	3	Root Ne	Swork (100142)	4	Pcap C	10:17:77 8/15/24	mk_carrie System Administrator	M
(3)	System /	License Key Pool	ls							C
68	- Rend to Us	tor Group Key	Liet							
414	Bind v	with MyVigor /	Account							
4	Status		draytok_rd8	Log out Unbind						
T	Availa	able Keys								
		Interface I	of the second se	ung	Conception of the second secon					
⊕		8/26	4/11	1/5	3/10					
23	Bind F	Keys to User G	Group					Sein	ch User Group-C	g
0		User Group / Licer	use Type	Number Of Keys	Used Keys	Nodes				
	Ð	RootGroup							P Edit	
	÷	AutoTest							ar Edit	
	۲	fultLicense_A							@ Edit	
	(\bullet)	expireLicense_	A						de Edit	
	۲	uni1							P Edit.	
	٢	11114							🖉 Edit	
	Ð	titt5							Ø Fair	
	\oplus	mit2							di Edit	
	1								2000	

ltem	Description
Bind with MyVigor Ad	ccount
Status	To bind with MyVigor Account, make sure you already have one set of user account and user password to login MyVigor website. If not, apply one account first.
	Login with MyVigor – Enter the user name and user password using MyVigor account to login MyVigor website.
	Relogin MyVigor – This button appears if you have login MyVigor website previously and successfully. Click to access MyVigor again.
	Log out – Log out MyVigor website but still bind with MyVigor server.
	Unbind – Unbind from MyVigor website.
Available Keys	
Total Keys x/y	Display current status (Unsubscribed or Subscribed) of all service (B, A, silver card).
	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation B card x/y	Display current status (Unsubscribed or Subscribed) of the service (B card). In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation A	Display current status (Unsubscribed or Subscribed) of the service (A card).
card x/y	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
URL Reputation Silver Card x/y	Display current status (Unsubscribed or Subscribed) of the service silver card).
	In which, x means the number of unsubscribed keys; y means the number of subscribed keys.
Bind Keys to User Gro	quo

User Group / License Type	Displays the name of the user group and the license type used.
Number of Keys	Display the quantity of the service card purchased.
Used Keys	Display the quantity of the service card used.
Nodes	Display the number of nodes that have used this service card.
Edit	Click to bind another key used for the selected user group.

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

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

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

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

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

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

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

Now the available keys will be changed as follows:

ind to User Group Ke	yList				
Bind with MyVigor	Account				
50 alus-	draynek, rids	Log out Unbind			
Avaliable Keys					
	-	All and the second seco	100		
7/26	4/11	0/5	3/10		
Bind Keys to User					with Userbinoup Q.
Uner Group / Lik	ета туре	number or keys	used keys	Nodes	
() ReotGroup					e ² Lau
AutoTest.					1 East

6.5.17.2 Key List

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

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

9	Dray Tek VigorACS 3		(Root Networ	nk (100142)	~ a		Cap	P	11:13:37 8/16/24	mk_carrie System Administrator	1
3	System / License Key Pools											C
83	Bind to User Group											
494	Avaliable Keys											
2	init(bes-	10. m	A care		No.							
EP.	7 / 26	4/11	0/5		3/10							
<u>回</u>												
					Type	Ait 🍝	WORDONY All			Search	9	
(i)	Key List					Les Uplite Des 2024-2010	(04) #1 S	ync Lice	nse	Ín	nport License Key	
Åß	License Key	Activated Date		Expire Dat	le -	License Type	Validity			User G	roup	
1	5A219	-		-		URL Reputation - B Card	Available					
	B7B56-****-7CE08	-		-		URL Reputation - B Card	Available					
	8865267349	÷.		-		URL Reputation - E Cavil	Available					
	E1A40.*****.44***.74CEE			-		URL Reputation - B Card	Available					
						the second s						
	FAC9D	-		-		URI Reputation - Silver Card	Available					
	FAC8D	-		2		URI, Reputation - Silver Card	Available					
		1		1 1								
	03528-****-FB154			1 1 1 1		URI, Reputation - Silver Card	Available			Rooto	iroup	
	03528.*****.FB154				n	URL Reputation - Silver Card URL Reputation - Silver Card	Available			Rooto		

To import the license key to VigorACS,

1. Click the Import License Key button.

Туре	All ~	Validity	All	~	Search	Q
	Last Update Time : 2024-08-1	6 10:41:43	Sync License		Import Licer	nse Key
1	License Type		Validity		User Group	
	URL Reputation - B Card	Available				

A dialog will be shown as follows:

"LUpland uk	Download Template	Search	0.
License Key	Serla	i Number	
	No data ava	elable	
	4	ihow 10 ~ e	ntries + P

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

Rostata availanty Stores 10 - Stores 10 - Stores 10 Stores Key File
▲ Select Import License Key File
united linens keyeny
allada lason adves
Cancel Apply

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

Import License Key	
L Upload 🕹 Download Template	Search
License Key	Serial Number
CS80F-7ABCA-84CB4-ABC64	2204V0226375
59043-38804-7A897-5A8EF	220440226376
	Show 10 × entries 🔌 🚺 *

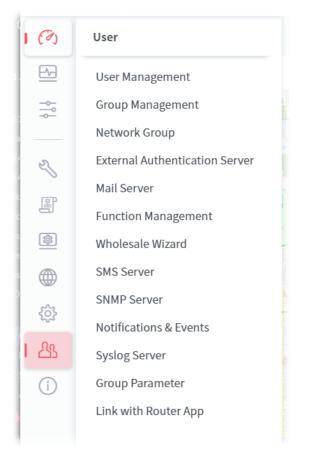
4. Later, the status of the license key(s) will be shown as "License imports success". Click Finish to apply the license to VigorACS and exit the dialog.

mport License Key	
License Key	Status
C5B0F-7ABICA-84CB4-ABIC64	License Imports Lecons.
59043-38804-2AB07-5A8EF	License Imports aucons.
	Show 40 - antries 11 1

6.6 User

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

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



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

6.6.1 User Management

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

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

+Add	🖉 User Batch	h Şeţi	lings.									Search	0
howin	g 1 to 10 of 133 entries								Show	10 v entries 🗰	1	2043	ă ê
	Username	17	Authentication	÷	Role	-27	Status 17	Email Notificatio	n 47	SMS Notification	Em	alt	4
	root		Internal		System Administrator		A	(Transfeet)		Distant	tim	yang@draytek.com	
	tim_radius		External - AutoTest		Group Administrator			_		-	tira	_yang@draytek.com	
	kc_radius		External - RootGroup,f…		System Administrator		Active	-		-			
	auto_test		Internal		System Administrator		-	-		(Disabled)	aut	o_test@draytelc.com	
0	AutoTestGroup, GA		Interna)		Group Administrator		-	Disabled		(Disible)	Aut	oTestGroup_GA@test.com	
0	artes		Internal		System Administrator		-	(1111)		(2000)	arie	es_chen@draytek.com	
0	fullLicense_A		Internal		Group Administrator		-	Disabled		Distant	full	License_A@test.email	
	expireLicense_A		Internal		Group Administrator		Active	-		-	exp	ireLicense_A@test.email	
	tim_yang		Internal		Group Administrator			(1111)		-			
0	eric lai		External - tttt1,tttt4,ttt		System Administrator		-	(1000		Disabled	orte	: lai@draytek.com	

ltem	Description					
+Add	Click to add a user.					
Delete	Click to remove the selected user.					
User Batch Setting	Click to configure user batch settings (for Out-of-box experience).					
	User Batch Settings ×					
	Apply to Users Operator (Internal)					
	Enable OOBE feature 🚱					
	OOBE pages to display Read the Agreements ~					
	Enable Auto Logout					
	 Note: When select multiple users includes "View Only Operator", "Auto Logout" will not apply to "View Only Operator", only to other users. 					
	Cancel Apply					
	Apply to Users - Select the user type (root, admin, operator) to apply the batch settings.					
	Enable OOBE feature - Switch the toggle to enable/disable the function. If enabled, the user will be guided to OOBE pages to modify settings (e.g., password, e-mail, notification, etc) for the next time to login VigorACS.					
	OOBE pages to display - Select the pages to display on the screen.					
	Disable Auto Logout - Switch the toggle to enable/disable the function. If disabled, the user has to logout the screen manually.					

The following setting page appears when +Add is clicked.

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

ltem	Description					
Enable	Click to enable the user profile.					
Username	Enter a name for the new user.					
Password	Enter the password for the user.					
Role	Choose the role for the selected user. Different role represents different authority that the user group will have. The great the authority is, the more functions the user can have.					
	System Administrator \sim					
	System Administrator					
	Group Administrator					
	Administrator					
	Commissioning					
	Operator					
	Customized Operator					
	View Only Operator					
	Customized View Only Operator					
	Auditor					
	 System Administrator – Have the highest authority. If it is selected, the corresponding settings configured in this page will be added to all user groups listed below. 					
	 Group Administrator – Have the middle authority high than 					

	"Administrator".
	 Administrator – Have the middle authority.
	 Commissioning - Have the authority to add a new network and view SD-WAN settings.
	 Operator – Have the low authority higher than View Only Operator.
	 Customized Operator – Have the low authority higher than View Only Operator, with restricted widget and Menu items.
	• View Only Operator – Have the lowest authority.
	 Customized View Only Operator – Have the lowest authority. In addition, with restricted widget and Menu items.
	 Auditor - Have limited authority different from other roles. It is available for choosing only when the system administrator accesses into VigorACS with the role of Root (default account). The only action allowed is to view the deleted log information (on the page of System>>Delete Logs Action).
Enable WUI Login	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the web user interface of VigorACS.
Enable API Service	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the API service.
	Confirm API Password - Enter the password for access the API service.
Disable Auto Logout	Switch the toggle to enable / disable the function. If enabled, the user must logout VigorACS manually.
Enable OOBE feature	Switch the toggle to enable / disable the function.
	When it is enabled, the user is allowed to access into the web user interface of VigorACS and allowed to view the OOBE page(s).
	OOBE pages to display - If the OOBE feature is enabled, select the page(s) to display on the screen.
Email Notification	Switch the toggle to enable / disable the function.
	When it is enabled, an email will be sent to the user as a notification when the connected device gets alarms.
	Email - Enter the email for communication between the user and VigorACS server.
SMS Notification	Switch the toggle to enable / disable the function.
	When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms.
	Telephone - Enter the telephone number for receiving the SMS notification.
Chatbot Notification	Switch the toggle to enable / disable the function.
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications and information related to VigorACS.
	If enabled, this user account can check general information of VigorACS server through specific mobile phone device and/or PC.
APP Notification	Only the login user has the right to enable the function of APP Notification. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of DrayTek APP Notification, go to the APP Notification setting page.

	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications, and information related to VigorACS.
Two-factor authentication	Only the login user has the right to enable the function of 2FA authentication. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of 2FA authentication, go to the Two-factor authentication setting page.
Description	Enter a brief description for the user.
Cancel	Discard current modification.
Create	Save the current settings and exit the page.

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

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

ser /	User Management							C
-Add	l 💼 Delete 🔗 User Batch S	ettings					Search	Q
nowii	ng 111 to 120 of 123 entries				Show	10 × entries 4 1	··· 9 10 11 12 13	₩
	Username ↓↑	Authentication 41	Role $\downarrow\uparrow$	Status↓↑	Email Notification	SMS Notification Email		$\downarrow\uparrow$
	zzz_test_094	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_095	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_096	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_097	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_098	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_099	Internal	Group Administrator	Active	Disabled	Disabled		
	zzz_test_100	Internal	Group Administrator	Active	Disabled	Disabled		
	mk_carrie	Internal	System Administrator	Active	Disabled	Disabled		
	T_2022-12-12_addUser_E	Internal	Group Administrator	Active	Enabled	Enabled		
	T_2022-12-12_addUser_D	Internal	View Only Operator	Active	Disabled	Disabled		
				_				_

The following shows the Edit User Profile page.

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

Item	Description			
Enable	Click to enable the user profile.			
Username	Enter a name for the new user.			
Password	Enter the password for the user.			
Confirm Password	Enter the password again.			
Role	Choose the role for the selected user. Different role represents different authority that the user group will have. The great the authority is, the more functions the user can have. System Administrator Group Administrator Group Administrator Commissioning Operator Customized Operator View Only Operator Customized View Only Operator Auditor			
	 System Administrator – Have the highest authority. Group Administrator – Have the middle authority high than 			
	"Administrator".			
	• Administrator – Have the middle authority.			

	 Commissioning - Have the authority to add a new network and view SD-WAN settings.
	• Operator – Have the low authority higher than View Only Operator.
	 Customized Operator – Have the low authority higher than View Only Operator, with restricted widget and Menu items.
	 View Only Operator – Have the lowest authority.
	 Customized View Only Operator – Have the lowest authority. In addition, with restricted widget and Menu items.
	 Auditor - Have limited authority different from other roles. It is available for choosing only when the system administrator accesses into VigorACS with the role of Root (default account). The only action allowed is to view the deleted log information (on the page of System>>Delete Logs Action).
Enable WUI Login	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the web user interface of VigorACS.
Enable API Service	Switch the toggle to enable / disable the function.
	If enabled, this user account is allowed to access the API service.
	Confirm API Password - Enter the password for access the API service.
Disable Auto Logout	Switch the toggle to enable / disable the function.
	If enabled, the user must logout VigorACS manually.
Enable OOBE feature	Switch the toggle to enable / disable the function.
	When it is enabled, the user is allowed to access into the web user
	interface of VigorACS and allowed to view the OOBE page(s).
	OOBE pages to display - If the OOBE feature is enabled, select the page(s) to display on the screen.
Email Notification	Switch the toggle to enable / disable the function.
	When it is enabled, an email will be sent to the user as a notification when the connected device gets alarms.
	Email - Enter the email for communication between the user and VigorACS server.
SMS Notification	Switch the toggle to enable / disable the function.
	When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms.
	Telephone - Enter the telephone number for receiving the SMS notification.
Chatbot Notification	Switch the toggle to enable / disable the function.
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications and information related to VigorACS.
	If enabled, this user account can check general information of VigorACS server through specific mobile phone device and/or PC.
APP Notification	Only the login user has the right to enable the function of APP Notification. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of DrayTek APP Notification, go to the APP Notification setting page.
	When it is enabled, a notification will be sent to the user with a pop-up message when the device gets alarms, events, notifications, and information related to VigorACS.

Two-factor authentication	Only the login user has the right to enable the function of 2FA authentication. The System Administrator of VigorACS is allowed to disable this feature only. To enable/disable the function of 2FA authentication, go to the Two-factor authentication setting page.
Description	Enter a brief description for the user.
Cancel	Discard current modification.
Create	Save the current settings and exit the page.

6.6.2 Group Management

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

6.6.2.1 Setting

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

Setting:	Management	Ul Customization						
Add							Search	a
	Group 10	Group Name	Max Nodes	1 Used Nodes	Enable Expire Date	xpire Date Cnable Global Mail Server	Enable Global SNMP Server	
ā	5	cetti	5	1	-		(Brakin)	
	1	RootGroup	No Limit Nodes	48	(111)	-	(1000)	
π	2	Intopp	No Limit Nodes	1	CHEMIC		-	
п	4	AltenGroup	No Limit Nodes	T.	(Dirable)	Bicaster	(Contract)	
D	h	FR_APP_Group	No Limit Nodes	a		(Truster)	(Timber)	
п	1	CPE_Install_Group	No Limit Nodes	a	(Brader)	(Broaking)	(Contract)	
11	a	RD5_Henry	No Limit Nodes	1	Charles	· (Builder) ·		
Nodes In	formation							
Current N	odes in Used	Configured Max Nodes	Purchased License Nodes					

These parameters are explained as follows:

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

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

er / Grrup Management		
Setting Management UI Customization		
Add Group		
Group name	Markiting2025	
Nodes	-1	
	(-L: No Limit Rodes)	
Enable CPE Notity Mail/SMS/SNMP		
Enable Global Mall Server		
Enable Global SNMP Server		
Enable Expire Date		
Expire Date	Joinet à étale	
	 Jan, ✓ 	
	2025 🛩	Cancel Sa
	Su Ha Tu We Th Fr Sa	
Nodes Information	1 7 3 4	
Current Nodes in Used Configured Max Nodes	5 6 7 8 9 10 11 12 13 14 15 16 17 18	
58 5	19 20 21 22 23 24 25	
	26 27 29 29 30 31	

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

6.6.2.2 Management

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

User / Group Management		С
Setting Management UI Customization		
User Group : RootGroup	× −	
	ne © diego_li © iouis © andyc © colec © arthurroot © PP_Ann © ackh © c4193 © henry_wang © IBD_James © IBD_Ellie © an_custom ©	

These parameters are explained as follows:

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

6.6.2.3 UI Customization

The administrators can set the required WUI components for the Customized Operator and the Customized View Only Operator profiles.

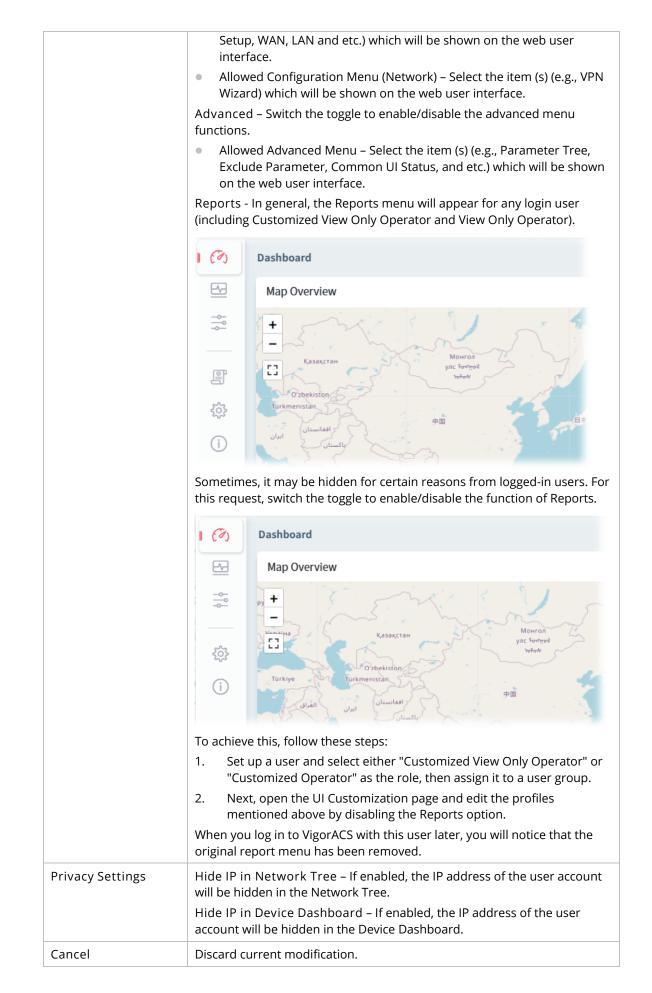
er / Group Management		
Setting Management UI Customiza	tion	
User Group : RootGroup	v	
Profile Name	Role	Option
Customized Operator	Customized Operator	
Customized View Only Operator	Customized View Only Operator	

ltem	Description
User Group	Use the drop down list to specify a user group. In which, RootGroup contains all of the users with the role of system administrator in default.
Option	Edit – Click to modify the UI for the Customized Operator and the Customized View Only Operator.

Click Edit to open the following page.

r / Group Management	c
Setting Management UI Customizatio	n
Edit UI Customization Profile	
Profile Name	
FIGHERALIE	Customized Operator
Role	Customized Operator
UI Customization	
Allowed Dashboard Widgets	Map Overview, Network/Device Ove ~
Allowed Dushboard Wagets	Note: Select which widgets to display on Dashboard page.
Statistics	
Allowed Statistics Widgets	Usage Overview, Clients, Wireless Cl $\scriptstyle{ imes}$
	Note: Select which widgets to display on Statistics page.
Monitoring	
Allowed Monitoring Menu (Device)	Alarm, Logs, GPS, WAN (SD-WAN), VI $\scriptstyle{\sim}$
Allowed Monitoring Menu (Network)	Alarm, Logs, Devices, Clients, Celluli ~ Iothe: Safect which Monitoring menus to display for Network and CPE
	посе, чески поклани при непи на мариа у на технали али стъ. рада,
Configuration	
Allowed Configuration Menu (Device)	Port Setup, WAN, LAN, Hotspot Web ${\scriptstyle \lor}$
Allowed Configuration Menu (Network)	VPN Wizard v
	Note: Select which Configuration menu to display for Network and CPE page.
Advanced	
Allowed Advanced Menu	Parameter Tree, Exclude Parameters ~
ntonea narancea nena	Note: Select which Advanced menu to display for CPE page.
Reports	
Privacy Settings	
Hide IP in Network Tree	
Hide IP In Device Dashboard	
	1
	Cancel Save

ltem	Description	
Edit UI Customization Profile	Profile Name – Displays the name of the profile. Role – Displays the role of the profile is associated with.	
UI Customization	Allowed Dashboard Widgets – Select the widget (s) (e.g., Map Overview, Network/Device Overview, Active Clients and etc.) which will be shown on the dashboard.	
	Statistics – Switch the toggle to enable/disable this feature.	
	• Allowed Statistics Widgets – Select the widget (s) (e.g., Usage Overview, Clients, Wireless, and etc.) which will be shown on the dashboard.	
	Monitoring – Switch the toggle to enable/disable the feature of monitoring.	
	 Allowed Monitoring Menu (Device) – Select the item(s) (e.g., Alarm, Logs, GPS, and etc.) which will be shown for monitoring. 	
	 Allowed Monitoring Menu (Network) - Select the item (s) (e.g., Alarm, Devices, Cellular Data Usage and etc.) which will be shown for monitoring. 	
	Configuration – Switch the toggle to enable/disable the menu selections for the web configuration.	
	• Allowed Configuration Menu (Device) – Select the item (s) (e.g., Port	



Save Save the current settings and exit the page.

6.6.3 Network Group

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

ame	User Group	
S Root Network(100142)	RootGroup	~
AutoTestNetwork(1)	AutoTest	*
p 🕜 AutoTest_Dev(9)	AutoTest_Dev	*
AutoTest_SD-WAN(2)	(As Parent)	*
D & AutoTest_VPN(1)	AutoTest_VPN	ζ.
D O Hotspot_Web_Portal(2)	Hotspot_Web_Portat	*
Router_App_Network(2)	Router_App_Group	*
p 3 T_2074 08 01_Wholesale_GA_D(0)	T_2024-08-01_Wholesale_GA_D	*
1- 3 T_2024-08-01_Wholesale_GA_E(0)	T_2024.08.01_Wholesale_GA_F	*
b 🐼 T 2024-08-01 Wholesale GA OOBE(0)	T 2024-08-01 Wholesale GA OOBE	~
P 🐼 T_2024-08-01_addNetwork_A(0)	T_2024-08-01_addGroup_E	2
T_2024-08-01_addNetwork_B(0)	(As Parent)	*
	(As Parent)	*
↓ ③ U_2865_5(2)	AutoTest	*
b 🐼 U 2866 5(4)	AutoTest	÷
D 🐼 U 2927_5(5)	AutoTest	~
VigorSwitch(2)	(As Parent)	~
i> 🐼 aaa(5)	(As Parent)	v.
↓ ② expireLicense_A(0)	expirel icense_A	ų.
b S fullLicense A(1)	fullLicense_A	¥

These parameters are explained as follows:

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

6.6.4 External Authentication Server

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

User / External Authentication Server User Group: All User Group						С
Enable						
Choose User Role at Registration	View Only Operator ~					
Authentication Server Type	Active Directory / LDAP ~					
Server IP Address						
Destination Port	636					
Use SSL						
Bind Type	Simple Anonymous Regular					
Regular DN						
Regular Password		•				
						Profile Number Limit: 0/5
Id Profile Name Common Name	Base Distinguished Name	Ac	ditional Filter	Group Distinguished Name	Action	
		No da	ta available			
						Save
						Save

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

	as Bind Type.
	RADIUS –
	 Server IP Address - Enter the IP address of LDAP server.
	 Destination Port - Enter a port number as the destination port for LDAP server.
	 Shared Secret –The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.
	• Confirm Shared Secret - Re-type the Shared Secret for confirmation.
	TACACS+ –
	• Server IP Address - Enter the IP address of TACACS+ server.
	• Destination Port - Enter a port number as the destination port for LDAP server.
	• Authentication Protocol – Select PAP or CHAP.
	• Shared Secret - Enter the Shared Secret for confirmation.
	• Confirmed Shared Secret - Re-enter the Shared Secret for confirmation.
	Single Sign-On (SSO) – Single sign-on (SSO) is an authentication method that enables a user to log in to multiple independent but related software systems using a single SSO ID. If this type is selected, the system administrator can access VigorACS via Microsoft Azure SAML (Security Assertion Markup Language). To use Azure Single Sign-On to access VigorACS, please configure the ACS SSO on Azure first to get the following settings.
	 Protocol – Display the default setting.
	 Identifier (Entity ID) – Enter the ID value applied from the service provider.
	• Reply URL (ACS URL) – Enter the ACS URL.
	 Certificate – Use the Browser button to locate the certificate (Base 64) generated by VigorACS and SAML.
	• Login URL – It is optional. Copy the login URL generated by ACS SSO.
	 Logout URL – Copy the logout URL generated by ACS SSO.
+Add	It is available for Active Directory / LDAP server type. After finished the general settings for the authentication server type, click Save to activate the +Add link.
	+Add - Click to create a profile related to LDAP.
Save	Save the current settings and exit the page.
1	

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

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

These parameters are explained as follows:

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

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

					Profile Number Limit: 2/5
Profile Name	Common Name	Base Distinguished Name	Additional Filter	Group Distinguished Name	Action
Idap	uid	ou=People,dc=ms,dc=draytek,dc=com			🗊 Delete
LD_1	UID	MARKET		GROUP	Delete
	ldap	ldap uid	ldap uid ou=People,dc=ms,dc=draytek,dc=com	ldap uid ou=People,dc=ms,dc=draytek,dc=com	ldap uid ou=People,dc=ms,dc=draytek,dc=com

6.6.5 Mail Server

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

r / Mail Server		
Group : All User Group	w l	
Send Test Email		
Enable Server		
Authentication Method	No Authentication Rasic OAuth2	
Security	None SSL 11.5	
Hast	ms.draytek.com	
Port	465	
Sender Email	6m_yang@draytek.com	
Username	tim_yang	
Password		
Subject	Vigen/ACS ③ Nami Level ④	
	Network Name ③ Device Name ③ Model Name ③ MAC Address ③ Device IP ④	
	Alarm Message 🛞 User Name Ø	
D Reset To Default		
Prost to believe.		

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

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

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

Click Save to save the change.

6.6.6 Function Management

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

Role	Show Unknown Device	Wireless Is Writable	Show About Menu	Show Version Number	Show Maps	Can Reboot Device	Manage Public Area Files	Can Delete Log
hole	Show onknown bence	initia de la companya	onon noout richa		onon napo	Gan neboot benee	Hundger abneratearnes	cun betete Eby
System Administrator								
Group Administrator								
Administrator								
Commissioning								
Operator	\bigcirc							
Customized Operator								
View Only Operator						\bigcirc		
Customized View Only Operator						\bigcirc		
Auditor								
								Save

ltem	Description			
Show Unknown Device	Unknown device can be seen / hidden if it is enabled / disabled.			
Wireless is Writable	When it is enabled, settings related to wireless connection are allowed to be configured.			
Show About Menu	he About menu with information of VigorACS can be seen if it is enabled or the role.			
Show Version Number	The version number can be displayed/hidden separately for various roles of users. Switch this toggle to display (enable) or hide (disable) the version number.			
	By default, the version number of VigorACS will be shown for System Administrator and displayed on the page of About VigorACS.			
Show Maps	Google Maps/ Leaflet Maps can be displayed/hidden for various role of user accounts. Switch this toggle to display (enable) or hide (disable) the version number.			
Can Reboot Device	Determine if the logged-in user can reboot the CPE device directly from the dashboard of the CPE. Switch this toggle to enable the function (with a 'Reboot Now' link) or disable it (without a 'Reboot Now' link).			
	Quick Tools			
	D Backup Config つ Restore Last Config 🕹 Download Last Config 🕛 Reboot Now			

	Quick Tools Description T Backup Config Description Restore Last Config Description					
Manage Public Area Files	Determine if the logged-in user (limited to the user role of System Administrator, Group Administrator, Administrator, and Commissioning) can manage the files in the Public Area. If enabled, on Maintenance>>File Manager, the PublicArea will be available for choosing as the User Group. Corresponding information will be shown on the page and allowed to be uploaded or downloaded.					
	Maintenance / File Manager User Group: PublicArea Y					
	🗘 Upload 👍 Download 💼 Delete 🖼 New Folder 👁 DrayTek FTP					
	□ Filename ↓↑ Device Name ↓↑ Property					
	The PublicArea is designed for sharing firmware files. It allows users to upload and delete files.					
Can Delete Logs	If enabled, logs can be deleted by the user with the role of System Administrator, Group Administrator and Administrator.					

6.6.7 Wholesale Wizard

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

1. Open User >> Wholesale Wizard.

r / Wholesale Wizard				
0	-0			
Create user	Contraction of Contraction	1-00000	hereci	instant.
Streate user				
Username *	Carrie003			
Password*	=			
	medium			
Telephone	5972727			
Email	carriegidraytek.com			
Role	Group Administrator			
Enable Master Group Admin				
Enable Auto Logout	0			
Enable 008E feature				
DDBE pages to display	Read the Agreements, Set new password, Verify -			
Status	Active			
Mall Notification				
SMS Notification				
				140
				-

These parameters are explained as follows:

•				
ltem	Description			
Username	Enter a new name for a new user.			
Password	Enter a new password.			
Telephone	Enter the telephone number of such user for receiving the SMS notification.			
Email	Enter the email address of such user for receiving the mail notification.			
Role	Assign a Role for such user.			
Enable Master Group Admin	Switch the toggle to enable / disable the function of master group admin.			
Enable Auto Logout	Switch the toggle to enable / disable the function of auto logout.			
Enable OOBE feature	Switch the toggle to enable / disable the function of OOBE feature. OOBE pages to display - Select the pages to display on the screen.			
Status	Choose Active to make this user being seen on the network.			
Mail Notification	When this function is enabled, an e-mail will be sent to the user as a notification when the device gets alarms.			
SMS Notification	When this function is enabled, an SMS will be sent to the user as a notification when the device gets alarms.			
Description	Give a brief introduction of such user.			
Next	Go to next configuration page.			

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

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

These parameters are explained as follows:

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

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

r / Wholesale Wizard				
		3		
provide and	Course they pro-	Create network	Comments of	-menod
Step 3- Create network				
Select network:	Existing network. New network			
New network				
Parent Network	Root Network	ā.		
Network Name *	CARRIE003			
Username	cardtest			
Password		D.		
Location	HsinChu			
				Previous: Nest

These parameters are explained as follows:

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

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

	0	- 0
learner	Summary	(manual)
Soop 4- Summary		
ser		
Userbagon	Note:-	
Carrie003	Group Administrator	
Enable Master Group Admin	Enable Auto Logout	
Enable	Enable	
Status	Mail NotIllGallon	
Active	Disable	
SMS #Addication	reciptore.	
Disable	5972727	
Ermill	Enable OODE feature	
carrie@draytek.com	Enable	
008E pages to the pay Read the Agreements, Set new password, Verify email address, Notification settings, Default auto logout behavior, Two Factor Authentication, Website Theme	2	
lser Group		
Group Name	Global Milli Server	
	- 14 -	

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

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

6. Click Finish to save the settings.

6.6.8 SMS Server

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

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

ltem	Description
User Group	Specify a user group to apply the SMS server settings.
Enable SMS Server	Switch the toggle to enable /disable the SMS server.
SMS API	Use the drop down list to choose an ISP for sending SMS.
Connection URL	Enter the CPE's URL (WAN or LAN IP, e.g., 192.168.1.1).
User Name	Type the user name for authentication.
Password	Type the password for authentication.
From Telephone	Type the phone number of the sender.
Save	Save the current settings.

6.6.9 SNMP Server

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

User / SNMP S	Server		
User Group :	All User Group 🗸 🗸		
Enable SNM	P server	\bigcirc	
SNMP server	address		
Port		0	
Community			
SNMP versio	n	version1	~
SNMP API		SNMP_2_GLOBAL	~
Alarm Level		Critical	🔽 Major
		✓ Minor	🔽 Warning
		Normal	

ltem	Description
User Group	Specify a user group to apply the SNMP server settings.
Enable SNMP Server	Switch the toggle to enable /disable the SNMP server.
SNMP server address	Enter the IP address of SNMP server.
Port	Enter the port number of SNMP server.
Community	Set the name for getting community by typing a proper character. In general, it depends on the setting that SNMP service provider offers. The default setting is public.
SNMP version	Choose the version of the SNMP server that you apply to.
SNMP API	Choose SNMP API from the drop down list.
Alarm Level	There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS mail server sends e-mail to the recipient. Specify the severity level of the mail.
Save	Save the current settings.

6.6.10 Notifications & Events

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

6.6.10.1 Recipients

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

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

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

6.6.10.2 Severity Definition

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

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

Click Save to save the configuration.

6.6.11 Syslog Server

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

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

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

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

6.6.12 Group Parameter

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

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

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

6.6.13 Link with Router App

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

6.6.13.1 Settings

Configure the general settings related to VigorACS.

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

ltem	Description		
General Setup			
Enable Access from	Switch the toggle to enable/disable the function.		
Router App	To complete the router installation by connecting VigorACS using the Vigor router APP, this feature must be enabled.		
Authorized User	Only the users profiles(with Enabled API Service) listed here are allowed to connect VigorACS using the Vigor router APP.		
Profile Name	Display the name of VigorACS server.		
URL / Port	URL – Enter the URL representing VigorACS server. Port – Enter a port value. The default is 443 (for ACS server).		
QR Code	The QR Code is generated according to the profile name, URL and port value defined above.		
Onboard Information	·		
Enabled	Switch the toggle to enable/disable the function. The onboard information will be shown on the mobile APP if enabled.		
Onboard Information List	A table lists all onboard information.		
	when first logging in. Up to 8 entries can be added here. Question – Enter a name for a question which will be shown on the APP. Type – Options are Text and Dropdown. Default is Text. Regex Validation – The default value is empty if the Type is set as Text. Action – Click Delete to remove the selected entry.		
Steps before Provision			
Validate Site Configuration before Provisioning	Switch the toggle to enable/disable the function. Enabled – Write the parameters to the CPE device via the mobile phone. Disabled – The behavior of set parameter is the same as present.		
Site Configuration	Determine which site (AP, router, switch) settings will be configured in the installation process.		
	Required – If the entry is required for the router APP, switch the toggle to enable the entry of the site configuration.		

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

6.6.13.2 Status Checking Profile

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

Up to five profiles can be created.

User / Link w	ith Router App					C
User Group :	RootGroup ~					
Settings	Status Checking Profile	Monitoring HelpDe	k			
+ Add						Profile Number Limit: 0/5
Profile Name		$\downarrow \uparrow$ Comments	↓↑ Hardwa	are Installation Hint Images	Action	
			No data available	e		

Click +Add to create a new checking profile.

User / Link with Router App		C
User Group : RootGroup		
Settings Status Checking Profile Monitoring Help	Desk	
General Setup		
Profile Name		
Comments		
Hardware Installation Hint Images	Nothing selected v	
Parameter Group		
ාmport XML		
+ Add Parameter Group Max: 5 Groups		
	Cance	el Save

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

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

6.6.13.3 Monitoring

This page displays the information of CPEs monitored by VigorACS.

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

ltem	Description
Install Status	Information Submitted – It means VigorACS receives the install command. Installation Completed – It means VigorACS receives the logout API command.

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

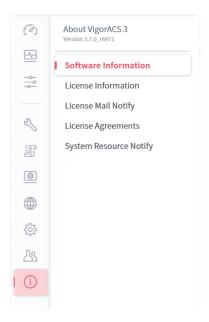
6.6.13.4 HelpDesk

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

User / Link with Router App User Group: RootGroup	С
Settings Status Checking Profile Monitoring HelpDesk	
Device Information	
MAC Address	
Configuration for Installation	
Site Type Nothing selected ~	
Location	
 B Note: Enter either address or the latitude and longitude coordinates with the following format.	
	Save

ltem	Description	
Device Information		
MAC Address	Enter the MAC address of the CPE device.	
Configuration for Inst	allation	
Site Type	Select one of the Status Checking Profiles.	
Location	Enter either address or the latitude and longitude coordinates of the CPE device with the following format: Latitude; Longitude (e.g., 24.868162980491277;121.006106339836)	
Save	Click to save the configuration.	

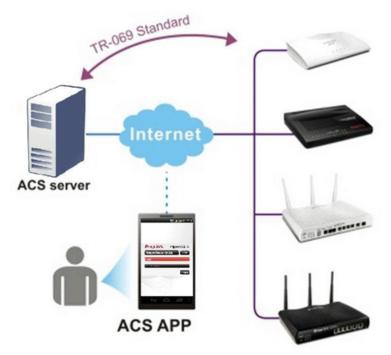
6.7 About VigorACS



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

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

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



6.7.1 Software Information

System Information	Release Notes	Others	
ACS Version	3.7.0dev_r56.00		
Java Version	17.0.11		
MariaDB Version	10.6.3		
InfluxDB Version	1.8.3		
Operation System	Linux.		

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

6.7.2 License Information

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

Host ID	AC\$3240600007			
License ID	00217cf0			
License Type	Trial			
	Start Date	Today	Expire Date	
License Period	0	0	0	
	202 5 06 06	2006.01.01	2024-02-04	
Licensed Node Usage	Used: 106 / Max: 100000			
Activate License	P Activate License			

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

6.7.3 License Mail Notify

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

6.7.3.1 Sync License Info Failed

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

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

Sync License Info Falled	License Expired License Capacity	
Enable		
	About failure to sync license info ACS will delete the license record on the system if ACS cannot get the license info for 3 times. At this time, you will need to login to MyVigor and activate the license manually.	
	Configure Mail Server You can enable this feature to receive a notification mail. Please go to User > Mail Server to configure the email server setting for All_USerGroup.	
Subject	ACS cannot get the license info from M	
Content	Normal : Sano Senti : B I U A G IE E - 46 IB ID 72 [Get Lucense Failed] ACS cannot get the lucence into from MyVgor ACS serviced the lucence. ACS removed the lucence. You can by spain to advise the lucence from <u>MyVgor</u> server.	
Recipients	+ Add Recipient 1/10	

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

6.7.3.2 License Expired

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

About / License Mail Notify		
Sync License Info Failed	License Expired License Capacity	
Enable		
	Configure Mail Server You can enable this feature to receive a notification mail. Please go to User > Mail Server to configure the email server setting for All_USerGroup.	
Subject	Service License Expires Soon	
Content	Normal : Sans Senif : B I U A A E = - % B A + T_e	
	ACS license is going to expire all [DATE]. Please contact your provider to renew the idense.	
Recipients	+ Add Recipient 1/10	
	Recipient	
	Invalid email format	

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

6.7.3.3 License Capacity

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

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

(3)	About / License Mail Notify		c
10 E	Sync License Info Failed Licen	Ilicense Capacity	
1 II II		Configure Mail Server You can enable this feature to receive a notification mail. Please go- to User - Mail Server to configure the email server setting for All_UserGroup.	
@ @	Subject	Service Node usage exceeds [PERCENT.	
125	Capacity (%)	80	
0	Content	Normal : Sans Sant : B I U A K I≣ ≡ 4 G G ↔ Ta TUSED_NODE_COUNT Nodes used, IAVAIL_NODE_COUNT Nodes available. Pinase contact your provider to entend this iconse	
	Recipients	+ Add Recipient 1/10	
		Racipient O Invalid email format	
			Save
	1		

ltem	Description
Enable	Switch the toggle to enable /disable the mail notification function. You can enable this feature to receive a notification mail. Please go to User >> Mail Server to configure the email server setting for all user groups.
Subject	Enter the subject of the mail.
Capacity	Specify the percentage of the current node. For example, the default is 80. That means if there are 2000 nodes in total, once 1600 nodes are used, VigorACS will notify the listed recipients.
Content	Enter the actual text for informing the recipient.
Recipients	Enter the e-mail address of the one to receive the mail.
+Add Recipient	Click to enter a new e-mail address.
Delete	Click to remove the selected e-mail address.
Save	Save the current settings.

6.7.4 License Agreements

En About / License Agreements e 63 Q Search Keyword Website Package Name 14 Author 1 Modified Source Codes License Type 14 4 & Link 🗹 Ant Apache License, Version 2.0 g Apache POI Apache License, Version 2.0 0 P Link 🖒 Axis Apache License, Version 2.0 (†) Castor Apache License, Version 2.0 DB of Link 🖒 Commons FileUpload Apache License, Version 2.0 10 P Link 🖄 Apache License, Version 2.0 Dashboard Google Inc. olamy of Link 🗹 EasySSL Apache License, Version 2.0 of Link 🖸 Jakarta common tool Apache License, Version 2.0 d? Link 🖸 JCasbin Apache License, Version 2.0 of Link 🖄 JDBC Adapter Apache License, Version 2.0 & Link 🗹 JSTUN Apache License, Version 2.0

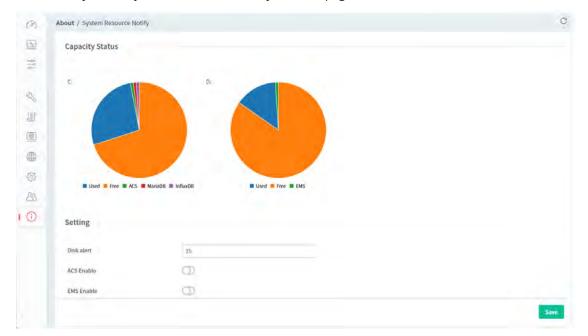
This page displays relational license information required by VigorACS 3.

6.7.5 System Resource Notify

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

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

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



These parameters are explained as follows.	These parameters are explained as follo	ws:
--	---	-----

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

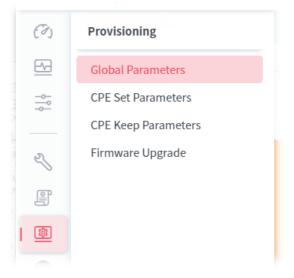
Capacity alert(%)	Set the upper limit percentage (by default, 1) of the disk space for the Influx database. If the hard disk reaches the threshold, VigorACS will send a notification mail to the recipients listed below.
MariaDB Enable	Switch the toggle to enable/disable the function of checking Maria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

Applications

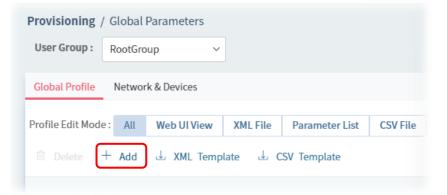
A.1 How to Create a Provision Profile with Global Parameters?

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

1. Open Provisioning>> Global Parameters.



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



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

visioning / Global Parameters	
er Group : RootGroup -	
Network & Devices	
Add a Profile	
Create Profile by	Creating a New Parameter List 🥪
Profile Name	
Always Keep	0
Reboot after Provisioning	0
R. Note: - After applying the parameter	ers, ACS will check the CPE responses and ask the CPE to reboot it readest.
Provisioning Time	Nwry Scheduled Schedule Profile
	Cancer Add
	Have TV/Inv

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

Profile Edit Mode : All Web UI View XML File	Parameter List								
+ Add the XML Template									
Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action			
888888	Parameter List		No	3	2018/11/28 04:43:07 PM	e? Edit	Delete	С Сору То	W View Log
angela test	Parameter List		No	1	2018/11/12 02:48:25 PM	Ø Edit	B Detete	🗅 сору То	@ View Log
tt	Parameter List		Yes	0	2018/11/08 02:38:05 PM	d Edit	IT Delete	C Copy To	E View Log
Global_parameter_Example_Parameter_List	Parameter List		No	0	2018/11/08 03:13:55 PM	/ Edit	E Delete	С Сору То	W View Log
66667	Parameter List		No	2	2019/05/31 08:47:36 AM	de Edit	Delete	С Сору То	D View Log
Marketing	Parameter List		Yes	0	2020/11/03 02:18:29 PM	2 Edit	B Delete	C Copy To	Wiew Log

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

1. Open Provisioning>> Global Parameters.

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

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

	oning / Global Parameters								c
Global	Vrofilie Network & Devices								
Violite 6	dif Mode: All Web UT View XML File Parameter List CSV File								
	1 Add d. XML Template d. CSV Template								
	Profile Name	Profile Edit Mode	Model	Always Keep	Revision	Last Modification At	Action		
Π	vigo/2860	Parameter List		Yes	19	2019/05/09 04:15:20 PM	8 Edit	CI Copy To	E View
0	Viger/71/0	Parameter List		No	15	2010/05/09 04:15:20 PM	/ Edt	Copy To	@ View I
'n	m	Parameter List		No	0	2019/05/09 02:39:36 PM	1 tan	Copy To	Q View)
	wgor28606	Parameter List		No	1	2019/05/09 04:12:05 PM	e 501	El Copy To	€ View L
0	123456789123456789122145678912345678912345678912345648978920939900000000000000000000000000000000	Parameter List		No	0	2020/02/27 11:20:32 AM	@ Edit	Copy To	€ View L
	Marketing	Parameter List		Yes	0	2024/08/05 11:31:46 AM	2 Ean	Copy To	- View-L

3. Click the Add link in this page.

Provisioning	🖹 Profile Name: Marketing	
		+ Add 🖉 Edit 🚨 Copy 🐵 Delete
		Parameter

4. Modify the Value, Keep, Order and Applied Model if you are not satisfied with the configuration above and want to make change. After finished the changes, click Save.

~	Parameter	Value	Keep Orde	er	Applied Model	Source Mode
			×	0	All models	~

() For the detailed information of parameters definition, refer to User's Guide of each device if required.

A.3 How to Create a Network for Managing Devices?

1. Open Network Management.



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

Network Management			
Search by Device ID/Name/Mode(/MAC/IP Address	C Setting Map		
Root Network(277) ALANWEN(3)	+Add New Network		
p 🚓 Alvaco(1)	General Settings		
p. AnPhat_VN(8)			
h 🚠 Angela(5)	Notwork D	Usernáme	
Artistest(0)	2	305	
E CARRIE(0)	Name	Password	
5 ARRIE003(0)	Roat Network		•
p 🚠 Cshih(2)	Location		
p 🚠 DraytekChina(0)	Koldingweg 19-1, Groningen, Nederland		
D			
p A GetterNetwork(1)			Save
1			
(🚠 Marketing_carrie(0)			
b 41 Novanet(0)			
• ATTARCHIN			

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

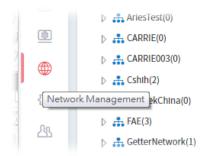
Parent Network	
Root Network	
Name	
Marketing_carrie	
Location	
HS	
User Name	
carrie	
Password	
	✓ Φ

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

Network Management	
Search by Device ID/Name/Model/MAC/IP Addre $~~\mathcal{Q}~~$	Setting Map
A Root Network(240)	+Add New Network
▷ ♣ 1111(0)	General Settings
 ALANWEN(3) Alvaco(0) 	Network ID 2
Marketing_carrie(0)	

A.4 How to Change the Network of a Device?

1. Open Network Management.



2. Choose and click a CPE displayed on Root Network tree view.

Network Management		
Search by Device ID/Name/Model/MAC/IP Address	C	Setting Map
 2865Lax 1449BC0C5920 2865ac_001DAA000000 		Delete This Device 4 Change Network
		General Settings
2865ac_001DAA41DF78		
2866ac_001DAA41DFC0		Status Disable Enable
2912n_001DAA8E14B0	- L	
2922n_001DAA8CAC84	- L	Device ID 141436
2925Ln_001DAADD75B0	_	
2925ac_001DAA512820	- L	Model Name Vigor2865ac
2926Vac_001DAA5DCAD0	1	
2927Lac_1449BC023720		Note 1
2927Lac_1449BC023740		
2927Lac_1449BC023768		Serial number
> 00000000000000000000000000000000000		

3. Click Change Network.

Network Management	
Search by Device ID/Name/Model/MAC/IP Address	C' Setting Map
2865Lax_1449BC0C5920	節Delete This Duvice 品 Change Network
2865ac_001DAA000000	
2865ac_001DAA41DF18	General Settings
2865ac_001DAA41DF78	General Settings
2866ac_001DAA41DFC0	Status Disable Enable
2912n_001DAA8E14B0	
2922n_001DAA8CAC84	Device ID
2925Ln_001DAADD75B0	141436
2925ac_001DAA512820	Model Name
2926Vac 001DAA5DCAD0	Vigor2865ac
2927Lac_1449BC023720	Note 1
2927Lac_1449BC023740	
2927Lac 1449BC023768	Serial number
> 2027 1440BC083030(1)	

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

Name		
2865ac_001DAA000000		
\dd to network		
	Q	
🔺 👬 Root Network		
🚑 ALANWEN		
🚓 Alvaco		
🚓 AnPhat_VN		
🚓 Angela		
👬 ArlesTest		
CARRIE		
Cshih		
👬 DraytekChina		
👬 FAE		
GetterNetwork		
👬 IK1		
击 Marketing_carrie		
🚓 Novanet		
A OCTOBER		
👬 RD1		
RD2		
RD3		
• ppr		
	× Cancel + Apply	

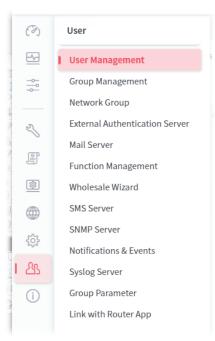
Sel	(100%)				nave b e is as follo		comp	leted.		
	\bigcirc	 Suc 	ceed: 1	•	Process	ing: 0	• W	alting: 0	Failed: 0	
GE	Device Name	¢↑	Model	$\downarrow\uparrow$	Retry	1 Pro	ogress	Status		$\downarrow\uparrow$
Sta	2865ac_001DAA0	000000	Vigor286	5ac	0	8	100%		offline. Settings will hen device is online	
Der 14					— Hide	Detail	s			
Мо					×C	lose				
	UI 28658C								2865	ac_ooi

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

arch by Device ID/Name/Model/MAC/IP Address	C Setting	Мар	
👬 Root Network(277)	🗊 Delete T	his Device 🚓 Change Network	
ALANWEN(3)			
Alvaco(1)	Genera	al Settings	
AnPhat_VN(8)	1		
Angela(5)	Status	Isable Enable	
ArlesTest(0)			
 A CARRIE(1) 	Device ID 141436		
2865ac_001DAA000000			
CARRIF003(0)	Model Na Vigor28		
Cshih(2)	Note 1		
DraytekChina(0)	Note 1		

A.5 How to Add a User?

1. Open User>>User Management.



2. Click +Add.

Jser / User Management							C
+Add 🥔 User B	atch Settings					Search_	9,
Showing I to 10 of 133 entries					Show 10 ~ entries **	3 X X X = 4	a m
Username	Authentication	Role	11 status	Email Notification	SMS Notification - Email		-44
E root	Internal	System Administrator	(10)	-	tim yangièd	raytek.com	

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

/ User Management		
dd User Profile		
nahle		
sarriame	CNIII ar-	
assword		
inte	Dperator	
nable Auto Logout		
nable OOBE feature 0		
OBE pages to display	Read the Agreements, Set new pass	
mail Notification		
mail	karrie@straytek.com	
MS Notification		
etephone		
excription		
		Cancel

4. Click Create.

Add	Ø User Batch Settings							Selech.	
howin	g 131 to 134 of 134 entries.						Show 10 v entries **	10 11 12	0.00
	Usemane	Authentication	Role	Status	Email Notification	SMS Notification	a mait		
D	T_2024-08-04_Wholesale_GA_E	Internal	Group Administrator	-	-	-	T 2024-08-04 Wholesak	GA_E@test.email	
Ð,	T_2024-09-04_Wholesale_GA_D	Internal.	Group Administrator	-	-	-	T_2024-08-04_Wholesale	GA_D@test.email	
0	T_2024-08-04_Wholesale_GA_OOBE	internal	Group Administrator	-	-	-	T_2024-08-04_Wholesak	_GA_OOBE@test.email	
b'	CNIII	Internal	Öperator	-	-	-	came@draytek.com		

A.6 How to Add a Group?

1. Open User>>Group Management.

(3)	User
	User Management
11	Group Management
	Network Group
D	External Authentication Server
1000	Mall Server
H.	Function Management
	Wholesale Wizard
	SMS Server
{ 0}	SNMP Server
7.61	Notifications & Events
As	Syslog Server
0	Group Parameter
	Link with Router App

2. Click +Add.

User / Grou	p Managemen	t		
Setting	Management	UI Customization		
+Add 🗊				
	Group ID 🛛 🗸	↑ Group Name ↓↑	Max Nodes ↓↑	Used Nodes
	4239	tttt7	200000	0
	4240	tttt8	200000	0

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

Management UI Cu	tomization	
dd Group		
Group name	yints.	
Nodes	-1	
	(-I: No Limit Nodes)	
Enable CPE Notify Mail/SMS/SNMP		
Enable Global Mail Server	-	
Enable Global SNMP Server		
Enable Expire Date	•	
Expire Date	2024/06/31	

- Group Name Enter a new name of the user group.
- Nodes Define number of node.
- Enable CPE Notify Mail/SMS/SNMP Server Switch the toggle to enable /disable global mail server.
- Enable Global Mail Server Switch the toggle to enable /disable global mail server.
- Enable Global SNMP Server Switch the toggle to enable /disable global SNMP server.
- Enable Expire Date Click to enable/disable the expire date.
- Expire Date Choose the expire date for such user group.
- 4. Click Save.

	5063	Router_App_Group		No Limit Nodes	2	Disabled		Disabled	Disabled	
	5395	AutoTest_Dev		No Limit Nodes	7	Disabled		Disabled	Disabled	
	6611	yfnts		No Limit Nodes	0	Enabled	2024/08/31	Disabled	Enabled	
Nodes In	Iformation									Ŧ
	iformation odes In Used	Configured Max Nodes	Purchased L	Icense Nodes						$\overline{\uparrow}$

This page is left blank.



Network Menu



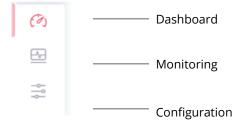
Chapter 7 Root Network Menu

Network contains two types, Root Network and User-defined Network (e.g., RD8). For the user-defined network group, refer to Chapter 5.

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

Root Network(267		
	Model	
읆 RU3(14)		
옲 RD5(9)		
옲 RD6(3)		
& R07(15)		
25 RD8(58)		
읊 RD8-1(1)		

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



7.1 Dashboard for the Root Network

= Dray Tek VigorACS 3 a 11:51:11 \sim Dashboard 10 CØ Auto Refresh: Disable Map Overview Network Overview 2 × × Su O, Network ¥ -0-0-0 + 100138 124 5 _ Root Netw 0 3 Go To Dat 187 1 est Des 1.40 Test SD.WAM AutoTest VPN 23 ot Web Porta ter_App_Network T_2024-08-04_Wholesale_GA_D 1 vices Device Name Device Type 192.168.143.10:80 2120n 001DAA7FF2A4 stun 192.168.105.144:80 2865Lac 1449BC3D7A08 Vieor2865Lad 192.168.106.143:80 2952Pn 001DAAF8D818 https Vigor2952Pn 192.168.106.143.80 2962P 1449BC39F110 https Vigor2962P

For more detailed information, refer to 3.2 Dashboard.

M

7.2 Monitoring

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

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

7.2.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

Ionit	oring / Alarr	17						2024/07/06 1	2024/08/05 · Sourch No	, / Device Nam	o/MAC O
Alam	0 H	story									
	11 Delet	All ADo	mloud						11 11 1	$f(x) = \sum_{i=1}^{n} (x_i - x_i)^{-1} (x$	4 Q
	No.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Type	Ack Time	Ack User
n.	38517749	Not Ack	2024/08/05 05:19:53	Q2121x_14490C506AA4	Root Network	14:49:BC:50;6A:A4	💩 Major	Device Loss Connection	Device Lost Connection		
Ū.	38517748	Not Ack	2024/08/05 05:19:53	P1282_1449BC43CD19	Root Network	14:49:BC-43:CD:19	🕹 Major	Device Loss Connection	Device-Lost Connection		
p	39517747	Not Ack	2024/08/05 05:19:53	P1280_001DAA4E6C33	Root Network	00:10:AA:4E:6C:33	A Major	Device Loss Connection	Device Lost Connection		
۵	38517746	Not Ack	2024/08/05 05:19:53	39125_14498C3072A0	Root Network	14:49:9C:30:72:A0	As Major	Device Loss Connection	Device Lost Connection		
1	38517745	Not Ack	2024/08/05 05:19:53	3910_1449BC6B9178	Root Network	14:49:0C:60:91:78	& Major	Device Loss Connection	Device Lost Connection		
d,	38517744	Not Ack	2024/08/05 05:19:53	3910_1449BC1CA218	Root Network	14:49:8C:1CA2:18	A Major	Device Loss Connection	Device Lost Connection		
ġ,	38517743	Not Ack	2024/08/05 05:19:53	2962 1449BC0D2040	Root Network	14:49:BC:00:20:40	A Major	Device Loss Connection	Device Lost Connection		
n	38517742	Not Ack	2024/08/05 05:19:53	2865ac_14498C1430A0	Root Network	14:49:9C:14:30:A0	& Major	Device Loss Connection	Device Lost Connection		
a	36517740	NotAck	2024/08/05 05:19:53	2665ac_001DAA4ACFB0	Root Network	00:10:AA:4A:CP:80	🔥 Major	Device Loss Connection	Device Lost Connection		
n	38517737	Not Ack	2024/08/05 05:19:53	2850V_001DAA709CCB	Root Network	00:10:AA-70:9C-09	🚲 Major	Device Loss Connection	Device Lost Connection		
ū	38517735	Not Ack	2024/08/05 05:19:51	2765Vac_14498C2C42E8	Real Network	14:49:BC:2C:42:E8	A Major	Device Loss Connection	Device Lost Connection		
1	38517733	Net Ack	2024/08/05 05:19:53	2762Vac_001DAA653308	Rept Network	00:10:AA:65:33:08	🙆 Majtar	Device Loss Connection	Device Lost Connection		
1	38517732	Not Ack	2024/08/05 05:19:57	21339ac_001DAA66E070	Root Network	00:10:AA:66:E0:20	A Major	Device Loss Connection	Device Lost Connection		

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

7.2.2 Logs

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

CPE Ac	tions De	vice Reboot Reboot By CPE Reset Sys	stem Password Set Pa	arameter File Transfer Se	etting Profile Device SysLog	CPE Notify Device Register Dev	rice Operate	
Delet	te 🗇 De	lete All 🚽 Download						
	ID	Device Name	Device ID	MAC Address	Device IP	Action	Action ID	Time
	4248	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2287	2020/03/09 09:53:57 AM
	4247	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2286	2020/03/09 09:53:55 AM
	4246	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2285	2020/03/09 09:53:41 AM
	4245	2927Lac_1449BC023720	154	1449BC023720	192.168.27.1	Set Parameter Values	2284	2020/03/09 09:53:39 AM
	4244	2865ac_001DAA000000	4339	001DAA000000	172.16.3.134	Inform		2020/03/09 09:41:04 AM
	4243	2926Vac_001DAA7033E0	129	001DAA7033E0	172.16.3.136	Inform		2020/03/09 09:39:49 AM
	4242	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Set Parameter Values	2283	2020/03/06 02:57:58 PM
	4241	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:57:43 PM
	4240	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:57:42 PM
	4239	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Set Parameter Values	2282	2020/03/06 02:47:23 PM
	4238	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:46:48 PM
	4237	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:46:48 PM
	4236	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:41:43 PM
	4235	G2280x_001DAA43AB4B	4342	001DAA43AB4B	192.168.1.159	Inform		2020/03/06 02:41:42 PM

ltem	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 and etc.) to display related log on this page.
search ID / Device Name / De Q	Enter the condition for VigorACS to search and display relational information.
Delete	Clear the alarm record which has been solved by VigorACS.
Delete All	Clear all of the alarm records which have been solved by VigorACS.
Download	Click this button to save the log as an XLS file.

7.2.3 Devices

The administrator (user) can check information (such as Device name, IP address, MAC address, model name, network, status, up time, firmware version, number of current connected client, data traffic, and so on) of CPE under the selected network group by this page. The network group (e.g., Root Network in this case) selected above is the group to be monitored and information related to this selected network group will be shown below.

Simply open Monitoring>>Devices to get the following page.

Monitoring / Devices									Auto	Refresh: Disable 🤒 🤇
Search Device-Naros / IP / N/	c	Model Vigor16	T, Vigor2120n+, V	/igor213: ~	Status	Alt		SSID All		v
								Rows 10	» н « <mark>н</mark>	710015 7 H @
A Download									General	Wireless
Device 21	IP Address	MAC Address	Model	Network	status	up Time 🖃	F/W Version	Last Inform Time -	Current Client	Current Traffic
7927Lax 14498C023768	197.168.106.140:80	14:49:BC:02:37:58	Vigor2927Lac	AutoTestNetwork	Online	0 days 08/28:50	44230	2024/08/05 11:46:45	0 (Local Wireless: 0)	638.74 KB (1 60.63 KB 4 578
2120n 0010AA7EE2A4 stuo	192.168,105.143.80	00:10:AA:7F:F2:A4	Vigor2120n+	AutoTest_Dev	Online	54 days 22:51:03	18.100	2024/08/05 11:55:05	0 (Local Wireless 0)	52,49 KB (1 36.13 KB 1 16.36
2465Lac 14495800007A08	192,168,106,144:80	14:49:BC:3D:7A:08	Vigor7865Lac	AutoTest_Dev	Office	0. days 00:00:00	4.4.5_STD 3	2024/07/11 16:42:09	0 (Local Winkless: 0)	0 Byte († 0 Byte 1 0 Byte)
7952Ph 0010AAEE08US hitros	192 168.106.143.80	00:10:AA:F8:08:18	Vigor2952Pn	AutoTest_Dev	Offine	0 days 10:00:00	3.9.7.2.	2023/09/25 10:41:51	0 (Local Wineless: 0)	0 Byte († 0 Byte 1 0 Byte)
2962P 1449BC39F110 bttps	192.168,106.143:80	14:49:BC:39:F1:10	Vigor2962P	AutoTest Dev	Online	59 days 22:20:48	4.3.2.6 🥥	2024/08/05 11:50:33	1 (Local Wineless: 0)	1.03 MB (7 111.50 KB L 038.
1720n 0030//4554/58	192.168.105.22.80	00:10:A35:47:58	Vigor3220n	AutoTest_Dev	Offine	0.days00:00:00	3.9.1.4 😒	2023/07/06 15:02:44	0 (Local Wireless: 0)	0 Byte (7 0 Byte 1 0 Byte)
AP NIO DDIDAA/C7850	197.168.106.150:80	00:10:AA:7C:28:50	VigorAP 810	AutoTest_Dev	Office	0 days 00:00:00	1.3.4 (2)	2023/09/12 06:03:00	0 (Local Wineless: 0)	
AP 902 001DAA3F150E sour	192.168,106.143:80	00:10:AA:37:15:0E	VigorAP 902	AutoTest_Dev	Dilline	0 dáys 00:00:00	1340	2024/04/16 02:53:44	0 (Local Wireless: 0)	2
AP 903 144900509405	192,168,106,151:80	14:49:BC:5D:8A:FC	VigorAP 903	AutoTest_Dev	Office	0. days 00:00:00	14.130	2024/06/02 11:22:46	0 (Local Wineless: 0)	
AP 960C 14496C477D85	192 168 105 52:80	14:49:80:42:70:85	VigorAP 960C	AutoTest Dev	Office	0 days U0-00:00	1.4.3_RC2.	2022/01/21 13:28:37	0 (Local Wireless: 0)	2

These parameters are	explained as follows	5:
----------------------	----------------------	----

ltem	Description
search Device Name / IP / MAC	Enter the condition for VigorACS to search and display relational information.
Model	This area lists all of the devices that monitored by VigorACS.
	Check Select all to display information for all of the devices; or check the name of the device to display the information related to the selected device.
Status	Online – This page displays information for the device which is online currently.
	Offline – This page displays information for the device which is offline currently.
	All – This page displays information for all of the devices no matter it is online or offline.
SSID	This area lists information for CPE with wireless features monitored by VigorACS.
	Check All to display all of the devices; or check the name of the device to display the information related to the selected device.
	SSID - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.
General / Wireless	General – List the general information for the CPE under the selected group.
	Wireless – List only the wireless information for the CPE under the selected group.

7.2.4 Cellular Data Usage

This page displays traffic information including data used, data cycle, status, percentage, downloaded data, uploaded data for device equipped with LTE features (such as Vigor2925Ln, Vigor2860Ln and so on). The values defined in Quota Settings indicate total amount of quota for all LTE devices managed by VigorACS.

Monitoring / Cellular	Data Usage							C
LTE Data Usage Over	rview			Quota Settings				
bita libed D Byte	Data Cycle 01/19 - 01/25	Statuse WARNING	ONG THE OWNER	Data Usage Alarm	0			
1 Brytte				Data Quota	0.	MB ~		
				Trigger Alarm When Usage Reached	0	% of Quota (0 Dyte)		
				Data Usage Cycle	Arealy-	Monthly Custom		
				Weekly Reset Day	Sunday		- 1	
0 Byte								
Device	Total	Download	Upload				Cancel	Save
FAF_Allen_2865las	0 Byte						cancer	Save
DrayTek	O Byte							
DrayTek	0 Byte-							
Drayfek	0 Byte							
DrayTe%	0 Byle							
TY2927	0 Byte-							
Allers 2865ar NEW	0 Byle							
Vigor2927Lot	0 Byte-							
DrayTek	0 Byte							
v29771.Vax	0 Byte							
DrayTek	O Byte-							
firayTek	0 Byte-							
DrayIek.	O Byte							
DrayTek	0 Byin-							
DrawTela	0 Byle-							

ltem	Description
LTE Data Usage Overview	Status - The bar chart displays the data usage in yellow, green and grey based on values defined in Quota Settings. If data usage for the LTE model exceeds the percentage of quota configured in the field of Trigger Alarm When Usage Reached in Quota Settings, the amount of used data will be shown in Yellow; if not, it will be displayed in Green. The rest quota will be shown in gray.
	In addition, device name, throughput, downloaded data and uploaded data for each LTE can be seen on the table below this page.
Quota Settings	
Data Usage Alarm	When it is enabled, a warning message will be shown in the page of DEVICE MENU>>Monitoring>>Alarm once the data usage reaches the threshold defined in Trigger Alarm When Usage Reached.
Data Quota	The value (unit is MB/GB) defined here means total amount of data quota available for all LTE devices managed by VigorACS.
Trigger Alarm When Usage Reached	Set a threshold for triggering alarm mechanism.
Data Usage Cycle	Select one of the options (Weekly, Monthly, Custom) as data usage cycle. Cycle Duration(days) – When Custom is selected, please specify the cycle

	duration. The data quota for LTE model will be reset after the days configured here.
	Cycle Starts On –When Custom is selected, specify one date as a starting point to reset the data quota for LTE model.
	Weekly Reset Day - When Weekly is selected as Data Usage Cycle, please use the drop down list to choose one day (Monday to Sunday) for VigorACS to reset the data quota for LTE model.
	Monthly Reset Day - When Monthly is selected as Data Usage Cycle, please use the drop down list to choose a date for VigorACS to reset the data quota for LTE model.
Cancel	Discard current modification.
Save	Save the current settings.

7.2.5 Floor Plan

This function is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength.

Tay Tek VigorACS 3	(Root Network (100143) 💛 🔍	Pcap 12:02:07 mk_carrie N 8/2/24 System Adventisitation
Monitoring / Floor Plan		
+ Add		58
Profile Name	↓ [↑] Devices	Action
20240605	r-	🥙 Edit. 💷 Delete
test	φ.	2 Edit 🗇 Delete

ltem	Description					
+Add	Creates a new profile.					
88	Click to change to browse view. It displays all of the floor plan profiles with the map used.					
	bedroom 0 jog 0 tte 0					
	You can click Add on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click Edit Map & Plan to perform the modification, or click Delete Map Profile to remove the selected floor plan profile.					

	marketing		
Profile Name	Displays the name of the floor plan profile.		
Device	Displays the number of AP devices placed on the plan profile.		
Action	Edit - Click to modify the profile. Delete - Click to remove the selected profile.		

To create a new profile:

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

Root Network 🗸 🗸		Dray Tek VigorACS 3
Monitoring / Floor Plan		
Profile Name	marketing_carrie	
Upload Map	Floor_MAP.png	Browse
		Cancel Continue

3. Click Edit to display the following figure.

oot Network 🗸 🗸	Dray Tek VigorACS 3	Capture Packets Y System Administrator
onitoring / Floor Plan		
Profile Name	marketing_carrie	
Edit Dimension		
		Cancel Sa

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

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

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

		Capture Packets System Admi	carrie nistrator
nitoring / Floor Plan			
Profile Name	marketing_carrie		
Edit Dimension Add Device	e		
ag and drop a virtual AP or an un-a	assigned AP to the floor plan.		
		Un-assigned APs	\odot
		Device Name	Model
		Device Name	VigorAP 8
		Device Name 810_001DAA7D6514 AP 1000C_001DAA04F084	VigorAP (VigorAP)
		Device Name	VigorAP 8 VigorAP 1 VigorAP 1
		Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04F084 ▲ AP 1000C_001DAA575D38	VigorAP 8 VigorAP 7 VigorAP 7 VigorAP 7
		Device Name ▲ 810_001DAA7D6514 ▲ AP 1000C_001DAA04P084 ▲ AP 1000C_001DAA575D38 ▲ AP 710_00507FF138F7	VigorAP (VigorAP VigorAP VigorAP VigorAP (
		Device Name & 810_001DAA706514 & AP 1000C_001DAA706514 & AP 1000C_001DAA575D38 & AP 710_00507FF138F7 & AP 800_001DAA2A5870	VigorAP 8 VigorAP 1

5. Select the AP you want from right side of this page. Drag and drop the icon on the map. Later, an icon with effective signal range will be seen on the screen.

itoring / Floor Plan ofile Name		
ofile Name	marketing_carrie	
Edit Dimension + Add Dev		
and drop a virtual AP or an u	gned AP to the floor plan.	
	Δ 810_001DAA/450314 Vigor	
4		
-	I ▲ AP 800_001DAA2A5B70 Vigor	AP 8
		AP 9
	▲ AP 903_00507FF19216 Vigori	AP 9

6. Slightly click the AP icon on the map. Two links of Link to an AP and Remove Device will be shown on the right side.

Root Network	Dray Tek	VigorACS 3	Carrie Capture Packets Y System Administrator	С
Monitoring / Floor Plan				
Profile Name	marketing_carrie			
Edit Dimension + Add Device				
			<pre></pre>	×

- Remove Device If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.
- Link to an AP If you satisfy the location of AP icon, click this link to select VigorAP. All of un-assigned AP names will be shown on the list. Choose the one you want and click Apply. Then such map has been connected with the specified AP.

7. Click Link to an AP to select the AP you want. After clicking Apply, the name of the VigorAP will be displayed below the icon on the map.



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

Monitoring / Floor Plan			
			B
+ Add			
Profile Name	↓ ↑	Devices	J↑ Action
bedroom		2	🖉 Edit 🖞 Delete
jpg		0	🖉 Edit 🛛 🗓 Delete
marketing_carrie		1	🖉 Edit 🛛 🛅 Delete

7.3 Configuration

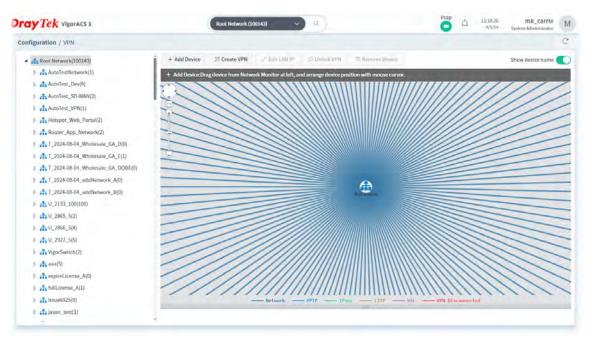
Configuration menu will vary for root network, group network and specified CPE.

(7)	Configuration	
<u></u>	VPN Wizard	~
	AP Profile	
- 1		

7.3.1 VPN Wizard

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

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



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

For detailed, refer to section 8.4.1.

7.3.2 AP Profile

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

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

AP Profile		
AP Profile Emoty	*	
Empty	*	
Emoty (As Parent)	*	
Emoty (As Parent) (As Parent)		
Empty (As Parent) (As Parent) (As Parent)	* * *	
Empty (As Parent) (As Parent) (As Parent) (As Parent)	* * * *	
Empty (As Parent) (As Parent) (As Parent)	* * *	

ltem	Description
+Add	Create a new AP profile with basic settings.
Profile Name	Display the name of AP profile.
Action	Edit - Configure detailed settings for the selected AP profile. Delete –Delete the selected AP profile. Duplicate – Click to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).
	Copy To – Click to open the following page. Then select a network (e.g., Marketing_carrie in this case) from the tree view of Root Network. After clicking the Copy To button, the configuration of selected AP profile will be applied to the selected network (e.g., Marketing_carrie).

	Common
	+ Change Network
	Still 2 Million
	1 m m m m m m m m m m m m m m m m m m m
	A foreit formus A solitorative A solit
Device Provisioning	Locate the access points for applying suitable AP profile. Name – Display a tree view for model managed by VigorACS.
	Model Name – Display the name of the model.
	Last Provisioned – Display the time that AP profile was applied to the selected device.
	Status – Display the status (updating, complete and "-") of the AP.
	AP Profile – Choose an AP profile for applying to the selected AP. In which, "As Parent" means to apply the profile listed on the top to the selected AP.
Refresh	Click to refresh current page.
Save	Click to save the changes in this page.

7.3.2.1 Add an AP Profile

Click +Add to create a new AP profile.

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

7.3.2.2 Edit an AP Profile

To configure detailed settings for each AP profile, click the Edit button for the selected profile. The setting page appears as follows:

figuration / AP Profile				
	Operation Mode:	Access Point Range Extende Mesh Node	r Mesh Root	
SSID Settings	2.4G General Setup			
Roaming.	2,40 General Setup		В	
Load Balance	2.4G Wireless LAN		D	
Loud balance	802.11 Mode	Mixed(IIb+IIg+11n)	14	
LAN	2.4G Channel	Channel_11,2462MHz		
Airtime Fairness				
	Channel Width	Auto_20/40_MHz	*	
Mobile Device Management	Extension Channel	Channel_7,2442MHz	~	
Application	Antenna	212R	*	
M Configuration	TX Power	100%		
System	MAC Clone			
Profile Setting	MAC Address			
	Band Steering			
	5G capability Check Time (sec.)	15		
	secondariant reaction united and	12		

These parameters are explained as follows:

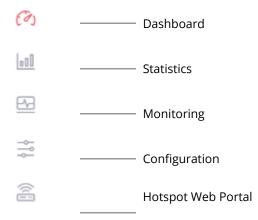
ltem	Description
Item Area A - Menu Item	 At present, the available menu items contain, General Setup SSID Settings Roaming Load Balance LAN Airtime Fairness
	 Mobile Device Management Application WMM Configuration System Profile Setting
Area B - Settings	This area will vary according to the item selected in Area A - Menu Item.

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

This page is left blank.

Chapter 8 Network Group Menu

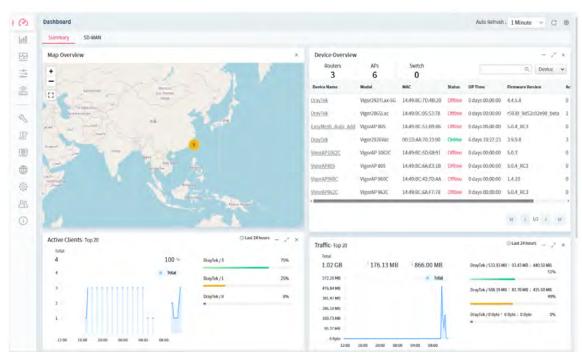
The menu items related to the network group:



8.1 Dashboard for the Network Group

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

U_2865_5 (2)		~ Q	
Root Network (100143)			×
Network Model			C ~
Root Network > U_2865_5			
器 U_2865_5 (2)	>	⊌ 2865Vac_1449BC34F660_109.1	
器 U_2866_5 (4)	>	⊌ 2865Vac_1449BC34F690_108.1	
器 U_2927_5 (5)	>		
器 VigorSwitch (2)	>		
器 aaa (5)	>		
器 expireLicense_A (0)	>		
希 fullLicense_A (1)	>		



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

8.2 Statistics for Network Group

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

Statistics						С
Last 24 Hours Last 7 Days Last	30 Days Custom Start: 2020/03/08	End: 2020/03/09				Export
Usage Overview (_)		- 2 ×	Wireless Clients Overview $\{j\}$			- 2 ×
Total Number of Clients	Wireless Clients Wir 1 (50%) 1 (ed Clients 50%)				
Total amount of Traffic 270.79 MB	Download Up 254.05 MB (93.8%) 16	.75 MB (6.2%)	Band	SSID		05
Max. Number of Concurrent Client 2	Avg. Number of Hourly C 1	lient 🛛	100.0% 2.4G 5 G	100.0%	Android IC	
Clients	OV	— ₂² ×	Traffic			- 2 ×
2	22:00 00:00 02:00 04:00 06:00	08:00 10:00 12:00 14:00	190,73 MB 143,05 MB 95,37 MB 47,68 MB 0 Byre 16:00 18:00 20	200 0000 0200 040	○ Wired ○ Wireles	An
Device Ranking (,)		≡Client • - 🗸 ×	Client Ranking (,)			Traffic • - 🗸 ×
J↑ Device	J↑ MAC	↓↑ Client ↓↑	ليث Host Name	.↓↑ MAC	4↑ Traffic	41
1 2865ac_001DAA000000	001 DAA000000	1	1 MKHL	406C8F525BFF	269.83 MB (99.6%)	
2 2926Vac_001DAA7033E0	001 DAA7033E0	1	2 AngelaCYsiPhone	DC0C5CEE583E	986.13 KB (0.4%)	

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

8.3 Monitoring for Network Group

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

(7)	Monitoring	
1 600	Alarm	80
I 🗠	Logs	
-~	Devices	W
	Clients	0 5
((()))	Cellular Data Usage	Do 58
	Floor Plan	
Z	Rogue AP Detection	
e	WAN (SD-WAN)	
-	VPN (SD-WAN)	
	VoIP (SD-WAN)	
	Data Usage (SD-WAN)	
ŝ		
쓰		
(j)		

In this case, we choose RD8 as an example.

8.3.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

5	Monite	oring / Alars	17						2024/97/06 02	2024/06/05 · Sound N	o. / Device Man	NO/MAE CI
il.	Marr	NO H	story									
3		10 Dete	e An J. Dov	beelme						8 K C	NA	8 C
19		No.	Ack Status	Time	Desice Name	Network Name	MAC Address	Alarm Level	Alarm Hessage	Alarm Type	Ack Time	Ack User
	n i	38617870	Not Ack	2024/08/05 05:33:10	AP 903_1449BC5D8AFC	AutoTest_Dev	14:49:BC:5D(8A3FC	🛆 Critical	Device Loss Connection	Device Lost Connection		
a.,	D.	38517763	Not Ack	2024/08/05 05:20:19	AP 960C_14490C427006	AutoTest_Dev	14:49:00:42:70:06		Device Loss Connection	Device Lost Connection		
	p	38517741	Not Ack	2024/08/05 05:19:53	AP 902_001DAA3F150E_stun	AutoTest_Dev	00-10-AA-3F-15-0E	A. Critical	Device Loss Connection	Device Lost Connection		
8	10	38517739	Not Ack	2024/08/05 05:19:53	AP 810_001DAA7C2B50	AutoTest_Dev	00:10:AA:70:28:50	Critical	Device Loss Connection	Device Lost Connection		
7		38517738	Not Ack	2024/08/05 05:19:53	3220n_001DAA554758	AutoTest_Dev	00-10-AA-55-47:58	Critical	Device Loss Consection	Device Lost Connection		
	2	38517736	Not Ack	2024/08/05 05:19:53	2952Fm_001DAAF8D818_https	AutoTest_Dev	00-10-AA-F8-D8-18		Device Loss Connection	Device Lost Connection		
þ.	P	38517734	NotAck	2024/08/05 05:19:53	2865Lac_14498C307A08	AutoTest_Dev	14:49:80:30;74:08	A Critical	Device Loss Connection	Device Lost Connection		
2												

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

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

8.3.2 Logs

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

Monit	oring / La	NES					2024/1	2/31 to 2025/01/20 ~	search (D./ Device Name / Device
ALC	É Áctions	Device Reboot	Reboot By CPE.	Reset System Password	Set Parameter File Transfer	Setting Profile Device Syslog	CPE Notify Device Registe	r Device Operate	Device Reject Add Object
Delete	Object								
	2D	Hete All	Dealn					10 K	A 74 5 8 3
	10	Device Name	Device ID	MAC Address	Current IP	Logged IP	Action	Action ID	Time
Ξ.	23690	DrayTek	279	14:49:80:05:53:78	192.168.26.14	192.168.26.14	Inform	-	2025/01/20 09:57:10
	23688	DrayTek.	279	1449;80.05;53:78	197.168.26.14	192 168 26 14	Indorm		2025/01/1717:27:02
Ξ	73687	шаулы.	279	14-49-80-05-53-78	192.168.26.14	192 168 26 14	17MOV TO-		2025/01/17 13:52:06
	23696	DrayTek	279	14:49:BC05:53:78	192.168.26.14	111.251.234.108	inform	-	2025/01/17 13:30:47
	23685	DrayTek.	279	14:49:8C05:53:78	192.168.26.14	111.251.226.17	Inform	-	2025/01/17 13:24:49
а.	23584	DrayTek	279	14:49:80:05:53:78	192.168.26.14	1.169.215.35	Inform	-	2015/01/17 13:21:42
	23683	DrayTek	153	00:10:44:70:33:90	1.169.208.116	1.169.208.116	Set Paramoter Values	6448	2025/01/17 10:59:53
Ξ	23682	DeayTek	151	00-10-AA-70:33-90	1.169.208.116	111.251.218.39	Inform	-	20125/01/17 10:57:27
	23681	DesyTek.	279	14-05-53-78	192.168.26.14	111.251.277.164	Inform	-	2025/01/16 18:50:06
	23677	DrayTek.	279	14:49:80:05:53:78	192.168.26.14	1.169.205.106	inform	~	2025/01/16 15:10:46
•	23676	DrayTek.	379	14:49:80:05:53:78	192.168.26.14	1.169.224.85	inform	-	2025/01/1614:06:40
a.	73675	DrayTek	775	14:49:80:05:51:78	192.168.26.14	111.251.225.220	Inform		7075/01/16 14:02:37
0	73674	DrayTek	779	14:49:80:05:53:78	192.168.26.14	111.251.227.8	Inform		7025/01/16 13:20-13
8	21672	DrayTek	279	14-49-80:05-53-78	197,168,26,14	1.169.200.74	Inform	-	2025/01/16 12:02:55

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

8.3.3 Devices

The administrator (user) can check information (such as Device name, IP address, MAC address, model name, network, status, up time, firmware version, number of current connected client, data traffic, and so on) of CPE under the selected network group by this page. The network group (e.g., Root Network in this case) selected above is the group to be monitored and information related to this selected network group will be shown below. This page shows all the devices (e.g., router, access points and switches) under the selected network group.

3	Monitoring / Devices										Auto Refresh: Disable 🔗	0
d	Search Drince Norme / IP / MA		Model Vigor2120	On+, Vigor2865La	c, Vigos -	Status	All	~	SSID AI		Y	
2										Rows 10 - 10	< 11 > 34	a
191	- Download									General	Wireless	
(6E)	Device in	IP Address	MAC Address	Nodel .:	Network	Status 1	Up Time	F/W Version	Last inform Time	Current Client	Current Traffic	
	J120m SOUDAATECIAL stom	192,168,106,143:80	00:10:AA:7F:F2.M	Vigor2120n+	AutoTest Dev	Dpline	55 days 00:41;41	3.8.10	2024/08/05 13:39:59	0 (Local Wineless: 0)	12.65 KB (7 9.84 KB 4 2.82 KB)	
	2865Lac 14498E3D7A08	197.168.106.144.80	L4:49:BC:3D:7A:08	Vigor286SLac	AutoTest_Dev	Offlow	0.days 00:00:00	4.4.5_STD @	2024/07/11 16:42:09	0 (Local Wireless: 0)	0 Byte (1 0 Byte 1 0 Dyte)	
8	2952Pn.001DAAFEDG18.https	192,168,106,143,80	00;10:AA:F8;08:18	Vigor2952Pm	AutoTest_Dev	Óffine	0.elays 00:00:00	3.9.7.2	2023/09/25 10:41:51	0 (Local Wireless: 0)	O Byte († O Byte J D Byte)	
	2962P 14498C39F110 https	192.168.106.143:80	14:49:BC:89:F1:10	Vigor2962P	AutoTest_Dev	Óniniz	60 days 00:11:16	4.3.3.6	2024/08/05 13:35:49	9. 0 (Local Wireless: 0)	1.03 ME (7 95.87 KE 1 937.20 M	(R)
0	3230n 001DAA554758	192.168.105.22:80	00:10:AA:55:47:58	Vigor3220n	AutoTest_Dev	Offline	0 days 00:00:00	3,9.7.4	2023/07/06 15:02:44	0 (Local Wireless: 0)	0.0yte († 0.0yte ± 0.0yte)	
Ð.	APAID DOIDAATC2B50	192.168,105,150;80	00:10:AA:7C:2B:50	VigorAP 810	AutoTest_Dev	Offline	0 days 00:00:00	1342	2023/09/12 06:03:00	0 (Local Wireless; 0)		
	AP 902 COTFIA 35 1505 MUR	192.168.106.143:80	00-10:AA-3F-15:0E	VigorAP 902	AutoTest_Dev	Offline	0 days 00:00:00	1.3.4 🖸	2024/04/16 02:53:44	0 (Local Wireless: 0)		
i)	AP-993 IMM99CSDBAFC	192.168.106.151:80	14:49:8C:5D:8A-FC	VigorAP 903	AutoTest_Dev	OWNINE	0 days 00:00:00	1.4.13	2024/06/02 11:22:46	0 (Local Wireless: 0)		
ß.	AP 960C 1449BC 427786	197.168.105.52:80	14:49-BC:42:7D:B5	VietorAP 960C	AutoTest_Dev	Offline	0 days 00:00:00	1.4.3 .RC2 @	2022/01/21 13:28:33	0 (Local Wireless: 0)	-	

ltem	Description
pearch Device Name / IP / MAC	Enter the condition for VigorACS to search and display relational information.
Model	This area lists all of the devices that monitored by VigorACS. Check Select all to display information for all of the devices; or check the
	name of the device to display the information related to the selected device.
Status	Online – This page displays information for the device which is online currently.
	Offline – This page displays information for the device which is offline currently.
	All – This page displays information for all of the devices no matter it is online or offline.
SSID	This area lists information for CPE with wireless features monitored by VigorACS.
	Check All to display all of the devices; or check the name of the device to display the information related to the selected device.
	SSID - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.
General / Wireless	General – List the general information for the CPE under the selected group.
	Wireless – List only the wireless information for the CPE under the selected group.
Download	Click this button to save information for monitored devices as a XLS file.

8.3.4 Clients

This page displays general information (such as hostname, MAC address, IP address, name of connected device, type, SSID, connection time, and etc.) for wireless / wired clients which connect to CPEs under the selected network group by this page. The network group (e.g., rd8 in this case) selected above is the group to be monitored and information related to this selected network group will be shown below.

	Dray Tek VigorACS 3	utoTest_Dev (9) 🗸 🔍			150:36 mk_carrie M 8/5/24 System Administrator
(3)	Monitoring / Clients				
<u>bid</u>	Last 24 Hours Last 7 Days Last 30 Days Custom Sore 2024-08-04	End: 2024-08-05			Create Report
		Alt	🐖 SSID: Ali	D#	
B) 414 (0	3		Ri	ows ~ iq <	// I H C @
		e Connected Device MA		ConnectionTime	-
B		39F110_hups 14:49:80:39:F1:10	WIRED	54d 12h 53m 26s 43.87N	IB(†23.77MB / 20.10MB)
ø					
(11)					

ltem	Description
Last 24 Hours / Last 7 Days / Last 30 Days / Custom	Display the clients detected within 24 hours, 7 days, 30 days or user defined days.
Search Hostname / MAC / IP	Enter the condition for VigorACS to search and display relational information.
Type	Check All to display information for all of the devices (including wired and wireless devices).
All WIRED	Wired – This page displays information for the device without wireless feature.
WIRELESS_2.4g WIRELESS_5g ↓↑ Connected Device MAC ↓↑	Wireless_2.4g – This page displays information for the device with 2.4GHz wireless feature.
	Wireless_5g – This page displays information for the devices with 5GHz wireless feature.
SSID	This area lists information for CPE with wireless features monitored by VigorACS.
	Check All to display all of the devices; or check the name of the device to display the information related to the selected device.
	SSID - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page.
Create Report	Click this button to save client's information as a "XLS" file.
	After clicking the button, the following page will appear.

Select the columns				
And a set of the set o				
Hompson-	S MAC Ad	dnex	E P Address	
Convected Deel in	Corned	2 d D Min	2 05	
Type	S5/0		ConvectionTime-	
Traffic				
Select devices				
Name	Modet Name	Firmware Version		
4 - Q (00,40)	and the second	Contraction Meridian		
410 1012AA7D6(18	VIJORAP #10	1.2.5		
© 902 001DA3D4716	VigorAP 903	12.14		
	vepcility			
	VigorLip	170003 5614		
C LIG 0715MA854204	Veprille	1720ED biesa		
0 130 001DAA8037A0	Vervillo	1		
C 2120m 0010A40FE030	vagor2120mm	1892		
@ 1130% 00100000000	Vigor2130W0	21541		
@ 2132FVm 001DAA844665		1,13,1,08/2,1		
O 3133Vic 001044660020		3.8.0 902		
C 2620L/L 001D4A926F58	Vigor2628/	3.8.10 PC1		
@ 2110n 00507F9A3648	Vij62v2710vi	1488		
28309_00507FT08028	VIDACIEN	3.8.6.2 59 745302		
💆 38307_001DAAA09418	Vigor28301	1.6.8.7 (0), 913		
C 2860n+_0010AA2112290	Vigor29628-	issism		
				> Cancel - Create

8.3.5 Cellular Data Usage

This page displays traffic information including data used, data cycle, status, percentage, downloaded data, uploaded data for device equipped with LTE features (e.g., Vigor2927Lac). The values defined in Quota Settings indicate total amount of quota for all LTE devices managed by VigorACS.

Monitoring / Cellu	ılar Data Usage						С			
LTE Data Usage C	Overview				Quota Settings					
Data Used 0 Byte	Data Cycle 2025-01-19 -	Status: WARNING		0% of 0MB	Data Usage Alarm	\bigcirc				
· ·	2025-01-25				Data Quota	0 MB ~				
1 Byte					Trigger Alarm When Usage	0 % of Quota (0 Byte)				
					Reached					
					Data Usage Cycle	Weekly Monthly Custom				
0 Byte					Weekly Reset Day	Sunday	~			
Device		Total	Download	Upload						
2136Lax_1449BC78	BE30	0 Byte	Download	opioad			Cancel Save			
2865Lax_1449BC00		0 Byte								
2865L_1449BC37E7	740	0 Byte								

ltem	Description	
LTE Data Usage Overview	Status - The bar chart displays the data usage in yellow, green and grey based on values defined in Quota Settings. If data usage for the LTE model exceeds the percentage of quota configured in the field of Trigger Alarm When Usage Reached in Quota Settings, the amount of used data will be shown in Yellow; if not, it will be displayed in Green. The rest quota will be shown in gray.	
	In addition, device name, throughput, downloaded data and uploaded data for each LTE can be seen on the table below this page.	
Quota Settings		
Data Usage Alarm	When it is enabled, a warning message will be shown in the page of DEVICE MENU>>Monitoring>>Alarm once the data usage reaches the	

	threshold defined in Trigger Alarm When Usage Reached.	
Data Quota	The value (unit is MB/GB) defined here means total amount of data quota available for all LTE devices managed by VigorACS.	
Trigger Alarm When Usage Reached	Set a threshold for triggering alarm mechanism.	
Alarm Severity Level	Set the alarm severity (critical, major, minor, warning and normal). Such severity will be shown on DEVICE MENU>>Monitoring>>Alarm when the data usage for LTE model(s) reaches the threshold.	
Data Usage Cycle	 Select one of the options (Weekly, Monthly, Custom) as data usage cycle. Cycle Duration(days) – When Custom is selected, please specify the cycle duration. The data quota for LTE model will be reset after the days configured here. Cycle Starts On –When Custom is selected, specify one date as a starting point to reset the data quota for LTE model. Weekly Reset Day - When Weekly is selected as Data Usage Cycle, please use the drop down list to choose one day (Monday to Sunday) for VigorACS to reset the data quota for LTE model. Monthly Reset Day - When Monthly is selected as Data Usage Cycle, please use the drop down list to choose a date for VigorACS to reset the data quota for LTE model. 	
Cancel	Discard current modification.	
Save	Save the current settings.	

8.3.6 Floor Plan

This function is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength.

Monitoring / Floor Plan		
+ Add		88
Profile Name	↓↑ Devices	J↑ Action
test	2	🖉 Edit 🛛 🖻 Delete

ltem	Description
+Add	Creates a new profile.
	Moinitoring / Floor Plan
	Profile Name tod., Carrie
	Upled Hap Room 34/0 pmg - Room 2
	Conol Contar
88	Click to change to browse view.
	It displays all of the floor plan profiles with the map used.

	Monitoring / Floor Plan				
	bedroom O	ire.	O lie	•	OAdd
				_	н с 1 /1
	You can click Add on existed profile, click t Then click Edit Map & Map Profile to remo	he icon on the r & Plan to perfor ve the selected Delete Edit M	right-top to dis rm the modific floor plan prot Map Profile ap & Plan	play a drop c ation, or clicl	lown menu.
Profile Name	Displays the name of	the floor plan p	orofile.		
Device	Displays the number	of AP devices p	laced on the p	lan profile.	
Action	Edit - Click to modify	the profile.			
	Delete - Click to rem	ove the selected	d profile.		

To create a new profile:

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

Dray Tek Vigoracs 3		U_2927_5 (5)	× (4)	Pcap.	۵	1357/26 8/5/24	mk_carrie System Administrator	М
Monitoring / Floor Plan								
Profile Name	test_Carrie		2					
Upload Map	Floor_MARpres	liteuro						
							Cancel Contin	64
-					-		Lancei	

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

Profile Name	test_Carrie	
Edit Dimension + Add D	vice	

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.

rofile Name	marketing_carrie	
Edit Dimension + Add De	lice	
g and drop a virtual AP or an u	Fassigned AP to the floor plan.	
		\bigcirc
		Model
		VigorAP 8
		VigorAP (VigorAP
		VigorAP (VigorAP) VigorAP)
		VigorAP (VigorAP) VigorAP) VigorAP)
	A 810_001DAA706514 A P 1000C_001DAA706514 A P 1000C_001DAA7057038 A AP 1000C_001DAA5057038 A AP 1000C_001DAA5057038	VigorAP (VigorAP) VigorAP) VigorAP (VigorAP)

5. Select the AP you want (e.g., VigorAP910C icon, in this case) from right side of this page. Drag and drop the icon on the map. Later, an icon with effective signal range will be seen on the screen.

ofile Name	marketing_carrie		
Edit Dimension + Add De	vice		
and drop a virtual AP or an u	in-assigned AP to the floor plan.		
		Un-assigned APs	٢
		Device Name	Model
		A 810_001DAA7D6514	VigorAP 81
		AP 1000C_001DAA04F084	VigorAP 10
		AP 1000C_001DAA575D38	VigorAP 10
		AP 710_00507FF138F7	VigorAP 7
		AP 800_001DAA2A5B70	VigorAP 80
			VigorAP 90
-		AP 903_00507FF17ECA	
		AP 903_00507FF17ECA AP 903_00507FF19216	VigorAP 90
			VigorAP 9 VigorAP 9

6. Slightly click the AP icon on the map. Two links of Link to an AP and Remove Device will be shown on the right side.

Monitoring / Floor Plan		
Profile Name	markeling_carrie	
Edit Dimension		
		×

- Remove Device If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.
- Link to an AP If you satisfy the location of AP icon, click this link to select VigorAP. All of un-assigned AP names will be shown on the list. Choose the one you want and click Apply. Then such map has been connected with the specified AP.

7. Click Link to an AP to select the AP you want. After clicking Apply, the name of the VigorAP will be displayed below the icon on the map.



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

Monitoring / Floor Plan			
			8
+ Add			
Profile Name	↓↑ Devices	↓↑ Action	
bedroom	2	🖉 Edit	🗊 Delete
jpg	0	🖉 Edit 🛛	🗊 Delete
marketing_carrie	1	🖉 Edit	🗊 Delete

8.3.7 Rouge AP Detection

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

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

Pray Tek VigorACS 3	AutoTest_Dev (9)	9 q	Pa	р Д 14:02:20 8/8/24	mk_carri System Administrate	te M
Monitoring / Rogue AP Detection						
Last 74 Hours Last 7 Days Last 30 Days Custom stan	2024-08-04 Viet 2024-08-05					
Scan Now Periodic Scan 🕥 👔	ally Wookly Start Time 1:	00 v				Save
Rogue AP Known AP						Jure
Delete All				11 × 1	11 7 8	e
ESSID SSID IT Band	channel 0 secur	rity Detector	signal	Last Detected		-se
	No	a datā available.				

ltem	Description
Last 24 Hours / Last 7 Days / Last 30 Days / Custom	Display the access point(s) detected within 24 hours, 7 days, 30 days or user defined days.
Scan Now	Perform device detection immediately.
Periodic Scan	After enabling this feature, access points will be detected periodically based on the setting configured here.
	Daily –VigorACS will detect access point on certain time every day.
	 Start Time – Specify a time point as starting time for device detection.
	Weekly – VigorACS will detect access point on certain time every week.
	• On – Choose the day to perform device detection.
	 Start Time - Specify a time point as starting time for device detection.
+Mark as Known	Vigor access points can be detected and be shown in the table under Rogue AP. However, some of them might be known to you and should not be listed here. To solve this problem, simply click the access point and then click Mark as Known. The selected access point will be transferred and listed under Known AP.
Delete	Remove the selected access point from the list.
Delete All	Remove all of the access points from the list.

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

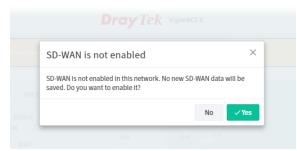
Scan Now	Periodic Scan 🌔	Daily Weekly	Start Time 10:00 v		Sav
Rogue AP K	_	bony meeny			
	lit 📋 Delete 🐵 Delete All				
	BSSID		Channel	Security	Comments
	00:1d:aa:00:00:02		Any	Any	
	22:33:11:22:33:33		Any	Any	
	00:1d:aa:04:f0:81		Any	Any	

ltem	Description							
Add	Click to create a new entry for entering information for access point.							
Edit	Change the settings for a selected access point.	Change the settings for a selected access point.						
	Select one of the access points. The Edit link will be available for clicking, then.After clicking it, channel, security and comments will be allowed to be modified with different values.							
	Scan Now Periodic Scan O Daily Weekly Start Time 10:00	•						
	Rogue AP Known AP + Add Edit Delete Delete All							
	BSSID Channel Security							
Delete	00:1d:aa:00:00:02 Any Any							
	□ 22:33:11:22:33:33 Any ▼ Any ▼ Any							
	00:1d:aa:04:f0:81 Any Disable WPA/PSK WPA/PSK WP/302.1x WPA/802.1x WPA/802.1x WPA/802.1x							
	Remove the selected access point from the list.							
Delete All	Remove all of the access points from the list.							
BSSID	Display the MAC address of the detected access point.							
Channel	Display the channel used by the access point. Check the box of the selected access point and click Edit.							
Security	Display the security mode used by the access point. It can be changed.							

Comments	Display a brief explanation for the access point. It can be changed.
Save	Save the settings.

8.3.8 WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN)

These pages (WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN)) are only available when SD-WAN feature for the selected network group has been enabled. If not, after accessing into these page, the following dialog will appear.



If you click Yes, the system will open the Network Management web page and pop-up the following dialog.

Use default settings
Bulk Data is not configured on this network. Do you want to apply the default settings?
No Yes

Click Yes to use the default settings.

When the SD-WAN is enabled, refer to 4.4 Monitoring for SD-WAN Network Group for detailed information of corresponding configuration pages.

Setting Map				
Add New Network 🐵 Delete This N	etwork 🛛 🚓 Change Network			
General Settings				
Network ID		U	sername	
254			fae	~
Name		P	assword	
FAE		~	•••	\$
Location				
Enable SD-WAN Bulk Data Settings et the category of data to be collected f hich the profile returns a bulk data to t Profile 21				category in the corresponding profile, and specify the report interval at Available / Disabled Bulk Data Categories
	Enable		Enable	
Report Interval (sec) 120	~	Report Interval (sec) 300	~	
220	Y	500	~	
Bulk Data Categories		Bulk Data Categortes		
Bulk Data Categories	Size: 8	Bulk Data Categories Users and Apps	Size: 4	
-	Stze: 8 Stze: 1	_	Size: 4	

8.4 Configuration Menu for Network Group,

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

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

8.4.1 VPN Wizard

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

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



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

8.4.2 AP Profile

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

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

rofile Namo	Action				
estDray054	🦉 East	8 Delete 13 Depticate 13 Copy To			
estDrayO55	P EdW	El Belete Gl Duplicais G Copy Th			
evice Provisioning					
Name		Model Name	Last Provisioned	Status	AP Profile
Allen Installs					Empty ~
A EasyMesh_Auto_Add		VigorAP BUS			(As Parent) 👻
A VigorAP1062C		VigorAP 1062C	1.1		(As Parent) 👻
A VigorAP805		VigorAP 805			(As Parent) 🕤
A VigorAP960C		VigorAP 960C			(As Parent) 🛁
A VigurAP962C		VigorAP 962C			(As Parent) ~
A		VigorAP 903			(As Parent) ~

ltem	Description			
+Add	Create a new AP profile with basic settings.			
Profile Name	Display the name of the AP profile.			
Action	Edit - Configure detailed settings for the selected AP profile.			
	Delete –Delete the selected AP profile.			
	Duplicate – Click to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).			
	Copy To – Click to open the following page. Then select a network (e.g., Marketing_carrie in this case) from the tree view of Root Network. After clicking the Copy To button, the configuration of selected AP profile will applied to the selected network (e.g., Marketing_carrie).			
	Root Network VigorACS 3 Carrie System Administrator			
	Root Network Dray Tek VigorACS 3 Capture Packets Carrie + Change Network ×			
	System Administrator			
	+ Change Network			

Device Provisioning	Locate the access points for applying suitable AP profile.
	Name – Display a tree view for model managed by VigorACS.
	Model Name – Display the name of the model.
	Last Provisioned – Display the time that AP profile was applied to the selected device.
	Status – Display the status (updating, complete and "-") of the AP.
	AP Profile – Choose an AP profile for applying to the selected AP. In which, "As Parent" means to apply the profile listed on the top to the selected AP.
Refresh	Click to refresh current page.
Save	Click to save the changes in this page.

8.4.2.1 Add an AP Profile

Click +Add to create a new AP profile.

dd a Profile			
Profile Type:	DrayOS # AP DrayOS 5 AP		
Profile Name:	AP_Carrie	2	
AP Login Username:	admin	2	
AP Login Password:		1	
* Back to profile list			s

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

8.4.2.2 Edit an AP Profile

To configure detailed settings for each AP profile, click the Edit button for the selected profile. The setting page appears as follows:

Content of Content	Overation Mode:	Access Point Range Extender Mesh Root Mesh Node	· · · · · · · · · · · · · · · · · · ·
SSID Setting:		MENT GOUR	
loaming	2.4G General Setup		
	2.4G Wireless LAN		
oad Balance		B	
AN	802.11 Mode	Mixed(l1b+l1g+l1n) ~	
	2.4G Channel	Channel_11,2462MHz ~	
Nirtime Fairness	Channel Width	Auto_20/40_MHz ~	
Mobile Device Management	Extension Channel	Channel 7,2442MHz ~	
Application			
	Antenna	2T2R 🗢	
WMM Configuration	TX Power	100% ~1	
System	MAC Clone		
Profile Setting	MAC Address		
4	Band Steering		
	56 capability Check Time (sec.)	15	

These parameters are explained as follows:

ltem	Description
Item Area A - Menu Item	Description At present, the available menu items contain, General Setup SSID Settings Roaming Load Balance LAN Airtime Fairness Mobile Device Management Application WMM Configuration System
Area B - Settings	 Profile Setting This area will vary according to the item selected in Area A - Menu Item.

If required, refer to User's Guide of VigorAP for the detailed information of settings definition.

8.4.3 Load Balance

While detecting the connection quality for the whole network group, the ACS server will consider the values of latency, loss, and jitter to get load balance for packets.

This page allows you to configure the weight for latency, jitter and packets loss.

onfiguration / Load Balance		
Load Balance Mode	1P filated Service Rated	
Line Speed	Auto Detect According To Line Speed	
Load Balance Weights	Custom 🗠 🖉	
Upload Bandwidth Weight	Long Herric	
Download Bandwidth Weight	Com HBM	
Low Latency Weight	Com - High-	
Low Jitter Weight	00m	
Less Packet Loss Weight	(see regs)	
自 Clear		Save and Apply to CPEs

ltem	Description
Load Balance Mode	IP Based - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.
	Session Based - All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed.
Line Speed	Auto Detect - Select to let the CPE reach the best load balance. It is the default setting.
	According to Line Speed - Select it if you know the practical bandwidth for your WAN interface.
Load Balance	There are four weight types for choosing to meet your request.
Weights	Bandwidth-Based - The load balance weight for each WAN will be executed according to line speed setting (DownLink/UpLink Rate).
	Quality-Based - The load balance weight for each WAN will be executed according to the transmission rate, latency time and the jitter time.
	Reliability-Based - The load balance weight for each WAN will be executed according to line speed and packet loss value. Usually, the WAN interface with low packet loss will have the higher ratio to be used.
	Custom - You can distribute the usage ratio for each WAN interface by setting weights for bandwidth, latency, jitter, and packet loss respectively.
	 Upload /Download Bandwidth Weight - The higher the weight is, the WAN interface with higher bandwidth will get higher usage.
	 Low Latency Weight - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower latency will get higher usage.
	• Low Jitter Weight - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage.
	 Less Packet Loss Weight - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection.

	The higher the weight is, the WAN interface with lower packet loss will get higher usage.
Clear	Click to return to factory default setting.
Save and Apply to CPE's	Click to save the settings and apply them to all the CPE devices under the selected network group.

8.4.4 Route Policy

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

edð	~				Dray Tek VigorACS 3	In Capture Packets -	synam Administration	c
Configuration / Route	Policy							C
+ Add New Rouse Policy								
App Service Profile	lin Use O	Remaining 32	Maximum 32	i)) Noder App service conflicts a	er zammty managed by WgarACS, amount profiles will be r	vrevved autometically.		
e – status	1 Commen	e		Source	Destination	mertas	Alles	
					AP) Altes available			

(i) It is available only when SD-WAN feature is enabled for current used network group. If not enabled, a notification will appear to ask for SD-WAN activation.

SD-WAN function is not enabled in this network.	
\bigcirc	

8.4.4.1 Creating a Route Policy with Basic Mode

1. Click +Add New Route Policy to create a new profile. In default, the settings based on Basic Mode will be shown as follows.

- Add a New Route Po	licy
Enable	
Comment	Marketing_Carrie
Source	Any 🗸 🗸
Destination	App Services 🗸 🗸
App Service Profile	Create a new profile From an existing profile
Selected App Service	FTP 🛞 DNS 🛞 Wikipedia 🛞
Send via Interface	WAN 1 ~
① Note If you want to send via Go to SD-WAN VPN Set	VPN (to the Hub), please dial VPN Hub and Spoke connection first. ings + Advanced Mode
	Cancel Save and set to CPEs

These parameters for Basic Mode are explained as follows:

ltem	Description
Enable	Click the icon to enable / disable the policy profile.
Comment	Enter a name of the route policy profile.
Source	Set the source IP addresses to which this rule is to be applied.
	Any - This rule applies to all source IP addresses.
	IP Range - This rule applies to the specified range of source IP addresses. If there is only one source IP address, enter the address in both the Start and End fields.
Destination	Set the destination IP addresses to which this rule is to be applied.
	Any - This rule applies to all destination IP addresses.
	IP Range - This rule applies to the specified range of destination IP addresses. If there is only one destination IP address, enter the address in both the Start and End fields.
	VoIP - This rule applies to VoIP packets.
	App Services - This rule applies to App services.
	 Create a new profile - Click this tab to create a new App Service Profile.
	Selected App Service - Specify required App services (e.g., CNN, FTP, DNS, SMTP/SMTP STARTTLS, Wikipedia).
	 From an existing profile - If an App service profile has been created previously, click this tab to choose an existing route policy profile.
	Selected an AP Service Profile - From the drop-down list, choose the one you want.
	Note that, when a route policy is set with App services, it will be applied to the router at the same time. Open Configuration>>Routing>>Load Balance / Policy Route. The routing rule with APP service will be highlighed and marked as "Managed By SD-WAN". It means the policy was created by ACS SD-WAN, and can be edited or deleted by ACS SD-WAN only.

	€ Lonigunation	c_001DAA00	0000 /	Configuratio	n / Routing				¢
	Static Route IPv4 Static Route IPv6 IBGP	CC and by SD WANN	Index 1 2 3	Enable Enable Enable Disable	Comment	Protocol Any Any Any	Interface WANE WANE WANE	Sic IP Range Any Any	Dest IP Any APP Service Any
Send via Interface	WAN#/LAN#/E The traffic will t							ce from	the list.
+Advanced Mode	Click to open th	ie con	fig	uratio	n page wit	th more c	options.		
Save and Set to CPEs	Save the above	confi	gur	ation	and set to	OCPE dev	ices.		

2. Click Save and set to CPEs.

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

3. A route policy has been set successfully.

fdð	~			Dray Tek	VigorACS 3	B+ Capture Fackets	Carrier System Administration	C
Configuration / Rout	te Policy							4
- Add New Route Policy	y							
App Service Profile	in Use O	Remaining 32	Maximum 32	Write Approximate profiles are commity exampled by	y Vigot ACS, annual y mblies will be commendant	and the p		
				Searca	Destination	intertace	Action	
e status	4: Comme	er.		and the second s		Principal Princi		

- 8.4.4.2 Creating a Route Policy with Advanced Mode
- 1. Click +Add New Route Policy to create a new profile. In default, the settings based on Basic Mode will be shown as follows.

Fnable		
Comment	Marketing_Carrie	
Source	Any	~
Destination	Any	~
Send via Interface	WAN 1	~
(i) Note		

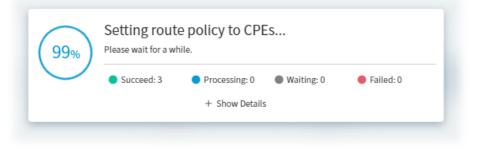
2. Click +Advanced Mode to get the following page.

Send via Gateway	Default Gatewa	ay Specific	Gateway	
Packet Forwarding to WAN/LAN	Force NAT	Force Routing		
via				
Failover	\bigcirc			
Failback	\bigcirc			
	— Bas	ic Mode		

ltem	Description
Send via Gateway	Default Gateway - Traffic will be sent to the default gateway address of the specified interface.
	Specific Gateway - Traffic will be sent to the specified gateway address instead of the default gateway address.
	• Specific Gateway - Enter an IP address.
Packet Forwarding to WAN/LAN	Force NAT - The source IP address will not be used to connect to the remote destination. Network Address Translation (NAT) will be used, where a common IP address will be used.
	Force Routing - The source IP address will be preserved when connecting to the remote destination.
Failover	Click the icon to enable / disable the failover function.

	Failover			
		Failover to	Default WAN 💊	when
		interface offline		_
	Failover to Gateway	Default Gatev	vay Specific Gateway	
	Failover to - If the interface be forwarded to an alternate route policy. Use the drop de failover interface.	e interface or l	pe scrutinized by an a	lternate
	Failover to Gateway - The f Default Gateway - Cli			gateway.
	 Specific Gateway - Cli 		• •	
	Failover to Specify Ga	ateway - Ente	r an IP address.	
	Failback - Click the icon to e	nable / disabl	e the failback function	
Basic Mode	Click to return to configurati	on page with	ess options.	
Save and set to CPEs	Save the above configuration	n and set to C	PE devices.	

4. Click Save and set to CPEs.



5. A route policy has been set successfully.

rdå	Y			DrayTek	VigorACS 3	Bie Capitore Fackets	carrie Signature Administration	С
Configuration / Rout	e Policy							Q
= Add New Route Policy				_				_
App Service Profile	In Use	Remaining 32	Maximum 32	© Hote Approximate profiles are commity exampled	by Vigotički, orozani preble, and he removed just	makany		
e - Status	4: Comme	et :		Sentre	Destination	intertace	Action	
1 Enabled	Marketi	ing Carrie		key	Any	WANT .	S Ide @ Deiete	

8.4.5 Link Health Check

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

ay Tek Vigor A	C5 3	U_2927_5 (5)	 <th></th><th>Co D</th><th>14:24:34 6/5/24 Syst</th><th>mk_carrie tem Administrator</th>		Co D	14:24:34 6/5/24 Syst	mk_carrie tem Administrator
Configuration / Link H	iealth Check						
NM F						Profi	le Number Limit: 1
a Profile Name	Detection Method	Primary Target	Secondary Target	Interval		Action	
1 Default	Ping Detect	8.8.8.8	8,8,4,4	10		Ad your	

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

dd		
Profile Name		
letection Mode	PingBister: HTTP Detect 🛷	
farget Type	IP Address	
Primary Target		
econdary Target (Optional)	(Pref formal (EFe: 123.12.1.1)	
nterval (sec)	0	
		Cancel

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

8.4.6 Interface Settings

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

8.4.6.1 Performance Probe

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

onfiguration / Interface Setti	ngs.				C
Performance Probe VolP WA	N				
Profile Name	Enable		Link Health Check		Action
PTOTRE Mame	Tuesday Compared	Profile	- Detection Method	Target	L'I
Wired WAN Performance	(2200)	Delault	Ping Detect	8.8.8.8, 8.8.4.4	@ Edn
Wireless WAN Performance	Distance	Default	Ping Detect.	8.8.8.8.8.8.4.4	2 Edit

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

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

Vired WAN Performance Probe				
nable Wired WAN Performance Prote				
Link Health Check Profile	Default (8.8.8.8, 8, 8, 4, 4)		*	
ink Health Check Detail	u ⁿ Edic			
	Detection Method :	Ping Detect		
	Primary :	8,8,8.B		
	Secondary :	8.8.4,4		
				Cancel

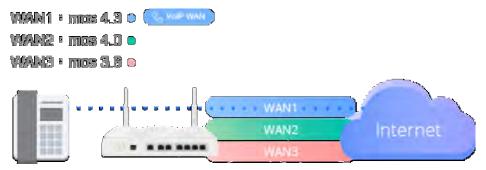
These parameters are explained as follows:

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

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

8.4.6.2 VoIP WAN

At present, the routers which support VoIP WAN (SD-WAN) are Vigor2927, Vigor2865 and Vigor2866.



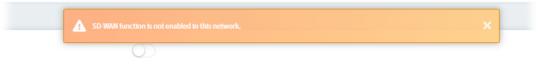
Digital phones can be connected to any router via Ethernet interface (no need to support VoIP function). With the VoIP WAN function, we can set a range. As long as the signal strength falls within this range, you can use digital phones to communicate with the remote end.

0	
35 >	
0.3 ~	
	Swe and Apply to Cl
	25 ×

These parameters are explained as follows:

ltem	Description
Enable VoIP WAN	Switch the toggle to enable or disable the VoIP WAN connection. If enabled, set a range for detecting the VoIP packets to pass through VigorACS server.
Change VoIP WAN when current WAN MOS score is less than	Specify a MOS number as the starting point. MOS, the abbreviation of "Mean opinion score", represents overall quality of a system. The rating for MOS is from 3.0(bad) to 4.0 (excellent).
And anther WAN is better by	Specify a MOS number as the ending point. The rating for MOS is from 0.1(bad) to 0.9 (excellent).
Clear	Click to return to factory default setting.
Save and Apply to CPEs	Click to save the settings and apply to all of the CPE devices managed by VigorACS server.

() It is available only when SD-WAN feature is enabled for current used network group. If not enabled, a notification will appear to ask for SD-WAN activation.



8.5 Hotspot Web Portal for SD-WAN Network Group

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

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

8.5.1 Profile

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

ray Tel	VigorACS 3			U_2927_5 (5)	~	Q			Pcap	Q 1	4:57:19 8/5/21	mk_c System Admini	
Hotspot Web	Portal / Profile												4
User Group :	RootGroup	÷											
Hadd												Profile Numb	er Limit: 5/2
1d 4°	Profile Name		- Enable	Hotspöt Server Mode	Login Method		-67	Applied interfaces	-07	Action			
z	105.169		(Citation)	ACS3 as Hotspot Server	Google			(AN (1) WLAN 2.4G (1) WLAI	4.5G (1)	<i>∅</i> ∈đit	TT Diviete	С сору	R View Lo
6	copy root_itest		Disting	ACS3 as Hotspot Server	Click Through			LAN (1,2) WLAN 2.4G (1,2) W	LAN 5G (1,2)	Ø Edit	C Detete	Ссору	4 View Lo
7	****		(Titation)	ACS3 as Hotspot Server	Click Through			LAN (1,2) WLAN 2.46 (1,2) W	LAN 5G (1,2)	2 Edit	T Desette	Copy	H View Lo
8			(Institut)	ACS3 as Hotspot Server	Click Through			LAN (1)		/ Edit	Tr Detete	ci còpy	G View Lo
18	d		(15140)	ACS3 as Hotspot Server	Click Through			LAN (I)		2 Edit	TO Delete	C CODY	@ Vew Lo

ltem	Description
+Add	Click to create a new hotspot web portal profile.
Index	Displays the index number of the profile.
Profile Name	Displays the name of the profile.
Enable	Displays if this profile is enabled or disabled.
Hotspot Sever Mode	 Displays the hotspot server mode. ACS3 as Hotspot Server The 3rd Party Hotspot Server
Login Method	Displays the login method used by this profile.
Applied Interfaces	Displays the interfaces specified by this profile.
Action	Edit – Click to configure settings for the selected profile. Delete – Click to delete the profile. Copy – The hotspot profile can be copied to another hotspot profile. Enter

·	ne and s	elect items to	be copied. The	п сиск Арр	ıy.
(Copy Pro	ofile				
New Pro Name	ofile	Please enter a	profile name		
Copy Ite	m	Configuratio			
copyrice		Configuratio	211		
		□ Locales			
/iew Log – Cli Hotspot Web Portal / Hotspot Pro		iew detailed in	nformation for	the selected	d profile.
Hotspot Web Portal / Hotspot Pro		iew detailed in	formation for	the selected	d profile.
Hotspot Web Portal / Hotspot Pro	file	iew detailed in	formation for	the selected	d profile.
Hotspot Web Portal / Hotspot Pro User Group : RootGroup	file	iew detailed in	nformation for	the selected	d profile.
Hotspot Web Portal / Hotspot Pro User Group: RootGroup A Back To Profile List	file	iew detailed in		the selected	d profile.
Hotspot Web Portal / Hotspot Pro User Group : RockGroup Back To Profile List Profile Information Profile ID Profile Name	9 9 NYF_Carrie	iew detailed in			d profile.
Hotspot Web Portal / Hotspot Pro User Group: RootGroup Back To Profile Liss Profile Information Profile Name Comments	file 9 9 NYF_Carrie (ACS) just for test			the selected	d profile.
Hotspot Web Portal / Hotspot Pro User Group : RootGroup Back To Profile List Profile Information Profile ID Profile Name	9 9 NYF_Carrie	pn	Satus Overview		d profile.
Hotspot Web Portal / Hotspot Pro User Group : RootGroup Back To Profile List Profile Information Profile Name Comments Login Method	9 NYF_Carrie (ACS) Just for test Various Hotspot Lo	pin (1) WLAN 5G (1)	Satus Overview	Status zameter intate	
Hotspot Web Portal / Hotspot Pro User Group: RootGroup A Back To Profile Inter Profile Information Profile ID Profile ID Profile Name Comments Login Method Applied Interfaces	9 N/P_Carrie (ACS) Just for test Various Hosport Lo. LAN (1) WLAN 2.4G	pin (1) WLAN 5G (1)	Status Overview	Status zameter intate	Compete Field
erspot Web Portal / Hotspot Pro erer Group : RoctGroup * Back To Profile List Profile Information Profile ID Profile Name Comments Login Method Applied Inserfaces	9 N/P_Carrie (ACS) Just for test Various Hosport Lo. LAN (1) WLAN 2.4G	pin (1) WLAN 5G (1)	Status Overview	Status zameter intate	Compete Field

To create a new hotspot web portal profile:

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

+ Create New Profile	2	
New Profile Name	NYF_Carrie	
		Cancel Create

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

otspot	Web Portal / Prolile								1
Iser Gro	up: RootGroup								
Ant								Profil	le Number Limit: 3
dex 47	Profile Name	Enable	Hotspot Server Mode	Login Method	Applied Intertaces	Action			
	NYF_Catrie	(Distant)	ACS3 as Hotspot Server	Click Through	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	े हता.	Di Deseto	D KOPY	S StewLog
	disadas	Ossilved	AC53 as Hotspot Server	Click Through	LAN (1)	al Edit	1) Delete	C CODY	N VIEW LOE
	NVF_tarma	Distant	ACS3 as Hotspot Server	Click Through	LAN (1)	el Edit	W Doleto-	Ci slopy	H ViewLog

4. Click Edit for modifying the detailed settings.

Hotspot Web Portal / Hotspot Profile User Group: RootGroup *	с
1 Profile S	etup Splash Page Customization Whitelies Setup (Optional)
Basic Settings	
Enable Profile	
Profile Name	NYF_Carrie
Comments	just for test
Hotspot Server Mode	ACS3 as Hotspot Server ACS3 as Hotspot Server ACS3 as Hotspot Server The 34P dark Hotspot Server
Applied Interfaces	
Subnet	S LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 LAN7 LAN8
WLAN 2.4G	SSID1 SSID2 SSID3 SSID4
WLAN 5G	SSID1 SSID2 SSID3 SSID4
External RADIUS Server	
External RADIUS Server	No External RADIUS Server 🖉 Edit
RADIUS MAC Authentication	\Box
RADIUS MAC Format	aa:bb:cc:ddiee:ff 🔹
RADIUS NAS-Idenfifier	
Portal Server	
Login Method	Click Through Facebook Google RADIUS Account Leave Info
Captive Portal URL	
	Example:https://Your/VigorACS Server/ACSServer/HotspotPortal/home
Redirection URL	Http:// • portal.draytek.com
HTTPS Redirection ()	
Captive Portal Detection	
Landing Page Method	Fixed URL *
Landing Page URL	http://draytolcforod.url
	β Note: Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.
Quate Policy	
Quota Profile	Default •
	Expired Time After 1 st Login Idle Timeout Bandwidth Limit
	0d 6h 0m Disabled Unlimited
	Cancel Continue

lt a ma	Description
ltem	Description
	Basic Settings
Enable Profile	Check to enable this profile.
Profile Name	Enter a name for hotspot profile.
Comments	Enter a brief description to identify this profile.
Hotspot Server Mode	 Specify the hotspot server. ACS3 as Hotspot Server - VigorACS server will be used as the server for authentication. The 3rd Party Hotspot Server - The third party server will be used as the server for authentication.
	Applied Interfaces
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN 2.4G/5G	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
	External RADIUS Server

External RADIUS Server	Displays the IP address of the external RADIUS Server. Edit - If required, Click to modify the RADIUS Server.		
	External RADIUS Server		
	Enable C		
	Primary Server		
	Server 172.16.3.88		
	Destination Port		
	Retry 2		
	Secondary Server		
	Server IPv4 format (EX : 123.12.1.1)		
	Destination Port		
	Secret		
	Cancel Confirm		
	Carrier Commit		
RADIUS MAC Authentication	If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server.		
RADIUS MAC Format	Select the MAC address format.		
RADIUS NAS-Identifier	Enter the server's ID.		
	Portal Server		
Login Method	There are several methods to be selected as for portal server.		
	Click Through -		
	• Facebook -		
	• Google -		
	RADIUS Account -		
	Leave Info -		
Captive Portal URL	Enter the captive portal URL.		
Redirection URL	Enter the URL to which the client will be redirected.		
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.		
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet.		
Landing Page	Specify the landing page for the client after passing the authentication.		
Method	• Fixed URL - Specify a landing page URL.		
	 User Request - The user will be redirected to the URL they initially requested. 		
	 Bulletin Message - Show a message on Bulletin. 		
Landing Page	It is available when Fixed URL is selected as Landing Page Method.		
URL	Specifies the webpage that will be displayed after the user has successfully authenticated.		

Cancel Continue	Click to Discard current modification. Click to get into next page.
Quota Profile	Choose a policy profile to apply to web portal clients. Refer to 8.5.2 Quota Management to define more profiles if required.
	Quota Policy
Google Secret	It is available when Google is selected as Landing Page Method. Enter the secret configured for the APP ID entered above.
Google ID	It is available when Google is selected as Landing Page Method. Enter a valid Google app ID.
Facebook Secret	It is available when Facebook is selected as Landing Page Method. Enter the secret configured for the APP ID entered above.
Facebook ID	lt is available when Facebook is selected as Landing Page Method. Enter a valid Facebook developer app ID.
HTML/Image for Bulletin Message	HTML/Image is available when Bulletin Message is selected as Landing Page Method. The message configured here will be briefly shown for a few seconds to the user.
	The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.

5. Choose Click Through as Login Method. Then, click Continue for Splash Page Customization. Splash Page Customization is available for ACS3 as Hotspot Server only.

	Profile Se	tup Splash Page Cust (Optiona	comization Whitelist Secup (Optional)
Layout	Components	Login Method	
Background Layout	Color Image		
Background 1 Color 🔗	#4a4972	5	Dray Tek
Background 2 Color 🔗	#FFFFF	C	
Login Method Background Color 🔗	#4a4972	C	Welcome! Please log in to enjoy Wi- Fi.
ogin Method Opacity 🔗	97		Connect
Browser Tab Title	Draytek Hotspot		
nable Browser Tab Icon	\bigcirc		
inable Logo			
Splash Page Logo 🔗	DrayTek Red Image Upload		
	Dray Tek		
			Cancel Previous Continue

ltem	Description
	Layout
Background Layout	Select either Color or Image as the login page background scheme.
Background 1 / 2	Select the background color of the login window (up and down layer) from

Color	the predefined color list, or er	nter the RGB value (with the format of HEX).	
Login Method Background Color	Select the background color of the login panel from the predefined color list, or enter the RGB value (with the format of HEX).		
Login Method Adjust the opacity (1-100) of Opacity		he login panel.	
Browser Tab Tit	le Enter the text to be shown as	the webpage title in the browser.	
Enable Browser Tab Icon	Click to enable / disable the b	rowser tab icon for VigorACS WUI.	
Browser Tab Ico	.,	age by using Browse and upload to VigorACS.	
Enable Logo	Click to enable / disable the lo	ogo display on the login window.	
Splash Page Log	-	age by using Browse and upload to VigorACS.	
Layout	Components Components Login Method	, () ()	
Splash Page Components Welcome Message <i>P</i> Terms & Conditions Text <i>P</i>	Velcome Message Terms & Conditions Marketing Language Option Velcomel Please log in to enjoy Wi-FL I have read and accept the Terms and Conditions.	Dray Tek # English (UK) Wekcome! Please log in to enjoy Wi- FL Connect	
Content 🖉	For information on the data Draytek collects and how it is used please see the Draytek Privacy Policy.		
Splash Page Components	login page.Welcome Message	I have read and accept the Terms and Conditions. Would like to receive emails about the latest events, products, and services from you. Reject Accept Bash page. Select the one(s) to show on the	
	Terms & ConditionsMarketing		

	Language Option			
Welcome Message	Enter the text to be displayed as the welcome message.			
Terms & Conditions Text	If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.			
	Enter the text which will be Conditions.	shown after the checkbox for Terms and		
Content	Connect / Submit button or	own on the second page after clicking the n the login page. ed in the Terms and Conditions window.		
Marketing Text	Connect / Submit button or	own on the second page after clicking the n the login page. shown after the checkbox for marketing		
Marketing Content	Connect / Submit button or	own on the second page after clicking the n the login page. ed in the Terms and Conditions window.		
Language	Use the drop down menu to Browse - Select a propertie Upload - Click to upload a l Download - Click to downlo	es file from your host. anguage file.		
	Login Method			
Connect Button Text &	Components Login Method	Connect Connect		
Connect	Connect Button Color - Se predefined color list, or usin HEX). Connect Button Text - Ent	nrough is selected as Landing Page Method. elect the color of the connect button from the ng the RGB value (entered with the format of eer the text to be displayed on the connect at can be set from the predefined color list or ed with the format of HEX).		
	Connect Button Color 🔗	linear-gradient(to right, #ef5568 0)		
	Connect Button Text 🔗	Connect		
	Enable Hint Message 🔗			
		Click to Get Internet Access		
Facebook		ok is selected as Landing Page Method.		

	Welcome! Please log in to enjoy Wi- Fi.
	f Log in with Facebook
	Facebook Login (Login with Facebook) - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
Google	It is available when Google is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi.
	G Sign in with Google
	Google Login (Sign in with Google) - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
RADIUS	It is available when RADIUS Account is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi. Username Password
	RADIUS Username - Enter the account name for passing the RADIUS authentication.
	RADIUS Password - Enter the password for passing the RADIUS authentication.
	RADIUS Login Button Color - Select the color of the login button from the predefined color list, or using the RGB value (entered with the format of HEX).
	RADIUS Login Button Text - Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).
Submit	It is available when Leave Info is selected as Landing Page Method.
	Welcome! Please log in to enjoy Wi- Fi. information carrie_ni@draytek.com Agree Submit

	+Add			Prot	file Number Limit:
	Leave Info Type	Text (Max: 170 characters)	F	Required	
		information			Ē
	Email 🔹	carrie_ni@draytek.com			Ē
	Checkbox 🗸	Agree			Û
	Submit Button Color 🔗	##3100	5		
	Submit Button Text 🔗	Submit	C		
	Enable Hint Message	\bigcirc			
	panel which will b Submit Button C	ld general informatic be shown on the logi Color - Select the colo list, or using the RGF	n panel as e or of the sub	ntry b omit bu	ox or che utton fror
	panel which will b Submit Button C predefined color l HEX).	be shown on the logi Color - Select the colo list, or using the RGE	n panel as e or of the sub value (ente	ntry bo omit bu ered wi	ox or che utton fror ith the foi
	panel which will b Submit Button C predefined color l HEX). Submit Button T The color of the te	be shown on the logi Color - Select the colo	n panel as e or of the sub value (ente o be display he predefin	ntry bo omit bu ered wi ved on	ox or che utton fror ith the for the subn
Enable Hint	panel which will b Submit Button C predefined color l HEX). Submit Button T The color of the te RGB value (entere	be shown on the logi Color - Select the colo list, or using the RGE Fext - Enter the text t ext can be set from t	n panel as e or of the sub value (ente o be display he predefin f HEX).	ntry bo omit bu ered wi ved on	ox or che utton fror ith the for the subn
Enable Hint Message	panel which will b Submit Button C predefined color b HEX). Submit Button T The color of the te RGB value (entered	be shown on the logi Color - Select the colo list, or using the RGE Text - Enter the text t ext can be set from t ed with the format o	n panel as e or of the sub value (ente o be display he predefin f HEX). age.	ntry bo omit bu ered wi ved on	ox or che utton fror ith the for the subn
	panel which will b Submit Button C predefined color l HEX). Submit Button T The color of the te RGB value (entered Click to enable / d If enabled, enter a	be shown on the logi Color - Select the colo list, or using the RGE Fext - Enter the text t ext can be set from t ed with the format o disable the hint mess	n panel as e or of the sub value (ente o be display he predefin f HEX). age.	ntry bo omit bu ered wi ved on	ox or che utton fror ith the for the subn
Message	 panel which will b Submit Button C predefined color b HEX). Submit Button T The color of the te RGB value (entered) Click to enable / do If enabled, enter a Click to Discard compared) 	be shown on the logi Color - Select the colo list, or using the RGE Text - Enter the text t ext can be set from t ed with the format or disable the hint mess a sentence as a hint	n panel as e or of the sub value (ente o be display he predefin f HEX). age.	ntry bo omit bu ered wi ved on	ox or che utton fror ith the for the subn

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

Group : RootGroup *				
	Profile Setup	2 Solarh Dage Customization	3 Minimalian Sanua	
	Prome Secup	Splash Page Customization (Optional)	Whitelist Setup (Optional)	
All NAT Rules Destina	ation Domain Destination IP Destin	nation Port Source IP Search .		+Add

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

				Profile Setup		Splash Page Customization (Optional)	3 Whitelist Setup (Optional)	
Type: All	NAT Rules Dest	ination Domain	Destination IP	Destination Port	Source IP	Search		+ Add 🛛 🗟 Clear All
Index	Туре			Enable		Content		Action
1	NAT Rules	•		\bigcirc			*	🗇 Delete
	Destination Domain Destination IP Destination Port							Cancel Previous Save

ltem	Description
+Add	Click to add a new whitelist profile.
Clear All	Click to remove all of the whitelist profiles.

Туре	Use the drop-down list to specify the type of the whitelist profile.		
	NAT Rules		
	Destination Domain		
	Destination IP		
	Destination Port		
	Source IP		
Enable	Click to enable / disable the whitelist profile.		
Content	Enter the value if required. It varies according to the type selected.		
Action	Delete - Click to remove the selected whitelist profile.		
Cancel	Click to Discard current modification.		
Previous	Click to return to the previous page.		
Save	Click to save the changes in this page.		

7. Click Save to finish and save the configuration.

RD8 V	Dray Te	ek VigorACS 3	Capture Packets 👻	Carrie System Administrator
tspot Web Portal / Hotspot Profile				
er Group : RootGroup				
-Add				
Profile ID: Profile Name 41 Enable	↓↑ Login Method	4 Applied Interfaces	↓↑ Action	
9 NYF_Carrie Enabled	Click Through	LAN (1) WLAN 2.4G (1) WLAN 5G (1)	🖉 Edit 📋 Delete	e 🗘 Copy 🗟 View Log

8.5.2 Quota Management

Quota management integrates bandwidth limit, session limit, applicable device number and validity period into one profile. This profile is prepared for a hotspot web portal profile.

-		VigorACS 3				•		3/5/24	System Administrator	10
lotspo	t Web P	ortal / Quota Management								0
User G	roup :	RootGroup								
†Add									Profile Number Limi	it:2
	index	↓ Profile Name	Expired Time After 1 st Login	Idle Timeout	Bandwidth Limit		-10	Session Lin	ut.	
	1	Default	0d 6h 0m	Disabled	Unlimited			Unlimited		
	2	IL_root	6d 6h 6m	(Disabled)	Unlimited			Unlimited		

ltem	Description
User Group	Specify a user group to display the quota management profiles under that group.
+Add	Create a new profile.
Delete	Click to delete the profile.
Index	Displays the index number of the profile.
Profile Name	Displays the name of the profile.

Expired Time After 1st Login	Displays the time remained for use after the first login.
Idle Timeout	Displays if the function is enabled or disabled.
Bandwidth Limit	Displays the number of bandwidth limit.
Session Limit	Displays the number of session limit.

The following setting page appears when +Add is clicked.

Hotspot Web Portal / Quota Manager	nent	С
User Group : RootGroup		
Add Quota Policy Profile		
Profile Name	0P_1 ~	
Account Validity		
Expired Time After 1 st Login	0 days 6 hours minutes	
Enable Idle Timeout		
Idle Timeout	0	
Device Control		
Devices Allowed	Unlimited v /account	
Enable Reconnection Restriction		
Restriction Type	Set Particular Time Set Time Period	
	$0 \rightarrow \text{hours} 0 \rightarrow \text{mins}$	
	Block the same user from reconnecting for the set period	
		Cancel Save

ltem	Description
	Add Quota Policy Profile
Profile Name	Enter a name for this profile.
Account Validity	
Expired Time After 1st Login	Enter the time (days, hours and minutes) remained for use after the first login.
Enable Idle Timeout	Click to enable the function of idle timeout.
	Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.
	Device Control
Devices Allowed	Enter a number (1-100) of devices applied with this profile.
	"Unlimited" means no number limitation.
Enable Reconnection	Click to block the same client reconnecting to Internet.
Restriction	Restriction Type - There are two types to set the time period.
	• Set Particular Time - The same user is unable to connect to Internet before the time setting.
	 Set Time Period - The same user is unable to connect to Internet

	before the time period.
	Bandwidth and Session Limit
Enable Bandwidth Limit	Click to enable the function of bandwidth limit. Download Limit - Enter a value to define the maximum data traffic (downloading) for each client connecting to Vigor device. Upload Limit - Enter a value to define the maximum data traffic (uploading) for each client connecting to Vigor device.
Enable Session Limit	Click to enable and set session limit. Session Limit - Enter a value to define the maximum sessions for each client connecting to Vigor device.
Cancel	Discard current modification.
Save	Save the current settings.

8.5.3 Network & Devices

Each network group and / or device can be assigned with different hotspot profile.

Dray Tek VigorACS 3	(U_2977_5(6)		0	C 15-01-57 mk_carrie N 5/5/20 System Administrator
Hotspot Web Portal / Network & Device				Stanch Dewize Name / Model / MAC
Name	Model Name	Hotspot Profile		
⊿ 👬 U_2927_5		As Parent	14 I	
@ 2927Vuc_14498C22C2C0_104.1	Vigor2927Vac	As Parent	<i></i>	
2927Vac_14498C22C400_103.1	Vigor2927Vac	As Parent	(Ae	
● 2927Vac_14490C22C438_101.1	Vigor2927Vac	As Parent	*	
2927Vac_14498C22C588_105.1	Vigor2927Vac	As Parent	34	
@ 2927Vac_1449862226630_102.1	Vigor2927Vac	As Parent	-	

ltem	Description
User Group	Specify a network group. Specify the hotspot profile(s) for the device under the selected network group.
Hotspot Profile	Select a hotspot profile for the selected group / device. As Parent - Use the same setting as the previous layer.
Save	Save the current settings.

8.5.4 PIN Generator

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

8.5.4.1PIN Generator

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

Dray Tek VigorACS 3	U_2927_5 (5)	v) a	Prap D	15-04-74 0/5/24	mk_carrie System Administrator	М
Hotspot Web Portal / PIN Generator						¢
User Group : RootGroup ~						
PIN Generator PIN Status						
+Generate new PIN					Profile Number Limit: 0	0/600
Show 10 - entries				Search		
and the second sec	Hotspot Profile/ Qu	ota Management	Quantity			
nd 4: Profile Name Create Time Hotspot P	roffle Quota	Expired Time after 1 th Login Generated	Used Unused	Action		
		No data available				
						н
Delete Expired Profiles automatizally						

These parameters are explained as follows:

ltem	Description
User Group	Specify a network group. Specify the hotspot profile(s) for the device under the selected network group.
+Generate new PIN	Click to generate a new PIN profile.
Delete Expired Profiles automatically	If enabled, the expired profile will be automatically removed at 12:00 AM every night. Switch the toggle to enable or disable this function.

Click Generate new PIN to create a new profile.

U_2927_5 (5)	v Q			
+ Generate new PIN				×
PIN Generator Profile				- Î
Profile Name			×	
PIN Digits	6	~		
Quantity	1	~		
PIN Validity	1 Day	~		
Bind PIN Code to Router	Nothing selected	~		4
Hotspot Profile	105.169	~		
Quota Management Policy	Default			
Expired Time after 1 st Login	0d 6h 0m			
Device(s) Allowed per PIN	Unlimited			
Speed Limit	Inlimited (Inload) Inlimited (Download)			
		Cancel	Apply	
				-

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

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

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

						c
						Profile Number Limit: 1/60
						Search
	Haispot Protice/ Quota			Quantity		Action
Hotspot Profile	l' Quota	Expired Time after 1 st Login	Generated	Used	Unused	10000
105.169	Detault	Did 6h 0m	1	0	T	🕾 Print Unused PIN 🐵 Deleb
		Hotspot Profile	Expired Time after 1 st Hotspot Profile Quota Login	Expired Time after 1 st . Hotspot Profile if Quota T Login Generated if	Expired Time after 1 st Hotspot Profile I st Quota Used Generated II Used	Expired Time after 1 st . Hotspot Profile if Quota T Login Generated II Used If Unused

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

8.5.4.2 PIN Status

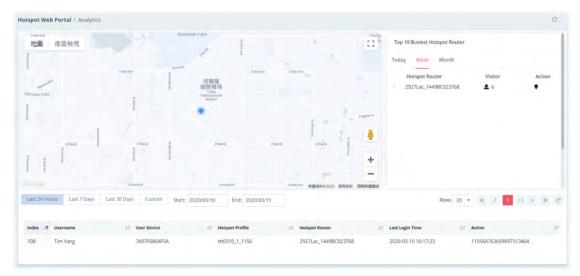
This page displays the PIN codes generated by PIN Generator.

er Group : RootGroup					
N Generator P/N-Statul					
Status	Alà Used Unused				
Generator Profile	Show All				
Hatspot Router	Search Device MAC or Device Name				
Client Device	Sourch Client MAC				
w 10 - entries					Search.,
ow 10 ~ entries PIN Codel Status - Generator Pr	offie Quota Profile	-† Create Time	PIN Expire Date	Hotspot Kouter	Search
ow 10 - entries PIN codel - Status - Generator Pr 458560 UNUSCO PIN_Carrie	ofile quota Profile Default	-1 create time 2024/08/19 09:27:48	РИК EXpire Date 2024/08/20 09:27:48	Hotspot Nouter 2927_1449BC13	Action

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

8.5.5 Analytics

This page displays the locations of the routers on the map, top 10 busiest hotspot routers and a list of clients accessing into the Internet via the hotspot web portal.



ltem	Description
Мар	Displays the location of the client.
Top 10 Busiest Hotspot Router	Displays the top 10 busiest routers. Today - Display the name of the router, number of clients and performed action at the present day. Week - Displays the name of the router, number of clients and performed action within one week. Month - Displays the name of the router, number of clients and performed action within one month.
Last 24 Hours, Last 7 Days, Last 30 Days, Custom	Choose the time period, last 24 hours, 7 days or 30 days. Or click Custom to specify a certain period, for displaying the router location.
Index	Displays the index number of the router.
Username	Displays the username of the client.
User Device	Displays the MAC address of the router.
Hotspot Profile	Displays the name of the hotspot profile used.
Hotspot Router	Displays the name of the router used by the client to access into Internet.
Last Login Time	Displays the last login time.

Applications

A.1 How to apply an AP profile to AP device(s)?

1. Choose a group containing with access points (e.g., "RD8" in this case) from Root Network.

RDS	~	Dray Te
Root Network(241)		a x
	Model	
₩ RD5(9)		AP 910C_001DAA7F5D8C
器 RD6(2)		AP 912C_001DAA72E14A
옮 RD7(15)		AP 918RPD_001DAA3F580C
		AP 920R_001DAA632C78
욺 RD999(3)		BX 2000ac_001DAAD7EC88
器 SEG1(1)		Español_2832n_001DAAE60E00
윯 Shanghai(15)		▲ G2500_001DAA4C194F

2. Open Configuration>>AP Profile.

(7)	Configuration / AP Profile				
000	Configuration				
<u></u>	VPN		Action		
	AP Profile		🖉 Edit 🔟 Delete	C Duplicate	🗇 Сору То
ŝţ	Load Balance (SD-WAN)				
	Route Policy (SD-WAN)				
	VOIP WAN (SD-WAN)				
Z					
	Device Provisioning				
\$	Name	Model Name	Last Provisioned	Status	AP Profile
	4 📥 RD8				•
	AP 1000C_001DAA04F06C				

In the Device Provisioning, all of the access points grouped under "RD8" are displayed under the field of Name.

3. Select the AP (e.g., AP 920R in this case) required to apply new AP profile; and use the drop down list of AP Profile to specify a profile (e.g., Marketing_carrie in this case).

Refresh Save

(i) You can click +Add New Profile to create a new AP profile if there is no AP profile to be chosen or the existed AP profile is not suitable for the AP model.

Click Save. The settings in web user interface of the selected VigorAP will be overwritten with the settings configured in AP profile immediately.



Device Menu



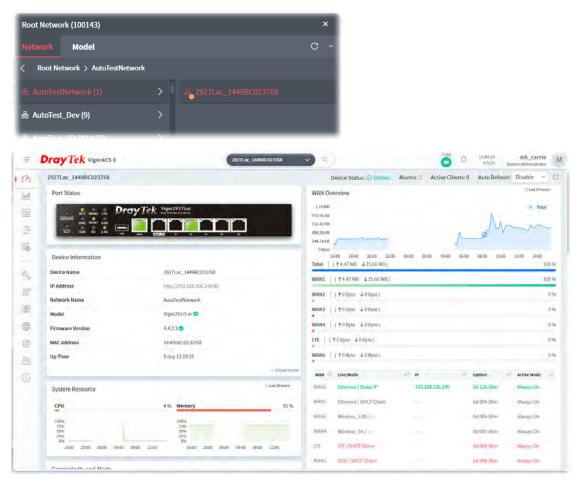
Chapter 9 Device Menu

On the dashboard for CPE, the Device menu contains:



9.1 Dashboard for CPE

Use the drop-down menu on the top of the left side to select a CPE (e.g., Vigor2927 series).



9.2 Statistics for CPE

Statistics is available for a selected group network or CPE.

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

Dray Tek VigorACS 3		2927Lac_1449BC023768	~	Q	Pcap	15:50:35 8/5/24	mk_carrie System Administrator	М
Statistics								С
Last 24 Hours Last 7 Days	Last 30 Days Custom Start: 2	024-06-23 End: 2024-08-05					Export	٨
Usage Overview		- 2	* × 1	Wireless Clients Overview			- 2	×
Total Number of Clients	Wireless Clients 0 (0%)	Wired Clients 1 (100%)						
Total amount of Traffic 130.17 MB	Download 124.87 MB (95.9%)	^{Upload} 5.30 MB (4.1%)		Band	SSID		05	
Max. Number of Concurrent Clier 1	nts Avg. Number 1	of Daily Client 🕢		2 .4G 5 G	No Data	Andro	oid 📕 iOS 📕 Windows	
Clients		- 2	* × .	Traffic			- 2	×
		OWired OWireless O2.4G O50	G	5.72 MB		⊖Wired ⊖V	Vireless () 2.4G () 5G	
2				4.77 MB				
				3.81 MB				
1		A A		2.86 MB				
				976.56 KB				
0				0 Byte				
07-01	07-08 07-16	07-24 08-01		07-01	07-08 07-16	07-24	08-01	

9.3 Monitoring

Monitoring menu offers options for monitoring the normal and abnormal actions for network, group and CPE. This section offers Monitoring menu items for a selected CPE (in this case, Vigor2135 series is used as an example).

(7)	Monitoring	
000	Alarm	
I 🗠	Logs	
¢°¢		
E.		

9.3.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

Ionito	oring / Alarr	n						2024/07/06	to 2074/08/05 -	Search N	o, / Device Nar	ne/MAC C
Alam	юн	story										
	li Delet	te All LDov	wiload						6	< 17	14 2	8 0
	NO.	Ack Status	Time	Device Name	Network Name	MAC Address	Alarm Level	Alarm Message	Alarm Type		Ack Time	Ack User
	38517757	Not Ack	2024/08/05 05:20:19	2135Vac_14498C038060	626	14;49;BC;03;B0;60	🖄 Major	Device Loss Connection	Device Lost	Connection		

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

Alarm Level	Displays the alarm message with the severity (e.g., Critical) specified.
Alarm Message	Displays a brief explanation for the alarm sent by VigorACS 3 automatically.
Alarm Type	Displays the alarm message with the type specified.

9.3.2 Logs

It provides records of action executed, name of the selected device, MAC address, Device IP, and Current Time for CPE device managed and monitored by VigorACS.

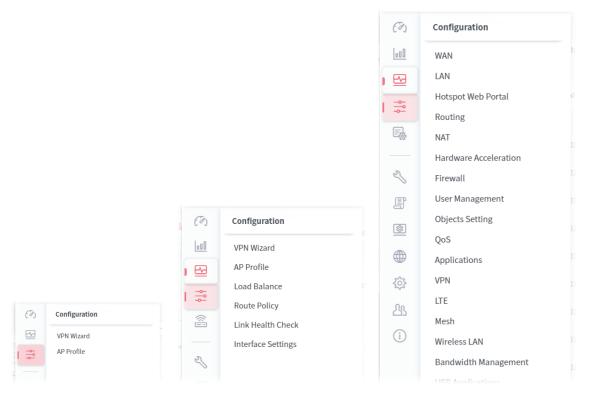
PE Actio	Device Re	eboot Reboot By CPE	Reset System Password	Set Parameter	File Transfer	Setting Profile	Device SysLog	CPE Notify	Device Register	Device Operate	
elete	Delete All	Download								KI < 1 /2	> N C @
	ID	Device Name	Device ID	MAC Address	De	rvice IP	Action		Action ID	Time	
	2968439	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Set Parame	ter Values	13923	2020/03/06 05:18:	11 PM
0	2968051	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Set Parame	ter Values	13788	2020/02/24 05:25:	40 PM
	2968049	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Set Parame	ter Values	13786	2020/02/24 02:42:	06 PM
0	2968041	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Set Parame	ter Values	13783	2020/02/24 02:37:	23 PM
	2968040	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		42	2020/02/24 02:37:	21 PM
	2968039	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		41	2020/02/24 02:37:	20 PM
	2968038	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		40	2020/02/24 02:37:	19 PM
	2968037	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		39	2020/02/24 02:37:	18 PM
	2968035	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		38	2020/02/24 02:37:	16 PM
	2968033	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		37	2020/02/24 02:37:	15 PM
	2968031	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		36	2020/02/24 02:37:	13 PM
	2968029	2865ac_001DAA41DF78	141326	001DAA41DF	78 19	2.168.105.67	Add Object		35	2020/02/24 02:37:	12 PM

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

9.4 Configuration

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

Available configuration settings will vary for root network, group network and specified CPE.



Root Network

Group Network

CPE

The menu items for a selected CPE device, generally, are the same as the settings on web user interface of the selected device (CPE, AP and etc.).

It is not necessary for the administrator to access into the web user interface of the selected CPE to make setting changes. If required, the administrator can modify the settings for the selected device through the options displayed under Configuration. The modifications will be applied to the selected device immediately.

How to select a CPE? On the left-top side of the home page of VigorACS 3, click the Network tab and find out the CPE you want. Then, click the CPE. A dashboard of the selected CPE will be shown on the screen.

The menu items under Configuration will vary based on the CPE selected.



The menu items for Configuration will vary based on the selected CPE (AP / router).

(7)	Configuration	
000	WAN	b
<u></u>	LAN	
	Hotspot Web Portal	d
Ű¢	Routing	
E.	NAT	
	Hardware Acceleration	
Z	Firewall	
F	User Management	
\$	Objects Setting	
<u>e</u>	QoS	
	Applications	
<u> </u>	VPN	
23	LTE	
	Mesh	
(j)	Wireless LAN	
	Bandwidth Management	

(i) If the administrator wants to access into the web user interface of the selected CPE, click the IP address link of the selected CPE on the CPE dashboard.

9.4.1 WAN

WAN settings relate to access Internet for CPEs. For more detailed information, please refer to the user guide for the CPE.

Connection Aum Index Databas Databas Databas Status Status Status Status Prigrations Pring Attams Pring Atta Pring Attams Pring Att	Multi VI AN ER WAN IZVE D WAN IIVE D WAN IIvites D DREP Climit Option IIVA ER DREP Climit Option IIVA ER	sable WAI sable WAI sable WAI sable WAI sable UTI	41 42 43 44 46 Cannection	Ethernet Ezhernet Wireless 2:4G Wireless 5G	Static or Dynamic IP Scatsc or Dynamic IP None:	Enable Disable	9/7 0/0	8.8 ms. Dims	2.9 ms	
WAN FAGE Disable WAN 2 Schermet Scape or Dynamic IP Disable 0/0 Dms 0ms 0ms<	WAA HAVE D WAA Havings D BHCDP Client Option 11V4 G DHCDP Client Option 11V4 G	sable WAI sable WAI sable WAI sable UTL	42 43 44 46 Connection	Ezhernet Wireless 2.4G Wireless 5G	Static or Dynamic IP None	Disable	ā).ā	Dims.		
WARTPG: Dicable Wortgss 2,45 None Disable 0/0 Oms O	WAALENG	sable WA sable WA sable 171	13 14 4G Connection	Wireless 2.4G Wireless 5G	None				0 ma	0%e
WMM Rudget Disable Warde Werdensis 56 None Disable 0/0 Dms Dms Oms	WAN Bladges DHCP Client Option IIV4 E DHCP Client Option IIV4 E DHCP Client Option IIV6 E	table WAI	44 46 Connection	Wirthless 5G		Disable	0/0			
Dicade WANA Weight Clear Option IVAL Dicade UTI 46 Connectory USB 36/46 USB Maxim (DicDP mode) Coald (O) Dime 0 ms 0 ms 0 ms Dicade UTI 46 Connectory USB 36/46 USB Maxim (DicDP mode) Coald (O) Dime 0 ms 0 ms 0 ms Dicade Dicade Balance Setup Moder IP Based ~ Weight Type Bandedth-Based ~	DHCP Client Option IN4 G	uble 111	46 Connection		Noos		070	0 ms	0 ms	0%
BACP Clent Option IPvE Enable WANG USB 36/46 USB Modern(DHCP moder) Enable 0/0 Enable 0/0 Enable 0/0 Load Balance Setup Moder IP Based ~ Line Speed Auto Detect ~ Weight Type Bandwrith-Based ~	DHCP Client Option IPv6				The second s	Disable		0 mis	0 ms	
Load Balance Setup Mode IP Based ~ Line Speed Auto Detect ~ Weight Type Bandwitth Based ~	annar sanan sajaon in re	nable WAI		USB		Enable		Il ens.		
Mode IP Based ~ Line Speed Auto Detect ~ Weight Type Bandwidth>Based ~			NG.	USB	35/4G USE Modem(DHCP mode)	Enable	0/0	ti ens:	Duns	Dile
Moder IP Based ~ Line Speed Auto Detect ~ Weight Type Bandwitth-Based ~										
Line Speed Auto Detect ~ Weight Type Bandweitti-Based ~		Load Bala	nce Setup							
Weight Type Bandwittl-Based ~		Mode		IP E	Based					
@ Note:		Line Speed		Aut	to Detect ~					
		Weight Type		Bar	ndwidth-Based ~					
		@ Note-								
			alency, jitler, and pad	el-foto require o	etting Link Condition Detection in each	WAN INTERING	page			
										00 1
						_				-

9.4.1.1 Internet Access

Item	Description			
Table	Alarm - Display if the alarm function is enabled or disabled.			
	Index - Displays the index number of the WAN interface.			
	Display Name - Displays the description for the WAN interface.			
	Physical Mode - Display the physical mode (e.g., Wireless 2.4G / Wireless 5G) of the interface.			
	Access Mode - Displays the access mode for the WAN interface.			
	Status - Displays if the WAN interface is enabled or disabled.			
	Bandwidth(Kbps)DownLink/UpLink - Displays the downlink / uplink bandwidth ratio.			
	Ping Latency / Ping Jitter / Ping Pkt Loss - Displays the latency / jitter / packet loss value.			
Load Balance Setup	Mode - The default is IP Based. Choose Session Based to get better transmission speed.			
	Line Speed - Choose Auto Weight to let the router reach the best load balance. According to Line Speed to let the router reach the best load balance based on line speed.			
	Weight Type - Choose Bandwidth-Based / Quality-Based / Reliability-Based as the weight type. Or choose Custom to define Upload Weight, Download Weight, Latency Weight, Jitter Weight, Pkt Loss Weight respectively.			
	 Upload / Download Weight- The higher the weight is, the WAN interface with higher bandwidth will get higher usage. 			
	 Latency Weight - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The 			

	higher the weight is, the WAN interface with lower latency will get higher usage.
	 Jitter Weight - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage.
	 Pkt Loss Weight - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower packet loss will get higher usage.
Save	Save the current settings.

To modify the general setup settings for each WAN, move the mouse cursor on the WAN# under Index and click to open the following page.

General Setup		
Alarm	Show an alarm message when this WAN interface disconnects. Alarm option will follow WAN Alarm Setting in Network management. If you change Alarm option on Configuration > WAN, you need to set WAN Alarm again for all enabled WAN interfaces on this CPE.	
inable	0	
isplay Name		
hysical Mode	Ethernet	
nable Load Balance	0	
active Mode	Always On Fallover	
Physical Type(Ethernet)	Auto negotiation ~	
ustomer VLAN Tag Insertion	\bigcirc	
ervice VLAN Tag Insertion	D	
ternet Access		
access Mode	None PPPoE Static or Dynamic IP PPTP/L2TP	
MTU		
PPPoE MTU	1492	
		Cancel Sa

ltem	Description
	General Setup
Alarm	Click to show/hide an alarm message.
Enable	Click to enable/disable settings of the WAN interface.
Display Name	Enter the description for the interface.
Physical Mode	Display the physical mode (e.g., DSL) of the interface.
DSL Mode (DSL model only)	Specify the physical mode (Auto, VDSL or ADSL) for the router manually.
DSL Modem Code (DSL model only)	Choose the correct DSL modem code for ensuring the network connection. If you have no idea about the selection, simply choose Default or contact the dealer for assistance.
Enable Load Balance	Click to enable auto load balance function for this WAN interface.

Active Mode	Always On - Make the WAN connection being activated always. Failover - Make the WAN connection as a backup connection.		
Failover	It is available when Failover is selected as Active Mode. Backup WAN - When the active WAN failed, such WAN will be activated as the main network connection.		
	Active When - It is available when Failover is selected as Active Mode.		
	• Any - The backup WAN will be activated when any master WAN interface disconnects.		
	• All - The backup WAN will be activated only when all master WAN interfaces disconnect.		
	Backup Type - Choose Fails to connect or Meet Any/all of the following condition. When Meet Any/all of the following condition is selected:		
	 Meet of the following conditions - If the packet meets any one of the conditions, the failover WAN will be enabled; if the packet meets All of the conditions, the failover WAN will be enabled. 		
	 Upload traffic / Download traffic - Set the values for upload and download respectively. 		
	• Latency - After selecting Check Latency, enter a value as a threshold.		
	• Jitter - After selecting Check Jitter, enter a value as a threshold.		
	 Packet loss After selecting Check Packet loss, enter a value as a threshold. 		
	When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.		
VLAN Tag Insertion /	Click to enable the function of VLAN with tag.		
Customer VLAN Tag Insertion / VDSL2	Tag Value –Enter the value as the VLAN ID number. The range is form 0 to 4095.		
VLAN Tag Insertion / VDSL2 Service VLAN Tag Insertion	Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.		
	Interne Access		
Access Mode	Set the access mode for this WAN.		
	None - No mode used.		
	PPPoE - Click to select PPPoE as the accessing protocol of the Internet.		
	• PPPoE MTU - Set a number as the Max Transmit Unit for packet.		
	Static or Dynamic IP - Click to select a static IP or use dynamic IP as the accessing protocol of the Internet.		
	• Static IP MTU - Set a number as the Max Transmit Unit for packet.		
	Modem Settings (for ADSL only)		
Multi-PVC channel	The selections displayed here are determined by the setting page of Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be chosen.		
VPI/VCI	Enter the value provided by ISP.		
Encapsulating Type	Choose the type provided by ISP.		
Protocol	Choose the one (PPPoE or PPPoA) provided by ISP.		
Modulation Type	Default setting is Multimode.		
	Choose the one that fits the requirement of your router.		

	PPPoE (available when PPPoE is selected as the Protocol		
For Wired LAN / For Wireless LAN	For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.		
	For Wireless LAN – It is available for n model. If you check this box, PCs or the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.		
PPP Service Name / PPP User Name / PPP Password	Enter the service name, username and password provided by ISP.		
Schedule Setup(1-15)	Enter four sets of time schedule for your request.		
PPP Authentication	Select PAP only or PAP or CHAP for PPP.		
Fixed IP Enable	Click Yes to enable the fixed IP setting.		
	Or, click No to disable the fixed IP setting.		
Fixed IP Address	Enter a fixed IP address in the box.		
	MTU		
Static IP MTU	It means Max Transmit Unit for packet. The default is 1500.		
Path MTU Discovery	Click to enable the path MTU discovery function for this WAN interface.		
	Path MTU Discovery		
Path MTU to	Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox.		
MTU size start from	Determine the starting point value of the packet.		
MTU reduce size by	Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached.		
	TTL		
Change the TTL value	Enable/disable the function of changing the TTL value.		
	Keep WAN Connection		
Enable PING to keep alive	Some ISPs will drop connections if there is no traffic within certain periods of time.		
	Switch the toggle to enable/disable this function.		
PING to the IP	If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.		
PING Interval	Enter the interval for the system to execute the PING operation.		
	RIP Protocol		
Enable RIP	Click to enable the RIP function.		
	Bridge Mode		
Enable Bridge Mode	Enable - Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded.		
	 Enable Firewall - If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. 		
Enable Full Bridge	Click to make the router work as a bridge modem which is able to		

Mode	forward incoming packets with VLAN tags.		
Bridge Subnet	Make a bridge between the selected LAN subnet and such WAN interface.		
	WAN IP Network Settings		
Connection Type	Static or Dynamic IP (available when Static or Dynamic IP is selected as the Connection Mode)		
	DHCP - Click to obtain the IP address automatically.		
	 Router Name - Enter the router name provided by ISP. 		
	 Domain Name - Enter the domain name that you have assigned. 		
	 DHCP Client Identifier - Click to enable and specify username and password as the DHCP client identifier for some ISP. 		
	Static - Click to specify some data.		
	 IP Address - Enter the private IP address. 		
	 Subnet Mask - Enter the subnet mask. 		
	 Gateway IP Address – Enter gateway IP address. 		
Primary DNS Server / Secondary DNS Server	Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future.		
	WAN IP Alias (Multi-NAT)		
Index	Display the index number of the WAN IP alias.		
Enable	Click to enable the selected WAN IP alias.		
Aux. WAN IP	Display the IP address of the WAN IP alias.		
Cancel	Discard current modification.		
Save	Save the current settings.		

9.4.1.2 Connection Detection

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

Internet Access	2927Lac_1449B	C023768 / Configuration / WAN		C @
domedion behiltons	Index	Physical Mode	Access Mode	
Mills-VLAN	WANI	Ethernet	Static or Dynamic IP	
WAN DVG	WAN2	Etherniet	Static or Dynamic IIV	
WAN Badget	WANE	Wurdess 2.4G	None	
WAN Eladget	WAN-6	Wireless 5G	None	
DHCP Client Option IPv4	UTE	USB	3G/4G USB Modern(DIVCP mode)	
OHCP Client Option IPv6	WANKS.	USB	3G/4G USB Modern(DHCP mode)	

ltem	Description
Index	Displays the index number of the WAN interface.
Physical Mode	Displays the physical connection for WAN interfaces according to the real network connection.

Access Mode

Displays the accessing mode of the Internet.

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

2927Lac_1449BC023768 / Configuration / W	/AN	C
WAN Connection Detection		
Index	1	
Mode	ARP Detect ~	
Link Condition Detection		
Mode	Ping Detect ~	
Primary Ping IP	8.8.8.8	
Secondary Ping IP	8.8.4.4	
Ping Interval	10	
		Cancel Save

ltem	Description				
	WAN Connection Detection				
Index	Displays the index number of the WAN interface.				
Mode	Choose PPP Detect or Ping Detect or Always for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.				
	 Primary / Secondary Ping IP - Enter the Primary or Secondary IP address in this field for pinging. 				
	 Ping Gateway IP - Use the WAN gateway IP address for pinging. Vigor router can check if the WAN connection is on or off. 				
	• TTL - Set TTL value of PING operation.				
	• Ping Interval - Enter the interval for the system to execute the PING operation.				
	• Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.				
	Link Condition Detection				
Mode	In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface.				
	Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option.				
Primary Ping IP	Enter an IP address.				
Secondary Ping IP	Enter an IP address.				
Ping Interval	Set a time interval (unit: second) for the system to ping the IP address specified above.				
Cancel	Discard current modification.				
Save	Save the current settings.				

9.4.1.3 Multi-VLAN

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

All VAN 7 Disable Lithermet(WANLI) Nome Disable N IP-A B. WAX 8 Disable Ethermet(WANLI) Nome Disable N IP-A 9. WINK 9 Disable Lithermet(WANLI) Nome Disable N Rindget 10 Disable Ethermet(WANLI) Nome Disable CP/Dent Option IP-4 11 Disable Ethermet(WANLI) Nome Disable	nnection Detection. INFVIAN			and type	45164 148	Cold named ministr	
N Pvic. B WAI # Disable Ethernet(WAI1) None Disable 9 WAI 9 Disable Libernet(WAI1) None Disable 10 Disable Ethernet(WAI1) None Disable CP Cleard Option Pvic 11 Disable Ethernet(WAI1) None Disable CP Cleard Option Pvic 13 Disable Ethernet(WAI1) None Disable 13 Disable Ethernet(WAI1) None Disable 14 Disable Ethernet(WAI1) None Disable 15 Disable Ethernet(WAI1) None Disable 26 Disable Ethernet(WAI1) None Disable		7 WAN 7					
NPAC. 9 WM49 Diable Libernet(WAN1) Nome Diable NRidegit 10 Diable Ethernet(WAN1) Nome Diable CPCDext Option IP46 11 Diable Ethernet(WAN1) Nome Diable CPCDext Option IP46 12 Diable Ethernet(WAN1) Nome Diable 13 Diable Ethernet(WAN1) Nome Diable 14 Diable Ethernet(WAN1) Nome Diable 15 Diable Ethernet(WAN1) Nome Diable 26 Diable Ethernet(WAN1) Nome Diable 15 Diable Ethernet(WAN1) Nome Diable 26 Diable Ethernet(WAN1) Nome Diable 26 Diable Ethernet(WAN1) Nome Diable				Ethernet(WAN1)	None	Disable	
NEWdget 10 Disable Ethernet(WAR1) None Disable CP Clevit Option PA4 11 Disable Ethernet(WAR1) None Disable CP Clevit Option PA6 12 Disable Ethernet(WAR1) None Disable 13 Disable Ethernet(WAR1) None Disable 14 Disable Ethernet(WAR1) None Disable 15 Disable Ethernet(WAR1) None Disable 16 Disable Ethernet(WAR1) None Disable 16 Disable Ethernet(WAR1) None Disable • Exercit option the fiber MARS are reserved. • Secret option to thinker WARS are reserved. • Secret option to thinker WARS are reserved.	W IPv6		Disable	Ethernet(WAN1)	None	Disable	
10 Disable Ethernet(WA(1)) None Disable CP Clevit Option Pvin 11 Disable Ethernet(WA(1)) None Disable CP Clevit Option Pvin 12 Disable Ethernet(WA(1)) None Disable 13 Disable Ethernet(WA(1)) None Disable 14 Disable Ethernet(WA(1)) None Disable 15 Disable Ethernet(WA(1)) None Disable 16 Disable Ethernet(WA(1)) None Disable 16 Disable Ethernet(WA(1)) None Disable	and the second se	9 WAN9	Dtsable	Ethernet(WAN1)	None	Disable	
CPC Clevel Option (PvG 11 Diable Chornet(WAQ1) None Diable CPC Clevel Option (PvG 12 Diable Ethernet(WAQ1)) None Diable 13 Diable Ethernet(WAQ1) None Diable 14 Diable Ethernet(WAQ1) None Diable 15 Diable Ethernet(WAQ1) None Diable 26 Diable (thernet(WAQ1)) None Diable 26 Diable (thernet(WAQ1)) None Diable	an euroger	10	Disable	Ethernet(WAN1)		Desable	
13 Disable Ethernet(WANL) None Disable 14 Disable Ethernet(WANL) None Disable 15 Disable Ethernet(WANL) None Disable 16 Disable Uthernet(WANL) None Disable 16 Disable Uthernet(WANL) None Disable • Exercision out or hisident WANLis are reserved. • Exercision out or hisident WANLis are reserved.	ICP Client Option IPv4	11	Disable	Ethernet(WAN1)		Disable	
13 Disable Ethernet(WAN1) None Disable 14 Disable Ethernet(WAN1) None Disable 15 Disable Ethernet(WAN1) None Disable 16 Disable (thernet(WAN1)) None Disable Mole: • Greynel out or hidden WANs are reserved.	ICP Client Option IPv6	12	Disable	Ethernet(WAN3)	None	Disable	
14 Drusole Ethermet(WANI) None Drusole 15 Drusole Ethermet(WANI) None Drusole 16 Drusole (Thermet(WANI)) None Drusole 0 Mole: - - -				Ethernet(WAN1)	None	Disable	
16 Disable Ethemet(WANI) None Disable 0 Note: • Greynel out or hidden WANs are reserved. •				Ethernet(WAN1)	None	Desable	
Hole: Greyed out or hidden WANs are reserved.		15	Disable	Ethernet(WAN1)	None	Disable	
 Greyed out of hidden WANs are reserved. 		16	Disable	(thismet(WAN1)	None	Druable	
 Ports conlighted for orkige mode carries to selected in CAN 22 YEAR conlightation 		 Greyed or 	it or hidden WANs are reserving to bridge mode can	ved. not be selected in LAN >> VLAN Configuratio			

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

27Lac_1449BC023768 / Config	uration / WAN		C
Enable Channel 7			
WAN Type	Ethernet(WAN1) ~		
General Settings			
VLAN Tag	0		
Service Tag Value	Disable		
Priority	0 ~		
 ① Note: Tag value must be set Only one channel can 	etween 1-4095 and unique for each channel. e untagged (equal to 0) at a time.		
Open Port-based Bridge Connection	for this		
 Note: P1 is reserved for NAT If the port be configure 	ise, and cannot be configured for bridge mode. d for bridge mode, the setting of the port in LAN >> VLAN Configuration will not work.		
		Cancel	Save

ltem	Description
Enable Channel #	Click to enable or disable the channel.
	General Settings
VLAN Tag	Enter the value as the VLAN ID number.
Priority	Choose the number to determine the packet priority for this VLAN. The range is from 0 to 7.
Open Port-based Bridge Connection for this channel	Click to enable or disable the function. If enabled, you have to enter required settings for the following items. Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.

Open WAN Interface for this Channel	Click to enable or disable the function.
	If enabled, you have to enter required settings for the following items.
	WAN Application -
	 Management - The configuration for this VLAN will be effective for Web configuration/telnet/TR069.
	 IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
	Mode - Select ARP Detect or Ping Detect. If Ping Detect is selected, you
	have to set the following options.
	 Primary Ping IP / Secondary Ping IP - Enter Primary or Secondary IP address in this field for pinging.
	• Ping Gateway IP - Enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.
	 TTL - Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
	 Ping Interval - Set a time interval (unit: second) for the system to ping the IP address specified above.
	• Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
	WAN Setup - Choose Static or Dynamic IP or PPPoE/PPPoA.
WAN IP Network	It is available when Static_or_Dynamic_IP is selected as WAN Setup.
Settings	Auto IP - Click to enable / disable the settings.
	If Auto IP is enabled, you have to enter required settings for the following items.
	• Router Name - Enter the router name provided by ISP.
	• Domain Name - Enter the domain name provided by ISP.
	If Auto IP is disabled, you have to enter required settings for the following items.
	IP Address - Enter the IP address.
	• Subnet Mask - Enter the subnet mask.
	• Gateway - Enter gateway IP address.
	Primary DNS IP - Enter the primary IP address for the router if you want to use Static IP mode.
	Secondary DNS IP - If necessary, Enter secondary IP address for necessity in the future.
ISP Access Setup	It is available when PPPoE/PPPoA is selected as WAN Setup.
·	ISP Name - PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank.
	Username - Name provided by the ISP for PPPoE/PPPoA authentication.
	Password - Password provided by the ISP for PPPoE/PPPoA authentication.
	Authentication - Choose the protocol used for PPP authentication.
	Always On - The router will maintain the PPPoE/PPPoA connection.
	Fixed IP - If enabled, the IP address entered in the Fixed IP Address field
	will be used as the IP address of the virtual WAN.
	will be used as the IP address of the virtual WAN. Fixed IP Address - Enter an IP address.

9.4.1.4 WAN IPv6

This page allows to configure IPv6 settings for each WAN interface.

Internet Access	2865ac_001DAA151	EB8 / Configuration / WAN		
Connection Detection	Index	Physical Mode	Connection Type	
Multi-PVC/VLAN	WAN1	DSL	Offline	
WAN IPV6	WAN2	Ethernet	ррр	
WAN Budget	WAN5	USB	Offline	
	WAN6	USB	Offline	

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the WAN interface.
Physical Mode	Displays the physical connection for WAN interfaces according to the real network connection.
Access Mode	Displays the accessing mode of the Internet.

To modify the IPv6 setting, move the mouse cursor to any entry (WAN1/WAN2/WAN5/WAN6) and click to open the setting page.

2865ac_001DAA151EB8 / Configur	ation / WAN			
Basic				
Connection Type	Offline	¥		
	Offline			
	PPP TSPC AICCU DHCPv6 Client Static IPv6 6in4 Static Tunnel 6rd		Cancel Save	

Offline

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

PPP

2865Lac_1449BC0D8F00 / Configuration / WAN		
Basic		
Connection Type	ppp v	
RIPng Protocol	0	
WAN Connection Detection		
Mode	Ping Detect ~	
Ping IP/Hostname		
TTL(1-255,0:Auto)	0	
		Cancel Save

TSPC

2865Lac_1449BC0D8F00 / Configuration / WAN		
Basic		
Connection Type	TSPC ~	
TSPC		
Username		
Password	\$	
Tunnel Broker		
WAN Connection Detection		
Mode	Ping Detect ~	
Ping IP/Hostname		
TTL(1-255,0:Auto)	0	
		Cancel Save

AICCU

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Basic	
Connection Type	AICCU ~
AICCU	
Always On	0
Username	
Password	•
Tunnel Broker	tic.sixxs.net
Tunnel ID	
Subnet Prefix	/ 0
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

DHCPv6 Client

2865Lac_1449BC0D8F00 / Configuration / WAN	
Basic	
Connection Type	DHCPv6 Client v
IAID	0
DUID	000300011449bc0d8f01
505	000300114430C00001
Authentication Protocol	None v
RIPng Protocol	D
Enable Bridge Mode	0
Enable Firewall	Ø
Bridge Subnet	LANI
WAN Connection Detection	
Mode	Ping Detect ~
Ping IP/Hostname	
TTL(1-255,0:Auto)	0
	Cancel Save

Static IPv6

65Lac_1449BC0D8F00 / Configuration / W	NN			
Basic				
Connection Type	Static IPv6	~		
Static IPv6				
Current IPv6 Address Table				
Index IPv6 Address	Prefix	Length	Action	
1			+ Add	
IPv6 Gateway Address	**			
RIPng Protocol	\bigcirc			
Enable Bridge Mode				
Enable Firewall	\bigcirc			
Bridge Subnet	LAN1	~		
VAN Connection Detection				
Mode		~		
noue	Ping Detect	· ·		
Ping IP/Hostname				
TTL(1-255.0:Auto)	n			
				Cancel

6in4 Static Tunnel

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

6rd

27ac_1449BC30C3F0 / Config	guration / WAN	
lasic		
onnection Type	brd ~	
rd Settings		
ind Mode	Auto_Brd State_cont	
tatic 6rd Settings		
Pv4 Border Relay	1644 Intrast (UX) (125.12.1.1)	
Pv4 Mask Length	0	
ind Prefix		
and Prelix Length	64	
AN Connection Detection	n	
Made	Always On .	
		Cancel Sav
		cances

The parameters for connection type (PPP to 6rd) are explained as follows:

ltem	Description
	PPP
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode,

	you have to type TTL value
	you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	TSPC
TSPC	Username - Enter the name obtained from the broker.
	Password - Enter the password assigned with the user name.
	Tunnel Broker - Enter the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	AICCU
AICCU	Always On - Check this box to keep the network connection always.
	Username - Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.
	Password - Enter the password assigned with the user name.
	Tunnel Broker - It means a server of AICCU. The server can provide IPv6
	tunnels to sites or end users over IPv4.
	Tunnel ID - One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394). Enter the ID offered by Tunnel Broker.
	Subnet Prefix - Enter the subnet prefix address obtained from service provider.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	DHCPv6 Client
DHCPv6 Client	IAID - Enter a number as IAID.
	Authentication Protocol - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key, Delayed and None. In general, the default setting is None.
	 Key ID – Enter a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.
	 Realm – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.

	 Secret –Enter a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.
	RIPng Protocol - RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.
	 Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.
	Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	Static IPv6
Current IPv6 Address	IPv6 Address – Enter the IPv6 Static IP Address.
Table	Prefix Length – Enter the fixed value for prefix length.
	Add – Click it to add a new entry.
	IPv6 Gateway Address - Type your IPv6 gateway address here.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.
	Enable Firewall – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.
	Bridge Subnet – Make a bridge between the selected LAN subnet and such WAN interface.
	6in4 Static Tunnel
6in4 Static Tunnel	Remote Endpoint IPv4 Address - Enter the static IPv4 address for the remote server.

	6in4 IPv6 Address - Enter the static IPv6 address for IPv4 tunnel with the value for prefix length.
	LAN Routed Prefix - Enter the static IPv6 address for LAN routing with the value for prefix length.
	Tunnel TTL - Enter the number for the data lifetime in tunnel.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
	6rd
6rd Mode	Auto_6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP".
	Static_6rd – Set 6rd options manually.
	If Static_6rd is selected as the 6rd Mode:
	IPv4 Border Relay – Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
	IPv4 Mask Length – Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain.
	It may be any value between 0 and 32.
	6rd Prefix – Enter the 6rd IPv6 address.
	6rd Prefix Length - Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.
	 Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	 TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
Cancel	Discard current modification.

After finished the above settings, click Save to save the settings.

9.4.1.5 WAN Budget

WAN Budget determines the data *traffic volume* for each WAN interface respectively to prevent overcharges for data transmission by the ISP.

- Configuration		ac_1449BC0D8F00											
nlamet Access	Gener	al Setop Status											
onniction Detection	index	WAN Budget Enable	Quota Limit	Limit Limit	Shutdown WAN Interface	Cyrse Mode	Monthly Cycle Day	Monthly Cycle Hour	User Defined Cycle Days	User Defined Cycle Hours	User Defined Current Day	Nutricables Object	t üs
DRI-PACALAN	WAN1	fatse	0	MB	fakse	Monthly	1	00.00	1	0	1	-	W
	WANZ	Ester	0	MB	faine	Monthly	1	00:00	3	0	1	-	W
NAN DIWA	WAN3	labe	0	MB	Tabue.	Monthly	1	00-00	-1	0	1	-	w
	WANA	talsa	0	MB.	taise	Monthly	1	00:00	1	0	Ĩ.	_	w
HEP Circle Option IING	LTE	false	0	MB	false	Monthly	1.	00:00	1	0	1	2	W
	WANG	talsé	0	MB	false	Monthly	r	00.00	1	0	i	-	W
	0			_				_			_		
		 The budget test 			ern is for released only, p								
		 2. Winn burdward 	e accoloration (function late	wid, the mentioned WAII in	whic of Ether	ood WAN Inter Simes n	wy be slightly inscore	-				
													-

To modify the budget profile setting, move the mouse cursor to any entry (index 1 to index 6) and click to open the setting page.

able		
uota Limit	0 M ~	
utdown WAN interface		
tification Object	V	
cle Mode	Monthly Custom	
able	Use Cycle in hours Use Cycle in days 🗸	
er Defined Cycle Days	1 ~	
er Defined Current Day	1 ~	
er Defined Reset Hours	00:00 ~	
 Note: 1. Please make sure the Time at 2. SMS message and mail will b 	d Date of the router is configured. sent when the usage reaches 99% and 100% of quota.	

ltem	Description
Enable	Click to enable the budget function.
Quota Limit	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
Shutdown WAN Interface	Click to let all the outgoing traffic through such WAN interface be terminated.
Notification Object	The system will send out a notification based on the content of the notification object.
Cycle Mode	Choose Monthly or Custom to define the billing cycle according to request.
	Monthly is default setting. If long period or a short period is required, use Custom. The period of cycle duration is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.
Monthly Cycle Day /	It is available when Monthly is selected as Cycle Mode.
Monthly Cycle Hour	Set the day and time in a month.
Enable	It is available when Custom is selected as Cycle Mode.

	Use Cycle in hours - Set a time cycle (including days and hours) for Vigor
	CPE to reset the data record automatically.
	 User Defined Cycle Days - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.
	 User Defined Cycle Hours - Select a number (0~23) of the hours for a cycle. For example, 12 means 12 hours. Based on the cycle days and cycle hours settings, Vigor CPE will reset the data record once reaching 7 days and 12 hours.
	 User Defined Current Day - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.
	Use Cycle in days - Set a cycle (with days) for Vigor CPE to reset the data record on a particular hour automatically.
	 User Defined Cycle Days - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.
	 User Defined Current Day - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.
	 User Defined Reset Hours - Select a particular time (00:00~23:00). For example, choose 15:00. Later, the CPE will reset the data record at 15:00 for every cycle.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.1.6 DHCP Client Option IPv4/IPv6

DHCP packets can be processed by adding option number and data information when it is enabled.

Internet Access	DrayTek / Configu	ration / wan			Set to Factory Default	t
Connection Detection	Enable	Interface	Option	Type	Data	
Aulti-VLAN	false		0	ASCII		
VAN IPV6						
VAN Budget Ht.B. Client Option (Pv6 HCP Client Option (Pv6	Internet A = 2. Option = 3. Config Field. = 4. Hoxado	12 is reserved. You cannot configure fit h (cccss >> Details Page". 55 is reserved and configured with value rring option G1 here will override the set (cimal Digit: Input the hosadocimal repre	as 1, 3, 6, 15, 212, also 33 and 121 for so ting in "WAN ≫ Internet Access" page's	me models. s DHCP Client Identifier		
	(/path)				_	
internet Access.	DrayTek / Configur	ation / WAN			Set to Factory Default	C
		ation / WAN interface	Option	Туре	Set to Factory Default Data	C
onnection Detection	DrayTek / Configur		Option 0	Type ASCII		C
onnection Delection	DrayTek / Configur Enable					C
onnection Defection iulti-VLAN IAN IPVG	DrayTek / Configur Enable false () Note: • 1. Options	interface 1, 7, 3, 4, 5, 8, 13, 70, 73, 25, 75 are reserve	0 ved.	ASCII		C
hternet Access. Connection Defection Auti-VLAN WAN IPvis WAN Budget DHCP Client Option IPv4	DrayTek / Configur Enable false O Note: • 1. Options • 2. Vigor wi Authentics	interface	0 ed. ccces* page's "IPv6 >> DHCPv6 Client C in this page.	ASCII		с

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

2865Lac_1449BC0D8F00 / Configuration / WAN		Set to Factory Default	C
Index	1		
Enable			
Interface	WAN1 🗸		
Option Number	0		
Туре	ASCII Hex Address 🗸		
Data			
🗎 Clear		Cancel Save	

The parameters are explained as follows:

ltem	Description
Index	Displays the index number for the DHCP option.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.
Interface	The interface(s) to which this entry is applicable.
Option Number	DHCP option number (e.g., 100).
Туре	Type of data in the Data field:
	ASCII Character - A text string. Example: /path.
	Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
	Address List - One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2 LAN

9.4.2.1 General Setup

This page provides you the general settings for LAN.

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

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

2865_1449BC080090 / Configuration / LAN		C
General Setup		
Index	1	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
RIP Protocol Control	Disable ~	
DHCP Server Setup		
DHCP Server Enable		
IP Pool Start	192.168.1.10	
IP Pool End	192.168.1.209	
Gateway IP Address	192.168.1.1	
DHCP Lease Time	86400	
Clear DHCP lease for inactive clients periodically		
DHCP Relay	\bigcirc	
DNS Server IP Address		
Primary IP Address	IPv4 format (EX : 123.12.1.1)	
Secondary IP Address	IPv4 format (EX : 123.12.1.1)	
		Cancel Save

ltem	Description
	General Setup
Index	Display the index number of LAN item.
IP Address	Display the IP address of the router.
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet.
RIP Protocol Control	It is available for LAN Port only.
	Click to enable / disable the function. If enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
Usage	It is available for DMZ Port only.
	NAT - Click to invoke NAT function.
	Routing - Click to invoke routing function.
	DHCP Server Setup
DHCP Server Enable	Click to enable / disable the DHCP server settings. If enabled:
	IP Pool Start - Enter an IP address. The beginning LAN IP address that is given out to LAN DHCP clients.
	IP Pool End - Enter an IP address. The ending LAN IP address that is given out to LAN DHCP clients.
	Gateway IP Address - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN.
	DHCP Lease Time - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.
	Clear DHCP lease for inactive clients periodically - If enabled, the router sends ARP requests recycles IP addresses previously assigned to inactive

	DHCP clients to prevent exhaustion of the IP address pool.
DHCP Relay	Click to enable / disable the DHCP Relay settings. If enabled:
	DHCP Relay IP Address - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
	DHCP 2nd Relay IP Address - Set the second IP address for the DHCP server.
	DNS Server IP Address
Primary IP Address	Specify a DNS server IP address.
Secondary IP Address	Specify secondary DNS server IP address.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.2 IP Routed Subnet

General Settup	2927ac_1449BC30C3F0 / Configu	iration / LAN	C.
15 Penalod Schweit VLAN	General Setup		
Ellind IP to MAC	Enable	•	
DHCP Server Option IPv4	II ¹ Address	197.168.0.1	
DHCP Server Option IPv6 Intest AN Reading	Subnet Mask	255,255,355,0	
LAN IPV6	RIP Protocol Control	Disable 🗠	
Port Minor Wired 802.1X	DHCP Server Setup		
Link Aggregation	IP Pool Start	0.0.0.0	
	IP Pool Counts	0 958.72	
	DHCP Lease Time	259200	
	Use LAN Port	0	
	Use LAN Port1	0	
	Use IAN Port2	0	
	Use MAC Address	•	
			Cancel Save

ltem	Description
	General Setup
Enable	Click to enable / disable the IP routed subnet configuration.
IP Address	It is the IP address of the router.
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0)
RIP Protocol Control	Enable - The router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
	DHCP Server Setup
IP Pool Start	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses.
IP Pool Counts	Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to.
DHCP Lease Time	Enter the time to determine how long the IP address assigned by DHCP server can be used.
Use LAN Port / Use LAN Port 1 /2	Specify an IP for IP Route Subnet. If Use LAN Port is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of Use LAN Port 1 and Use LAN Port 2.
Use MAC Address	Click to specify MAC address.
MAC Address Table	It displays the a list of MAC addresses. +Add - Enter the MAC address in the boxes and click this button to add. +Edit - Click to modify the address of the selected entry. Delete - Click to remove the selected entry.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.3 VLAN

LAN Enable				
ermit untagged device	in P1 to access router			
Name	Subnet	VLAN Tag Enable	VLAN Tag ID	VLAN Tag Priority
VLAN0	LAN1 🗸		0	0 🗸
VLAN1	LAN1 🗸		0	0 🗸
VLAN2	LAN1 🗸		0	0 🛩
VLAN3	LAN1 🗸		0	0 🛩
VLAN4	LAN1 🗸		0	0 🛩
VLAN5	LAN1 🖌		0	0 🛩
VLAN6	LAN1 🗸		0	0 🛩
VLAN7	LAN1 🗸		0	0 🛩
VLAN8	LAN1 🖌		0	0 🛩
VLAN9	LAN1 🛩		0	0 🛩
VLAN10	LAN1 🛩		0	0 🛩
VLAN11	LAN1 🛩		0	0 🛩
VLAN12	LAN1 ¥		0	0 🗸

ltem	Description
	VLAN Configuration
VLAN Enable	Click to enable / disable the VLAN configuration.
Permit untagged device P1 to access router	Click to enable / disable the function. If enabled, it allows untagged hosts connected to LAN port P1 to access the router.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only.
VLAN Tag Enable	Check to enable the function of VLAN with tag.
VLAN Tag ID	Enter the value as the VLAN ID number. The range is form 0 to 4095. VIDs must be unique.
VLAN Tag Priority	Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.
	VLAN Member(LAN)
P1 ~ P5	Check the LAN port(s) to group them under the selected VLAN.
	VLAN Member(Wireless 2.4G/5G)
SSID1~SSID4	Check the SSID boxes to group them under the selected VLAN.
Clear VLAN Setup	Discard the modification and return to the original configuration of this page.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network.

Bind IP to MAC			
Enable	\bigcirc		
Strict Bind	\bigcirc		
Strict Bind Interface			
			Cancel Save
IP Bind List			
🗄 Delete All			
Index			
	IP Address	MAC Address Comment	Action
1	IP Address 192.168.1.11	MAC Address Comment B0-6E-BF-C9-96-DE	Action
1			🖉 Edit 🍈 Delete
1			🖉 Edit 🍈 Delete
1			🖉 Edit 🍈 Delete
1 2 ARP Table			🖉 Edit 🍈 Delete

ltem	Description
	Bind IP to MAC
Enable	Click to enable or disable the function.
Strict Bind	Click to enable or disable the function. If enabled, the router will block the connection of the IP/MAC which is not listed in IP Bind List.
Strict Bind Interface	Choose the interface(s) for applying the rules of Bind IP to MAC.
Cancel	Discard current modification.
Save	Save the current settings.
	IP Bind List
Delete All	Delete all entries in IP Bind List.
+Add	After entering the IP address, MAC address and comment for a new entry, click +Add to create a new IP bind.
Edit	If IP address, MAC address and comment have been modified, click the Edit button to save the change.
Delete	Click the button to remove the selected index entry.
	ARP Table
+Add to Bind List	ARP table is the LAN ARP table of this router.
	Click to add the ARP table onto the Bind List.

9.4.2.5 DHCP Server Option IPv4/IPv6

DHCP packets can be processed by adding option number and data information when such function is enabled.

nable	Interface	Option	Туре	Data
alse		0	ASCII	
① Note:				
 1.Those option 		gure in this page: Option 1, 2, 3, 4, 5, 6, 8, 11, 13, 20, 2	3, 25 and 26.	
 2.0ption 23 cc 	uld be configured from DNS server field of LAN >> G	eneral Setup >> I AN {x} IPv6 Setup page.		

ltem	Description
+Add	Click to add a new option profile.
Delete	Click to remove a selected option profile.

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

2865Lac_1449BC0D8F00 / Configuration / LAN		Set to Factory Defau	Set to Factory Default			
Index	1					
Enable						
Interface	Nothing selected ~					
Data Type	ASCII Hex Address SIAddr					
Option Number	0					
Data						
🚔 Clear		Cancel	Cancel	Cancel	Cancel Sa	Cancel Save

Item	Description
Index	Displays the index number of the profile.
Enable	Click to enable or disable the DHCP option entry.
Interface	Select the LAN interface(s) to which this entry is applicable.
	Select All - Select all LAN interfaces.
Data Type	Select the type of data in the Data field.
	ASCII - A text string. Example: /path.
	Hex - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
	Address - One or more IPv4/IPv6 addresses, delimited by commas.
	SIAddr - It is available for DHCP Server Option IPv4 only. Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	Enter a DHCP option number (e.g., 100).
Data	Enter the data for this DHCP option based on the data type selected.
Next Server IPAddress/SIAddr	Enter the DHCP next server IP address. It is available for DHCP Server Option IPv4 only.
Cancel	Discard current modification.

9.4.2.6 InterLAN Routing

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

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	2								
LAN 2									
LAN 3			8						
LAN 4		0	0						
LAN 5	0	0	0	0					
LAN 6	0	0	0	0	D	5			
LAN 7	0	0	0	0	D	0			
LAN 8			0		D		0		
DMZ Port			0				0	0	
DMZ Port	0	0							Cancel S

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

9.4.2.7 LAN IPv6

This page allows to configure IPv6 settings for each LAN.

ndex	Status	DHCPv6 Enable	DNS Enable
AN1	Enable	true	Deploy_when_WAN_is_up
LAN2	Enable	true	Deploy_when_WAN_is_up
LAN3	Enable	true	Deploy_when_WAN_is_up
LAN4	Enable	true	Deploy_when_WAN_is_up
LAN5	Enable	true	Deploy_when_WAN_is_up
LAN6	Enable	true	Deploy_when_WAN_is_up
LAN7	Enable	true	Deploy_when_WAN_is_up
LAN8	Enable	true	Deploy_when_WAN_is_up
DMZ	Enable	true	Deploy_when_WAN_is_up

To modify the IPv6 setting for each LAN, move the mouse cursor on the entry and click to open the setting page.

Basic Setup				
LAN Name		LAN1		
Enable				
WAN Primary Interface		WAN1	~	
static IPv6				
ULA Config		Off	~	
ULA Config Address				
		Prefix Length: 64		
IPv6 Address Table	Index	IPv6 Address	Prefix Length	Action
	1	FE80::B9A1:14C0:2AB4:900B	64	Delete
	2			+ Add
DNS Server IPv6				
DNS Server IPv6		Deploy_when_WAN_Is_up	~	
		Deploy_when_WAN_is_up 2001:4860:4860:8888	~ 	
DNS Enable			~	
DNS Enable Primary DNS Secondary DNS		2001:4860:4860::8888	×	
DNS Enable Primary DNS		2001:4860:4860::8888	×	

ltem	Description
	Basic Setup
LAN Name	Display the name of the LAN interface.
Enable	Click to enable or disable the configuration of LAN IPv6 Setup.
WAN Primary Interface	Specify a WAN interface for IPv6.
	Static IPv6
ULA Config	Select the ULA mode (off, Auto_ ULA_Prefix, Manually_ULA_Prefix).
ULA Config Address	LAN clients will be assigned ULAs generated based on the prefix manually entered.
IPv6 Address Table	Display current used IPv6 addresses.

	DNS Server IPv6
DNS Enable	Select Deploy_when_WAN_is_up, disable or enable.
	Deploy when WAN is up - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.
	Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.
	Disable - DNS server will not be used.
Primary DNS	Enter the IPv6 address for Primary DNS server.
Secondary DNS	Enter another IPv6 address for DNS server if required.
	Management
Management	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.
	Off - No configuration information is sent using Route Advertisements.
	SLAAC(stateless) - M-bit is unset.
	DHCPv6(stateful) - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor2865, or a separate DHCPv6 server.
Other Option (O-bit)	Click to enable or disable the function. If enabled, the O-bit will be enabled for obtaining additional information (e.g., DNS) from DHCPv6.
	DHCPv6 Server
DHCPv6 Server Enable	Click to enable DHCPv6 server.
Auto IPv6 Range	If enabled, Vigor router will assign the IPv6 range automatically.
Start Address	Enter the start address for IPv6 server.
End Address	Enter the end address for IPv6 server.
	Router Advertisement
Enable	Click to enable or disable the router advertisement server.
Hop Limit	The value is required for the device behind the router when IPv6 is in use.
Min/Max Interval Time(sec)	It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.
Default Lifetime(sec)	Within the period of time, Vigor router can be treated as the default gateway.
Default Preference	It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.
MTU Auto	If enabled, the router will determine the MTU value for LAN.
	RIPng Protocol
Enable	If enabled, RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	Extension WAN
Selected WAN	Extension WAN Additional WANs selected to carry IPv6 traffic.

Save the current settings.

9.4.2.8 Port Mirror

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

Enable				
MirrorPort	Port3		*	
Mirrored Tx Port	Port1	Port2		
	Port3	Port4		
	DMZ	WAN1		
	WAN2			
Mirrored Rx Port	Port1	Port2		
	Port3	Port4		
	DMZ	WAN1		
	🗹 WAN2			

The parameters are explained as follows:

ltem	Description
Enable	Enables or disables LAN Port Mirroring.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Tx Port	Port(s) whose outbound traffic will be forwarded to the mirror port.
Mirrored Rx Port	Port(s) whose inbound traffic will be forwarded to the mirror port.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.9 Wired 802.1X

Wired 802.1X provides authentication for clients wishing to connect to the LAN by Ethernet.

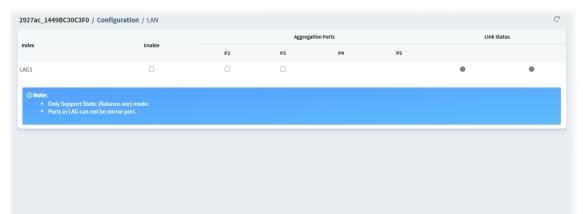
?7ac_1449BC30C3F0 / Config	uration / LAN	
Enable LAN 802.1X	\odot	
Authentication Type	External RADIUS ~	
802.1X Ports	D P1 D P2 D P3 D P4 D P5	
Note: 1.802.1X enabled LAN po	rts only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN	
2.Please configure Extern	-capable switch. Then configure 802.1X on the attached switch instead. al RADIUS or Local 802.1X for authentication. mal RADIUS supports PEAP, EAP-ITLS and EAP-ITLS.	

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

Enable LAN 802.1x	Check the box to enable LAN 802.1x function.
Authentication Type	External RADIUS - An external RADIUS server is to be used for 802.1X authentication. Local 802.1X - Use the user database on the router to authenticate clients.
802.1X ports	802.1X authentication will be available for the selected LAN ports.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.2.10 Link Aggregation

LAG means Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.



ltem	Description
Enable	Check the box to enable LAN 802.1x function.
Aggregation Ports	Select the port number (at least two ports) to make a high-bandwidth data path. At present, the available ports to be selected include P2 and P3.
Link Status	Green light means the LAG port is connected by Ethernet cable(s).
Cancel	Discard current modification.
Save	Save the current settings.

9.4.3 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

9.4.3.1 Profile Setup

Profile Setup is used to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

Index	Enable Comments	Login Mode	Applied Interface	
1	Disable	Click-through	None	
	Disable	Click-through	None	
	Disable	Click-through	None	
1	Disable	Click-through	None	
Preview	hotspot from WAN and VPN			
Preview	hotspot from WAN and VPN	D		
Preview	hotspot from WAN and VPN			Save
		•		Save
ឿ Note:	1. The router must connect to the Internet be		iery for domain name "portal.draytek.com" will be	_

To configure the profile, move the mouse cursor to any entry and click to open the setting page. Follow the on-screen steps to set the profile.

Step (1) Login Method

1 Login Method	2 Background	3 Login Page Setup	4 Whitelist Setting	5 More Options	
Step 1- Login Method					
Enable					
Comments					
Portal Server					
Portal Method		Various Hotspot Login	~		
Captive Portal URL		http:// ~ portal.dr	aytek.com		
Login Methods					
Choose Login Method		Login with Facebook			
		Login with Google			
		Receive PIN via SMS			
		Receive PIN via Mail			
		PIN with Voucher			
		Login with RADIUS			
		🗌 Leave Info Login			
				Cancel Prev	ious Save and Next

ltem	Description			
Enable	Check to enable this profile.			
Comments	Enter a brief description to identify this profile.			
	Portal Server			
Portal Method	 There are four methods to be selected as for portal server. Skip Login, landing page only Click Through Various Hospot Login Leave Info Login External Portal Server When Skip Loging, landing page only or Click through is selected as Portal Method			
Captive Portal URL	Enter the captive portal URL.			
	When Various Hotspot Login is selected as Portal Method			
Captive Portal URL	Enter the captive portal URL.			
Login Methods	 This setting is available when Various Hotspot Login is selected as the portal method. Choose Login Method - Select one or more desired login methods. Login with Facebook Login with Google Receive PIN via SMS Receive PIN via Mail PIN with Voucher Login with RADIUS 			

	Leave Info Login				
Facebook (Login with Facebook)	This setting is available when Login with Facebook is selected as the login method.				
()	Facebook APP ID - Enter a valid Facebook developer app ID.				
	Facebook APP Secret - Enter the secret configured for the APP ID entered above.				
Google (Login with Google)	This setting is available when Login with Google is selected as the login method.				
	Google App ID - Enter a valid Google app ID.				
	Google App Secret - Enter the secret configured for the APP ID entered above.				
SMS Provider (Receive PIN via SMS)	This setting is available when Receive PIN via SMS is selected as the login method.				
	Receiving PIN via SMS Provider - Select the SMS Provider used to send PIN notifications SMS providers.				
Mail Server (Receive PIN via Mail	This setting is available when Receive PIN via Mail is selected as the login method.				
Server)	Receiving PIN via Mail - Select the SMS Provider used to send PIN notifications SMS providers.				
Radius Server (Login with RADIUS)	This setting is available when Login with RADIUS is selected as the login method.				
(- 0 ,	Authentication Method – Click link to configure the external RADIUS server for authenticating web portal clients.				
	RADIUS MAC Authentication – Check Enable to activate user authentication by MAC address.				
	MAC Address Format – Select the MAC address format that is used by the RADIUS server.				
	When External Portal Server is selected as Portal Method				
Redirection URL	Enter the URL to which the client will be redirected.				
RADIUS Server	Authentication Method - To configure the RADIUS server, click the_ External RADIUS Server link and you will be presented with the configuration page.				
	RADIUS MAC Authentication - If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server.				
	MAC Address Format - Select the MAC address format.				
	RADIUS NAS-Identifier - Enter the ID (string) for RADIUS NAS-Identifier.				
Cancel	Discard current modification.				
Previous	Return to previous page.				
Save and Next	Save the current settings and get into next page.				

If you have chosen Skip Login, landing page only or External Portal Server as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

Step (2) Background

Select a background for the login page.

Login Method	2 Background	3.1 Login Page Setup	3.2 Login Page Setup	Whitelist Setting	S More Options	
Step 2 - Background Choose Login Background		Color Background	Image Background			
Brown and B	artuer	ab Trie ge & Logo Background Color hods Background Color				
Browser Table Title		Draytek Hotspot				
Logo Image	Logo Image		White •			
Logo Background Color		Vigor Red	•			
Login Method Background Color		Vigor Grey	•			
					Cancel Previous Save and	Next

The parameters are explained as follows:

ltem	Description
Choose Login Background	Select either Color Background or Image Background as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

If you have selected Skip Login, landing page only or External Portal Server as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

Step (3) Login Page Setup

Login Method	Background	3.1 Login Page Setup	32 Login Page Setup	4 Whitelist Setting	5 More Options	
Step 3.1 - Login Page Setup						
Configure Login Method and Deta	ils					
R						
Welcome Message		Welcomel Please	log in to enjoy Wi-Fi.			
		Default				
Privacy Policy & Terms and Condit	ions					
Terms and Conditions		 User must tick to ge 	t the internet access			
Description		By clicking the button b Terms and Conditions.				
		Default				
Content		Internal Content	External Content			
		(Max 1360 characters)				
Data Collection for Marketing		0	k			
		User must tick to ge				
Description		I would like to receive e	mails about the latest			

ltem	Description			
	if you have selected Click Through as the Portal Method.			
Welcome Message	Enter the text to be displayed as the welcome message.			
Terms and Conditions	Click to enable/disable the function. User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.			
Description	Enter the text to be displayed in the Terms and Conditions pop-up window.			
Content	If enabled, a check box with a description will be shown on the web portal login page.			
	Internal Content - Click it for displaying the message that you want the user knows on the web portal login page.			
	• Enter the text on the box below the Internal Content button.			
	External Content - Click it for opening another URL web page.External Content URL - Enter the URL.			
Data Collection for Marketing	If enabled, a check box with a description will be shown on the web portal login page.			
	User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.			
	Description - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier.			
Enter PIN Description	Enter the existing PIN code.			
Submit Button Description	Enter the text to be displayed on the Submit button			
Accept Button Description	Enter the text to be displayed on the accept button			

Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.			
	if you have selected Various Hotspot Login as the portal method.			
Welcome Message	Enter the text to be displayed as the welcome message.			
Terms and Conditions	Click to enable/disable the function. User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access.			
Description	Enter the text to be displayed in the Terms and Conditions pop-up wind			
Content	 If enabled, a check box with a description will be shown on the web portal login page. Internal Content - Click it for displaying the message that you want the user knows on the web portal login page. Enter the text (maximum 1360 characters) on the box below the Internal Content button. External Content - Click it for opening another URL web page. External Content URL - Enter the URL. 			
Data Collection for Marketing	If enabled, a check box with a description will be shown on the web portal login page. User must tick to get the internet access - Click to ask the user ticking the box for getting the Internet access. Description - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier.			
Facebook Login Description	Enter the text to be displayed on the Facebook login button.			
Google Login Description	Enter the text to be displayed on the Google login button.			
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.			
Receiving PIN Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.			
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <pin> within the message.</pin>			
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.			
Submit Button Description	Enter the text to be displayed on the submit PIN button			
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.			
Hint Message for RADIUS	Enter the text used to prompt the user to login.			
RADIUS Account Description	Enter the text to prompt the user to enter the username.			
RADIUS Password Description	Enter the text to prompt the user to enter the password.			

Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

If you have selected Various Hotspot Login as the portal method and selected Receive PIN via SMS as the login method, you will also need to configure (3.2 Login Page Setup) page.

- 6	3.2

Login Page Setup

1 Login Method	Background	3.1 Login Page Setup	3.2 Login Page Setup	4 Whitelist Setting	More Options
Step 3.2 - Login Page Setup					
Configure Login Method and Details					
	7				
< Back	Back Button		_		
	Dilli Carda Marca				
PIN Code will be sent over via SMS.	PIN Code Mess	age	_		
+ 886 enter your mobile number	Default Country	, Enter Mobile Number D	escription		
Send PIN	Send Button De	scription and Color	_		
	Send Succeede	d Message			
Enter PIN Submit	Enter PIN and S	ubmit Button			
Back Button Description		Back			
		Default			
PIN Code Message		PIN code will be sent ov	ver via SMS.		
			le		
		Default			
Default Country Code		+ 93 Afghanistan			
Enter Mobile Number Description		enter your mobile numb	er		

ltem	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country Code	Select the default country code to be displayed using the dropdown menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

Step (4) Whitelist Setting

Configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Login Method Step 4 - Whitelist Setting	2 Background	3.1 Login Page Setup	Login Page Setup	4 Whitelist Setting	3 More Options
NAT Rules Dest Domain Always allow outbound conn	Dest IP Dest Port	Source IP NAT >> Port Redirectio NAT >> Open Ports NAT >> DMZ	n		
					Cancel Previous Save and Next

ltem	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.
Cancel	Discard current modification.
Previous	Return to previous page.
Save and Next	Save the current settings and get into next page.

Step (5) More Options

Login Method	Background	3.1 Login Page Setup	Logir	32 Page Setup W	hitelist Setting M	ore Options
Step 5 - More Options						
Login Method	Quota Policy Profile		Valid Time	Device Allowed	Bandwidth Limit	Session Limit
Facebook Login	1. Default	*	0d 5h 0m	Unlimited	Unlimited	Unlimited
Google Login	1. Default	*	0d 5h 0m	Unlimited	Unlimited	Unlimited
SMS Login	1. Default	v	0d 5h 0m	Unlimited	Unlimited	Unlimited
	a settings, please go to Hotspot V	Veb Portal >> <u>Quota Manag</u>	<u>ement</u>			
To modify the quota eb Portal Options HTTPS Redirection	settings, please go to Hotspot V	Veb Portal >> <u>Quota Manag</u>	<u>emens</u>			
To modify the quota eb Portal Options HTTPS Redirection	settings, please go to Hotspot V isoted client opening a HTPS pa to redirect only HTTP pages. HT	e redirect will work but o	ertificate errors may			
To modify the quota eb Portal Options HTTPS Redirection Note: When an unauthent Disable this function	icated client opening a HTTPS pa	e redirect will work but o	ertificate errors may			
To modify the quota eb Portal Options HTTPS Redirection Note: When an unauthent Disable this function Captive Portal Detection Note: Trigger the unauthe	icated client opening a HTTPS pa to redirect only HTTP pages. HT nticated client to automatically p	age, redirect will work but o TIPS browsing will timeout to D oop up the Web Portal page	ertificate errors may without redirection -	and also no certificate errors. W-Fi.	5 bulb-in Captive Portal Detection.	
To modify the quota To modify the quota Veb Portal Options HTTPS Redirection When an unauthent Disable this function Captive Portal Detection Rote: Trigger the unauthe	icated client opening a HTPS pa to redirect only HTP pages. HT nticated client to automatically p available when using Social Login	age, redirect will work but o TIPS browsing will timeout to D oop up the Web Portal page	ertificate errors may without redirection -	and also no certificate errors. W-Fi.	5 bullt-in Captive Portal Detection.	

ltem	Description
	Quota Management
Quota Policy Profile	Choose a policy profile to apply to web portal clients.
	JSON API
Enable JSON API	If enabled, information (e.g., string, number, object and so on) will be saved as a text file on the JSON server.
Server URL	Enter the URL of the server which will store the JSON information.
Get JSON and Update user status every	Specify the time period for the JSON server sending the JSON information to other devices automatically.
Update Information	 The information sent out by JSON server might include the following types: NAS-Identifier (router's ID) MAC Address (routers' MAC address)
	 All User Number (total number of the users connecting to the router) Wi-Fi User Number (total number of the wireless users connecting to the router)
	Web Portal Options
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.

Landing Page After Authentication				
Landing Page Type	Fixed URL - Specifies the webpage that will be displayed after the user has successfully authenticated.			
	The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.			
	User Requested URL - The user will be redirected to the URL they initially requested.			
	Bulletin Message - The message configured here will be briefly shown for a few seconds to the user.			
	Bulletin Message Type - Select HTML or Image Upload.			
	 Default – This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox. 			
Force Landing Page Stay Enable	If enabled, the landing page will stay until you close it.			
	Applied Interfaces			
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.			
WLAN 2.4G / 5G	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.			
Cancel	Discard current modification.			
Previous	Return to previous page.			
Finish	Complete the configuration.			

9.4.3.2 Users Information

This page displays information of users accessing the Internet through the web portal.

9.4.3.2.1 User Info

yTek / Configuration / Hots	pot Web Portal				C
User Info Database Setup					
Select Columns to Filter Users				^	
Profile	🗌 Profile 1	Profile 2 Pr	ofile 3 🗌 Profile 4		
Login Method	🗌 Skip	Facebook	Google		
	Pincode	Click	□ RADIUS		
	Leave Info				
Data Collection	□ Marketing				
			Ap	pły	
User Table					
Avtive User ~ 0 Online Users	/ 0 All Users		Auto Refresh (per min):	off ~	
Index $\downarrow\uparrow$ Status $\downarrow\uparrow$ Profile $\downarrow\uparrow$	User↓↑ Login Method ↓↑	IP [↓] ↑ MAC [↓] ↑ Email [↓] ↑	Phone Number 4 Expired Ti	ime ↓↑	
	No dat	a available			
Go to page 1 Go					

These parameters are explained as follows:

ltem	Description
Select Columns to Filter Users	Select the profiles and the login methods to filter the displayed users. Apply - Save the settings.
User Table	Details of users accessing the Internet via Hotspot Web Portal will be displayed.
Active User / All Database	Displays the information for active user only or for all users in database.
Auto Refresh	On/off - Refresh current page automatically or not.
Go	Where there are more than one page, Click to open the page with specified number.

9.4.3.2.2 Database Setup

This page allows the user to configure settings for database on USB disk.

865ac_001DAA41DF78 / Configuration / Ho	ntspot Web Portal	Ø
User Info Database Setup		
Enable database		
Enable automatic database recovery		
Backup database every	1 v hours 0 v	
Enable sending user information to		
syslog		
File Path	No USB Disk Detected	
Database Usage	N/A	
	Clear User Info	
Notification and Action when Storage Exceed	ded	
Notification	Don't send notification •	
Action	Stop recording user information +	
Advanced options		
Database Encryption	\bigcirc	
	process. Once enable Database Encryption, router will create a new encrypted data from the non-encrypted database, and not able to change back to non-encrypted. Juter performance when writing data.	

Item	Description
Enable database	Check the box to record user information on router's database.
Enable automatic database recovery	Check the box to enable the functionality of the database recovery on the USB disk.
	Backup database every Set the interval to backup the database.
Enable sending user information to syslog	Check the box to send user information to syslog.
File Path	If a USB disk has been inserted into the USB port of Vigor router, the file path will be shown in this area.
Database Usage	Display the usage and remaining space on the database.

	Clear User Info – The user information will be displayed on the page of User Info. You can delete the information by clicking this button.
	Notification and Action when Storage Exceeded
Notification	Don't send notification - Vigor router system will not send any notification to any recipient.
	Send notification - Vigor router system will send a notification e-mail to specified recipient(s) that selected from Email Notification Object and SMS Notification Object.
	Email Notification Object
	 SMS Notification Object
Action	Stop recording user information - Vigor router system will stop to record the user information onto USB disk.
	Backup and clean up all user info, and start a new record - Vigor router system will backup all existed information on the USB disk onto the host and clean up the information from USB disk. Later, it will start a new record.
	Advanced Options
Database Encryption	Select to have the router create a new encrypted database. Once this is done, you will not be able to revert to an unencrypted database.
Password	Enter a password for encryption.
Confirm Password	Enter the password again for confirmation.
Save	Save the current settings.

9.4.3.3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

nable Bandwidth L	imit 🔘			
Enable Session Limit				
+Add 🗇 Delete			Profile Nur	iber Limit: 20
Index Name	Expired Time After First Logi	Device Allowed Per Account	Reconnection Time Restriction	Bandwidth
	0d 6h 0m	Unlimited	Unlimited	Unlimited

ltem	Description		
	Web Portal Bandwidth and Session Limit		
Enable Bandwidth Limit	Click to enable / disable the function. If enabled, it will override the policy configured in Bandwidth Management >> Bandwidth Limit.		
Enable Session Limit	Click to enable / disable the function.		

	If enabled, it will override the policy configured in Bandwidth Management >> Sessions Limit.		
	Quota Policy Profile		
+Add	Create up to 20 policy profiles.		
Delete	Delete the selected policy profile.		
Save	Save the current settings.		

To create a new policy profile, click +Add to create a new profile and display on the table.

Quot	a Polic	y Profile					
+a	dd 🍵					Profile N	lumber Limit: 20
	Index	Name	Expired Time After First Login	Device Allowed Per Account	Reconnection Time Restriction	Bandwidth Limit	Session Limit
	1	Default	0d 5h 0m	Unlimited	Unlimited	Unlimited	Unlimited
	2	level 2	0d 5h 0m	Unlimited	Unlimited	Unlimited	Unlimited

Check the box in front of the new entry and click to open the following page.

Index	2
Profile Name	level 2
Account Validity	
Expired Time After 1st Login	0 ✓ days hours minutes
Enable Idle Timeout	\bigcirc
Idle Timeout	0
Device Control	
Devices Allowed per account	Unlimited ~
Enable Reconnection Time Restriction	\square
Time Restriction	Set Time Set period
	0 v hours 0 v mins
	Block the same user from reconnecting for the set period
	Cancel Save

ltem	Description		
Index	Display the index number of the profile.		
Profile Name	Enter a name for a new profile.		
	Account Validity		
Expired Time After 1st Login			
Enable Idle Timeout	If enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.		
Idle Timeout	Enter a time value (unit: minutes).		

	Device Control
Devices Allowed per account	Select the maximum number of devices that can be connected to the network using the same account.
Enable Reconnection Time Restriction	Click to enable / disable the function.
Time Restriction	Blocks the account from being used to connect devices to the network in one of two ways:
	Set Time (At Everyday) - After the login expires, the account cannot be used to connect devices to the network until the set time of day.
	Set Period (Hours min)- After the login expires, the account cannot be used to connect devices to the network for a set period of time.
	Bandwidth and Session Limit
Enable Bandwidth Limit	Click to enable / disable the function.
Download /Upload Limit	Set the maximum upload and download speeds.
Enable Session Limit	Click to enable / disable the function.
Session Limit	Set a maximum session limit for web portal clients.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.3.4 PIN Generator

9.4.3.4.1 PIN Status

This page displays the detailed information for PIN codes generated by PIN Generator.

Profile Setup	/ Configuration / Hotspot Web Portal
Users Information	PIN Status PIN Generator Delete All M ▼ / 0 >
Quota Management	PIN Profile Status Batch Name Valid Through Quota Policy Activated On Expiry Time Action
	No data available

9.4.3.4.2 PIN Generator

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

Profile • Batch Name • PIN code length • PIN Validity Days 0 •
PIN code length v
PIN Validity Days 0 •
PIN Validity Hours 0 🔹
The period of time the PIN will be kept in the database.
Quantity 0
Quota Management Policy 👻
Genetate

These parameters are explained as follows:

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

9.4.4 Routing

9.4.4.1 Load Balance/Policy Route

This page lists the configured policies coming from Vigor CPE.

-	nfiguration / Routing						Set to Factory Default	C
	Index	Enable	Comment	Protocol	Interface	Src IP	Dest IP	
	1	Disable		Any	WAN1	Any	Any	
 Note: The policies in blue are SD-WAN related, and can only be edited via ACS. 								

ltem	Description
Delete	Click to remove the selected routing policy.
Index	Displays the index number of the routing policy.
Enable	Displays the status (enable / disable) of the routing policy.
Comment	Displays the description for the routing policy.
Protocol	Displays the protocol used for this policy.
Interface	Displays the interface to send packets to once the policy is matched.

Src IP	Displays the mode for the source IP.
Dest IP	Displays the mode for the destination IP.

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

Index	1
Enable	0
Comment	
Criteria	
Protocol	Any ~
Source IP	Any ~
Destination IP	Any
Destination Port	Any ~
Send via if Criteria Matched	
Interface Type	WAN ~
Interface Address	WAN1 ~ 1-10.3.8.4 ~
	Delete
	Add
🗊 Clear	Cancel Save

ltem	Description		
Index	Displays the index number of the routing policy.		
Enable	Click to enable / disable the routing policy.		
Comment	Enter a brief explanation for the routing policy.		
	Criteria		
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.		
Source IP	Select the mode (Any, IP Range, IP Subnet, IP Object or IP Group) of the source IP.		
	Enter the IP address(es), network, mask, or select IP object/group as the source IP based on the source IP mode used.		
Destination IP	Select the mode (Any, IP Range, IP Subnet, Domain Name, IP Object, IP Group or Country Object) of the destination IP.		
	Enter the IP address(es), network, mask, domain name, or select an object/group as the destination IP based on the destination IP mode used.		
Destination Port	Select the mode (Any or Range) for the destination port.		
	Enter the port values as the destination port based on the destination port mode used.		
	Send via if Criteria Matched		
Interface Type	Select the type of the interface.		
Interface	Use the drop down list to choose a WAN or LAN interface or PVC or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.		

Interface Address	Select the WAN interface that has an assigned IP address. Click Add to	
	specify more WAN interfaces.	
Interface Mode	It is available if WAN is selected as the Interface.	
	IP Based Load Balance - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.	
	Session Based Load Balance - All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP.	
Gateway IP	Default Gateway - Default Gateway is selected in default. Traffic will be sent to the default gateway address of the specified interface.	
	Specific Gateway - Traffic will be sent to the specified gateway address instead of the default gateway address. It is used only when you want to forward the packets to the desired gateway.	
	Priority	
Priority	The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.	
More Options		
Packet Forwarding Via	When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose Force NAT or Force Routing.	
Enable Failover	Click to enable / disable the failover function.	
Failover to	If enabled, it will lead the data passing through specific interface (e.g., WAN/LAN) automatically when the selected interface is down.	
Failover to Gateway IP	Specific gateway is used only when you want to forward the packets to the desired gateway.	
	Default Gateway - Usually, Default Gateway is selected in default.	
	Specific Gateway - Enter a gateway IP address.	
Cancel	Discard current modification.	

9.4.4.2 Static Route IPv4

The router offers IPv4 for you to configure the static route.

4	0.0.0.0 0.0.0.0 0.0.0.0	0.0.0.0	0.0.0.0	LAN1	B. 11
B 4		0.0.0.0			Disable
4	0.0.0.0		0.0.0.0	LAN1	Disable
		0.0.0.0	0.0.0.0	LAN1	Disable
5	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
-	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
5	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
7	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
В	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
9	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
10	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
11	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
12	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
13	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
14	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
15	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
16	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
17	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
18	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
19	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable
20	0.0.0.0	0.0.0.0	0.0.0.0	LAN1	Disable

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

2865ac_001DAA000000 / Configurati	n / Routing	Q
Static Route IPv4		
Index	2	
Enable	Œ	
Destination IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
Network Interface	LAN1 •	
🗊 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the static route policy.
Enable	Click to enable or disable the static route policy.
Destination IP Address	Enter an IP address as the destination of such static route.
Subnet Mask	Enter the subnet mask for such static route.
Gateway IP Address	Enter the IP address of the gateway.
Network Interface	Specify an interface for this static route.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.4.3 Static Route IPv6

The router offers IPv6 for you to configure the static route.

Index	Destination IPv6 Address	Prefix Len	Gateway IPv6 Address	Interface	Status
1		0		LAN1	DIsable
2	::	0		LAN1	Dtsable
3	:	0		LAN1	DIsable
4	:	0		LAN1	DIsable
5	::	0		LAN1	DIsable
6	:	0		LAN1	DIsable
7	:	0		LAN1	DIsable
8	::	0		LAN1	Disable
9	:	0		LAN1	Disable
10		0	=	LAN1	Disable
11	:	0		LAN1	Disable
12		0		LAN1	Disable
13		0	=	LAN1	Disable
14	:	0		LAN1	Disable
15		0		LAN1	Disable
16	::	0		LAN1	Disable
17	:	0	:	LAN1	Disable
18		0		LAN1	Disable
19	::	0		LAN1	Disable
20		0		LAN1	DIsable
21		0		LAN1	Disable
22	::	0		LAN1	Disable
23		0		LAN1	DIsable

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

865ac_001DAA000000 / Configuratio	n / Routing	S
Static Route IPv6		
Index	1	
Enable	0	
Destination IPv6 Address		
Prefix Len	0	
Gateway IPv6 Address		
Network Interface	LAN1 *	
🗊 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the static route policy.
Enable	Click to enable or disable the static route policy.
Destination IPv6 Address / Prefix Len	Enter the IP address with the prefix length for this entry.
Gateway lPv6 Address	Enter the gateway address for this entry.
Network Interface	Specify an interface for this static route.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.4.4 BGP

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

Load Balance/Policy Route	2927ac_14498C30C3F0 / Configuration	/ Routing				E.
Static Route IPv4 Static Route IPv6	Basic Settings					
101	Enable Local BGP	Ð				
CSP4	Redistribute OSPF routes into BGP	0				
	Local AS Number	(1-1204067296)				
	Hold Time	160				
	Connect Retry Time	120				
	Router ID	192.168.1.1				
						Eincel Save
	Thiad					
	Enable index AS Number	Profile Name	iP Address	HDS Auth	Status	4-Byte As Number
	Disable I			Disable	None	Tatse
	Static Network					
	+Ada					

ltem	Description
Enable Local BGP	Click to enable / disable the BGP function.
Redistribute OSPF routes into BGP	Click to enable / disable the distribution OSPF routes into BGP function.
Local AS Number	Enter the value as local AS nubmer.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect.
Router ID	Specify the LAN subnet for the router.
Cancel	Discard current modification.
Save	Save the current settings.
Basic Settings	 Displays general settings for for local router and neighboring routers. +Add - Add a new neighbor profile. Delete - Remove a selected neighbor profile. Enable - Displays the status of the BGP profile. Index - Displays the index number of the BGP profile. AS Number - Displays the value of AS number. Profile Name - Displays the name of the BGP profile. IP Address - Displays the IP address of the BGP profile. MD5 Auth - Displays the status (enabled / disabled) of MD5 Auth. Status - Display the connection status for local router and neighboring router.
Static Network	Displays the neighboring routers for exchanging the routing information with the local router. +Add - Add a new static network profile by giving IP address and subnet mask.

	Delete - Remove a selected neighbor profile.
	Index - Displays the index number of the BGP profile.
	IP Address - Displays the IP address of the router.
	Subnet Mask - Displays the subnet mask of the router.
Cancel	Discard current modification.
Save	Save the current settings.

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

ayTek / Configuration /	0	
ndex	1	
nable	\bigcirc	
Profile Name		
S Number	(1~4294967295)	
P Address	IPv4 format (EX : 123.12.1.1)	
1D5 Auth	\bigcirc	
Password	٩	
-Byte As Number	\bigcirc	
Veight	0 ~	
Prepend	0 ~	
		Cancel Sav

These parameters are explained as follows:

ltem	Description
Basic Settings	Index - Displays the index number of the profile.
	Enable - Click to enable / disable the profile.
	Profile Name - Enter the name of the profile.
	AS Number - Enter a value for AS number.
	IP Address - Enter the IP address for the profile.
	MD5 Auth - Click to enable / disable the MD5 authentication.
	Password - Enter the password for authentication.
	4-Byte As Number - Click to enable / disable the setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

To configure the BGP profile for static network, click +Add to open the setting page. Or move the mouse cursor to any existed entry and click to open the setting page.

2865ac_001DAA000000 / Configuration / F	louting		S
Index	1		
IP Address	IPv4 format (EX : 123.12.1.1)		
Subnet Mask			
		Cancel Save	
		Caricer 3996	-

These parameters are explained as follows:

ltem	Description
Static Network	Index - Displays the index number of the profile.
	IP Address - Enter the IP address for a router.
	Subnet Mask - Specify a subnet mask for the IP address.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5 NAT

9.4.5.1 Port Redirection

This page lists the configured Port Redirection policies coming from Vigor CPE.

2865ac_001DAA000000				Dray	Tek Vigo	orACS 3			Capture Pac	kets ~ Sy	stern Admir	carrie nistrator
Port Redirection	2865ac_0	001DAA0	00000 / Configuration /	NAT								Ŕ
										e) Set to Fac	tory Default
	Index	Status	Port Redirection Mode	Service Name	Protocol	Public Port Start	Public Port End	Private IP Start	Private IP End	Private Port	WAN IP	Source IP
Port Triggering	1	false	Single			0	0		0	0	All	0

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

NAT	
Enabled	
Port Redirection Mode	Single Range
Service Name	
Protocol	TCP UDP
WAN IP	~
Public Port Start	0
Public Port End	0
Source IP	Any IP Object IP Group
Private IP Start	IPv4 format (EX: 123.12.1.1)
Private Port	0
 Note: In "Range" Mode the End IP will be calculated in the second s	ted automatically once the Public Port and Start IP have been entered.
聞 Clear	Cancel

ltem	Description
Enabled	Click to enable / disable the port redirection profile.
Port Redirection Mode	Two options (Single and Range) are provided here for you to choose. Single / Range - To set a range for the specific service, select Range. Otherwise, select Single.
Service Name	Enter the description of the specific network service.
Protocol	TCP/UDP - Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN interface used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port Start / End	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will need to enter the required number on the first box (as the starting port) and the second box (as the ending port).
Source IP	 Select the source IP mode. Any - It means any IP address. IP Object - IP Object - Specify an IP object profile. IP Group - IP Group - Specify an IP group profile.
Private IP Start / End	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.2 DMZ Host

DMZ Host allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

2865ac_001DAA000000	~	Dray Tek VigorACS 3	Carrie Capture Packets > System Administrator
Port Redirection	2865ac_001DAA000000 / Con	figuration / NAT	S
	Index	Profile Name	
	1	WAN1	
Port Triggering	2	WAN2	
	3	WAN3	
	4	WAN4	
	5	WAN5	
	6	WAN6	

ltem	Description
Index	Displays the index number of the DMZ host profiles.

Profile Name

Displays the interface of the DMZ host profile.

To configure the DMZ host profile:

1. Move the mouse cursor to any entry (1 to 6) and click to open the following page.

nterface		WAN1				
Index	WAN Type	Mode	Enable	Private IP	WAN IP	
1	0	None	false	0.0.0.0		

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

/ Configuration / NAT				Q
NAT DMZ Host Setup				
Interface	WAN1			
Mode	Private IP v)		
Private IP	0.0.0.0			
WAN IP	192.168.105.120			
			Cancel	Save

These parameters are explained as follows:

ltem	Description
Interface	Displays the name of the DMZ host profiles.
Mode	Select a method to enter the IP address.Private IPNone
Private	Enter the private IP address of the DMZ host.
WAN IP	Displays the WAN IP alias for this interface.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

3. After finished the configuration, click Save to save the changes.

9.4.5.3 Open Ports

This page lists the configured Open Ports policies coming from Vigor CPE.

It allows you to open a range of ports for the traffic of special applications.

2865ac_001DAA41DF78	~			Dray Tek	VigorACS 3			Capture Packets *	carrie System Administrator	
Port Redirection	2865ac_0	01DAA41DF78 / Config	uration / NAT							Ø
DMZ Host									う Set to Factory Defa	sult
Open Ports	Index	Enable Open Ports	Comment	WAN Interface	WAN IP	Local IP Address	Source IP	Open Ports Factory Defau	t Source IP Type	e
Port Triggering	1	false		WAN1	WAN1_IP_Alias[1]	0.0.0	0	false	Any	
ALG										

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

Open Ports			
Index		1	
Enable		\bigcirc	
Comment			
WAN Interface		WAN1 •	
Source IP		Any IP Object IP Group	
Local IP Addre	55	0.0.0.0	
pen Port List			
Index	Protocol	Start Port	End Port
1		0	0
2		0	0
3		0	0
4		0	0
		0	0
5			
5		0	0
4 5 6 7 8		0	0

Item	Description
	Open Ports
Index	Displays the index number of the Open Port profile.
Enable	Click to enable / disable the Open Port profile.
Comment	Enter the description for the Open Port profile.
WAN Interface	Choose a WAN interface that will be used for this entry.
Source IP	 Select the source IP mode. Any - It means any IP address. IP Object - IP Object - Specify an IP object profile. IP Group - IP Group - Specify an IP group profile.
Local IP Address	Enter the private IP address of the local host.
Open Port List	It displays 1 to 10 open port profiles. Click any one of the index numbers to configure the settings for the selected open port profile.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.4 Port Triggering

Port Triggering is a variation of open ports function. This page lists the configured Port Triggering policies coming from Vigor CPE.

2865ac_001DAA41DF78	~			Dray Tek	VigorACS 3		Capture	Packets 👻	carrie System Administrator	
Port Redirection	2865ac_00	1DAA41DF7	8 / Configura	tion / NAT						Ø
									ら Set to Factory Def	ault
Open Ports	Index	Enable	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Source IP	Source IP Type	
	1	false						0	Any	

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

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

ltem	Description		
Enable	Click to enable / disable the Port Triggering profile.		
Service	Choose the service type to apply for this triggering profile.		
Comment	Enter the text to memorize the application of this rule.		
Source IP	 Select the source IP mode. Any - It means any IP address. IP Object IP Object - Specify an IP object profile. IP Group IP Group - Specify an IP group profile. 		
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.		
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.		

Incoming Port	Enter the port or port range for the incoming packets.
Clear	Click to return to factory default setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.5.5 ALG

There are two methods provided by Vigor router, RTSP (Real Time Streaming Protocol) ALG and SIP (Session Initiation Protocol) ALG, for processing the packets of voice and video.

- Configuration	2865_1449BC080090 / Configuration / NAT				Set to Factory Delautt	
And Medicection	ALG (Applicati	on Layer Gateway)				
OM/ Henst			-			
Open Ports	Enable		D			
Port Trippering						
	Index	Enable	Protocol	Listen Port	TOP	UDP
	1	false	SIP	5060	true	true
	2	false	RTSP	554	true	true
						Cancel Save

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

2865ac_001DAA41DF78 / Con	figuration / NAT	R
Enable		
Protocol	SIP	
Listen Port	5060	
тср		
UDP		
		Cancel Save

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

9.4.6 Hardware Acceleration

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

Acceleration		Disable	Feature				
IAI							
Votocol Paec		C TCP					
Paec		0					
votacial		TCP	I UDP				
xception List		0					
ndez	MAC Address			Туре	Description		
	00.00000000000						

ltem	Description				
Acceleration	Disable – The default setting. Enable - The sessions with the heaviest loading and the lower latency traffic will be added into PPA.				
NAT	Click to enable / disable NAT setting.				
Protocol	There are two types supported by this function, TCP and UDP.				
IPsec	Click to enable / disable IPsec setting.				
Protocol	There are two types supported by this function, TCP and UDP.				
Exception List	If you want to restrict some users/clients from transmitting data through the router by using the hardware acceleration function, switch the toggle to enable the function. Then click the index number to create an exclusion list.				
	Exception List				
	Index 1				
	MAC Address 00:00:00:00:00				
	Exception Type NAT IPsec Description				
	Delete				
	MAC Address - Enter the MAC address of the client. ARP Table - Click to select the client listed on the ARP table. Then, the MAC address of the selected client will be shown on the MAC Address field. Exception Type - Select NAT and / or IPsec. Description - Enter a brief explanation for the selected client.				
Cancel	Discard current modification.				
Save	Save the current settings.				

9.4.7 Firewall

9.4.7.1 General Setup

It allows you to enable / disable Data Filter, determine general rule for filtering the incoming and outgoing data.

Filter Setup		
Data Filter		
Data Filter Set Start	Set#2 🔻	
abound Policy		
Allow pass inbound fragmented large packets (required for certain games and streaming)		
Enable Strict Security Firewall		
lock routing connections initiated from W	AN	
Block IPv4 Routing Packet	\bigcirc	
Block IPv6 Routing Packet		
 Bote: Packets are filtered by firewall fun 1. Data Filter Sets and Rules. Block routing connections initiat 3. Default Rule. 		

Description
Filter Setup
Click to enable / disable the function.
lf enabled, choose a Start Filter Set.
Choose a Start Filter Set.
Inbound Policy
Click to enable / disable the function.
Certain games and video streaming service use fragmented UDP packets to transfer data. Enabling this option allows these applications to function properly.
Click to enable / disable the function.
If this option and the Web Content Filter (WCF) are both enabled, web traffic will be blocked if the WCF server fails to respond to lookup requests.
Block routing connections initiated from WAN
For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, enable this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.
IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN. Enable this option to block WAN hosts from connecting to LAN hosts using IPv6.

Save

Save the current settings.

9.4.7.2 Default Rule

This page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

Default Action	Pass Block	
Session Control	60000	
Quality of Service	None 👻	
User Management	None 👻	
APP Enforcement	None 👻	
URL Content Filter	None •	
Web Content Filter	None *	
DNS Filter	None 👻	
Syslog	Default Action Session Control	
	Quality of Service User Management	
	APP Enforcement URL Content Filter	
	Web Content Filter DNS Filter	
dvanced Settings		
Codepage	ANSI(1252)-Latin I	
Window Size	65535	
Session Timeout (min.)	60	

ltem	Description
	Default Rule
Default Action	Select Pass or Block for the packets that do not match with the filter rules. When the setting is Block, all other fields on the page are disabled because they are not applicable.
Session Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable.
Quality of Service	Select one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
User Management	This setting is only available when Rule-Based is selected in User Management>>General Setup. The default firewall rule will be applied to the selected user or user group.
APP Enforcement	Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule.
URL Content Filter	Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule.
Web Content Filter	Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for

	the Default Rule.
Syslog	Select the items to send and store the records to Syslog.
	Advanced Settings
Codepage	Selecting the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed.
Window Size	Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535.
Session Timeout	Sets the timeout sessions are allowed to idle before they are removed from the system.
Save	Save the current settings.

9.4.7.3 Filter Setup

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

Sel	Comments	Next Filler Sei	
L.	Default Data Filter	None	
C		None	
K		None	
e		None	
		None	
6 C		None	
		None	
£		None	
		None	
0		None	
u.		None	
2		None	

These parameters are explained as follows:

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

To configure the filter rule set profile, move the mouse cursor to any set number and click to open the setting page.

Inde			1				
Corr	ments		Default Data Filter				
Next	Filtor Set		None ~				
Rule	Active	Comments	Direction	SIC IP	DST IP	Service Type	Action
C		xNetRios > DNS	LAN/DM2/RT/VPN-WAN	Any	Any	TCP/UDP	Block Immediately
2	0		LAN/DMZ/RT/VPN->WAN	Any	Any	Any	Pass Immediately
3	0		LAN/DMZ/RT/VPN->WAN	Any	Any	Any	Pass Immediately
4	CD -		LAN/DMZ/RT/VPNWAN	Any	Λαγ	Any	Pass Immediately
5	CD		LAN/DMZ/RT/VPNWAN	Any	Any	Any	Pass Immediately
6	0		LAN/DMZ/RT/VPN~WAN	Any	Any	Any	Pass Immediately
	0		LAN/DMZ/RT/VPN-WAN	Any	Any	Any	Pass Immediately

These parameters are explained as follows:

ltem	Description
	Filter Rules
Index	Displays the index number of the filter rule set.
	Each filter set contains up to 7 rules.
Comments	Enter a comment to identify the filter rule.
Next Filter Set	Select the filter set for the firewall to process after the current filter set
	Table
Rule	Displays the index number of the filter rule.
Active	Click to enabled or disabled the filter rule.
Comments	Optional comment entered in the settings page to identify the rule.
Direction	Displays the direction of packet.
Src IP	Displays the IP address of source /destination.
Dst IP	Displays the type and port number of the packet.
Service Type	Displays the type and port number of the packet.
Action	Displays the packets to be passed /blocked.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

Click any rule in the table to display the filter conditions:

ieneral Settings			
Fliter Rule	1.		
Comments	aNetBios->DNS		
Active	0		
ilter Conditions			
Direction	LAN/DMZ/RT/VP	N->WAN or	
Incoming Interface	CAN1	U LANZ	
	Z LAN3	C LAN4	
	Cans.	CI LANG	
	I LANY	I ANS	
	CIMZ	IP Routed Subnet	
	VPN		
Outgoing Interface	WAND	🜌 WANZ	
	E WANE	S WAN4	
		- water	
	E WANS	WAN6	

After adjusting the filter conditions, click Save and return to previous page.

9.4.7.4 DoS Defense

2865Lac_1449BC0D8F00 / Configuration	/ Firewall	C
DoS Defense		
DoS Defense	O	
	White/Black List Option	
DoS defense Log	Enable ~	
Flood Defense		
SYN Flood Defense	O)	
SYN Flood Threshold (pkts/sec)	2000	
Session Time-Out (sec.)	10	
UDP Flood Defense	\bigcirc	
UDP Flood Threshold (pkts/sec)	5000	
Session Time-Out (sec.)	10	
ICMP Flood Defense		
ICMP Flood Threshold (pkts/sec)	250	
Session Time-Out (sec.)	10	
Port Scan Detection		
		Cancel 💼 Clear All Save

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

	Pickar LastRobis(s) / Configuentes 1 Innue Innue Innue
	26 KAN
DoS defense Log	Click to enable / disable the function of recording DoS defense log onto Syslog.
	Flood Defense
SYN Flood Defense	 Click to enable / disable the SYN flood defense. If enabled, SYN Flood Threshold - Set a threshold value. The default values of threshold is 2000 packets per second. Session Time-Out - Set a threshold value. The default value of timeout is 10 seconds.
UDP Flood Defense	 Click to enable / disable the UDP flood defense. If enabled, UDP Flood Threshold - Set a threshold value. The default values of threshold is 2000 packets per second. Session Time-Out - Set a threshold value. The default value of timeout is 10 seconds.
ICMP Flood Defense	 Click to enable / disable the ICMP flood defense. If enabled, ICMP Flood Threshold - Set a threshold value. The default values of threshold is 250 packets per second. Session Time-Out - Set a threshold value. The default value of timeout is 10 seconds.
	Port Scan Detection
Port Scan Detection	 Click to enable / disable the port scan defense. If enabled, Port Scan Threshold - Set a threshold value. The default values of threshold is 2000 packets per second.
	Others
Select All	Click to select and enable all items under Others.
	Spoofing Defense
ARP Spoofing Defense Log	Click to enable / disable the store the ARP log to Syslog.
ARP Spoofing Defense	 There are two types for spoofing defense. Block ARP replies with inconsistent source MAC address Block ARP replies with inconsistent Decline VRRP MAC into ARP table

IP Spoofing Defense	 There are two types for spoofing defense. Block IP packet from WAN with Inconsistent source IP addresses
	 Block IP replies from LAN with Inconsistent source IP addresses
Cancel	Discard current modification and keep current configuration.
Clear All	Discard current modification and return to factory default setting.
Save	Save the current settings.

9.4.7.5 APP Enforcement

The APP Enforcement Filter can be used to prevent users from using undesirable or inappropriate network applications such as online chat and peer-to-peer programs. The filter works by detecting and blocking network traffic of applications by means of traffic patterns.

General Setup	2865ac_001DAA41DF78 / Configuratio	n / Firewall	Ø
Default Rule	+Add 📋 Delete		
Filter Rules	Index	Profile Name	
DoS Defense			
APP Enforcement			
URL Content Filter			

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

2865Lac_1449BC0D8F00 / Configuration / Firewall			Set to Factory Default 🛛 🖓
Index	1		
Profile Name			
Instant Message	AIM Login	□ AliWW	Ares
Select All Clear All	🗌 BaiduHi	Facebook/Instagram	Fetion
	🗌 GaduGadu Protocol		□ iSpQ
	□ КС	LINE	LinkedIn
	Paltalk	PocoCall	Qnext
	□ Signal	Slack	Snapchat
	Telegram	Tencent QQ	🗆 uc
	WebIM URLs	U WhatsApp	WhatsApp Call
VoIP	RC Voice	Skype/Teams	TeamSpeak
Select All Clear All	TelTel	WeChat	
P2P	Ares	BitTorrent	ClubBox
Select All Clear All	eDonkey	FastTrack	Gnutella
	Huntmine	🗌 Киwo	OpenFT
	OpenNap	Pando	SoulSeek
	🗌 Vagaa	Xunlei(Thunder)	
Protocol	BGP	DNS	FTP
Select All Clear All	GIT	□ H.323	□ HTTP
	IBM Informix	IRM DR2	ПІСМР
			Cancel Save

ltem	Description
Index	Displays the index number of the profile.
Profile Name	Displays the name of the profile.
Select All	Click to select all of the items on this page.
Clear All	Click to deselect all selected items.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.

9.4.7.6 URL Content Filter

The URL Content Filter scans URL strings in HTTP requests for predefined keywords to restrict browsing activities.

			Set to Factory Default
URL Access Control	URL Access Control Action	Web Feature	Web Feature Action
false	Pass	false	Pass
<body><center> The requ</center></body>			
page has been blocked by URL Co Filter.Please contact your systematic systematic structure of the systematic systemati	em		
administrator for further informatio	n.		
			Default Message Save

These parameters are explained as follows:

ltem	Description
+Add	Click to create a new UCF profile.
Delete	Click to remove the selected UCF profile.
Default Message	Click to reset the administration message to the factory default.
Save	Save the current settings.

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

65ac_001DAA41DF	F78 / Configuration / Firewa	all Set to Factory Default	: Ø
URL Content Filter	Profile		
Index	1		
Profile Name			
Priority		Either: URL Access Control First	
Log		Block 👻	
URL Access Contro	ol		
URL Access Cont	trol	D	
Prevent web acc	cess from IP address	D	
Action		Pass Block	
Index	Keyword Object	Action	
1	None	▼ + Add	
Index	Keyword Group	Action	
1	None	▼ + Add	
Exception List	C	D	
		Cancel Se	ave

ltem	Description		
	URL Content Filter Profile		
Index	Displays the index number of the UCF profile.		

Profile Name	Displays the name of the UCF profile.
Priority	Select the order of evaluation of URL Access Control and Web Feature.
Log	Select the access attempts (None, Pass, Block or All) to be recorded on Syslog.
	URL Access Control
URL Access Control	Click to enable or disable the URL access control.
Prevent web access from IP Address	Click to enable or disable the function of preventing users from circumventing URL Access Control.
Action	This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First.
	Pass - Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked
	Block - Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed.
Keyword Object	Index - Displays the index number of keyword object profile.
Table	Keyword Object - Displays the name of the keyword object profile.
	Action - +Add - Click to add a new entry to specify a keyword object profile.
Keyword Group Table	Index - Displays the index number of keyword group profile.
	Keyword Group - Displays the name of the keyword group profile.
	Action (+Add) - Click to add a new entry to specify a keyword group profile.
Exception List	It is available when URL Access Control is enabled.
	Index - Displays the index number of exception object profile.
	Exception Keyword Object /Group - Displays the name of the exception keyword object/group profile.
	Action (+Add) - Click to add a new entry to specify an exception keyword object / group profile.
	Web Feature
Web Feature Restriction	Click to enable or disable the web feature restriction function.
Action	Pass - Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects.
	Block - Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects.
File Extension	Choose one of the profiles for passing or blocking the file downloading.
Cookie, Proxy,	Click to enable or disable cookie function.
Upload	If enabled, it can block cookies from Internet websites.
Proxy	Click to enable or disable proxy function. If enabled, it can block web proxy servers that relay HTTP traffic.
Upload	Click to enable or disable upload function.
	If enabled, it can block HTTP uploads from the LAN to the Internet.
Cancel	Discard current modification and return to previous page.

Save	Save the current settings and return to previous page.
	Save

9.4.7.7 Web Content Filter

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

General Setup	2865ac_001DAA41DF78 / Configuration / Firewall Set to Factory Default 🖓							
Default Rule	Web Content Filter License Not A	Web Content Filter License Not Activated						
Filter Rules	+Add 🗊 Delete	+Add 🔋 Delete						
DoS Defense	Index	Profile Name	Log	Action	Black/White List:Action			
APP Enforcement	0 1	Default	Block	Block	Block			
URL Content Filter								
Web Content Filter								
DNS Filter	Cache	L1+L2 Cache	*					
Diagnose	Administration Message	«body» «center» «br»-br requested Web page-th «br=0 %URL% «br=has been bio %DL% «br=has been bio Legend: %SIPM - Source IP, (%DL% - URL% - URL %CL% - Category, Name	> from %SIP% is categorized with cked by %RNAME%					
					Default Message			

ltem	Description
Set to Factory Default	Clear all profile settings.
+Add	Click to create a new WCF profile.
Delete	Click to remove the selected WCF profile.
Index	Displays the index number of the WCF profile.
Profile Name	Displays the name of the WCF profile.
Log	Displays the type (Pass or Block or All) of the log to be recorded.
Action	Displays the type (Pass or Block) of the action selected.
Black/White List	Displays the action to be taken when a WCF matches keyword group and object selections.
Cache	None – The router verifies every HTTP URL requested by communicating with the WCF server on the Internet.
	L1 – The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs.
	L2 – After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server.
	L1+L2 Cache – The router will utilize both L1 and L2 caches.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box.
Default Message	Click to reset the administration message to the factory default.

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

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

2927ac_1449BC30C3	2927ac_1449BC30C3F0 / Configuration / Firewall		
Web Content Filte	er Profile		
Index	2		
Profile Name			
Syslog	Block	~	
Action	Pass Block		
White/Black List			
Black/White List	\bigcirc		
Action	Pass Block		
Index	Keyword Object	Action	
1	None	+ Add	
Index	Keyword Group	Action	
1	None	+ Add	
			Cancel Save

ltem	Description
	Web Content Filter Profile
Index	Displays the index number of the WCF profile.
Profile Name	Displays the name of the WCF profile.
Syslog	Displays the type (Pass or Block or All) of the log to be recorded.
Action	Pass - Only passed access attempts will be recorded in Syslog. Block - Only blocked access attempts will be recorded in Syslog.
	White/Black List
Black/White List	Click to enable or disable the function of Black/White List. Keyword objects and groups can be applied to the URL to override WCF category filtering.
Action	Action to take when a URL matches keyword group and object selections. Pass - Allow access to the URL. Block - Disallow access to the URL.
Keyword Object Table	Index - Displays the index number of keyword object profile. Keyword Object - Displays the name of the keyword object profile. Action - +Add - Click to add a new entry to specify a keyword object profile.
Keyword Group Table	Index - Displays the index number of keyword group profile. Keyword Group - Displays the name of the keyword group profile. Action (+Add) - Click to add a new entry to specify a keyword group profile.
	Selections for Security, Parent Control, Productivity, General Use
Select/Clear All	Click to select or deselect all items under Category Selection.

Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.7.8 DNS Filter

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames.

← Configuration	2865ac_001DAA000000 / C	onfiguration / Firewall			Set to Factory Default 🛛 🕾
General Setup	+ Add				
Default Rale	Index	Profile Name	DNS Syslog	DNS WCF	DNS UCF
Fitter Rules	C 1		Block	None	None
DoS Defense					
APP Enforcement	DNS Filter Local Settin	Ig			
UR. Content Filter	DNS Fitter	Ø			
Web Content Filler	Systog	None			
1011 Filling	WCF	None	÷		
Diagreese	UCF				
	UCF	None	~		
	Administration Message	Web page obc- fr -brothat is cating blocked by WRN -onder Linear card Legend: %SPN: Source IP.6r	-bro-bro-bro-bro-bro-bro-bro- om %SDP%-bro-bro-f%LRK% ontzed with %CL%-bro-has been MMCN DMS Filter-po-Please anni-sitematricetae for fuelbar. desp: %URMM %- Bouter Name		
					10 Default Message Save

These parameters are explained as follows:

ltem	Description
+Add	Click to add a new DNS filter profile.
Delete	Click to remove the selected DNS filter profile.
Index	Displays the index number of the DNS filter profile.
Profile Name	Displays the name of the DNS filter profile.
DNS Syslog	Displays the filtering type (Block, Pass, All or None) of the DNS syslog.
DNS WCF	Displays the name of the WCF profile.
DNS UCF	Displays the name of the UCF profile.
	DNS Filter Local Setting
DNS Filter	Click to enable / disable the DNS filter function.
Syslog	Select the filtering type (Block, Pass, All or None) of the DNS syslog.
WCF	Select a WCF profile.
UCF	Select a UCF profile.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box.
Default Message	Click to reset the administration message to the factory default.
Save	Save the current settings.

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

INS Filter		
Index	Y.	
2rnfile Namo		
yslog	Block 🗸	
ICF	None	
JCF	None	
NS Security Setting		
lock DoT (DNS over TLS)		
tock DoH (DNS over HTTPS)		
efault DoH Servers		
Sustamized Doll Server (Up to 8)		

ltem	Description
	DNS Filter
Index	Displays the index number of the DNS filter profile.
Profile Name	Enter a name of the DNS filter profile.
Syslog	Select the filtering type (Block, Pass, All or None) of the DNS syslog.
WCF	Select a WCF profile.
UCF	Select a UCF profile.
	DNS Security Setting
Block DoT	Select to block the DNS inquiry (plain text) encrypted through TLS (security protocol).
Block DoH	Select to block the DNS inquiry (plain text) encrypted through HTTPS (security protocol).
Default DoH Servers	Check the box to select the service provider(s) for the DoH server.
Customized DoH Server	Check the box to select the service provider(defined in String Object) for the DoH server.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.7.9 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet.

← Configuration	2865ac_001DA	A000000 / Configuration	I / Firewall			¢.
General Setup	Firewall Dia	agnose				
Default Rule						
Filter Rules	Mode		UDP-	~		
DoS Delense	Direction		From LAN	N		
APP Enforcement	IP Ver		1Pv4	*		
1318. Content Filler	LAN IP		192.168.1.12			
Web Content Filter	LAN Port		0			
ONS TIME	LAN MAC		00:00:00:00:00:00			
Dispara	WANIP		0.00.0			
	WAN Port.		0			
					Analyze Reset Save	
	() Note: • Pag	use set "Mode" and save first b	elone modily Packet & Reylocci.			
	Packet & Pa	yload				
	Index	Enable	Direction	Payload Type	Payload Data	TCP Flag
	1	Enable	AtoB	CUSTOMIZE		
	2	Dtsable	AtoB-	CUSTOMIZE		
	() Note:					
	+ This	is threwall two test which needs	setop WAN and plug cable in.			

ltem	Description
	Firewall FwDiagnose
Mode	Specify the service type (ICMP, UDP, TCP) of the packet.
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test.
IP Ver	Select the type of the IP address (IPv4/IPv6).
LAN IP	Enter the IPv4/IPv6 address of the packet's source.
LAN Port	Enter the port number of the packet's source.
LAN MAC	Enter the MAC address of the packet's source.
WAN IP	Enter the IPv4/IPv6 address of the packet's destination.
WAN Port	Enter the IPv4/IPv6 address of the packet's destination.
Analyze	Execute the test and analyze the result.
Reset	Reset the diagnose settings.
	Packet & Payload
Index	Displays the index number of the profile.
Enable	Displays if the profile is enabled or disabled.
Direction	The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet.
Payload Type	Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET).
Payload Data	It is available when Customize is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transferred with protocol (ICMP/UDP/TCP) which is different to Type

	setting.
Save	Save the current settings.

Click the index number (1 - 5) to configure detailed settings for Packet & Payload.

DrayTek / Configuration / Firewall		C
Packet & Payload		
Packet	1	
Enable	Enable Disable	
Direction	AtoB BtoA	
Payload Type	CUSTOMIZE ~	
Payload		
	Cancel Sa	ve

ltem	Description
Packet	Display the index number of the profile.
Enable	Enable - Enable this profile. Disable - Disable this profile.
Direction	Select the direction for the second packet.AtoBBtoA
Payload Type	Select the mode (CUSTOMIZE, Trace Route, DNS Query).
Payload	It is available when Customize is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transferred with protocol (ICMP/UDP/TCP) which is different to Type setting.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.8 User Management

9.4.8.1 General Setup

Global settings for User Management can be configured in this section.

	Configu	ration / User Management		
ae Ppolite ae Group	Mode Selection			
ay Online Status	Mode	Hole Basing User-Rased		
	Authentication page			
	Web Authentication	HTTP HITPS		
	Display IP Enable	Login Page Greeting		
	per construction of the	nog bei that pops up atter saccessful login.		
	Landing page		Set to Factory Default	
	Landing Page	 -shady data-1sample wind ow location="https://www.draytek.com" bt= though 		

ltem	Description
	Mode Selection
Mode	Rule-Based - Router applies filter rules configured in Firewall>>General Setup and Filter Rule. User-Based - Router applies filter rules configured in User Management>>User Profile.
	Authentication page
Web Authentication	 Set the Web protocol for the web authentication page. HTTP HTTPS
Login Page Greeting	Click to be redirected to Configuration>>Admin Account >> Login Page Greeting,
Display IP Enable	Click to enable or disable the function. If enabled, the IP address of the client will be shown on the tracking window.
	Landing page
Landing Page	HTML code to be shown on the Login Page Greeting.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.8.2 User Profile

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

General Setup		-	/ Configurat	tion / Use	r Managemer	nt					С
	Index	Enable This Account	User Name	Password	Idle Timeout	Max User Login	External Server Authentication	Log	Pop Browser Tracking Window	Anthentication:Web	Authentical
User Group	1	true	admin		0	9	None	None	faise	true	true
tser Online Status	2	true	Dial-In User		0	0	None	None	talso	true	talse
	2	false			10	0	None	None	true:	true	true

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

/ Configur	ation / User Management	
ieneral Settings		
index	1	
nable This Account		
Jsername	admin	
Password	Ø	
og	None ~	
external Server Authentication	None ~	
ogin Settings		
dle Timeout	0	
lax User Login	0	
uthentication: Web		
uthentication: Alert Tool		
uthentication:Telnet		
		Cancel Save

ltem	Description
	General Settings
Index	Displays the index number of the user profile.
Enable This Account	Click to enable or disable this user profile.
Username	Enter the login name of this user profile.
Password	Enter the password of this user profile.
Log	Select which activities (None, Login, Event or All) of the user can be recorded by Syslog.
External Server Authentication	The router will authenticate dial-in users using either a built-in (None) or external service (LDAP, Radius or TACACS+).
	Login Settings
Idle Timeout	If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will

	need to re-authenticate before Internet access is once again allowed.
Max Llaar Lagin	
Max User Login	Enter the maximum number of concurrent logins allowed for this profile.
Authentication:Web	Click to enable or disable the function. If enabled, user will need to authenticate by entering a username and password when attempting to access an external website for the first time The user will be redirected to the external website after a successful authentication.
Authentication:Alert	Click to enable or disable the function.
Tool	If enabled, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed.
Authentication:Telne	Click to enable or disable the function.
t	If enabled, the user can authenticate by logging in to the router using telnet.
Landing Page	Click to enable or disable the function.
	If enabled, when a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in 6.3.8.1 General Setup.
Auto Logout(minutes)	This account will be forced to logout after a certain time set here.
Pop Browser	Click to enable or disable the function.
Tracking Window	If enabled, a browser window will pop up showing the session time remaining.
	Quota Policy
Login Permission Schedule 1/2/3/4	Enter four sets of time schedule for your request.
Time Quota Enable	Click to enable or disable the function.
Time Quota:Mins	Specify the amount of time (after a successful authentication).
	Click + / - to increase / decrease the time quota for this profile.
Data Quota Enable	Click to enable or disable the function.
Data Quota Value	Specify the amount of data (after a successful authentication).
	Click + / - to increase / decrease the data quota for this profile.
	Reset Quota Automatically
Enable	Click to enable or disable the function.
Default Time Quota(Mins)	Enter value for default time quota.
Default Data Quota(MB)	Enter value for default data quota.
Quota reset	When login permission schedule expired - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.
	At the start time of Schedule -
	 Quota reset schedule - Specify a time schedule index number for this profile.

	Internal Services
Internal RADIUS	Click to enable or disable the function.
Local 802.1x	Click to enable or disable the function.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.8.3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in Firewall>>General Setup.

General Setup	-	/ Configuration / User Manag	ement	C
User Profile	index	Name	Selected User Objects	
	1			
User Online Status	-			

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

2865ac_001DAA151EB8 / Configuration	/ UserManagement	Q
User Group		
Name		
Selected User Objects		
🖹 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description
Name	Enter a name for identifying this user group.
Selected User Objects	Use the drop down menu to select the user object(s).
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.8.4 User Online Status

This page displays the users that are currently logged into the router. The list refreshes periodically to show the most up-to-date information.

2000		0 / Configuration)	User Managemer	nt					C
index	User	IP Address	Profile	Last LogIn Time	Expired Time	Data Quota	Idle Time	Action	
1	admin	192.168.1.10	admin	02-10 10:10:05	Unlimited	Unlimited	Unlimited	Block Logout	Delete
-									
	index 1	10-12-12-12-12-12-12-12-12-12-12-12-12-12-	Index User IP Address	Index User IP Address Profile		Index User IPAddress Profile Last Login Time Expired Time	Index User (P-Address Profile Last Login Time Expired Time Data Quota	index User IP Address Profile Last Legin Time Expired Time Data Quota. Idle Time	index User IPAddress Profile Last Login Time Expired Time Data Quota Hele Time Action 1 admin 197,158,1.10 admin 07.10 (0:10:05 Untimited Untimited Ellock Logout

ltem	Description
User	The name of the user that is logged on. Clicking this will bring up the following page which allows setting time and data quotas of the user.
	For details, refer to the description on the Enable Time Quota and Enable Data Quota items in the User Profile section.
IP Address	IP LAN address of the device that initiated the login.
Profile	Name of the user profile. If the logged-in user is a VPN user, Dial-in User will be displayed. Otherwise it will be the same as User.
Last Login Time	The most recent login time of the user.
Expired Time	The expiration time of the current login session.
Data Quota	Display the quota for data transmission.
	The remaining data quota of this login session.
Idle Time	Amount of time the session has been idled.
Action	Block – Stops user from accessing the Internet.
	Unblock –Resumes Internet access of a blocked user.
	Logout – Terminates the current login session.
	Delete – Removes the user entry from the User Online Status page.

9.4.9 Object Setting

9.4.9.1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with objects and bind them with groups for using conveniently.

	2865ac_001DA	AA151EB8 / Configura	ation / Objects Setting			
	Index	Name	Interface	Address Type	Information	
	1		Any	Subnet Address		
	2		Any	Subnet Address		
	3		Any	Subnet Address		
	4		Any	Subnet Address		
	5		Any	Subnet Address		
	6		Any	Subnet Address		
	7		Any	Subnet Address		
SMS Service Object	8		Any	Subnet Address		
Mail Service Object	9		Any	Subnet Address		
Notification Object	10		Any	Subnet Address		
- String Object	11		Any	Subnet Address		
Country Object	12		Any	Subnet Address		
	13		Any	Subnet Address		
	14		Any	Subnet Address		
	① Note:• Excla	imation mark (!) on Inf	ormation column means that Inv	ert Selection is enabled.		

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

/ Configuratio	n / Objects Setting	Set to Factory Default	C
Index	1		
Name	RD Department 🗸		
Interface	Any ~		
Address Type	Range Address 🗸 🗸		
Start IP Address	192.168.1.9		
End IP Address	192.168.1.9		
Invert Selection			
🗓 Clear		Cancel Sa	ive

ltem	Description				
Index	Displays the index number of the IP object profile.				
Name	Enter the name of the IP object profile.				
Interface	Select the network interface on which the IP address or addresses are to be found.				
Address Type	Any Address - Object covers all IP addresses.				
	Mac Address - Object contains a MAC address.				
	 MAC Address - Enter the MAC address. 				
	Range Address - Object covers a range of IP addresses.				
	• Start IP Address - Enter an IP address as the starting point.				
	• End IP Address - Enter an IP address as the ending point.				
	Single Address - Object covers one IP address.				
	• Start IP Address - Enter an IP address as the starting point.				
	Subnet Address - Object covers a range of IP addresses specified in subnet notation.				
	• Start IP Address - Enter an IP address as the starting point.				
	• Subnet Mask - Enter the subnet mask.				
Invert Selection	Click to enable or disable the function.				
	If enabled, all addresses except the ones entered above will be used.				
Cancel	Discard current modification and return to previous page.				
Save	Save the current settings and return to previous page.				

9.4.9.2 IP Group

Multiple IP Objects can be placed into an IP Group.

bject	2865ac_001D	AA151EB8 / Configur	ation / Objects Setting		
	Index	Name	Interface	Selected IP Objects	
	1		Any		
	2		Any		
	3		Any		
	4		Any		
	5		Any		
	6		Any		
	7		Any		
S Service Object	8		Any		
I Service Object	9		Any		
ification Object	10		Any		
ng Object	11		Any		
	12		Any		
	13		Any		
	14		Any		
	15		Any		
	16		Any		

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

/ Configuration	/ Objects Setting	Set to Factory Default C ⁴
Index	1	
Name		
Interface	Any ~	
Selected IP Objects		
🗊 Clear		Cancel Save

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the IP object profile.
Name	Enter the name of the IP object profile.
Interface	Select WAN, LAN or Any to filter IP objects.
Selected IP Objects	Use the drop down menu to select the IP object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.3 IPv6 Object

Up to 64 IPv6 Objects can be created.

	2865ac_0010	AA151EB8 / Configura	tion / Objects Setting			
	Index	Name	Address Type	Information	Match Type	Prefix
	1		Subnet Address	:		0
	2		Subnet Address	:		0
	3		Subnet Address			0
	4		Subnet Address	::	**	0
	5		Subnet Address	:		0
	6		Subnet Address	:		0
	7		Subnet Address		-	0
ice Object	8		Subnet Address	:	-	0
ice Object	9		Subnet Address	::		0
on Object	10		Subnet Address	::		0
	11		Subnet Address	:	**	0
	12		Subnet Address	:	**	0
	13		Subnet Address			0
	14		Subnet Address	::		0
	15		Subnet Address			0
	16		Subnet Address	:	-	0

To configure the IPv6 object profile, move the mouse cursor to any entry and click to open the setting page.

/ Co	figuration / Objects Setting	Set to Factory Default
Index		
Name	1	
Address Type	Subnet Address ~	
Start IP Address	:	
Prefix Length	0	
nvert Selection	\bigcirc	
l Clear		Cancel Save
🗊 Clear		Cancel Sa

ltem	Description
Index	Displays the index number of the IPv6 object profile.
Name	Enter the name of the IPv6 object profile.
Address Type	Any Address - Object covers all IPv6 addresses.
	 Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	Mac Address - Object contains a MAC address.
	 Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	• MAC Address - Enter the MAC address.
	Range Address - Object covers a range of IPv6 addresses.
	 Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	• Start IP Address - Enter an IPv6 address as the starting point.
	• End IP Address - Enter an IPv6 address as the ending point.
	 Invert Selection - If enabled, all addresses except the ones entered above will be used.

	Single Address - Object covers one IPv6 address.
	 Match Type - Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
	• Start IP Address - Enter an IPv6 address as the starting point.
	 Invert Selection - If enabled, all addresses except the ones entered above will be used.
	Subnet Address - Object covers a range of IPv6 addresses specified in subnet notation.
	• Start IP Address - Enter an IPv6 address as the starting point.
	 Prefix Length - Enter IPv6 prefix length, if Address type is Subnet Address.
	 Invert Selection - If enabled, all addresses except the ones entered above will be used.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.4 IPv6 Group

Multiple IPv6 Objects can be placed into an IPv6 Group.

IP Object	2	/ Configuration /	Objects Setting	Set to Factory Default	C
IP Group	index	Name	Selected iPv6 Objects		
IPv6 Object	1				
	2				
	3				
Service Type Object	4				
Service Type Group	5				
Keyword Object	1				
	8				
Keyword Group	9				
File Extension Object	10				
	u				
SMS Service Object	12				
Mail Service Object	13				
Notification Object	14				
Notification Object	15				
String Object	16				
Country Object	11				
and a color	18				
	19				
	20				
	21				
	22				
	23				
	24				
	25				
	76				

To configure the IPv6 group profile, move the mouse cursor to any entry and click to open the setting page.

F0 / Configuration	n / Objects Setting	Set to Factory Default	C
Index	1		
Name Selected IPv6 Objects			
⑪ Clear		Cancel Sa	ve

ltem	Description
Index	Displays the index number of the IPv6 group profile.
Name	Enter the name of the IPv6 group profile.
Selected IPv6 Object	Use the drop down menu to select the IPv6 object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.5 Service Type Object

Up to 96 Service Type Objects can be created.

IP Group	Index	Name	Protocol	Protocol Number	Source Port Option	Source Port From
IPv6 Object	1		Any	0	-	0
IPv6 Group	2		Any	0	=	0
Service Type Object	3		Any	0	-	0
Service Type Group	4		Any	0		0
Keyword Object	5		Any	0	-	0
Keyword Group	6		Any	0	=	0
File Extension Object	7		Any	0	-	0
SMS Service Object	8		Any	0		0
Mail Service Object	9		Any	0		0
Notification Object	10		Any	0	-	0
	11		Any	0	=	0
String Object	12		Any	0	=	0
Country Object	13		Any	0	-	0
	14		Any	0		0
	15		Any	0	-	0
	16		Any	0	=	0
	-					

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

/	Configuration / Objects Setting	Set to Factory D
ndex	1	
ame		
rotocol		
1010001	Any ~	
	ІСМР	
Clear	IGMP	Cancel
	ТСР	
	UDP	
	TCP/UDP	
	ICMPv6	
	Other	

ltem	Description
Index	Displays the index number of the service type object profile.
Name	Enter the name of the service type object profile.
Protocol	Choose a protocol to which this profile applies.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.6 Service Type Group

Multiple Service Type Objects can be placed into a Service Type Group.

IP Object.	and the second second	Configuration / Objects Setting		Set to Factory Default	C
IP Group	index	Name	Selected Service Type Objects		
IPv6 Object	T				
IPv6 Group	2				
	4				
	5				
Keyword Object	7				
Keyword Group	8				
File Extension Object	10				
SMS Service Object	11				
Mall Service Object	13				
Notification Object	14 15				
String Object	16				
Country Object	17 18				
	19 20				
	21				
	22				
	23				
	24				
	25				
	26				

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

2 D / Configuration	on / Objects Setting	Set to Factory Default C
Index	1	
Selected Service Type Objects		
🗓 Clear		Cancel Save

ltem	Description
Index	Displays the index number of the service type group profile.
Name	Enter the name of the service type group profile.
Selected Service Type Objects	Use the drop down menu to select the service type object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.7 Keyword Object

200 Keyword Object Profiles can be created for use as blacklists or white lists in CSM >>URL Content Filter Profile and Web Content Filter Profile.

IP Object	2 Configuration / Objects	Setting	Set to Factory Default
IP Group	Index Name	Contents	
Pv6 Object	1		
Pv6 Group	2		
rws Group	3		
ervice Type Object	4		
	5.		
ervice Type Group	5		
	7		
	8		
eyword Group	9		
le Extension Object	10.		
	11		
MS Service Object	12.		
tail Service Object	12		
iotification Object	14		
odination Colyse	15.		
tring Object	16		
ountry Object	17		
DOUDY COJECT	18		
	19		
	20		
	21		
	22		
	23		
	24		
	25		
	76		

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

) / Configuration	n / Objects Setting	Set to Factory Default	C
Index	1		
Name			
Contents			
D Clear		Cancel Sav	ve

ltem	Description
Index	Displays the index number of the keyword object profile.
Name	Enter the name of the keyword object profile.
Contents	Enter the keywords to be matched. Up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

IP Object	2) / Configuration /	Objects Setting	Set to Factory Default
IP Group.	Index	Name	Selected Keyword Objects	
IPv6 Object	1			
IPv5Group	2			
Service Type Object	4			
Service Type Group	5			
Keyword Object	Ť.			
	8			
File Extension Object	10			
SMS Service Object	11			
Mail Service Object	13			
Notification Object	14			
String Object	15 16			
Country Object	17			
Loundry Unject	18			
	19			
	20			
	21			
	22			
	23			
	24			
	25			
-	76			

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

0 / Configuration	I / Objects Setting	Set to Factory Default	C
Index	,		
Name	1		
Selected Keyword Objects			
🗊 Clear		Cancel Sav	ve

ltem	Description
Index	Displays the index number of the keyword group profile.
Name	Enter the name of the keyword group profile.
Selected Keyword Objects	Use the drop down menu to select the keyword object(s).
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.9 File Extension Object

Up to 8 File Extension Objects can be set up for use.

IP Object	2 2 0 / Cor	figuration / Objects Setting	Set to Factory Default C
IP Group	mdex	Profile Name	
IPv6 Object	1		
IPv6 Group	2		
Service Type Object	3		
Service Type Group	4		
Keyword Object	5		
Keyword Group	6		
	8		
SMS Service Object			
Mail Service Object			
Notification Object			
Siring Object			

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

/ Configuration	on / Objects Setting	Set to Factory Default	C
File Extension Object Setup			
Index	1		
Profile Name			
Categories			
Index	Categary Name		
1	Image		
2	Video		
3	Audio		
4	Java		
5	ActiveX		
6	Compression		
7	Execution		
8	P2P		
9	Document		
🗊 Clear		Cancel Sa	ve

ltem	Description
Index	Displays the index number of the file extension object profile.
Profile Name	Enter the name of the file extension object profile.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.10 SMS Service Object

Up to 10 SMS Service Objects can be set up for use.

II ¹ Object	21	3F0 / Configurati	on / Objects Setting	Set to Factory Default 📿
IP Group	Index	Profile Name	Service Provider	
IPv6 Object	I		kotsms.com.tw (TW)	
IPv6 Group	2		kotsms.com.tw (TW)	
Service Type Object	3		kotsms.com.tw (TW)	
Service Type Group	4		kotsms.com.tw (TW)	
Keyword Object	5		liotsms.com.tw (TW)	
Keyword Group	6		kotsmis.com.tw (TW)	
File Extension Object	7 8		kotsms.com.tw (TW) kotsms.com.tw (TW)	
	9	Custom 1		
Mail Service Object	10.	Custom 2		
Notification Object				
String Object				

To configure the SMS service object profile, move the mouse cursor to index 1 to index 8 and click to open the setting page.

Index	1	
Profile Name	Local number	
Service Provider	kotsms.com.tw(TW) ~	
Connection Protocol	HTTP HTTPS	
Username	abc5026	
Password	Φ	
Quota	3	
Sending Interval	3	
 6 Note: Only one message can be sent during the "! If the "Sending Interval" was set to 0, there 	iending interval" time. Wil be no limitation.	
🖹 Clear		

ltem	Description
Index	Displays the index number of the SMS service object profile.
Profile Name	Enter the name of the SMS service object profile.
Service Provider Select a Service Provider from the dropdown list.	
Connection Protocol	Select HTTP or HTTPs.
Username Enter a name to log in to the server.	
Password Enter a password to log in to the server.	
Quota	Set the remaining number of text messages allowed to be sent.
Sending Interval	Set the minimum amount of time, in seconds, to wait between sending SMS messages.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

To configure the customized SMS service object profile, move the mouse cursor to index 9 to index 10 and click to open the setting page.

	9 Custom 1			
Profile Name Service Provider				
Service Provider	Custom 1			
Exact URL				
	1			
S	Please contact with your SMS provide to get the exact URL string gybulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0? username=###btUser###&password=###btPwd###&msisdn=#	###btDest###&message=###btMsg###		
Server Response				
Username				
Password	•			
Quota	10			
Sending Interval	3			
ß Note:				
 Only one message can be sent during the "Se If the "Sending Interval" was set to 0, there was set to 0. 	ending Interval" time. vill be no limitation.			
💼 Clear			Cancel	Save

ltem	Description	
Index	Displays the index number of the SMS service object profile.	
Profile Name	Displays the name of the SMS service object profile.	
Service Provider	Enter an identifier for the service provider. Maximum length is 23 characters.	
Exact URL	Enter the URL for the SMS service.	
Username	Enter a name to log in to the service.	
Password	Enter a password to log in to the service.	
Quota	Set the remaining number of text messages allowed to be sent.	
Sending Interval	Set the minimum amount of time, in seconds, to wait between sending SMS messages.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.11 Mail Service Object

Up to 10 Mail Service Objects can be set up for use.

IP Object	-	0 / Configuration	/ Objects Setting		Set to Factory Default 🛛 🥲
IP Gmap	index	Profile Name	SMTP service	SMTP Port	sender Address
IPv6 Object	3			0	
IPv6 Group	2			0.	
Service Type Object	3			a.	
Service Type Group	4			Ω.	
Keyward Object	ŝ			Ċ.	
Keyword Group	6			0	
File Extension Object	7			0.	
SMS Service Object	8			0	
All Service Object	9			0	
	10			0.	
Notification Object	-				
String Object					
Country Object					

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

Index	1	
Profile Name		
Interface	Any ~	
SMTP Server		
SMTP Port	0	
Sender Address		
Connection Security	Plaintext ~	
Authentication	\bigcirc	
Username		
Password	©	
Sending Interval	0	
 8 Note: Only one mail can be sent of If the "Sending Interval" was 	luring the "Sending Interval" time. is set to 0, there will be no limitation.	
) Clear		Cancel

ltem	Description	
Index	Displays the index number of the mail service object profile.	
Profile Name	Enter the name of the mail service object profile.	
SMTP Server	Enter the IP address of the SMTP server.	
SMTP Port	Enter the port number of the SMTP server.	

Sender Address	Enter the e-mail address of the sender.
Connection Security	Use Plaintext, StartTLS or SSL to communicate with the SMTP server.
Authentication	Click to enable or disable the function. Username - Enter a name for authentication. Password - Enter the password for authentication.
Sending Interval	Specify the minimum amount of time, in seconds, to wait between sending e-mail messages.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.9.12 Notification Object

Up to 8 Notification Objects can be set up for use.

IP Object	-	Configuration (Configuration	on / Objects Setting	Set to Factory Default
Р Group	Index	Profile Name	Settings	
Pv6 Object	4			
V6 Group	2			
ervice Type Object	3			
ervice Type Group	4			
eyword Object	5			
eyword Group	6			
le Extension Object	8			
AS Service Object				
ail Service Object				
tring Object				
Country Object				

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

ndex	1	
Profile Name		
VAN		
VAN	Disconnected Reconnected	
/PN Tunnel	Disconnected	
	Reconnected	
emperature Alert	USB Out of Range	
VAN Budget	LimitReached	
entral VPN Management	CPE Offline	
	CPE Config Backup Fail	
	CPE Config Restore Fail	
	CPE Firmware Upgrade Fail	
	CPE VPN Profile Setup Fail	
ligh Availability	Failover Occurred Config Sync Fail Router Unstable	
Clear		Cance
		Calice

ltem	Description	
Index	Displays the index number of the notification object profile.	
Profile Name	Enter the name of the mail service object profile.	
Check boxes	Select the states to be monitored.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.13 String Object

Set string profiles which will be applied in route policy.

IP Object	2	1 0	Configuration / Objects Setting		Set to Factory Default	C
IP Group						
IPv6 Object		index	string			
IPv6 Group	0.	1	level 2			
Service Type Object		2				
Service Type Group						_
Keyword Object						
Keyword Group						
File Extension Object						
SMS Service Object						
Mail Service Object						
Notification Object						
Country Object						

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

2 F0 / Configuration	/ Objects Setting	Set to Factory Default	C
Index String	2 (Max.253 chars.)		
î Clear		Cancel Sav	ve

Item	Description	
Index	Displays the index number of the string object profile.	
String	Enter a string.	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.9.14 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

IP Object	BF0 / Configuration / Objects S	Setting	Set to Factory Default
P Group	Index Name	Selected Objects	
Pv6 Object	1		
Pv6 Group	2 3		
iervice Type Object	4		
iervice Type Group	5		
leyword Object	7		
Keyword Group	8		
le Extension Object	10		
MS Service Object	11		
tail Service Object	13		
lotification Object	14		
string Object	15		

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

D / Configuration	n / Objects Setting	Set to Factory Default	G
Index	1		
Name			
Selected Country Objects			
දි Note: • The maximum number of Se	lected Countries is 16.		
			_
🗊 Clear		Cancel Sa	ve

ltem	Description	
Index	Displays the index number of the country object profile.	
Name	Enter the name of the mail country object profile.	
Selected Country Objects	Use the drop down menu to select the country object(s).	
Clear	Clear all modifications on this page.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.10 QoS

9.4.10.1 Hardware QoS General Setup

Before using Hardware QoS, enable Hardware Acceleration first.

ftware QoS General Setup	Index	Enable	Direction	Egress Bandwidth	Class1	Class2	Class3	Others	
S Class	WAN1	Disabled	Egress (Upload)	1000000 Kbps	25 %	25%	25 %	25 %	
S Service Type	WANZ	Disabled	Egress (Upload)	1000000 Kbps	25 %	25%	25.96	25.96	
^a Prioritization	Port1	Disabled	Egress (Download)	1000000 Kbps	25 %	25.%	25.%	25.96.	
Jutbound Traffic	Port2	Disabled	Egress (Download	1000000 Kbps	25 %	25 %	25.96	25 %	
	Port3	Disabled	Egress (Download	1000000 Kbps	25.%	25 %	25 %	25.%	
	Port4	Disabled	Egress (Download	1000000 Kbps	25 %	25 %	25.96	25 %	
	Port5	Disabled	Egress (Download)	1000000 Kbps	25%	25.96	25.96	25.96	

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

0 / Configu	uration / QoS	C
Hardware QoS General Setu	q	
Index	1	
Enable		
Egress Bandwidth (Kbps)	1000000	
Class1 Ratio (%)	25	
Class2 Ratio (%)	25	
Class3 Ratio (%)	25	
Others Ratio (%)	25	
		Cancel Save

Item	Description
Index	Display the index number of the interface.
Enable	Click to enable or disable this QoS policy.
Egress Bandwidth(Kbps)	Set the outbound bandwidth of the WAN/LAN.
Class1 Ratio ~ Class3 Ratio	Set the percentage of bandwidth reserved for each class.
Others Ratio	Set the percentage of bandwidth for others.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10.2 Software QoS General Setup

	index	Enable	Direction	ingress Bandwidth	Egress Bandwidth	ciass 1	class 2	class 3	others	Enable UDP Bandwidth Control	status
oS Class	WAN1	taba-	вотн	100000	100000	25.98	25.9%	25.95	25.9h	talsas	Status
а5 Беглісе Туре	WAN2	false	BOTH	100000	100000	25 %	25.96	25.%	25 96	false	Status
alP Prioritization	WAN3.	Jalse	BOTH	100000	100000	25 %	25.96	25%	25.96	Talso.	Status
ng Outbound Irallic	WAN4	false	BOTH	100000	100000	25 %	25%	25%	25.96	false	Status
	WAN5	false	BOTH	100000	100000	25.%	25.%	25%	25 %	false	Status
	WANG	false	BOTH	100000	100000	25.96	25.96	25.06	25 %	falke	Status
	-					_					

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

/ Configu	ration / QoS	C
Interface Settings		
WAN	1	
QoS Policy Enable	\square	
Direction	BOTH ~	
Inbound Bandwidth (kbps)	100000	
Outbound Bandwidth (kbps)	100000	
Bandwidth Reserved for eac	ch Class	
Class 1 Ratio (%)	25	
Class 2 Ratio (%)	25	
Class 3 Ratio (%)	25	
Others (%)	25	
Advanced Settings		
	Cancel	l Save

ltem	Description
	Interface Settings
WAN	Display the index number of the WAN interface.
QoS Policy Enable	Click to enable or disable this QoS policy.
Direction	Use the drop-down list to set the direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both).
Inbound Bandwidth(kbps)	Set the inbound bandwidth of the WAN.
Outbound	Set the outbound bandwidth of the WAN.

Bandwidth(kbps)							
	Bandwidth Reserved for each Class						
Class 1 ~3 Ratio (%)	Set the percentage of bandwidth reserved for each class.						
Others (%)	Set the percentage of bandwidth reserved for others.						
	Advanced Settings						
UDP Bandwidth	Click to enable or disable this function.						
Control	If enabled, the router will restrict the bandwidth available to UDP traffic.						
UDP Bandwidth Ratio(%)	Enter a percentage value.						
Prioritize Outbound	Click to enable or disable this function.						
ΤΟΡ ΑΟΚ	If enabled, the router will give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent.						
Cancel	Discard current modification and return to previous page.						
Save	Save the current settings and return to previous page.						

9.4.10.3 QoS Class

Configure Class 1 to Class 3 with detailed settings.

Software QoS General Setup	Index	Enable Tag Packel AS	Tag Packet AS	
	1	false	Default	
nS Service Type	2	false	Default	
alP Prioritization	3	false	Default	
ag Outbound Trallic	-			

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

Index	ACT	Local Address Type	Local Start IP	Local End IP	Local Mask	Remote Address Type	Remote Start IP	Remote End IP	Re	
1	false	Any	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0	
2	true	Any	0.0.0.0	0.0.0.0	0.0.0.0	Any	0.0.0.0	0.0.0.0	0.0	
3	true	Any	0.0.0.0	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0	
4	true	Any	0.0.00	255.255.255.255	0.0.0.0	Any	0.0.0.0	255.255.255.255	0.0	
5	false		0.0.0.0	0.0.0.0	0.0.0.0		0.0.0.0	0.0.0.0	0.0	

Then, click any index number to open the setting page.

/ Configuration / QoS		
\bigcirc		
IPv4 ~		
~		
~		
Any Select DiffServ CodePoint		
Nothing selected ~		
~		
×		
	Cancel Save	
	IPv4 ~ ~ Any Select DiffServ CodePoint Nothing selected ~ ~ ~	

Item	Description
ACT	Click to enable or disable this function.
IP Version	Select IPv4 or IPv6.
Local Address Type	 Set the remote (WAN) IP address or address range for the rule. Any - The rule covers all IP addresses. Range - The rule covers a range of IP addresses. Local Start IP Address - Enter an IP address as the starting point. Local End IP Address - Enter an IP address as the ending point. Single - The rule covers one IP address. Local Start IP Address - Enter an IP address as the starting point. Subnet - The rule covers a range of IP addresses specified in subnet notation. Local Start IP Address - Enter an IP address as the starting point. Subnet - The rule covers a range of IP addresses specified in subnet notation. Local Start IP Address - Enter an IP address as the starting point. Group and Object - The rules covers a range of IP address specified in a group or object profile.
Remote Address Type	 Set the remote (WAN) IP address or address range for the rule. Any - The rule covers all IP addresses. Range - The rule covers a range of IP addresses. Remote Start IP - Enter an IP address as the starting point. Remote End IP - Enter an IP address as the ending point. Single - The rule covers one IP address. Remote Start IP - Enter an IP address as the starting point. Subnet - The rule covers a range of IP address as the starting point. Subnet - The rule covers a range of IP address as the starting point. Remote Start IP - Enter an IP address as the starting point. Subnet - The rule covers a range of IP address as the starting point. Remote Start IP - Enter an IP address as the starting point. Remote Start IP - Enter an IP address as the starting point. Remote Mask - Enter the subnet mask for the above IP address. Group and Object - The rules covers a range of IP address specified in a group or object profile.

DiffServ CodePoint	Select Any or Select DiffServ CodePoint. If DiffServ CodePoint selected, set the precedence of packets to which this rule applies.
Service Type	Choose a service type to which this rule applies.
Change to Class	Specify a class for the QoS class profile.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.10.4 QoS Service Type

Hardware QuS General Setup	-	19	configuration / QoS				C
Software QoS General Setup	index	Name	Protocol Type	Port Type	Port Number From	Port Number To	
QoS Class	1				0	0	
Quil ханлан Тура	-						_
VolP Prioritization							
Tag Outbound Traffic							
- Income of the local division of the local							

To configure the QoS service type profile, move the mouse cursor to any entry and click to open the following page.

Index	1	
Name		
Service Type	TCP/UDP ~	
Port Type	Single Range ✓	
Port Number Start	0	
Port Number End	0	
D Clear		Ca

ltem	Description
Index	Display the index number of the profile.
Name	Enter a name of this profile.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Type	Single - Set a port number for this profile.
	 Port Number Start - Enter the starting port number.
	Range - You have to set the starting port number and the end porting number on the boxes below.
	 Port Number Start - Enter the starting port number.
	• Port Number End - Enter the end porting number.
Clear	Clear all modifications on this page.

Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.10.5 VoIP Prioritization

Hardware QoS General Setup	-	FO / Configuratio	n / Qo5						Ċ
Software QoS General Setup QuS Class	Enable the First Prior	ity for VolP SIP/RTP	•						
QoS Service Type	SIP UDP Port		5060						
Sen Providentier									
Jug Outbound Isatts.	VolP QoS Status							Cancel	Save
	NO. LAN IP	Peer IP V	a Delay(MS)	Jitter(MS)	Packet Loss(%)	start Time	Duration(sec)		status
	-			Nerd	atha awailaibile				

These parameters are explained as follows:

ltem	Description
Enable the First Priority for VoIP SIP/RTP	Click to enable or disable the function. If enabled, VoIP traffic will be received with the highest priority.
SIP UDP Port	Set a port number to be monitored for SIP traffic.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.
VoIP QoS Status	Displays current VoIP QoS status.

9.4.10.6 Tag Outbound Traffic

Tag the outgoing traffic with the DSCP or Precedence value.

Hardware QoS General Setup	-	FO / Configuration / QoS		Ċ
Software QoS General Setup	Class	Enable Tag Packet AS	Tag Packet AS	
QoS Class	1	false	Default	
ooS Service Type	2	lalse	Default	
VolP Prioritization	3	false	Default	
lag Curibound Traffic				

To configure the tag outbound traffic profile, move the mouse cursor to any entry and click to open the following page.

F0 / Configuration	n / QoS		C
Class	1		
Enable			
Add DSCP or Precedence Value	Default ~		
		Ca	ancel Save

These parameters are explained as follows:

ltem	Description
Class	Display the index number of the class.
Enable	Click to enable or disable the profile.
Add DSCP or Precedence Value	Use the drop-down list to choose the value for applying the DSCP or precedence value for each class.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11 Applications

9.4.11.1 Dynamic DNS

The Vigor router supports a wide range of DDNS providers, such as DynDNS, No-IP.com, DtDNS, and ChangeIP. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.

														View Log Ford	09.0100300
LAN ONS/ONS Forwarding															
DNS Security	Dyn	amic DNS Se	tup												
Schedule	Enabl	e		0											
External RADIUS	Auto-	Update Interval		14400											
Internal RADIUS															
Edemal TACACS+															Save
Active Directory /LDAP															-
	Index	Enable Account	Service Provider	Service Type	Host Name	Domain Name	Login Name	Password	Wildcards	Backup MX	Mail Extender	WAN Interface	Determine WAN IP	Provider Host	Service
	A	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
GMP	2	faise	dyn.com_(www.dyn.com)	Dynamic					false	fatse		WAN1_First	WAN_IP		
Wake on LAN	3	false	dyn.com_(www.dyn.com)	Dynamic					false	false		WAN1_First	WAN IP		
SMS / Mail Alert Service	4	faise	dyn.com_(www.dyn.com)	Dynamic					false	false		WANI_First	WAN_IP		
	5	false	dyn.com_(www.dyn.com)	Dynamic					tatse	false		WAN1_First	WAN_IP		
Bonjour	6	false	dyn.com (www.dyn.com)	Dynamic					false	false		WAN1_First	WAN_IP		
High Availability															

To configure the DDNS profile, move the mouse cursor to any entry (1 to 6) and click to open the following page.

able Account		
IAN Interface	WAN1 First ~	
ervice Provider	dyn.com (www.dyn.com) ~	
ervice Type	Dynamic ~	
ost Name		
omain Name	~	
ogin Name		
assword	•	
lildcards	\bigcirc	
ackup MX	\bigcirc	
all Extender		
etermine WAN IP	WAN IP ~	
lear		Cance

ltem	Description
Enable Account	Click to enable or disable the account.
WAN Interface	Select the WAN interface to monitor for IP address changes.
Service Provider	Select the DDNS provider. If your DDNS provider is not listed, select User-Defined and manually configure the profile.
Service Type	Select the service type (Custom, Dynamic, Static) that matches that of your DynDNS account.
Host Name	Enter the IP address or the domain name of the host which provides related service.
Domain Name	Select one domain name.
Login Name	Enter the login name of the DDNS account.
Password	Enter the password of the DDNS account.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please enter the name in this area. Such mail server will be used as backup mail exchange.
Determine WAN IP	 There are two methods offered for you to choose: WAN IP - The IP address of the router's WAN interface will be used. Internet IP - The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.
Let's Encrypt certificate	Status – Display the certificate status. Auto Renew – Switch the toggle to enable the function of making the system update the certificate automatically.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.2 LAN DNS/DNS Forwarding

LAN DNS allows the network administrator to override standard DNS resolutions for selecting domain addresses. The router will respond to queries on matched domain addresses with custom IP addresses.

Dynamic DNS	-		Configuration / Application	ans		Set to Factory Default	C
	index	Enable	Profile Name	Domain Name	DNS Server IP Address	Cname	
	1	Talse					
Schedule	2	false					
External RADIUS	3	laise					
	4.1	false					
Internal NADIUS	5	fatso					
Edemail TACACS+	6	false					
Active Directory /LDAP	1	falso					
	8	false					
UPnP	9.1	fable					
IGMP	10	false					
Wake on LAN/WAN	23	false					
SMS / Mail Alert Service	12	fatse					
	13	faise					
Bonjour	14	false					
High Availability	15	false					
local 802,1X General Setup	16	false					
	17	false					
	18	false					
	19	false					
	20.	faise					
	21	false					
	22	false					

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

Profile	Type DNS Forwarding ~ Domain Name	Enable	0
Domain Name	Domain Name	Profile	
		Туре	DNS Forwarding ~
DNS Server IP Address	DNS Server IP Address	Domain Name	
		DNS Server IP Address	

Or

Enable						
Profile						
Туре		LAN DNS ~				
Domain Name						
CNAME(Alias Domain Name)						
IP Address List						
	Index	IP Address	Same Subnet Reply	Action		
	1		\bigcirc	+ Add		

These parameters are explained as follows:

ltem [Description
Enable C	Click to enable or disable the profile.
Profile E	Enter a name to identify this profile.
Туре	Select LAN DNS or DNS Forwarding.
	Enter the domain name for the router to look for in DNS queries to intercept and reply to.
	Enter the IP address of the DNS server you want to use for DNS forwarding.
CNAME(Alias Domain E Name)	Enter a domain name alias for LAN DNS.
I	IP Address List
Index [Displays the index number of the IP address.
	The IP address entered here will be used for mapping with the domain name specified above.
Same Subnet Reply	Click to enable or disable the function.
	If enabled, the router will only respond to the DNS request which coming from the same subnet of the IP address specified in this entry.
	After entering the IP address, Click to save the setting and create a new entry.
Cancel [Discard current modification and return to previous page.
Save S	Save the current settings and return to previous page.

7.3.11.3 DNS Security

Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

Dynamic DHS	General	Setup						
LAN DNS / DNS Forwarding	Index	Interface	Enable	Primary DNS		Secondary DNS	Bogus DNS Reply	
	1	WAN1	faise	0.0.0.0		0.0.0.0	Pass	
Schedule	2	WAN2	false	0.0.0.0		0.0.0.0	Pass	
Edemal RADIUS	3	WAN3	false	0.0.0.0		0.0.0.0	Pass	
	4	WAN4	false	0.0.0.0		0.0.0.0	Pass	
Internial RADIUS	5	WANS	talise	0.0.0.0		0.0.0	Pass	
Edemai IACACS+	6	WANG	fatse	0.0.0		0.0.0.0	Pass	
Active Directory /LDNP	Domain	Diagnosis						
uPhp								
смр	Domai	n i						
Wake on LAN	Domai		IP	v4 IPv6				
SMS / Mall Alert Service	interfa		WA		~			
lonjour				H1	~			
High Aunilability	DNS Se	rver						
local 802.1X General Setup								
								Diagnose
	Domain Na	ame		IP Address	1	nterface	Verify Result	

ltem	Description
	General Setup

Index	Displays the index number of the WAN interface.
Interface	Displays the WAN interface name for which DNS security is to be configured.
Enable	Displays if the DNS security is enabled (true) or disabled (false).
Primary DNS	Displays the primary DNS server IP address in effect for this WAN.
Secondary DNS	Displays the secondary DNS server IP address in effect for this WAN.
Bogus DNS Reply	Displays the action to be taken for DNS responses that fail authentication. Pass – Pass DNS result. Drop – Do not pass DNS result.
	Domain Diagnosis
Domain	Enter domain address to be diagnosed.
Domain Type	Select the type of IP address to be looked up. IPv4 IPv6
Interface	Select the WAN port to be used for the lookup.
DNS Service	Enter the IPv4 / IPv6 address of the DNS server to be used for the lookup.
Diagnose	Click to begin DNS lookup.

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

2865ac_001DAA000000 / Configuration / A	pplications	C
General Setup		
Enable	0	
Interface	WAN1	
Bogus DNS Reply	Pass v Drop Pass	
	Canc	el Save

9.4.11.4 Schedule

Time schedules can be created and used with router features that support them, so that those features can be turned on and off automatically at preconfigured times.

LAN DNS / DNS Forwarding	Index	Enable	Comment	Time	Frequency
DNS Security Schedule	1	false		00:00 00:00	Sun.
External RADIUS	2	false		00:00 00:00	Sun.
	3	false		00:00 00:00	Sun.
	4	false		00:00 00:00	Sun.
	5	false		00:00 00:00	Sun.
SMS / Mail Alert Service Bonjour	6	false		00:00 00:00	Sun.
High Availability Local 802.1X General Setup	7	false		00:00 00:00	Sun.
Local auz. IX General Setup	8	false		00:00 00:00	Sun.
	9	false		00:00 00:00	Sun.
	10	false		00:00 00:00	Sun.
	11	false		00:00 00:00	Sun.
	12	false		00:00 00:00	Sun.
	13	false		00:00 00:00	Sun.
	14	false		00:00_00:00	Sun.

To configure the schedule profile, move the mouse cursor to any entry (1 to 15) and click to open the following page.

Enable						
Comment						
Start Date (yyyy-mm-dd)	2000 ~ - 1	✓ - 1				
Start Time (hh:mm)	0 ~ : 0	~				
Duration Time (hh:mm)	0 ~ : 0	~				
End Time (hh:mm)	0 : 0					
Action	Force On		~			
How Often	Weekdays		~			
Weekdays	🗆 Sun	Mon				
	🗹 Tue	🗹 Wed				
	🗹 Thu	Fri				
	🗆 Sat					
(i) Note:						
Comment can only contain A-Z	a-z 0-9 , . { } () ^ \$! ~ `					
1 Clear						Cano

ltem	Description
Enable	Click to enable or disable the schedule profile.
Comment	Enter a name to identify this schedule entry.
Start Date	Select the date when the entry comes into effect.
Start Time	Select the time when the schedule is triggered.

Duration Time	Select how long the action lasts when the scheduled is triggered.		
End Time	It will be calculated automatically when Start Time and Duration Time are configured well.		
Action	Specify the action to take when the schedule is triggered.Force On – The feature with which this schedule is associated will be turned on.Force Down – The feature with which this schedule is associated will be turned off.		
How Often	 Specify how frequently the schedule is triggered. Once - The schedule is triggered once, on the Start Date at the Start Time, for the Duration Time. Weekdays - The schedule will be triggered repeatedly, starting on the Start Date at the Start Time, on the selected days of the week, at the Start Time, for the Duration Time. Monthly, on date - The router will only execute the action applied such schedule on the date (1 to 28) of a month. Cycle duration - Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date. 		
Clear	Clear all modifications on this page.		
Cancel	Discard current modification and return to previous page.		
Save	Save the current settings and return to previous page.		

9.4.11.5 External RADIUS

Select External RADIUS to configure the router to use an external RADIUS server for user authentication.

LAN DNS / DNS Forwarding				
DNS Security	Primary Server			
Schedule	Enable	0		
External BADH/S	Enable Accounting	0		
Enterned TACACS+	Comments			
Active Directory /LDAP	RADIUS Request Interval	2		
UPnP	Primary Server			
KGMP	Secret		0	
Wake on LAN/WAN	Authentication Port	1912		
SMS / Mail Alert Service	Autrenoution For	1812		
Bonjour	Helry	2		
High Availability	Secondary Server			
Local 802.1X General Setup	Secondary Server			
	Secret		0	
	Authentication Port	1812		
				Save

These parameters are explained as follows:

ltem

	Primary Server
Enable	Click to enable or disable the server settings.
Enable Accounting	Click to enable or disable the accounting. RADIUS Accounting is a network customer billing mechanism for RADIUS server.
	If enabled, Vigor router will deliver accounting request (e.g., IP address, traffic from the client) to the specified RADIUS server periodically.
	Accounting Port - Set the UDP port number (1813 in default) as the accounting port.
	Disconnect Message Port - Set a UDP port number (3799 in default) for receiving the disconnected-request packets from the AAA server. Note that these packets have been accepted by the RADIUS server before being disconnected by the AAA server.
	Interim Update Interval - Set a value (10 minutes in default). It indicates the time between each transmittal of an interim update for a specific session.
Comments	Enter a brief description for this profile.
RADIUS Request Interval	Set a timeout value for the router waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again.
Primary Server	Enter the IP address of RADIUS server.
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Authentication Port	Enter the UDP port number that the RADIUS server is using.
Retry	Set the number of attempts to perform reconnection with RADIUS server.
	Secondary Server
Secondary Server	Enter the IP address of RADIUS server.
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Authentication Port	Enter the UDP port number that the RADIUS server is using.
Retry	Set the number of attempts to perform reconnection with RADIUS server.
Clear	Clear all modifications on this page.

9.4.11.6 Internal RADIUS

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication.

LAN DNS/DNS Forwarding	General Setup				
DHS SHORTY					
Schedule	10.00	-			
External RADIUS	Enable				
JORNOVAL ANNUARY	Authentication Port	1817			
External YACACS	Authentication Method	PAP Only			
Active Directory (LDAP	Support 802.1X Method	0			
UPnP	Authentication List				
Waka on LAN/WAN SMS/MailAkedService	Synchronize the Internal RADIUS user to 802.1X user list.	st to Local 💮			
Ponjour High Availability	Maintenance >> Internal 5	ich is enabled in User Management ≫-U iervice User List.	ser Profile will be listed here, and it sh	ows in the System	
Local 802.1X General Setup	 7. RADIUS Client Access List 	t is lind match.			
					Save
	RADIUS Client Access List				
	Index Client Access Enable	Client Access Shared Secret	Client Access IP Address	Client Access IP Mask	Client Access IPv6 Address
	1 talse		0.0.0.0	0.0.0.0	-
	2 false		0.0.0.0	0.0.0.0	
	3 Taluar		0000	6000	=

ltem	Description
	General Setup
Enable	Click to enable or disable the internal RADIUS server settings.
Authentication Port	Enter the UDP port for authentication messages.
Authentication Method	 Specify the way to authenticate the wireless client. PAP only PAP/CHAP/MS-CHAP/MS-CHAPv2
Support 802.1X Method	 Click to enable or disable the Support 802.1X Method function. EAP_TTLS/PAP EAP_TTLS/MSCHAP EAP_TTLS/MSCHAPv2 EAP_PEAP/MSCHAPv2
Authentication List	Use the drop down list to choose the use profile.
Synchronize Internal RADIUS user list to Local 802.1X user list	Users can be authenticated by RADIUS server and local 802.1X to get certain network service. It is not necessary to create new user profiles (containing user accounts and user passwords) for RADIUS and local 802.1X respectively. Simply select to update the 802.1X authentication list to match the RADIUS authentication list.
Save	Save the current settings
	RADIUS Client Access List
Client Access Enable	Displays the status (true or false) of the client entry. Only clients that meet the criteria configured in the access list are allowed

	to access the RADIUS server.
Client Access Shared Secret	Displays the text string that is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them.
Client Access IP Address	Displays the base address of the IP block.
Client Access IP Mask	Displays the IP mask to configure the size of the IP block.
Client Access IPv6 Address	Displays the base address of the IPv6 block.

To configure the profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

Enable			
Shared Secret		۵	
IP Address	0.0.0.0		
IP Mask	0.0.0.0		
IPv6 Address	**		
IPv6 Length	0		
			Cancel Sav

ltem	Description
Enable	Click to enable / disable the profile.
Shared Secret	Enter a text string. It is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them.
IP Address	Enter the base address of the IP block.
IP Mask	Enter the IP mask to configure the size of the IP block.
IPv6 Address	Enter the base address of the IPv6 block.
IPv6 Length	Enter the prefix length of the IPv6 block.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.7 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does.

LAN DNS / DNS Forwarding	0		
DNS Securey	Primary Server		
Schedule	Enable		
Faternal RADRES	Server IP Address	0.0.0.0	
Internal RADIUS			
	Destination Port	49	
Active Directory /LDAP	Туре	ASCII	
UPNP	Shared Secret		
KAND	Secondary Server		
Wake on LAN/WAN			
SMS / Mail Alert Service:	Server IP Address	0,0,0,0	
Bonjour	Destination Port	49	
High Availability	Туре	ASCII	
Local 802.1X General Setup	Shared Secret		
	1 Cieur		Save

ltem	Description
Enable	Click to enable / disable the external TACACS+ server settings.
Server IP Address	Enter the IP address of the TACACS+ server.
Destination Port	Enter a port number used by the TACACS+ server. Port 49 is most common.
Shared Secret	Enter a text string. It is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters.
Clear	Clear all modifications on this page.
Save	Save the current settings.

9.4.11.8 Active Directory/LDAP

Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

DNS/DNS Forwarding	General Setup				
Security	ouncial occup				
edule	Enable	O			
mal RADIUS	Bind Type	Simple Mode	:M ¹		
nal RADIUS	Server Address				
enal TACACS+	server nooress	IDv4 Iornsat (EX : 123.17.1.1)			
	Destination Port	389			
	Use SSL	0			
P					
e eo LAN/WAN					
/ Mail Alert Service	· · · · · · · · · · · · · · · · · · ·				
(our	Active Directory / LDAP	rofiles			
Availability				and the second second	
al 802.1X General Setup	index Name Common Na	ime identifier Distinguished Name	Additional Filter	Group Distinguished Name	
	2				
	3				
	1.11				
	4				
	4				
	4 5 6				

ltem	Description
	General Setup
Enable	Click to enable / disable the AD/LDAP function.
Bind Type	 Select from one of 3 bind types: Simple Mode – Initiate bind operation (authentication) without performing user search. Anonymous – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user search. Regular Mode – Same as Anonymous mode, except that the DN and password are sent to the server.
Server Address	Enter the network address of the LDAP server.
Destination Port	Enter a network port that the LDAP server listens on. The default ports are 389 for unsecured connections and 636 for LDAPS (LDAP over SSL) connections.
Use SSL	Click to enable or disable SSL. If enabled, the router will use Secure Sockets Layer (SSL) for LDAP traffic.
Regular DN	Enter the LDAP Distinguished Name for authentication if Bind Type is set to Regular Mode.
Regular Password	Enter the LDAP Password for authentication if Bind Type is set to Regular Mode.
Save	Save the current settings.
	Active Directory / LDAP Profiles

Index	Displays the index number of the profile. Up to 8 LDAP profiles can be configured.
Name	Displays the user-defined name that identifies this entry.
Distinguished Name	Displays the distinguished name (DN) configured in the profile.

To configure the profile, move the mouse cursor to any entry (1 to 8) and click to open the following page.

Name	
Common Name Identifier	
Base Distinguished Name	
Additional Filter	
Group Distinguished Name	
	Cancel

ltem	Description
Name	Enter a name that identifies this profile.
Common Name Identifier	Enter a common name attribute, which is typically "cn" in most LDAP configurations.
Base Distinguished Name	Enter a starting point of user search in the LDAP directory, for example, dc=draytek,dc=com.
Additional Filter	Additional filter to be applied to the search request to identify eligible users.
	For example,
	- "OpenLDAP: (gidNumber=500)"
Group Distinguished Name	The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.9 UPnP

The Vigor supports UPnP (Universal Plug and Play), which is a suite of network protocols that simplifies network configuration.

LAN DNS/DNS Forwarding	Enable UPnP Service	
DNS Security		Default WAN ~
Schedule		
Edemal RADIUS	Enable Connection Control Service	
Internal RADIUS	Enable Connection Status Service	
External TACACS+	① Note:	
Active Directory /LDAP	 To allow NAT pass through 	to a UPnP enabled client the connection control service must also be enabled. litles CVE-2020-12605, UPnP is not considered safe to use. Use it at your own
Line	risk.	
IGMP		
Wake on LAN/WAN	1 Clear	Save
SMS / Mail Alert Service	2.5	
Bonjour		
High Availability		
Local 802.1X General Setup		

ltem	Description
Enable UPnP Service	Click to enable or disable the UPnP function.
WAN Interface	Select the WAN port on which ports will be opened in response to UPnP commands.
Enable Connection Control Service	Click to enable or disable the connection control service.
Enable Connection Status Service	Click to enable or disable the connection status service.
Clear	Clear all modifications on this page.
Save	Save the current settings.

9.4.11.10 IGMP

Internet Group Management Protocol (IGMP) is an IPv4 communication protocol for establishing multicast group memberships.

amic DNS	IGMP Proxy		(D)						
NS/DNSForwarding	Interface		WANL		*				
Security	IGMP version		Auto		*				
hale									
mal RADIUS	General Query Interval E	seconds)	125						
mail RADIUS	Add PPP header		0						
emal IACACS+	Encopsulate	IGMP in PPPoE							
e Directory /LDAP			(D)						
	Enable IGMP sysing								
	IGMP Snooping		Ø						
/ Mail Alert Service									
	Working group								
n Availability	rection & Droop								
al 802.1X General Setup	Index	Group ID		P1	P2	PJ	P4	P5.	ĸ
					\wedge				
					No data available				

ltem	Description
IGMP Proxy	Click to enable or disable the IGMP proxy settings.
Interface	Select an interface for packets passing through.
IGMP version	At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe. Or choose Auto.
General Query Interval (seconds)	Set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router.
Add PPP header	Click to enable or disable the function.
	If you have no idea to enable or disable, simply contact your ISP providers.
Enable IGMP syslog	Click to enable or disable the function.
	If enabled, the router will store the IGMP status onto Syslog.
Enable IGMP	If enabled, the following option shall be configured.
Snooping	Enable IGMP Fast Leave - If enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message.
Save	Save the current settings.
	Working group
Group ID	Displays the ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1-PX	Displays the LAN ports that have IGMP hosts joined to this multicast group.

9.4.11.11 Wake on LAN / WAN

If you wish to be able to select the IP address of the Wake-on-LAN client, its MAC address must first be bound to a static IP address using the Bind IP to MAC function.

AN DNS / DNS Forwarding			
INS Security	Wake on LAN		
chedule	Wake by	MAC Address	
demal RADIUS	IP Address		
emai RADIUS			
ternal IACALS+	MAC Address		
tive Directory /LDAP		Wake Up	
que			
MP	Result		
ike on \$48/WAS			
S / Mail Alert Service	() Note:	ates with Bind IP to MAC function; only bound PCs can wake up through	
njour	 wake on LAW Integr 	ates with BING IP to MAC function, only bound PCs can wake up through	1995
gh Availability			
cal 807.1X General Setup	Wake on WAN		
	Enable Wake on WAN	a.	
	Wake on WAN Type	Any WAN IP Access List	
		and and a second second	
			Save

ltem	Description
	Wake on LAN
Wake by	To wake up the binded IP,
	 MAC Address - Enter the correct MAC address of the host in MAC Address boxes.
MAC Address	Enter any one of the MAC addresses of the bound PCs.
Wake Up	Click to wake up the selected device.
Result	Displays the result of WOL execution.
	Wake on WAN
Enable Wake on WAN	Click to enable or disable the function.
Wake on WAN Type	Set the path for the boot packet (sent by a mobile phone) to deliver to the remote device.
	Any WAN IP - Any WAN IP can be used as a path for waking the remote device.
	Access List - Enter the WAN IP address with the subnet mask. Later, use your mobile phone (installing an APP for sending the boot packets first) to connect to the Vigor router network. The boot packets will be transferred to the remote device via any WAN IP or the IP listed on Access List.
Save	Save the current settings.

9.4.11.12 SMS/Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Dynamic ONS	SMS Ale	ert					Set to Factory Defai
	1.00						
LAN DNS / DNS Forwarding	Index	SMS Enable	SMS Provider	SMS Recipient Number	SMS Notify Profile	SMS Schedule1	SMS Schedule2
DNS Security	1	fatse	1-Local number		1		
Schedule	2	false	1-Local number		1-		
Edemal RADIUS	3	fatse	1-Local number		1		
	4	false	1-Local number		I-		
Internal RADIUS	5	table	1-Local number		1		
Indermal INCACS	6	false	1-Local number		1-		
Active Directory /LDAP	T	false	1-Local number		1		
	8	false	1-Local number		1-		
UPnP	9	false	1-Local number		1-		
	10 (1) Not	false All the SMS Alert pro	1-Local number	; loterval" setting if they use the sa	1: ame SMS Provider.		
Wake on LAN 1988 - Mark Anna Service	() Not	a: All the SMS Alert pro		Interval [®] setting if they use the se	-		
Wake on LAN 1988 / Mask Astrik soredan Banjaur	() Not	a: All the SMS Alert pro		Interval" setting if they use the s	-		Set to Factory Defa
Maleo en LAN Alle I I de la Anne Anne Anne Anne Bongour High Availability	() Not	a: All the SMS Alert pro		Internal" setting if they use the so Mail Address	-	Mail Schedule I	Set to Factory Defa
Maleo en LAN Alle I I de la Anne Anne Anne Anne Bongour High Availability	Mail Ale	a: All the SMS Alert pro art	tiles share the same "Sending		ame.SMS Provider.	Mail Schedule I	
Maleo en LAN Alle I I de la Anne Anne Anne Anne Bongour High Availability	Mail Ale	ar All the SMS Alert pro art Mail Ecoble	Alles share the same "Sending Mail Service		anne SMS Providee Mail Notity Profile	Mait Schedule 1	
Maleo en LAN Alle I I de la Anne Anne Anne Anne Bongour High Availability	Mail Alo Index	ar All the SMS Alert pro ort Mall Enable faise	Rites share the same "Sending Mail Service 1-Mail, Notity		anne SMS Providee Med Nodly Profile L-	Mail Schedule I	
Wake on LAN Mill I black Konst onester Ranjaur Ranjaur	Mail Alo Index 1 Z	ne; All this SMS Alert pro ort Mail Enable false false	Allos share the same "Sending Mall Service 1-Mail_Notity 1-Mail_Notity		ann SMS Provider. Hell Notly hotte 1- 1-	Mail Schedyle 1	
Wake on LAN Mill I black Konst onester Ranjaur Ranjaur	Mail Alo Index 1 2 3	ns: All the SMS Allert pro ort Mail Feable False False False	Affles share the same "Sending Mail Service 1-Mail, Nootly 1-Mail, Nootly 1-Mail, Nootly		mm: SMS Provider. Mail Notly Profile 1- 1-	Mult Schedule I	
Wake on LAN Mill I black Konst onester Ranjaur Ranjaur	Mail Alo Index 1 2 3 4	er All the SMS Allert pro- ort false false false false false	Rics share the same 75 mding Mat Service 1-Mat, Northy 1-Mat, Northy 1-Mat, Northy 1-Mat, Northy 1-Mat, Northy		mer SMS Prinkler. Matt Notly Profile 1- 1- 1-	Mail Schedule 2	
Wake on LAN Mill I black Konst onester Ranjaur Ranjaur	Mail Alo Mail Alo Index 1 2 3 4 5	nt All the SMS Alext pro- ort Mail Enable False False False False False	Rikes schare the same 75-ending Mail Service 1-Hail, Notity 1-Hail, Notity 1-Hail, Notity 1-Hail, Notity 1-Hail, Notity		mme SMS Prinkibler. Kell Kooty Profile 1- 1- 1- 1-	Mult Schedule 3	
igan Wakens LAN Mark Falet Kens noorke Bangaa High haatiabay Local 802.1X Coveral Setup	Mail Alo Mail Alo Index 1 2 3 4 5 6	nt All the SMS Alert pro ort Mail Enable False False False False False False	Affles share the same "Sending Mail Service 1-Mail Northy 1-Mail Northy 1-Mail Northy 1-Mail Northy 1-Mail Northy 1-Mail Northy		Mail Konty Provider Kall Konty Protile I- I- I- I-	Mait Schedule I	Set to Factory Defai

These parameters are explained as follows:

ltem	Description
SMS Alert	It allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.
Mail Alert	It allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

To configure the SMS alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

2865ac_001DAA000000 / Configuration / Appl	cations	C
Enable	C	
SMS Provider	1 ~	
Recipient Number		
Notify Profile	1 ~	
Schedule 1		
Schedule 2		
		Cancel Save

ltem	Description
Enable	Click to enable or disable the SMS alert profile.
SMS Provider	Use the drop down list to choose SMS service provider.
Recipient Number	Enter the phone number of the one who will receive the SMS.

Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile.
Schedule 1 / 2	Enter the schedule number that the SMS will be sent out.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

To configure the mail alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

2865ac_001DAA000000 / Configuration / App	vlications	C
Enable		
Mail Service	1 ~	
Mail Address		
Notify Profile	1 ~	
Schedule 1		
Schedule 2		
	Cancel	ave

ltem	Description
Enable	Click to enable or disable the mail alert profile.
Mail Service	Use the drop down list to choose mail service object.
Mail Address	Enter the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile.
Schedule 1 / 2	Enter the schedule number (0~15) that the notification will be sent out.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.11.13 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.

LAN DNS / DNS Forwarding		-	
DNS Security	Enable Bonjour Service	C	
Schedule	HTTP Server	00	
External RADIUS	Telnet Server	B	
Internal RADJUS	FTP Server	0	
Edemal IACACS+			
Active Directory /LDAP	SSH Server		
UPnP	LPR Printer Server	CD.	
KSME ²			
Wake on LAN/WAN			Save
SMS / Mall Alert Service			

These parameters are explained as follows:

ltem	Description
Enable Bonjour Service	Click to enable or disable the Bonjour service. With bonjour service enabled, Vigor router can share the service (e.g., HTTP service, Telnet service, FTP service, SSH service, LRP Printer server and etc.) to the LAN clients.
Save	Save the current settings and return to previous page.

9.4.11.14 High Availability

The High Availability (HA) feature of the router provides redundancy of network resources, and reduces downtime in case of component failure.

a service of the serv			
Dynamic DNS	Contract and Contract	-	
LAN DNS/ UNSForwarding	Enable High Availability	0	
DNS Security	Redundancy Method	Active-Standby	÷
Schedule	General Setup		
Estermai RADLIS			
Internal RADIUS	Group ID	1	
External IACACS	Priority ID	10	
Active Directory /LDAP	Authentication Key	draytek	
use	Protocol	IPv4	~
KAP	Management Interface	LANI	*
Wake on LAN	Update DDNS	D	
SMS / Mail Alert Service			
Bonjour	Syslog	00	
	Config Sync		
Lincal M02.1X General Setup	Enable Config Sync (Max. Sync to 10 mouters)	D	
	Day	D	~
	Hour	0	~
	Minute	15	-
	WAN Settings	0	
		-	
A second s			

ltem	Description
Enable High	Click to enable or disable the HA function.

Availability	
Redundancy Method	Select the redundancy method (Hot-Standby or Active-Standby) for high availability.
	General Setup
Group ID	Enter a value (1~255). Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group.
Priority ID	Enter a value (1~30). Different routers must be configured with different IDs.
Authentication Key	Enter an authentication key up to 31 characters long.
Protocol	Select the IP protocol (IPv4 or IPv6) to be used for DARP.
Management Interface	Select the interface to be used for DARP negotiation between routers.
Update DDNS	Click to enable or disable the function. If enabled, the router will update the DDNS server for the secondary device when the primary router fails.
Syslog	Click to enable or disable the function. If enabled, the router will record required information on Syslog.
	Config Sync
Enable Config Sync	Click to enable or disable the Config Sync function.
Day / Hour / Minute	The primary router will synchronize its configuration with secondary routers at every specified time interval.
WAN Settings	Click to enable or disable the WAN settings. WAN settings will be excluded when executing configuration synchronization.
Enable Config Inherit	Click to enable or disable the function. The configuration inherits will be executed only when the device (router) plays the role of the master device. Once another device with the priority ID higher than this device is ready to take over the management as the master device, after acting as the primary master for a while, this device will sync the configuration to all
	members in the same group and return to the role of the backup device (secondary master). Config Inherit for () minute - Enter a value.
	Time Sync
Enable Time Sync	Click to enable or disable the function. Day / Hour / Minute - The primary router will synchronize its configuration with secondary routers at every specified time interval.
IPv4	Set IPv4 virtual IP for each LAN interface.
IPv6	Set IPv6 virtual IP for each LAN interface.
Save	Save the current settings and return to previous page.

To configure the IPv4 profile, move the mouse cursor to any entry and click to open the following page.

tions	
LAN1	
192.168.27.2	
	Cancel Save

To configure the IPv6 profile, move the mouse cursor to any entry and click to open the following page.

/ Configuration / Application	5	
Index	LAN1	
Enable		
Virtual IP	FE80::200:5EFF:FE00:101	

9.4.11.15 Local 802.1X General Setup

It allows you to configure general settings for Local 802.1X server built in Vigor router.

here.
Save

ltem	Description
Enable	Click to enable or disable the function.
EAP_TTLS/PAP	Click to enable or disable the EAP_TTLS/PAP server certificate.
EAP_TTLS/MSCHAP	Click to enable or disable the EAP_TTLS/MSCHAP server certificate.
EAP_TTLS/MSCHAPv2	Click to enable or disable the EAP_TTLS/MSCHAPv2 server certificate.
EAP_PEAP/MSCHAPv2	Click to enable or disable the EAP_PEAP/MSCHAPv2 server certificate.
Authentication List	Select user profiles.
Sync User Profile Settings to Internal Radius	Click to enable or disable the function. It will enable/disable setting for both Internal RADIUS and Local 802.1X synchronize for all of the user profiles.
Save	Save the current settings.

9.4.12 VPN

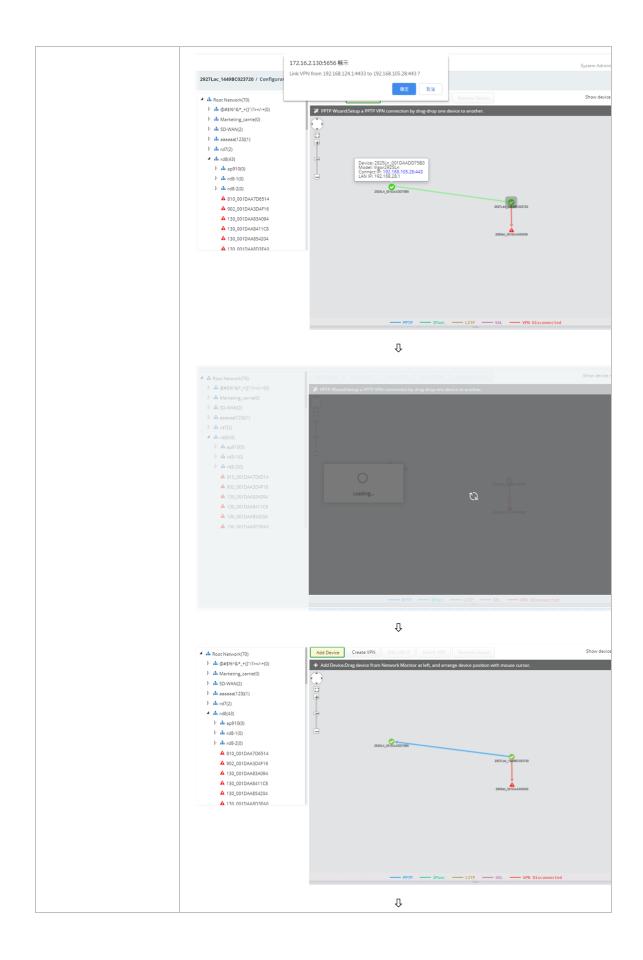
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

9.4.12.1 VPN Wizard

This page displays the VPN status related to the specified device.

/ Configuration	/ VPN	Ø
 ▲ Root Network(70) ▲ @#\$%^&*_+()*:><!--+(0)</li--> ▲ Marketing_carrie(0) ▲ SD-WAN(2) ▲ asasaa(123)(1) ▲ rd8(42) ▲ rd8(42)<!--</th--><th></th><th></th>		
	PPTP IPsec L2TP SSL VPN Disconnected	

Item Description	
Add Device	Click this button to add a device for building VPN connection. If you do not click this button first, you can not drag any device from Network view.
Create VPN Edit LAN Add Device Create VPN Edit LAN PPTP Wizard PPTP Wizard C Stand SSL Wizard SSL Wizard Customized Wizard	To build a quick VPN connection with PPTP/IPsec/L2TP/SSL/customized settings, simply click this button and choose one of the wizards for establishing VPN. Then, drag and drop one device to another. Here we take PPTP Wizard as an example.



	VPN Name: p_5B0_720 VPN Type: PPTP Encryption: MPPE TX Packets: 10 RX Packets: 1 TX Rate(Bps): 24 Up Time: 0:03:14
Edit LAN IP	If there is LAN IP segment conflict in VPN connection, please select that device and click this button to change LAN IP setting.
Unlink VPN	To disconnect a VPN connection, Click this button and move the mouse cursor to the VPN connection that you want to disconnect.
Remove Device	Click to remove the selected device without VPN connection.
Show device name	Click to display / hide the name of the device.

9.4.12.2 Remote Access Control

The Vigor router supports several protocols for VPNs, all of which can be enabled or disabled independently of one another.

distantial Arg and Childreni	Remote Access Control Set				
PPP General Setup	Remote Access Control Set	up			
SSL General Setup	PPTP VPN Service Enable	Ø			
IPsec General Setup	IPSec VPN Service Enable	CD			
IPsec Peer Identity	L2TP VPN Service Enable	0			
VPN Matcher	SSL VPN Service Enable	0			
OpenVPN	SSL VI'N Service Enable	00			
Win-Guard	OpenVPN Service Enable	00			
Hemote Dial-In User	WireGuard VPN Service Enable	CD			
LMI to LMI	and ensure that NAT Opp	an Ports or Port Redirectio	ron the LAN, disable any serv m is also configured rotection , and Block Unkno L2TP VPR Service		Save WireGuard Service

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

PPTP VPN Service	Click to enable or disable the service.			
Enable	If enabled, this VPN is easy to set up, has low overhead, and moderately secure.			
IPsec VPN Service Enable	Click to enable or disable the service.			
L2TP VPN Service Enable	Click to enable or disable the service.			
SSL VPN Service Enable	Click to enable or disable the service.			
OpenVPN Service	Click to enable or disable the service.			
Enable	If enabled, this VPN offers a convenient way for users to build VPN between local end and remote end.			
Enable WireGuard VPN Service	WireGuard is a secure, fast, and modern open-source VPN Protocol. This type of VPN connection is made by exchanging public keys and intends to be considerably more performant than OpenVPN.			
Save	Save the current settings			
	Bind to WAN			
Bind to WAN	Select the WAN interfaces to accept PPTP VPN, IPsec VPN, L2TP VPN, inbound SSL VPN, OpenVPN and WireGuard connections.			
Save	Save the current settings			

9.4.12.3 PPP General Setup

This page allows configuration of Point-to-Point Protocol (PPP) used by PPTP and L2TP VPN connections.

Remote Access Control 1999: General Vetup	PPP/MP Protocol		
55L General Setup	Dial-In PPP Authentication	PAP/CHAP/MS-CHAP/MS-CHAPv2 ~	
IPsec General Setup	Dial-In PPP Encryption(MPPE)	Optional_MPPE ~	
ll ^a ser Peer Identify	Mutual Authentication (PAP)		
VPN Matchey	Usemame		
OpenVPN			
WireGuard	Password		-
Remote Dial-In User	IP Address Assignment fo	or Dial-In Users when DHCP is disabled.	
AN to LAN			
Connection Management	Subnet Start IP Addr	IP Pool Counts	
	LAN1 192.168.1.200	50,	
	LAN2 192,168/2,200	50	
	LAN3 (92)168-3-2017	50	
	LAN4 1977-168-45200	50.	
	1485 192/168/5/200	50	
	LAN6 1972.168.6.200	50	
			Save

Item	Description
Dial-In PPP	PAP Only - Authenticate dial-in users using the PAP protocol only.

Authentication	PAP/CHAP/MS-CHAP/MS-CHAPv2 - Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP.
Dial-In PPP Encryption (MPPE)	Specifies if PPP encryption (MPPE) is to be used for dial-in VPN connections.
	Optional MPPE - MPPE is optional. If the VPN client supports MPPE, PPP data will be encrypted.
	Require MPPE (40/128bits) - Require PPP encryption for dial-in VPN connections. Both 40- and 128-bit encryption schemes are allowed. The remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.
	Maximum MPPE - Require 128-bit PPP encryption for all dial-in VPN connections.
Mutual Authentication (PAP)	Specifies if mutual authentication is to be used. Some VPN peers (e.g., certain Cisco routers) require bi-directional authentication used for providing stronger security.
	When mutual authentication is enabled, Username and Password fields should also be populated using values from the VPN peer. The maximum lengths of these fields are 23 and 19 characters, respectively.
	Click to enable or disable the function.
IP Address Assignment for Dial-In Users when DHCP is disabled	LAN1 - When the router's DHCP server is disabled, the router will assign IP addresses to dial-in VPN users starting with the IP address specified in Start IP Address. The total number of dial-in VPN IP addresses to be given out is specified in IP Pool Counts. LAN2 ~ LAN8 and DMZ will be available if it is enabled. Refer to
	LAN>>General Setup for enabling the LAN interface.
PPP Authentication Methods	The credentials to be used for PPP authentication will be obtained from the selected sources, in the following order:
	Remote Dial-in User – The usernames and passwords in VPN and Remote Access >> Remote Dial-in User section will be used.
	RADIUS – An external RADIUS server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.
	AD/LDAP – An Active Directory/LDAP server is to be used for authentication. Please be sure to configure AD and LDAP settings in Applications >> Active Directory/LDAP.
	TACACS+ – A TACACS+ server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.
PPTP LDAP Profile	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.
	However, if there is no profile listed, simply click the link of LDAP Profile link to create/add some new LDAP profiles you want.
While using Radius or LDAP Authentication	When the dial-in VPN user is authenticated using credentials from the Remote Dial-in User section, an IP address from the LAN specified in the user profile will be assigned. When the user is authenticated using credentials from other sources (RADIUS, AD, TACACS+), the assigned IP address will be drawn from the address pool of the LAN specified here.
VPN TCP maximum	Set the maximum segment size (MSS) for different VPN types.

segment size (MSS)	Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the IPsec VPN connection.
Save	Save the current settings.

9.4.12.4 SSL General Setup

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that encrypts traffic using SSL, which is the same technology used on secured websites. Because of SSL's prominence as an encryption protocol on the Internet, most networks have few restrictions on SSL traffic, and as a result SSL VPN is more likely to work when other VPN technologies experience difficulties due to obstacles such as firewalls and Network Address Translation (NAT).

note Access Control					
	SSL VPN General Setup				
General Setup					
	WAN Name		WAN Bind		
c General Setup	WAN1				
c Peer Identity	WAN2		•		
Matcher	WAND				
enVPN.	WAN4		•		
reGuard	WAN5		0		
mote Dial-In User	WANG		0		
to LAN					
nection Management	Port	443			
	Server Certificate	Default Certificate			
	_				
	() Note: Server Certificate fol	llow the Default Certificate now.Defau	Certificate can be configured at Certificate >>1	Local Services	
	List	now the penant certificate now penan	Certificate carrie comgared accertinate sys	COLUMNER WILLES	

These parameters are explained as follows:

ltem	Description
WAN	Select the WAN interfaces to accept inbound SSL VPN connections.
Port	The port to be used for SSL VPN server. The default setting is 443.
Save	Save the current settings.

9.4.12.5 IPsec General Setup

There are two phases of IPsec.

Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.

Phase 2: negotiation IPsec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

temate Access. Control	VPN IKE/IPsec General Setu	ID .		
PP General Setup				
SL General Setup.	(Dial-in settings for Remote Dial-In user IKE Authentication Method	s and LAN-to-LAN VPN Client with Dynamic (P.)		
	inc Automatication method			
ser. Peer Identity	Certificate	None	2 - 1	
N Matches	Preferred Local ID	Alternative_Subject_Name	~	
xen/VPN	General Pre-Shared Key			
reGuard	XAuth User Pre-Shared Key			
enote Dial-In User	AAUCH USER FRE-Shared Key			
NN to LAN	Security Method			
onresction Management	AH Enable	10		
	VPN TCP maximum segme	ent size (MSS)		
	IPSec.	1360		
	L2TP over IPSec	1360		
	GRE over IPSec	1360		
				Cancel Save

These parameters are explained as follows:

ltem	Description				
IKE Authentication Me	ethod				
Certificate	X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section.				
Preferred Local ID	Specify the preferred local ID information (Alternative Subject Name First or Subject Name First) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile).				
General Pre-Shared Key	Define the PSK key for general authentication.				
XAuth User Pre-Shared Key	Define the PSK key for IPsec XAuth authentication.				
Security Method	Available mthods include Basic, Medium and High. Each method offers different encryption, HMAC and DH Group.				
	Basic - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.				
	Medium - When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic.				
	High - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.				
AH Enable	It is available when Basic is selected as the security method.				
VPN TCP maximum	Set the maximum segment size (MSS) for different VPN types.				
segment size (MSS)	Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the IPsec VPN connection.				
Save	Save the current settings.				

9.4.12.6 IPsec Peer Identity

This screen allows creating profiles of subject alternative names (SANs) and distinguished names/subject names that can be used for IPsec peer authentication in LAN-to-LAN or remote user dial-in VPN connections.

Remote Access Control	Profile Name	Enable	Accept Type
PPP General Setup	777	false	Accept Any Peer ID
SSL General Setup			
IPsec General Setup			
IPsec Peer Identity			
VPN Matcher			
OpenVPN			
WireGuard			
Remote Dial-In User			
LAN to LAN			

To configure the IPsec Peer Identity profile, move the mouse cursor to any entry and click to open the following page.

ndex	1	
rofile Name	???	
nable		
ccept Type	Accept Subject Name 🗸	
ountry (C)	Accept Any Peer ID Accept Subject Alternative Name - IP address	
tate (ST)	Accept Subject Alternative Name - Domain Name Accept Subject Alternative Name - E-Mail	
ocation (L)	Accept Subject Name	
Prginization (O)		
Orginization Unit (OU)		
ommon Name (CN)		
mail (E)		

ltem	Description
Index	Display the index number of the profile.
Profile Name	A name that allows you to identify this profile.
Enable	Click to enable or disable the profile.
Accept Type	The router accepts the type and value of the specified subject alternative name as valid authentication. Supported subject alternative types are IP Address, Domain Name and E-Mail.
Accept Subject Name	When this option is selected, the router performs peer authentication by matching the values of the different subject name fields. These fields include Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

Cancel	Discard current modification and return to previous page.
Save	Save the current settings.

9.4.12.7 VPN Matcher

The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other.

Remote Access Control	VPN Matcher					
PPP General Setup SSI. General Setup	Enable					
IPiec General Setup	WAN Interface	WAN1_First	*			
IPse: Peer Identity	Server Ip	vpn-mätcher.dra	ytek.com			
OperNFN	Server Port	31503				
WireGuard	Router List Key			÷		
Remote Duil-In User	 Wote: You can get your Ro 	uter List Key on VFN Matcher Da	shboarti -			
Connection Management	STUN Server	Oetect				
	Group Device List	Get 1.64				
	Index 41 Description	- MAC - D	Remote Network	+ Model	L. Role	
			No data available			
					-	
						Cancel Save

ltem	Description
	VPN Matcher
Enable	Click to enable or disable the function of VPN Matcher Setup.
WAN Interface	The WAN interface to be used for dialing out to establish the VPN connection.
	WANx First –The Router first attempts to establish the VPN tunnel using this WAN interface. When that is unsuccessful, it will attempt to use other WAN interfaces.
	WANx Only –The Router will establish the VPN tunnel using this WAN interface only.
Server IP / Server Port	The IP address of the DrayTek VPN Matcher server is defined as "vpn-matcher.draytek.com" with the port number "31503".
Router List Key	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via VPN wizard.
STUN Server	Detect - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established.
	Group Device List
Get List	After entering the Authkey above, click to get available Vigor router which is within the same group as this device.

Cancel	Discard current modification and return to previous page.	
Save	Save the current settings.	

9.4.12.8 OpenVPN

9.4.12.8.1 OpenVPN Server Setup

OpenVPN requires the use of certificates. Certificates generated by the third party can be imported to your host and ready for use by Vigor router.

Remote Access Control	OpenVPN Server Setup Client Co	nfig	
PPP General Serup			
SSI. General Setup	General Setup		
IPsec General Selag	Enable UDP	0	
Parc Peer Identity	UDP Port	1194	
VPN Malcher	Enable TCP	•	
	TCP Port		
Windiscord	TCP Port	1194	
Remote Dial-In User	Cipher Algorithm	AE\$256-CBC	*
LANIDLAN	HMAC Algorithm	SHA256	÷
Connection Management	Certificate Authentication	•	
	Certificates Setup		
	Certificate Source	Uploading certificates to Router	w.
	Trust CA	default	~
	Server Certificate	None	~
	 Den/PN on Vigor Reute Den/PN on Vigor Reute Her climit state 	r only support TUN device interface isomethy	r Sa pin

Description
Description
General Setup
Click to enable or disable UDP protocol for OpenVPN connections. If enabled, please
UDP Port - Enter the UDP port number.
Click to enable or disable the TCP protocol for OpenVPN connections. If enabled, please
TCP Port - Enter the TCP port number.
Select the desired cipher algorithm.
Select the desired HMAC hash algorithm. It is used to validate the data integrity and authenticity of the VPN data.
Click to enable or disable the settings. If enabled, the router can validate that the client certificate was issued by a trusted CA.
Certificates Setup
 Select a source for the certificate to be used for OpenVPN. Router generated certificates - Router-generated certificates that will be used for OpenVPN. GENERATE - Click to generate a certificate. Delete all certificates - Click to remove all certificates generated by

	the router.
	Uploading certificates to Router - Third-party certificates will be used for OpenVPN.
	 Trust CA - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the Certificate Management >> Trusted CA Certificate page to perform the operation.
	 Server Certificate - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the Certificate Management >> Local Certificate page to perform the operation.
Save	Save the current settings.

9.4.12.8.2 Client Config

Create and export the configuration required for a remote OpenVPN client to connect to the router.

PP General Setup		
SL General Setup	Client Config	
Pace General Setup	Remote Server	IP Domain VPN Matcher
Purc Peer Identiliy	Transport Protocol	
PN Matcher	Auto Dial-Out	Eruble Disable
WireGuard	Set VPN as Default Gateway	Enable Disable
Remote Dial-In User	Cache password for auto reconnect	Enable Disable
LAN to LAN	File Name	Industrial Contract of Contrac
Convection Management	Client cert	.on
	Client key	Juy.
		Export
	 Please make sure that WAN can Eache password for auto rece Enables: Cache password in vi 	

These parameters are explained as follows:

ltem	Description	
	Client Config	
Remote Server	 There are three types of the remote server. IP - Use the numeric IP address as the server address. Domain - Use the domain as the server address. VPN Matcher - Use the VPN matcher as the server. 	
IP	If IP is selected as the remote server, enter the IP address of the server.	
Domain	If Domain is selected as the remote server, enter the domain name of the server.	
Transport Protocol	Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.	
Auto Dial-Out	Enable - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel. Disable - Select to disable the function.	

Set VPN as Default Gateway	Enable - If selected, the Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel. Disable - Select to disable the function.
Cache password for auto reconnect	Enable - OpenVPN will reconnect per hour. While reconnecting, the password is required. If the function is enabled, the password for OpenVPN connection will be kept and used by the Vigor system for reconnection every time. Disable - Select to disable the function.
File Name	Enter the filename of the configuration file to be downloaded from the router.
Client cert	Enter the filename of the client certificate obtained from 3rd party provider.
Client key	Enter the filename of the private key obtained from the 3rd party provider.
Export	Click to download the settings on this page as a file.

9.4.12.9 WireGuard

WireGuard is a secure, fast, simple, and modern open-source VPN Protocol. By using state-of-the-art cryptography, WireGuard can build a VPN by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., WireGuard VPN Client).

nate: Access Control	WireGuard			
General Setup				
General Setup	Private Key		Generate a Key Pair	
x General Setup	Public Key			
c Peer Identity				
Matcher	IP Address	192.168.1,1		
#WPN	Listen Port	51820		
note Dial-In User				Cancel Save
to LAN				
nection Management				

ltem	Description
Private Key	Displays the private key generated. Generate a Key Pair - Generate keys for the VPN server.
Public Key	It is required to be configured in the WireGuard VPN client router. After clicking Generate a Key Pair, the public key and a QR code representing the public key will be shown on this page
IP Address	Enter an IP address. Vigor router's LAN IP can be used as the WireGuard interface IP.
Listen Port	Enter a port number for WireGuard VPN server. The default number is 51820.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings

9.4.12.10 Remote Dial-In User

The system administrator can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

	index	Enable	Username	Status
PPP General Setup	1	Disable	222	Disable
SSL General Setup				10 5 171 5 20
IPsec General Setup				a 3, 171 2. 5
IPsec Peer Identity				
VPN Matcher	_			
OpenVPN				
WireGuard				
LAN to LAN				
Connection Management				

To configure the remote dial-in user profile, move the mouse cursor to any entry and click to open the following page.

Remote Dial In User		
User account and Authentica	ion	
ndex	1	
nable	\bigcirc	
Iultiple Concurrent Connections Allow	d 🚺	
dle Timeout	300	
Isername	???	
assword	•	
lobile One-Time Passwords(mOTP)		
i) Note:Username can not contain ch		
OpenVPN tunnel does not su Allowed Dial-In Type	port mOTP.	
РТР	0	
Psec Tunnel	0	
Clear		Cancel Save

ltem	Description
	User account and Authentication
Index	Displays the index number of the user account profile.
Enable	Click to enable or disable the user account profile.
Idle Timeout	Set the allowed idle time before the router disconnects the VPN connection.
Username	Set a username used for PPTP, L2TP or SSL Tunnel dial-in type

Password	Set a password used for PPTP, L2TP or SSL Tunnel dial-in type					
Mobile One-Time Passwords (mOTP)	Click to enable or disable one-time passwords (Mobile-OTP). If enabled, please PIN Code - Enter the code for authentication (e.g, 1234). Secret - Enter the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).					
	Allowed Dial-In type					
PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel	Click to enable (select) or disable (deselect) the PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel protocol.					
Specify Remote Node	Click to enable or disable the function. The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified.					
	Remote Client IP - Enter the IP address for remote client. Or Peer ID - Enter the string for peer ID.					
Netbios Naming	It is available when Specify Remote Node is disabled.					
Packet	Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.					
	 Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. 					
	 Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. 					
Multicast via VPN	It is available when Specify Remote Node is disabled.					
	Specifies whether to allow multicast packets to traverse through the VPN tunnel.					
	 Pass – Click this button to let multicast packets pass through the router. 					
	 Block – This is default setting. Click this button to let multicast packets be blocked by the router. 					
	Subnet					
Subnet	Select an interface.					
Assign Static IP	Click to enable or disable the function. IP Address - Enter a static IP address.					
Digital Signature(X.509)	It is available when Specify Remote Node is disabled. Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please Digital Signature(X.509) Index - Select an X.509 profile.					
	IKE Authentication Method					
Enable Pre-Shared Key	It is available when Specify Remote Node is enabled. Click to enable or disable the function. If enabled, please Pre-Shared Key - Enter an IKE PSK.					
Digital Signature(X.509)	Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please					

	Digital Signature(X.509) Index - Select an X.509 profile.
	IPsec Security Method
Medium(AH)	Click to enable or disable the function that data will be authenticated, but not be encrypted.
High(ESP)	The payload (data) will be encrypted and authenticated.
Local ID (optional)	Click to enable or disable the setting. Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.12.11 LAN to LAN

To create a LAN to LAN connection for the selected CPE, choose LAN to LAN. You can create up to 32 profiles for a CPE.

Remote Access Control	Alarm Enable	index	Enable	Always On	Default Route	Name	Remote Network	Remote Network Mask	Status
PP General Setup	disable	1	false	false	false	222	0.0.0.0	255.255.255.0	Othine
SL General Setup								61	5 111 5 1
Nac General Setup									
Psec Peer Identity	Pass packets fro	m LAN in Routi	ing mode to Vi	N .					
PN Matchev	Pass Packets to	WAN when the	VPN disconne	cts.	0				
lgscriVF%									
fireGuard	() Note:								
emote Dial-In Liser	 2.0nly 	1 Lan to Lan	profile can a	select "Always o elect "Default Re	ute".				
	 XXXXXX 	X:This Dial ou	at profile has	already joined fo	r VPN Load Balance r VPN Backup Mecha				
onnection Management	• XXXXX	X: (his Dial-or	at profile doe	s not join for VPI	TRUNK				

To create a new LAN to LAN profile, click the bottom one entry. To configure the LAN to LAN profile, move the mouse cursor to any entry and click to open the following page.

ommon Settings		
Index	1	
Enable this profile	\bigcirc	
Enable ACS Alarm	\bigcirc	
Profile Name	222	
Call Direction	Both Dial-Out Dial-In GRE Tunnel	
Dial-Out Through	WAN1 First ~	
Always on	\bigcirc	
Idle Timeout	300	
Quality Monitoring/Keep Alive	\bigcirc	
Netbios Naming Packet	Pass Block	
Multicast via VPN	Pass Block	
① (for some IGMP, IP-Camera,	DHCP Relayetc.)	
Dial-Out Settings		-
🗊 Clear		Cancel Sav

Item	Description
	Common Settings
Index	Displays the index number of the profile.
Enable this profile	Click to enable or disable this profile.
Enable ACS Alarm	Click to enable or disable the function.
Profile Name	Enter the name of the profile.
Call Direction	 Specify the allowed call direction of this LAN-to-LAN profile. Both Dial-Out Dial-In GRE Tunnel
Dial-Out Through	Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.
Always On	Click to enable or disable the function to maintain an always on dial-out connection. However, if disabled,Idle Timeout - Set a value if Always On is disabled. The router will close connection if no activity is observed in the VPN connection for this many seconds.
Quality Monitoring /Keep Alive	Click to enable or disable the function.
Netbios Naming Packet	 Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel. Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

	 Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. 						
Multicast via VPN	Specifies whether to allow multicast packets to traverse through the VPN tunnel.						
	 Pass – Click this button to let multicast packets pass through the router. 						
	 Block – This is default setting. Click this button to let multicast packets be blocked by the router. 						
	Dial-Out Settings						
VPN Server	Select the VPN protocol to be used.						
IPsec Tunnel Type	Select IKEv1 or IKEv2.						
Server IP/Host Name	Enter an IP address or DNS host name of remote VPN host.						
Dial-Out Schedule	Connect and disconnect according to schedule profiles.						
Profile	Up to four schedule profiles can be specified.						
	IKE Phase 1 Settings						
Mode	Select IKE phase 1 mode. Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session.						
	Main Mode						
	Aggressive Mode						
Authentication	Select PSK(IKE Pre-shared key) or X509 (X.509 digital signature).						
Pre-Shared Key	It is available when PSK is selected as Authentication. Enter the PSK.						
Local ID	Enter a string.						
Proposal Encryption	Select an proposal encryption mode.						
Proposal ECDH Group	Select an proposal ECDH group (e.g., G14).						
Proposal Authentication	Select SHA256 or SHA1.						
	IKE Phase 2 Settings						
Security Protocol	Select the dial-out protocol.						
	 ESP(High) 						
	AH(Medium)						
Proposal Encryption	Select an proposal encryption mode.						
Proposal Authentication	Select All, SHA256, SHA1 or None.						
	IKE Advanced Settings						
Phase 1 Key Lifetime	For security reason, the lifetime of key should be defined. The default value is 28800 seconds.						
Phase 2 Key Lifetime	For security reason, the lifetime of key should be defined. The default value is 3600 seconds.						
Phase 2 Network ID	In Aggressive mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 4 characters.						

Enable Perfect	Click to enable or disable t	the function.						
Forward Secret	If enabled, the IKE Phase 1 complexity in phase 2.	key will be reuse	ed to avoid the cor	mputation				
Ping to Keep Alive	Click to enable or disable t address.	he transmission	of PING packets to	a specified IP				
	PING Target IP - Enter the the other-end of the VPN t		e remote host tha	t located at				
	TCP/IP Network Settings							
Local Network IP / Mask	Display the local network l modify the settings if requ		CP / IP configurati	on. You can				
Remote Network IP / Mask	Add a static route to direct Address/Remote Network							
More Remote Subnet	Add a static route to direct Addresses/ Remote Netwo							
	More Remote Subnet	Index Network IP	Netmask	Action				
		1	0.0.0.0 / 0	▼ + Add				
	Enter the IP address and t and create a new entry.	he mask address	. Click +Add to sav	e the settings				
Mode	If the remote network only allows one IP address for the local network,							
	select NAT; otherwise, select Routing.Routing							
	 NAT 							
RIP via VPN	Specifies the direction of R	Routing Informati	on Protocol (RIP) p	oackets.				
Translate Local	lt is available when Routin	g is selected as N	1ode.					
Network	Click to enable or disable the function. This is usually used when you find there are several subnets behind the remote VPN router.							
	If enabled, the function of Change Default Route to this VPN tunnel will be disabled. And please configure the following options.							
	Type - There are two types (Translate Whole Subnet, Translate Specific IP) for you to choose.							
	For Translate Whole Subn	et;						
	 Local Subnet - Select the LAN whose IP addresses are to be translated. 							
	Translated IP - Specify an IP address.							
	 More Local Subnet - Add more subnets. 							
	More Local Subnet	Index Translated To	Local Network	Action				
		1	LAN1	▼ + Add				
	For Translate Specific IP,							
	 Virtual IP Mapping virtual IP address. 	- Specify the loca	l IP address and th	ne mapping				
	Virtual IP Mapping	ndex Local IP	Virtual IP	Action				
	1			+ Add				
Change Default	Click to enable or disable t	this option .						
Route to this VPN	Select this option to direct	•	not LAN-bound to	this VPN				

	tunnel.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.12.12 Connection Management

You can initiate outbound LAN-to-LAN VPN sessions, and view and disconnect all current LAN-to-LAN and dial-up VPN sessions.

Remote Access Control	VPN Name	VPN Type	Remote IP	virtual Network	Tx Packets	Tx Rate	Rx Packets	Rx Rate	Up Time
PPP General Setup				Ne	data available				
SSL General Setup									
IPsec General Setup									
IPsec Peer Identity									
VPN Matcher									
OpenVPN									
WineGuard									
Remote Dial-4n User									
LAN to LAN									
Correction Management									

9.4.13 Mesh

9.4.13.1 Mesh Setup

Vigor router is treated as a mesh root. You can search and specify mesh nodes as members under current mesh group.

				C
General Setup				
Mesh Enable				
Hole	Mesh Root			
Mesh Group Name	VignrMesh			
Auto Reselect				
Log Level	Dasic	*		
Mesh Group				
index	MAC Address	Model	Device Name	
		Mor (hain) contillables		
ි Reset Mesh Group 🔞 Delete				Cancel Save
	Mech Faable Holir Mech Group Name Auto Reselect Log Level Mesh Group	Mech Faable Kolr Mech Hoot Mech Group Name VigenMech Auto Reselect Log Level Gaaic	Mesh Enable Rolr Mesh Root Rolr Mesh Root RoseRect Control Data Control Root Rosh Group Mesh Group Mesh Group Mesh Group	Mesh Faable Hole Hole Mesh Root Mesh Group Name VigerMesh Auto Reselect Ling Level Mesh Group Model Device Name Device Name

Item Description			
	General Setup		
Mesh Enable	Click to enable or disable the mesh network function.		
Role	Displays the role of the router. For Vigor router, it is always Mesh Root.		

Mesh Group Name	Displays the name of the current mesh group.
Auto Reselect	Click to enable or disable the function. It is selected in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network.
Log Level	Choose Basic or Detailed.
	Mesh Group
Index, MAC Address, Model, Device Name	Basic information including MAC address, model and device name of the members in this Mesh Group will be shown in this area.
Reset Mesh Group	Click it to clear the Mesh Group information. All mesh nodes in the group will become isolated.
Cancel	Discard current modification.
Save	Save the current settings

9.4.13.2 Add Mesh Node

Before a Mesh Node is connected, it is unable to check the device status from Mesh Root. This page can help to discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.

F Configuration	2865ac_001DAA000000 / Configuration / Mesh	2
Mesh Setup	Search Mesh Nodes	
Adul Manda Kanag Meseh Statium	Search new mesh node: Sturch	_

1. Click Search. The system will search new mesh node around.

	Search new mesh node
2865ac_001DAA000000 / Configuration / Mesh	3%
Search Mesh Nodes	Searching mesh nodes, please wait for a while

2. Available mesh nodes will be listed on this page.

Configuration	2865ac	_001DA	A000000 / Con	figuration / M	sh	
esh Setup	Sear	rch Mes	sh Nodes			
18 Marili Note esh Status	Sear	ch new n	nesh node		Search	
Gin autos	Add	Index	MAC Address	Model	Device Name	
	.0	1	00507FF1918C	VigorAP 903	VigorAP903	
	(A)	2	1449BC426E1E	VigorAP 960C	VigorAP960C	

3. Select the device(s) you want to group under this mesh group and click +Add.

Mesh Setup	Search Me	esh Nodes			
Add Heats Stude	Search new	mesh node		Search	
Mesh Status	Add Index	MAC Address	Model	Device Name	
	1	00507FF191BC	VigorAP 903	VigorAP903	
	□ 2	1449BC426E1E	VigorAP 960C	WigorAP960C	

4. Wait for a moment.

Add new mesh node
3% Adding selected mesh nodes, this will take a minute, please wait

5. Open Configuration>>Mesh Setup. The new mesh node will be added.

MAC Address	Model	Device Name	
001DAA000000	Vigor 2865	DrayTek	
00507FF191BC	Unknown	VigorAP903	
	001DAA000000	001DAA000000 Vigor 2865	001DAA000000 Vigor 2865 DrayTek

9.4.13.3 Mesh Status

This page shows the mesh status.

One Mesh Group can contain up to 8 devices. A Device with hop 0 is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.

← Configuration	2865ac_00	1DAA000000 / Co	onfiguration	Mesh						
Mesh Setup	 Online(s) 	sync ready) 🥌 Onl	ine 🖕 Offline							
Add Mesh Nade	index	Status	Device Name	NAC Address (Model)	Нор	Up Link	Up Time	Cilents	Disconnect	
	1	 undefined 	DrayTek	001DAA000000 (Vigor 2865)	0		2d 15:22:57	0		
	7	undefined	1000120002	00507FF191BC (VigorAP 903)	4	0010AA000000	0d 00:03:36	0		

9.4.14 Wireless LAN

9.4.14.1 General

This page lets you configure the most basic settings of your wireless network, including the SSIDs, WLAN channels and bandwidth control.

2.40 SG	2927ac_1449BC30C3F0 / Con	figuration / Wireless LAN	c
Surround SSID	General Setup		
Security	Wireless LAN Enable		
Access Control	Mode	Mixed(11b+11g+11n) ~	
WPS	Channel	Channel 6, 2437MHz ~	
Advanced Setting	1.0		
Station Control			
Bandwidth Management			Cancel Save
AP Discovery	Index	Schedule	SSID
Airtime Faimess	1	D	
Band Steering	2	0	
Roaming	3	0.	
Station List	4	0	
Station List - Advance	() Note:		
Station List - Neighbor	 Isolate Member: Prev Isolate VPN: Block the Only the action "Foro 	Id not be changed while Wireless 7.4G WAN mode is in use. ent the cleants associated with this SSID form accessing each other, wireless cleants from accessing the VIN network and prevent wirele a Down" in the Schedule Profile will be applied to WLAN, other action high Availability Hot-Standby method and it's the Secundary Routes	ns will be ignored.

ltem	Description
	General Setup
Wireless LAN Enable	Click to enable or disable the wireless LAN function.
Mode	Select the 802.11 mode allowed on the band.
Channel	Allows you to specify a particular wireless channel to use.
Cancel	Discard current modification.
Save	Save the current settings.
Index	Displays the index number of the WLAN profile.
Schedule	Displays the number of the schedule profile.

To configure the schedule profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

WirelessLAN_General_SchSSID			
Index	1		
Schedule	None	~	
SSID	Nothing selected	~]
	Select All	Deselect All	
	SSID1(All)		
	SSID2		
	SSID3		
	SSID4		

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the schedule profile applied to the SSID.
Schedule	Select a name of the schedule profile.
SSID	Select a number of SSID.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14.2 SSID

Set Service Set Identification (SSID), which shows up as the AP identifier.

2.AG 56	2927ac_14	49BC30C3F0 / Co	nfiguration / Wireless	LAN		C	
General	Index	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN	
5510	1	true	false	DrayTek-30C3F0	false	false	
-	2	talse	Latse	DrayTek_Guest	lalse	table	
Security	3.1	false	false		fable	false	
Access Control	4	false	false		false	false	
WPS	-						
Advanced Setting	① Note:	solate Member: Pre	vent the clients associa	ted with this SSID from accessing ear	ch other:		
Station Control					ent wireless traffic being sent to VPN o	connections.	
Bandwidtis Management							

To configure the SSID profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

2865ac_001DAA000000 / Configuration	on / Wireless LAN	C
General Setup		
Index	1	
Hide SSID		
SSID	DrayTek	
Advance Setup		
Isolate Member		
Isolate VPN		
		Cancel Save

These parameters are explained as follows:

ltem	Description
	General Setup
Index	Display the index number of SSIDs. There are four SSIDs.
Hide SSID	Click to enable or disable the SSID settings.
SSID	Enter or display the name of SSID.
	Advance Setup
lsolate Member	Click to enable or disable the function. If enabled, the router disallows communication between wireless clients (stations) on the same SSID.
Isolate VPN	Click to enable or disable the function. If enabled, the router blocks wireless clients (stations) from accessing VPN clients.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14.3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to the bottom of the router. For extra security, you can set your own wireless password

2.40 36	2927ac_	1449BC30C3F0	/ Configuration / Wireless LAN		
General	index	Mode	WPN Encryption Mode	WEP Encryption Mode	WEP Key index
35ID	1	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
	2	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
	3	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
coss Control	4	Disable	TKIP_for_WPA/AES_for_WPA2_and_WPA3		1
WPS					
dvanced Setting					
Ration Control					
andwidth Management					
Diskovery					
rtime Fairness					
and Steering					
saming					
ation List.					
tation List - Advance					

To configure security settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

ndex	1			
lode	WEP/802.1x_Only	\checkmark		
IEP				
/EP Encryption Mode				
/EP Key Index	1			
VEP Key		٢		
N ote: Please configure the <u>Wirel</u>	ess LAN(2.4GHz) 802.1X Setting.			

ltem	Description
	General Setup
Index	Displays the index number of SSID1 to SSID4.
Mode	Disable - Encryption mechanism is disabled. WEP or WEP/802.1x_Only- Allows only connections from WEP clients. WPA/802.1x_Only or WPA2/802.1x_Only or Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE - Allows only connections from WPA clients.
	WEP or WEP/802.1x_Only
WEP Encryption Mode	Select 64-bit or 128-bit.
WEP Key Index	Select an index number to configure the WEP setting.
WEP Key	Enter the encryption key.
	WPA/802.1x_Only or WPA2/802.1x_Only or

	Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE
WPA Encryption Mode	Displays the encryption mode used for WPA.
WPA Pre-shared Key	Enter 8~63 ASCII characters.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14.4 Access Control

In the Access Control web page, users may configure the white/black list modes used by each SSID and the MAC addresses applied to their lists.

240 36	2927ac_1449BC30C3F0 / Configuration / Wireless LAN	c
General	General Setup	
Security	SSID 1 Enable	
	SSID J. Policy White_List >>>	
WPS	SSID 7 Enable	
Advanced Setting Station Control	SSID 2 Policy White_List ~	
Bandwidth Management	SSID 3 Enable	
AP Discovery	SSID 3 Policy White_Ust	
Airtime Fairness	5SID 4 Enable	
Band Steering Assaming	SSID 4 Policy White_Efst -	
Station List Station List - Advance	D Clear	Cancel Sawe
Station List - Neighbor	MAC Address Filter List	
	Index MACAddress Attribute 550D 1 550D 3 550D 4 Comment	
	10-	

These parameters are explained as follows:

ltem	Description
	General Setup
SSID 1 Enable ~ SSID 4 Enable	Click to enable or disable the MAC filter.
SSID 1 Policy ~ SSID 4 Policy	White List - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list.
	Black List - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list.
Clear	Clear all modifications on this page.
Cancel	Discard current modification.
Save	Save the current settings.
	MAC Address Filter List
Index	Displays the index number of entry.

MAC Address	Enter the MAC address of wireless client.
Attribute	Select to isolate the wireless client from LAN.
SSID1 ~ SSID4	Select the SSIDs to which the above MAC address filter will be applied.
Action	+Add - After entering MAC address and select SSIDs, click +Add to save the settings and create an additional setting entry.

9.4.14.5 WPS

It provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.

2.46 55	2927ac_1449BC30C3F0 / Configu	iration / Wireless LAN	ç
General SSID	Enable WPS	O	
Security	WPS Status	Configured	
Access Control	WPS SSID	Dray(ek-30C3F0	
16475	WPS Authentication Mode	Disable	
Advanced Setting			
Station Control			Cancel Save
Bandwidth Management			Control Survey

ltem	Description
Enable WPS	Click to enable or disable the WPS function.
WPS Status	Displays system information related to WPS. The message "Configured" means that the wireless security (encryption) function of the router is properly configured and functioning properly.
WPS SSID	Displays the name of SSID1. WPS is supported on SSID1 only.
WPS Authentication Mode	Displays the current authentication mode of the router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14.6 Advanced Setting

This page allows you to configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

2,45 36	2927ac_1449BC30C3F0 / Configur	ration / Wireless LAN		
ieneral	Operation Mode	Mixed_Mode	~	
SID				
Security	Channel Bandwidth	20/40	~	
cos Control	Guard Interval	auto	4	
YPS	Aggregation MSDU(A-MSDU)			
	Long Preamble	00		
tation Control	Packet OVERDRIVE TM TX Burst	0		
andwidth Management				
P Discovery	Antenna	212R	~	
irtime Fatmess	Tx Power	10096		
and Steering	WMM Capable			
aming	APSD Capable	00		
tation List	Rate Adaptation Algorithm	New		
ation List Advance	nate nearbadon nigorionn	NOW	-	
ation List - Neighbor	Fragment Length	2346		
		(256 - 2346 frytas)		
	RTS Threshold	2347		
		(1 - 2347 byras)		
				Cancel Save

These parameters are explained as follows:

ltem	Description
Operation Mode	Mixed_Mode - The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected.
	Green_Field - Select this mode to achieve the highest throughput. This mode supports data transmission between 802.11n systems only.
Channel Bandwidth	20 MHz - Vigor Router will utilize 20 MHz channels for data transmission and reception between the AP and wireless stations.
	40 MHz - Vigor Router will utilize 40 MHz channels for data transmission and reception between the AP and wireless stations.
	20/40 MHz - Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of nearby wireless APs.
Guard Interval	If you choose auto as guard interval, the router will choose short guard interval (which increases wireless performance) or long guard interval for data transmit depending on the station capability.
Aggregation MSDU	Click to enable or disable the function.
	If enabled, it will combine frames of different sizes to improve performance at the MAC layer for clients from certain manufacturers.
Long Preamble	Click to enable or disable the function.
	This option determines the length of the sync field in an 802.11 packet.
TX Burst	Click to enable or disable the function.
	If enabled, this feature can enhance the performance in data transmission

	about 40%*.			
Antenna	Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.			
TX Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.			
WMM Capable	Click to enable or disable the function. It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard.			
APSD Capable	Click to enable or disable the function. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption.			
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old".			
Fragment Length	Set the Fragment threshold. You are advised to leave the default value, 2346.			
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.			
Country Code	Vigor router broadcasts country codes according to the 802.11d standard. Click Reference to get detailed information.			
lsolate 2.4GHz and 5GHz bands	Click to enable or disable the function. If enabled, the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.			
Cancel	Discard current modification.			
Save	Save the current settings.			

9.4.14.7 Station Control

Station Control is used to specify the duration that the wireless client can connect to the Vigor router. If this function is disabled, wireless clients can connect to the router as long as the router is powered on and the wireless feature is enabled.

2.46 56	2927ac_14	449BC30C3F0 / Configuration	/ Wireless LAN			c
General	index	SSID	Enable	Connect Time	Reconnect Time	
SSID	1	DrayTelk 30C3F0	false	0 days: I hours:0 min	I days:0 hours:0 min	
	z	DrayTek_Guest	false	0 days:1 hours:0 min	1 days:0 hours:0 min	
Security	3		false	0 days:1 bours:0 min	1 days:0 hours:0 min	
Access Control	4		false	0 days:1 hours:0 min	1 days:0 hours:0 min	
WPS	-					
Advanced Setting						
Bandwidth Management						
AP Descovery						
Airtime Fairness						
Barni Streeting						
Roaming						
Station List						

To configure the station control settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

Index	1	
SSID	DrayTek	
Enable	O	
Connect Time	0 v 1 v 0 v days hours minutes	
Reconnect Time	1 • 0 • days hours minutes	
Display All Station Control List Hotspot Web Portal		
Note: Once the feature is enabled, t	ne connection time quota will apply to each wireless client (identified by MAC address).	
	Cancel	Save

ltem	Description	
Index	Displays the index number of SSID profile.	
SSID	Displays the name of the SSID.	
Enable	Click to enable or disable the station control function for this SSID.	
Connect Time /	Enter the time in days, hours and minutes.	
Reconnect Time	In the Connection Time dropdown box, select the maximum amount of time that a wireless client is allowed to connect within the period of time selected in the Reconnection Time dropdown box.	
Cancel	Discard current modification and return to previous page.	
Save	Save the current settings and return to previous page.	

9.4.14.8 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.

240 55	2927ac_1	449BC30C3F0 / Configuration	1 / Wireless LAN			C
General	index	SSID	Enable	UmilType	UploadLimit	DownloadLimit
5510	1	DrayTek 30C3F0	false	Auto Adjustment	30000	30000
Security	2	DrayTek_Guest	Galiste	Auto_Adjustment	30000	30000
	3		Taise	Auto_Adjustment	30000	30000
Acres Control	4		false	Auto_Adjustment	20000	30000
WPS						
Advanced Setting						
Station Control						
и Пессичну						
irtime l'aimess						
and Steering						
baming						
itation List						
Station List - Advance	1					

To configure the bandwidth management settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

SSID	DrayTek	
Enable		
Bandwidth Limit Type	Auto_Adjustment ~	
Total Upload Limit(Kbps)	30000	
Total Download Limit(Kbps)	30000	
Note: Download: Traffic going to any station. Allow auto adjustment could make the	Upload: Traffic being sent from a wireless static best utilization of available bandwidth.	on.

ltem	Description
SSID	Displays the specific SSID name.
Enable	Click to enable or disable the function.
Bandwidth Limit Type	Auto_Adjustment - Bandwidth limit is determined by the system automatically.
	 Total Upload - Enter a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to this router.
	 Total Download - Enter a value to define the maximum data client(stations) connecting to this router.
	Per_Station_Limit - Bandwidth limit is determined according to the limitation of the wireless client.
	 Upload Limit(Kbps) - Enter a value to define the maximum data traffic (uploading) for each wireless client connecting to this router.
	 Download Limit(Kbps)- Enter a value to define the maximum data traffic (downloading) for each wireless client connecting to this

	router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.14.9 AP Discovery

Vigor router can scan all regulatory channels to find working APs in the neighborhood.

ieral	Index		BSSID		Channel			RSSI	55	iD	Auth	entication		
							No	lata availablo						
rity.														
s Control	Statisti	cs												
	AP nu	mber v.	s. Channel											
nced Setting	1.0													
n Control	0.8													
width Management	0.6													
	0.4													
e Fairness	0.2													
Steering	0.0	1	2	3	4	5	6	ĩ	8	9	10	n.	12	13
ing	-							Scan		-				
n List	ONote	÷												
n List - Advance		During t			(~5 seconds rt up to 32 /				ect with t	he router.				
n List - Neighbor			nery can bi	all roppo	resp to set	a storapte	Jearenrait	addition in						
contract technical														

9.4.14.10 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

246 56	2927ac_1449BC30C3F0 / Configuration / Wireless LAN	C
General SSID Security Access Control	Enable Airtime Fairness Triggering Client Number Z (2 - C4, Default 2)	
WPS Advanced Settling Station Control Bandwidth Management AP Discovery. An Innuck connects Band Steering Reaming	 Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. Airtime: Airtime is the time where a wireless station occupies the wireless channel. Airtime Fairness function tries to assign similar airtime to each station by controlling TX traffic. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and Improve the overall wireless performance Suitable environment: (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection. Triggering Client Number: Airtime Fairness function is applied only when the active station number achieves this number. 	
Station List Station List - Advance Station List - Neighbor		Cancel Save

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

Enable Airtime Fairness	Click to enable or disable the airtime fairness.
Triggering Client Number	Airtime Fairness function is applied only when there are at least this many active wireless stations.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.14.11 Band Steering (for 2.4G only)

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to keep the 2.4 GHz band clear for legacy clients, and improves users' experience by reducing 2.4 GHz channel utilization.

+ Configuration	2865ac_001DAA000000 / Configurati	ion / Wireless LAN	P
240 50	Enable Band Steering		
General	5G Capability Check Timer	15	
SSID		(1 - 60 seconds, Desaut: 15)	
Security		a contraction of the second seco	
Access. Control	 Note: Please setup at least one pair 	ir of 2.4GHz and SGHz Wireless LAN with the same SSID and security.	
WPS	 Band Steering Note: Band steering is used to det 	ect if the wireless client is capable of dual band or not. If dual band is detected, the AP will let the wireless	
Bandwidth Management		sted wireless LAN, such as 5GHz to prevent from network congestion.	
Artime Fairness	 Rand steering would active client 5G capability* would 	ly block the client's attempts to associate with 2.4GHz Wireless LAN. So the setting of *Check time for WLAN cause the delay of 2.4G WLAN connection.	
Advanced Setting	-		
			Cantel Save
AP Discovery			

ltem	Description
Enable Band Steering	Click to enable to disable the Band Steering function.
5G Capability Check Timer	Set a check time value. When a wireless client attempts to connect, the router will block attempts to connect to the 2.4 GHz band for the specified period of time (default is 30 seconds), which hopefully will entice the client to connect to the 5 GHz band. If the client fails to connect to the 5 GHz band within the specified interval, it will then be able to connect to the 2.4 GHz band.
Cancel	Discard current modification.
Save	Save the current settings.
Add	Click to add a new entry to Access Control.

9.4.14.12 Roaming

WiFi roaming allows wireless stations to switch connections between access points within an area to achieve better coverage and signal quality.

2.46 56	2927ac_1449BC30C3F0 / Co	onfiguration / Wireless LAN	C
Senoral	Roaming Type	Minimum RSSI ~	
SSID			
Security	Minimum RSSI	-66	
		60% (Default: -66 dBm)	
Access Control	Adjacent AP RSSI over	5	
VPS		(Default: 5 fibm)	
dvanced Setting			
tation Control	AP-assisted Client Roa When AP detects the	ming Note: hat a station may need to roam, AP disconnects the station	
andwidth Management	This feature helps t	those stations with bad reaming ability. Avoid the situation that a station is e other AP but still sticky to the original AP and with bad performance	
P Discovery	Please notice that I	RSSI Requirement mode is common for 2.4G and 5G.	
virtime Fairness	() Minimum RSSI with Ad		
and Steering	 Disconnect clients through another Di 	with bad signal to encourage roaming only when they can have better signal rayTek AP.	
kana sueenng		ayTek APs which support this feature. The LANs assigned by the SSID of all cited by Ethernet and under the same subnet.	
tation List.			
tation List - Advance			Cancel Save
tation List - Neighbor			Concer Onvo

ltem	Description
Roaming Type	 Disable RSSI Requirement - The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations. Strictly Minimum RSSI
	Minimum RSSI
Strictly Minimum RSSI	The Vigor router will immediately disconnect the wireless station if its RSSI falls below the configured value.
	Specify a value as a threshold.
Minimum RSSI	The Vigor router will disconnect wireless clients whose RSSI falls below the minimum threshold only if there is also a neighboring wireless host (router or AP) that has an RSSI value (defined in the field of With Adjacent AP RSSI over) higher than a certain threshold.
	In order for this option to work, other wireless hosts connected to the same LAN subnet need to support the exchange of RSSI information with peer wireless hosts via Ethernet.
	Specify a value as a threshold.
Adjacent AP RSSI over	Specify a value as a threshold.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.14.13 Station List

Station List provides an overview of all currently connected wireless clients and their status.

2.46 56	2927ac_144	9BC30C3F0 / Config	guration / Wire	less LAN			
ආදාව	Station Li	st					
ND	Index	MAC Address		Status	Associated With	IP Ad	dress
curity	Status Codes :						
ess Control		nected, No encryption.					
5	- E: Con	nected, WEP.					
	• P: Con	nected, WPA:					
anced Setting		nected, WPA2.					
ion Control		nected, WPA:1.					
dwidth Management		mected, OWE					
Discovery	 IS: Bloc N: Con 	cked by Access Control.					
ime Fairness		neong. to pass WPA/PSK auther	dication.				
d Steering							
	Add to Ad	ccess Control :					
aming							
tion List	MAC						
tion List - Advance	SSID		(1-4)				
tion List - Neighbor			in th				
						-	
						Add	

These parameters are explained as follows:

ltem	Description
Station List	Displays wireless stations connected to the Vigor router.
Add to Access Control	MAC - Enter the MAC address. SSID - Specify the number of SSID.
Add	Click to add a new entry to Access Control.

9.4.14.14 Station List - Advance

Displays wireless stations connected to the Vigor router with more detailed information.

2,4G 5G	2927ac_14	449BC30C3F0 / Config	guration / Wirel	ess LAN						
General	Index	MAC Address	AID	RSSI	Rate	BW	PSM	WMM	PhMd	
SID					No data ava	Nable				
curity										
zess Control	Add to .	Access Control :								
PS										
dvanced Setting	MAC									
ation Control	SSID		(1-4)							
indwidth Management								_		
Discovery								Add		
irtime Fairness	Note: • Alter	r a station connects to the	router successfully	, it may be turn	ed off without r	rotice. In that	case, it will stil	I be on the list u	ntil the connection	ı expir
and Steering	_									
oaming										
tation List										

9.4.14.15 Station List - Neighbor

This page displays the nearby wireless stations connected to other access points that are detected by the Vigor router.

2.40 50	2927ac_14	49BC30C3F0 / Config	guration / Wireless LAN	1			C
General	Index	MAC Address	Vendor	RSSI	Approx Distance	SSID	Visit Time
SID							
ecurity	Add to /	Access Control :					
ccess Control	MAC						
ps	SSID		(1.4)				
dvanced Setting							
ation Control						Add	
andwidth Management	Note: • 1. Ap	prox. Distance is calculate	ed by actual signal strength	of device detecte	d. Inaccuracy might occur base	d on barrier encountered	
Discovery	• 2. Du	e to the differences in sig	nal strength for different de	wices, the calcuat	ed value of approximate distan	ce also might be different	
rtime Fairness	• 3. Tri	ademarks and brand nam	es are the properties of the	ir respective own	ers.		
and Steering							
parning							
ation List							
tation List - Advance							
tation Dist - Neighbor							

ltem	Description
Station List	Displays wireless stations connected to the Vigor router.
Add to Access Control	MAC - Enter the MAC address. SSID - Specify the number of SSID.

9.4.15 Bandwidth Management

9.4.15.1 Sessions Limit

When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is a finite number of sessions that can be tracked by the router. By setting session limits will ensure that the router does not run out of resources.

Sandweight Limit	IPv4		
APP Qo5	Enable	0	
	Default Max Sessions	100	
	Limitation List	Index Start IP End IP Max Sessions	
		1 0.0.0.0 0.0.0.0	
		管 Class All	
	IPv6		
	Enable	C	
	Default Max Sessions.	100	
	Limitation List	Index Start IP End IP Max Sessions	
		1 0	
		the Clear A1	
	Administration Message		
	Administration Message	You have reached the maximum number of	
	(Max 255 characters)	permitted internet sessions -go-Pilase close one or more applications to allow further internet access-go-Contact you system administrator for function internetions default	
			Cancel Save

ltem	Description
	IPv4 / IPv6
Enable	Click to enable or disable the sessions limit function.
Default Max Sessions	The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List.
Limitation List	Displays specific limitation entries.
Clear All	Clear all modifications on this page.
	Administration Message
Administration Message	Enter a message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached.
	Time Schedule
Schedule 1 ~ 4	Specify up to 4 time schedule entries to enable or disable the WAN. Specify up to 4 time schedule entries to apply the sessions limit management.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.15.2 Bandwidth Limit

Bandwidth Limit ensures LAN clients get their fair share of network bandwidth by placing restrictions on upstream and downstream network speeds.

Enable	0						
LINGO							
IP Routed Subnet	0						
Default TX Limit Per User	2000		Kbps	\sim			
Default RX Limit Per User	8000		Kbps.	. 97			
Limitation List	Index Start II	Endle	TXLimit	RXLimit	Eacl		
	1 None	None	0	0	Eac		
		_		_			
	E GaarAi						
IPv6	B Claar AL						
Enable	E ClasrAt						
			Kbps	~			
Enable	Ø			4			
Enable Default TX Limit Per User	2000	End IP		4	Éact		
Enable Default TX Limit Per User Default TX Limit Per User	2000	End IP None	Kbps TK Limit	4	Eact Eac		

ltem	Description					
	IPv4 / IPv6					
Enable	Click to enable or disable the bandwidth limit function. IP Routed Subnet - It is available for IPv4 only.					
	/ /					
Default TX Limit Per User	Set default upstream speed limit for each LAN client.					
Default RX Limit Per User	Set default downstream speed limit	t for each LAN client.				
Limitation List	Displays specific limitation entries.					
	To add a new profile, click the last i	ndex number to open the setting page.				
	IPv4 Bandwidth Limitation List					
	Add Entry By	IP Range IP Object				
	IP Group	None ~				
	IP Object	None ~				
	Each or Shared	Each Shared				
	TX Limit	0 Mbps ~				
	RX Limit	0 Mbps ~				
	💼 Clear					
	After finishing the settings, click Sav displayed on the limitation list.	ve. A new profile will be added and				

	Limitation List	Index	Start IP	End IP	тх
		1		192.168.1.65	10:
		2	None	None	0
				_	
		💼 Clear A	.11		
Clear All	Clear all profiles in the limitation	n list.			
Allow user to use more bandwidth than the assigned	Click to enable or disable this fu If enabled, it lets the router auto downstream limits based on ava	matically		upstream a	Ind
Smart Bandwidth Limit	Click to enable or disable this fu If enabled, it restricts the bandw limitation list when the network	vidth of L			
Apply the below limit to users not in	Enter the number of sessions th Smart Bandwidth Limit activates		client is allo	wed to hav	e before
TX Limit	Upstream speed limit for each L	AN client	. Unit can b	e either Kbp	os or Mbp
RX Limit	Downstream speed limit for eac Mbps.	h LAN cli	ent. Unit ca	n be either	Kbps or
	Time Schedule				
Schedule 1 ~ 4	Specify up to 4 time schedule er management.	itries to a	apply the ba	ndwidth lim	nit
Cancel	Discard current modification.				
Save	Save the current settings.				

9.4.15.3 APP QoS

APP QoS allows QoS to be applied to select protocols and applications. Protocols and applications fall into two categories: Traceable and Untraceable.



Click the Enable button to enable or disable the APP QoS function. Then click Save to save the settings.

Traceable

Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class.

PIS LIMP	Index	Type Name	
idth Limit	4	Instant Message	
	3	VoiP	
	3	Protocol	
	4	Tunneling	
acrable	5	Stream	
	6	Remote Control	
	7	Web HD	
	8	Game	
	9	Apple Services	
	10	Google Services	
	11	Amazon Services	
	.12	E-Lite-	

Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.

dwidth Umit	Type Name	Instan	nt Message			
	Select All Clear All				w study to ult	
tracewide:	App Name	Enable	Version	Action		
	Facebook/Instagram	Ø		Qo5 Class 1 (High)	~	
	UNE	D	5.23.0.2134	QoS Class 1 (High)	v	
	Linkedin	0		QoS Class 1 (High)		
	Signat	Ð	1.26.2	QoS Class 1 (High)	. 4	
	Slack	0	4.0.0	QoS Class 1 (High)	Y	
	Snapchat	0	10.79.5.0	QoS Class 1 (High)		
	Telegram	0	1.7.10	QoS Class J (High)		
	WhatsApp	0	0.3.2948	QoS Class 1 (High)		

ltem	Description
Enable	Click to enable or disable the bandwidth limit function.
Action	Select a QoS class to be applied to the application.
Cancel	Discard current modification.
Save	Save the current settings.

These parameters are explained as follows:

Untraceable

Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

Sestors Limit	Action	Qos Class 1 (High) -	
Benchwidth Limit	Index	Type Name	
APP QoS	1	Instant Message	
Traceable	2	VoiP	
Upto second de	3	P2P	
	4	Protocol	
	5	Tunneling	
	6	Stream	
	7	Remote Control	
	8	Web HD	
	D Rate Picad remember h - This will help QoS i	a adjest indugend (Chatteograf hanglehillfi of your network in "Quality of Sarvicer", o work moore efficient.	Save

Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.

sdwidth Limit:	Type Name-	Instant Message		
PQuS				
acable	Select All Clear All			
	App Name	Inable	Version	
	AlM Login	Ø	8	
	ÁIŴŴ	0	2008	
	Ares	0	2.0.9	
	BaiduHr	0	37378	
	Fetton	3	2010	
	GaduGadu Protocol	0		
	ICQ	CD	7	
	ISpQ	00	8.0.60	
	KC	00	2008	
	Paltaik	(2)	9	
	PocoCall	0	2007	
	Qnext	0	30.1	
	Tencent QQ	0	2012/2009 beta3	

ltem	Description
Enable	Click to enable or disable the bandwidth limit function.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.16 USB Applications

9.4.16.1 General Settings

This page allows you to configure the file sharing feature of the Vigor router, where USB mass storage devices such as thumb drives and hard drives can be made accessible to LAN clients.

General Settings	2927ac_1449BC30C3F0 / Configura	ition / USB Application				c
User Management	and a second second					
Temperature Sensor	Simultaneous FTP Connections	5				
Disk Status	Default Charset	English	~			
Modern Status	SMD File Sharing Service	D				
Printer Status	Workgroup Name	WORKGROUP				
Sensor Status	Host Name	Vigni				
	Printer Server	0				
	 Multi-session FTP download such as FileZilla, you should A workgroup name must be 	(Ich", only English long file name is with be banned by Router FTP serv Imit cleant connections to 1 to imp different from thre hartname. They racters. Names cannot contain any	ver. If your FTP da prove performant workgroup name	ce. can have up to 15 cha		Save

ltem	Description
Simultaneous FTP Connections	Enter the maximum number of simultaneous FTP sessions allowed.
Default Charset	Select the character set for file and directory names.
SMB File Sharing Service	Click to enable / disable the function.
Access Mode	LAN Only - Only users on the LAN can connect access the shared USB disk. LAN and WAN - Both LAN and WAN users can access SMB server of the router.
Workgroup Name	Enter the workgroup name. Maximum allowed length is 15 characters.
Host Name	Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters.
Printer Server	Click to enable / disable the function. If enabled, the Vigor router can act as a print server for printers connected the USB.
Save	Save the current settings.

9.4.16.2 User Management

This page allows you to set up profiles for FTP/SMB users.

General Settings	2927ac_14	49BC30C3F0 / Config	guration / USB Application			Set to Factory Default 🛛 📿
His Mittagerowit	index	Username	FTP/SMB User	Home Folder	File Access Rule	Directory Access Rule
Temperature Sensor	1		fatse			
Disk Status	-					
Modern Status						
Printer Status						
Sensor Status						

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

2865ac_001DAA000000 / Configuration / USB A	Application	Set to Factory Default	C
\bigtriangleup No USB disk Connected ! Please Insert the disk	k.		
Index	1		
FTP/SMB User	\bigcirc		
Username	(Max. 11 characters allowed)		
Password	(Hax. 11 characters allowed) $$\Phi$$		
Confirm Password	Φ		
Home Folder			
Create New Home Folder			
	+ Create		
 Note: The folder name can only contain the follow 	wing characters: A Z a -z 0-9 \$ % ' \odot – ' I () and space.		
Access Rule			
File	Read		
	Write		
	Delete		
Directory	List		
	Create		
🗎 Clear		Cancel Sa	ve

ltem	Description
Index	Displays the index number of USB application profile.
FTP/SMB User	Click to enable / disable the function. If enabled, this profile (account) for FTP service and / or SMB service will be activated.
Username	Enter the username for this user profile.
Password	Enter the password for this user profile.
Confirm Password	Enter the password again to confirm.
Home Folder	Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile.
Create New Home Folder	Enter a name as a new folder name. +Create - Click to create a new folder.

	Access Rule
Access Rule	File – Check the items (Read, Write and Delete) for such profile.
	Directory –Check the items (List, Create and Remove) for such profile.
Clear	Clear all modifications on this page.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.16.3 Temperature Sensor

This page displays the status information for the USB disk connecting to Vigor router.

General Settings	2927ac_1449BC30C3F0 / Config	uration / USB Application	c
User Management	Temperature Calibration	0	
Disk Status	Temperature Unit	Ceisus ("C) Fahrenheit ("F)	
Modern Status	Enable Sysleg Alarm	Ð	
Printer Status	Upper Temperature Limit	30	
Sensor Status	Lower Temperature Limit	18	
			Save

ltem	Description
Temperature Calibration	Enter the difference between the actual temperature and the temperature as reported by the thermometer.
Temperature Unit	Select the temperature scale to be used.
Enable Syslog Alarm	Select to enable recording of the temperature in Syslog.
Upper /Lower Temperature Limit	Enter the upper and lower temperature limits. If the temperature falls outside of this range, an alert will be sent.
Save	Save the current settings and return to previous page.

9.4.16.4 Disk Status

This page displays the status information for the USB disk connecting to Vigor router.

General Settings	2927ac_1449BC30C3F0 / Co	nfiguration / USB Application			c
User Management	i manazi				
Temperature Sensor	Connection Status	No Disk Connected Disconnect USB Bible			
		Disconvect USB prise			
Modern Status	Write Protect Status	NULL			
Printer Status	Disk Capacity	0 MR			
Sensor Status	Free Capacity	0 MB			
		e up in 4GB, which is the limitation of FAT3D format. which of the USB disk is turned on, the USB disk is in READ .	-OMLY mosde. No data can be written to i Username	ргор	

These parameters are explained as follows:

ltem	Description
Connection Status	Displays if the USB is connected or disconnected. Disconnect USB Disk - If connected, click to disconnect USB disk with the router.
Write Protect Status	Displays the total capacity of the USB storage disk.
Disk Capacity	Displays the disk capacity.
Free Capacity	Displays the free space on the USB storage disk.
USB Disk Users Connected	Displays the clients that are connected to the SMB/FTP server.

9.4.16.4 Modem Status

2927ac_1449B	C30C3F0 / Configuration / USB Applicati	ion		C
index	Connection Status	Manufacturer	Model	
1	No Modem Connected			
2	No Modem Connected			
-				
		Index Connection Status 1 No Modern Connected	1 No Modern Connected 2 No Modern Connected	Index Connection Status Manufacturer Model 1 No Modern Connected <

Click the index number to open the following for viewing detailed information for parameter settings.

/ Configuration / USB A	Application
Index	2
Connection Status	
Manufacturer	
Model	
Revision	
Serial Number	
IMSI	
Signal Quality (CINR)	
RSSI Signal	
Hardware	
SIMPIN	۵
Link Speed	

9.4.16.5 Printer Status

This page displays current status for the USB printer connecting to Vigor router managed by VigorACS 3.

General Settings	2927ac_1449BC30C3F0 / Configuration / USB Applica			n		2
the Management	Connection St	tatus	No Printer Connect			
Lemperature Sensor	Competenza a		No Printer Connec	rea		
Dok Status	Manufacturer		No Printer			
Modem Status	Model		No Printer			
PTIMET SCALAR	Serial Number	r	No Printer			
Sensor Status						
	Printer Que	ue				
	Index	User		Files Name	Status	
	1	No Printer		No Printer	No Printer	
	2	No Printer		No Printer	No Printer	
	3	No Printer		No Printer	No Printer	
		No Printer		No Printer	No Printer	
	-					

9.4.16.6 Sensor Status

This page displays current status for the USB thermometer connecting to Vigor router managed by VigorACS 3.

General Settings	2927ac_1449BC30C3F0 / Configuration / USB Application		C	
User Management	and the second			
Temperature Sensor	Connection Status	No Temper Connected		
Disk Status	Manufacturer	no Imper		
Modern Status	Product	no tmper		
Printer Status				
Service Streets				
No. of Concession, Name				

9.4.17 System

9.4.17.1 Maintenance

This page can be used for backup configuration for specified CPE, restoring configuration for specified CPE, making firmware upgrade for CPE, and even reboot the specified CPE via VigorACS 3.

Manthumes	2927ac_1449BC30C3F0 / Configur	ration / System	C
Time Settings	Configuration Backup		
NetFlaw			
Admin Account	Backup Cenfig	Backup	
Admin Local User	Restore Config	Last Config Local File Shared Folder	
SNMP Settings	negate samily	Kasi Goning Local ne Shares Policen Hinstone Nuse	
Management		HARPED MINN	
TR069 Settings	Download Config	Download	
Weblazok			
SysLog Settings	1		
Mull Abert	Firmware Upgrade		
Internal Service User List	Model Name	Vigor2921ar.	
Panel Control	Modem Firmware Version	No DSL	
	Firmware Version	r5952_eb0dc82250_beta	
	Choose a Firmware File From	Liocal File Shared Folder	
		Brokse	
	Protocol Options	TR069 HTTP HTTPS	
la substantia		Upgrade How	
	m Note:		

ltem	Description		
	Configuration Backup		
Backup Config	Backup - Click to backup the configuration from CPE to VigorACS server.		
Restore Config	 Select the type of configuration file. Last Config Local FIIe Shared Folder Restore Now - Click to initiate restoration of configuration immediately. 		
Download Config	Download - Click to download the lastest configuration backup file from VigorACS server.		
	Firmware Upgrade		
Model Name	Displays the model name of the CPE.		
Modem Firmware Version	Displays the modem version of the CPE. No DSL - It indicates the selected CPE is non-DSL device.		
Firmware Version	Displays the firmware version used by the CPE.		
Choose a Firmware File From	Local File - Select a firmware from the host by clicking Browse. Shared Folder - Select a firmware from the database by click Browse.		
Protocol Options	Select TR069, HTTP, or HTTPS.		
Upgrade Now	Click to upgrade the firmware immediately.		

	Device Reboot	
Restart the device	device Reboot Now - Click to reboot the router immediately.	
	Auto Reboot Time Schedule	
Schedule Profile	Select up to 4 user-configured schedules to reboot the router on a scheduled basis.	
ОК	Save the settings.	
	Reset	
Reset to factory default	ctory Reset Now - Click to reset the router with factory default setting immediately.	
Save	Save the current settings.	

9.4.17.2 Time Settings

This page allows you to configure settings related to the system date and time.

Maintenance	2927ac_1449BC30C3F0 / Configur	ation / System	c
The Setting	Current System Time	2025-02-17108:36:47	
NetFlow	Local Time Zone	+00:00	
Admin Local User	Time Setup	Use Browser Time Use Internet Time	
SNMP Settings	Primary Server	pool.ntp.org	
Management	Secondary Server		
TR069 Settings	Priority	Auto ~	
Webhook SysLog Settings	Time Zone	(GMT) Greenwich Mean Time : Dublin ~	
Mail Alert	Daylight Savings	D	
Internal Service User List	Daylight Saving Type	Default By Date By Weekday	
Pani-I Control	Start	Yearly on March last Sun	
	End	Yearly on October last Sun	
	Automatically Update Interval	30 mins 🐱	
	Send NTP Request Through	Auto ~	
			Save

ltem	Description	
Current System Time	Displays the current time obtained from the time server.	
Local Time Zone	Displays the time zone where the router is located.	
Time Setup	Use_Browser_Time - Click to let the router set its system time using the time reported by the web browser.	
	Use_Internet_Time - Click to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).	
Primary Server	Enter the address of the time server (primary).	
Secondary Server	Enter the address of the time server (secondary).	
Priority	Select Auto or IPv6 First as the priority.	
Time Zone	Select the time zone where the router is located.	

Daylight Savings	Click to enable or disable the Daylight Saving Time (DST) if it is applicable to your location.
Daylight Savings Type	Default - Uses the default DST schedule for the time zone. By Date - Select this option if DST starts and ends on fixed dates. By Weekday - Select this option if DST starts and ends on certain days of the week.
Start	It is available when By Date is selected as Daylight Saving Type. Use the drop down list to select month, day and hour settings as the starting point.
End	It is available when By Date is selected as Daylight Saving Type. Use the drop down list to select month, day and hour settings as the ending point.
Automatically Update Interval	Select the time interval at which the router updates the system time.
Send NTP Request Through	Select a WAN interface to send NTP request for time synchronization.
Save	Save the current settings.

9.4.17.3 NetFlow

This page allows you to set the IP address, port number, versions and timeout for collecting packet information monitored by NetFlow feature.

Maintenance	2927ac_1449BC30C3F0 / Co	nfiguration / System	C
Time Settings	Enable	•	
Halflow	Collector ip	19-yek formati (F.S.:: 123-12-1-1)	
Admin Account	Collector port	4739	
SMMP Settings	Version	IPFIX ~	
Management	Active timeout	300	
TR069 Settings	Inactive timeout	15	
Webhook.			
Systing Settings			Cancel Save
Muil Alert Internal Service User List			
Panel Control			
and the second second			

ltem	Description
Enable	Click to enable or disable the NetFlow function.
Collector ip	Enter the IP address of a server (e.g., VigorConnect) which can be used as the flow collector.
Collector port	Enter the port number of the server.
Version	The router supports three versions (v5, v9 and IPFIX) of NetFlow feature.
Active timeout	Range from 60 to 1800 seconds. Default is 300 (seconds). Set the time interval of activity that marks a flow active. The data flow information will be collected continuously until the active timeout.
Inactive timeout	Range from 15 to 1800 seconds.

Set the time interval of inactivity that marks a flow inactive. The coll data information will be exported after the inactive time interval.	
Save	Save the current settings.

9.4.17.4 Admin Account

This page allows you to set or change the administrator password.

Maintenance	2927ac_1449BC30C3F0 / Config	uration / System			c
Time Settings	Admin Account				
Admin Assessme	Admin Password			÷	
Admin Local User	 (i) Note: Ressourd can contain o 	ndya2AZ09,(:*>*+ 3@	er*()5%&		
Management	Enable "admin" account login to V from the Internet	Veb UI			
TR069 Settings Webbook	Use only advanced authentication	n method ①			
Sprilling Settings	for Admin."WAN" login				
Molt Alert.	User Account				
Internal Service User List Panel Control	Enable User Account	Ø			
	User Password			(D)	
	Note: Prevent can contain a Prevent can contain a Prevent can total a	ez A 2 D 9 ₄₁ *⇔*+ : [2@ r A 1 sterska]", for example, "* or ***	() "Is Niegal, but '123" or "	"45" H OK.	
					Cancel Save

ltem	Description	
	Admin Account	
Admin Password	Enter the new password.	
Enable admin account login to	Click to enable or disable the function. If enabled, it allows the administrator to log in from the Internet. This option is enabled when Administrator Local Account is enabled (see below).	
Use only advanced authentication	 Click to enable or disable the function. If enabled, Advanced Authentication - Advanced authentication method can offer a more secure network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. Mobile one-Time Password (mOTP) - Enter the PIN Code and Secret settings for getting one-time passwords. 2-Step Authentication - Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. 	
	User Account	
Enable User Account	Click to enable or disable the function. If enabled, other users are allowed to administer the router.	

User Password	Enter a string as the password for the user account.
	Login Greetings
Login Page Logo	Default - Choose it to use the default image. Blank - Choose it to discard the logo image. Upload a file - Choose it to specify an image as the logo.
Enable Login Greetings	Click to enable or disable the function.
Logo Image Upload	It is available when Upload a file is selected as Login Page Logo. Browse - Click to select an image file. +Upload - Click to upload the selected image file to VigorACS.
Title	Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Message	Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.17.5 Admin Local User

Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router.

Maintenänce	2927ac_1449BC30C3F0 / 0	Configuration / System			c
Time Settings	Local User	0			
NetHow					
Admin Account	Local User List				
	index Us	ername	Password	Action	
SNMP Settings	1			+ Add	
Monagement					
TR069 Settings	Administrator LDAP S	etting			
Webhook	Enable LDAP/AD login for Ad	dmin users			
Systing Settings	Charle Court has to Burrar and				
Mail Airt	Administrator TACACS	S+ Setting			
Internal Service User List	Enable TACACS+ login for a	dmin users 🔘			
Panel Control					
					Save

ltem	Description	
Local User	Click to enable or disable the local user setting.	
Local User List	Index - Displays the index number of local user profile. User Name - Displays the name of the local user profile. Password - Displays the password of the local user profile. Action +Add - Click to create a new user profile.	

	Specific User Index. Usersame Authentication method Base: Modific one-Trans Parawords(mOTTY) 2 Stray Authentication Paraword Confirm Paraword Confirm Paraword Confirm Paraword Confirm Paraword Confirm Paraword Confirm Paraword Confirm Confirm Paraword Confi
	 Index - Displays the index number of the profile. Username - Enter the name of the user profile. Authentication method - Choose Basic, mOTP or 2-Step
	 Authentication. If Basic is selected - Enter the password. If Mobile one-Time Password (mOTP) is selected- Enter the PIN Code and Secret settings for getting one-time passwords. If 2-Step Authentication is selected- Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
	Administrator LDAP Setting
Enable LDAP/AD login for Admin users	Click to enable or disable the LDAP/AD login profile.
	Administrator TACACS+ Setting
Enable TACACS+ login for admin users	Click to enable or disable the function. If it is enabled, any user can access into the web user interface of Vigor router through the TACACS+ server authentication.
Enable Fallback to Local Authentication	If it is enabled, the administrator can use other login methods for authentication once the TACACS+ server has no response.
Save	Save the current settings.

9.4.17.6 SNMP Settings

This page allows you to configure settings for SNMP and SNMPv3 services.

Maintenance	2927ac_1449BC30C3F0 / Configuratio	n / System C	C
Time Settings	Enable SNMP Agent		
NetFlow	Enable SNMPV1 Agent		
Admin Account	Lindse on in TXIBout	-	
Admin Local User	Enable SNMPV2C Agent		
SNMP Settings	Get Community	public	
Management	Set Community	private	
TR069 Settings	Trap Community	public	
Webhook	Trap Timeout	10	
SysLog Settings	nup micouc	10	
Mail Alert	Manager Host IP (IPv4)		
Internal Service User List			
Panel Control	Index 1: IP	0.0.0.0	
	Index 1: Subnet Mask	v	
	Index 2: IP	0.0.0.0	
	Index 2: Subnet Mask	~	
	Index 3: IP	0.0.0.0	
	Index 3: Subnet Mask	~ ·	
		Save	

ltem	Description
Enable SNMP Agent / Enable SNMPV1 Agent / Enable SNMPV2C Agent	Click to enable or disable the SNMP function.
Get Community	Enter the Get Community string. The default setting is public.
Set Community	Enter the Set Community string. The default setting is private.
Trap Community	Enter the Trap Community string. The default setting is public.
Trap Timeout	The default setting is 10 seconds.
	Manager Host IP (IPv4)
Index #:IP	Enter the IPv4 address of hosts that are allowed to issue SNMP commands.
Index #: Subnet Mask	Select a subnet mask for IP address configured above.
	Manager Host IP (IPv6)
Index #: IP	Enter the IPv6 address of hosts that are allowed to issue SNMP commands.
Index #: Prefix Length	Enter the fixed value for prefix length.
	Notification Host IP (IPv4)
Index #: IP	Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
	Notification Host IP (IPv6)
Index #: IPv6 Address	Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
	SNMPV3 Agent
Enable SNMPV3 Agent	Click to enable or disable the SNMPv3 function.

USM User	Enter the username to be used for authentication	
Auth Algorithm	Select one of the hashing methods to be used with the authentication algorithm.	
Auth Password	Enter a password for authentication.	
Privacy Algorithm	Select an encryption method as the privacy algorithm.	
Privacy Password	Enter a password for privacy.	
Save	Save the current settings.	

9.4.17.7 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

Maintenanae	2927ac_14498C30C3F0 / Configuration	on / System	G
Time Settings	Router Name	Draylek	
NetFlow	Contraction of the second		
Admin Account	Default:Disable Auto-Logout		
Admin Local Uter	Enable Validation Code in Internet/LAN		
SNMP Settings	Access		
Management	() Note:	and the second	
TR069 Settings	 IE8 and the below version do NC 	IT support DrayOS CAPTCHA auth code.	
Webhook	Internet Access Control		
Systing Settings	Allow management from the Internet	•	
Mall Alert	raiow management nom the internet	•	
Internal Service User List	Domain name allowed		
Panel Control		CTP Server	
		ITTP Server	
		Enforce HTTPS Access	
		HITPS Server	
		Z Telmet Server	
		Z TR069 Server	
		SSH Server	
		□ SNMP Server	
In case of the			Save

ltem	Description		
Router Name	Enter the router name as provided by ISP.		
Default:Disable Auto-Logout	Click to enable or disable the function. If enabled, the auto-logout function for web user interface will be disabled		
Enable Validation Code in Internet/LAN Access	Click to enable or disable the function. If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in.		
Internet Access Control			
Allow management from the Internet	Click to enable or disable the function. If enabled, it allows system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered.		
Domain name	Enter a domain name.		

allowed	This setting is only available if DNS filtering is enabled, applying DNS filter profile in firewall rules, or enabling DNS Filter Local Setting.			
Disable PING from the Internet	Click to enable or disable the function. If enabled, it will reject all PING packets from the Internet. For increased			
	security, this setting is enabled by default.			
Apply to Interface	Allow the user to access the router via the selected WAN interfaces.			
	LAN Access Control			
Allow management	Click to enable or disable the function.			
from LAN	If enabled, it allows system administrators to login from LAN interface.			
	There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.			
Apply to Subnet	Click to enable or disable the LAN interface.			
	If enabled, the selected interface can be used for accessing into web user interface of Vigor router.			
	IP Object Enable - Click to enable or disable the IP object setting.			
	Index in IP Object - Enter the index number of the IP object profile. Related IP address will appear automatically.			
	LoopBack Interface			
Enable LoopBack	Click to enable the function of Loopback Interface.			
Interface	LAN#- Select a LAN subnet as the Loopback Interface.			
	IPv6 Management Setup			
Allow management from the Internet	Click to enable the function. Select the servers that system administrators are allowed to manage from the Internet.			
Disable PING from the Internet	Click to reject all PING packets from the Internet. For increased security, this setting is enabled by default.			
	IPv6 Address Security Option			
Enable Random	Click to enable or disable the function.			
Interface Identifiers	If enabled, the IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker.			
	Access List from the Internet			
Apply Access List to	Click to enable or disable the function.			
PING	Access List #: IP Object - Enter the index number of the IP object profile. Related IP address will appear automatically.			
	IPv6 Access List			
Apply Access List to	Click to enable or disable the function.			
PING	Access List #: IPv6 Object - Enter the index number of the IP object profile. Related IP address will appear automatically.			
	Management Port Setup			
Management Port Setup	User Define Ports - Specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.			
	Default Ports - Use standard port numbers for the Telnet and HTTP servers.			
	Brute Force Protection			
Enable brute force	Click to enable or disable the function.			

login protection	If enabled, any client trying to access into Internet via Vigor router will be
	asked for passing through user authentication.
Maximum login failure	Specify the maximum number of failed login attempts before further login is blocked.
Penalty period	Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed.
	Blocked IP List
Table	Display, in a new browser window, IP addresses that are currently blocked from logging into the router.
	TLS/SSL Encryption Setup
TLS 1.3, 1.2, 1.1, 1.0 Enable, SSL 3.0 Enable	Check the box to enable SSL 3.0/1.0/1.1/1.2 encryption protocols.
	CVM Access Control
Туре	Click General Settings or IPsec VPN Settings to configure the basic settings for CVM mechanism.
	General Settings –
	• Enable CVM Port - Click to enable or disable the function.
	 CVM Port - Check the box to enable Central VPN Management port setting.
	• Enable CVM SSL Port - Click to enable or disable the function.
	 CVM SSL Port - Check the box to enable Central VPN Management SSL port setting.
	 CVM WAN Interface – For Vigor router can manage only the client from WAN interface, you have to specify which interface will be used for such function. If you choose MANUALLY, you have to specify WAN IP address.
	• CVM WAN IP – Specify WAN IP address.
	 Username – Enter a username which will be used by any CPE trying to connect to Vigor router.
	• Password – Enter the password for the user.
	 Polling Interval (sec.) - Enter the time value (unit is second). The range is from 60 ~ 86400.
	IPsec VPN Settings – Central VPN management is operated through IPsec VPN connection.
	 IPsec Mode – Choose Aggressive or Main as the IPsec Mode.
	 Security Method – Choose one of the following methods (AH or ESP) for the security of data transmission. For example, choose AH to specify the IPsec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
	 Encryption Type – Choose one of the selections as the encryption type.
	 Local Subnet – Select LAN1 or Manually.
	 CVM LAN IP / Mask –Enter the IP address and subnet mask of local host.
	AP Management
Enable AP	Click to enable or disable the access point management function.

Management	
	Device Management
Device Management	Click to enable or disable the device management function.
Respond to external device	Click to enable or disable the function. If enabled, the router will function as a slave device.
Save	Save the current settings.

9.4.17.8 TR069 Settings

CPE device supports the TR-069 standard for remote management by VigorACS.

Maintenance	2927ac_1449BC30C3F0 / Configu	ration / System		G.
Time Setting.	ACS Server			
NetFlaw				
Admin Account	Primary			
Admin Local User	Tr069 Enable			
SNMP Settings	HTTP compression Enable			
Management	ACS Server On	Internet ~		
TRONG Settings	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	interver		
Webbook	URL	http://rd8acs.draytek.com:8080/ACSSe		
SysLog Settings	1.1	Acquire URL from DHCP option 43		
Mail Alert	Usemame	rd3network		
Internal Service User List	Password		a	
Panel Control	STUN Setting			
	Enable STUN			
	Server Address			
	Server Port.	34/15		
	Minimum Keep Alive Period	6W		
	-		Save	

ltem	Description		
	Description		
	Primary		
Tr069 Enable	Click to enable or disable the TR-069 functionality.		
HTTP compression Enable	Click to enable or disable the HTTP compression function.		
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.		
URL	Enter the URL for connecting to the ACS. Acquire URL from DHCP option 43 - Select to acquire the ACS URL from DHCP option 43.		
Username	Enter the username required to connect to the ACS server.		
Password	Enter the password required to connect to the ACS server.		
	STUN Settings		
Enable STUN	Click to enable or disable the function.		

Server Address	Enter the IP address of the STUN server.		
Server Port	Enter the port number of the STUN server.		
Maximum Keep Alive Period	Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server.		
Minimum Keep Alive Period	Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server.		
	XMPP Settings		
Enable	Click to enable or disable the XMPP settings.		
Use SSL/TLS	Click to enable or disable the SSL/TLS encryption protocols.		
	Client Settings		
Protocol	Select Https if the connection is encrypted; otherwise select Http.		
Client URL	Displays the URL of the client.		
Port	In the event of port conflicts, change the port number of the CPE.		
Username	Enter the username that the VigorACS will use to connect to the CPE.		
Password	Enter the password that the VigorACS will use to connect to the CPE.		
	Periodic Inform Settings		
Enable Periodic	Click to enable or disable the function.		
Inform	If enabled, the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field.		
Inform Interval (sec.)	Set interval time or schedule time for the router to send notification to CPE.		
	Advanced		
Disable TR069 configuration change from CPE UI	Click to enable or disable the function.		
	Apply Settings to APs		
Enable	Click to enable or disable the function.		
AP Password	Enter the password of the VigorAP that you want to apply Vigor router's TR-069 settings		
Apply Specific STUN Settings to APs	Click to enable or disable the function of applying specific STUN settings to AP. If enabled,		
	Enable AP STUN - Click to enable or disable the STUN server settings.		
	Server Address - Enter the IP address of the STUN server.		
	Server Port - Enter the port number of the STUN server. Maximum Keep Alive Period - Enter the maximum interval between		
	keep-alive messages that the CPE client sends to the ACS server.		
	Minimum Keep Alive Period - Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server.		
	CPE Notification Settings		
Enable	Click to enable or disable the function.		
	If enabled, select the notification item(s) by clicking it. Vigor router will		

	 send the utilization status to VigorACS. Web Login Web Configuration High Availability SSH Login SSH Command 	
Bandwidth Utilization	Enable - Click to enable or disable this function. To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in mediand high fields), a notification will be sent to VigorACS. After a long time observation, the administrator can determine if it is necessary to increat the bandwidth setting for that CPE or not. The default is disabled.	
	Time Period – Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS.	
	 Enable / WAN – Choose the WAN interface by clicking Enable for applying the bandwidth utilization notification mechanism. 	
	 Threshold Level – Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization. 	
	 Line Speed – Set the transmission rate and receiving rate for specified WAN interface. 	
Save	Save the current settings.	

9.4.17.9 Webhook

Vigor router will send a report (webhook message) including WAN up, down, CPU usage, memory usage and etc. to a monitoring server periodically.

Maintenance	2927ac_1449BC30C3F0 / Configu	uration / System Webhook				C
Time SetLings	System Webhook					
NetFlow						
Admin Account	Enable					
Admin Local User	Monitoring Server URL					
SNMP Settings	Report Period (minutes)	a				
Management	() Note:					
TRD69 Settings			e by default. When the Mon	iltoring Server supports HTTP and		
Weitisrede						
Systog Setting,						
Mall Alert					Cancel	Save
Internal Service User List	-					
Panel Control						

These parameters are explained as follows:

Item	Description
Enable	Click to enable or disable the Webhook function.
Monitoring Server URL	Enter the URL of a server.
Report Period (minutes)	Define the interval time for each report to be sent.
Save	Save the current settings.

9.4.17.10 SysLog Settings

SysLog function is provided for users to monitor router.

Maintenance	2927ac_1449BC30C3F0 / Configur	ation / System		C
Fime Setting.	Enable	0		
NetFlow	Syslog Save to	Systog Server 🔲 USB Disk		
Admin Account	Sision Save to	Systeld States		
Admin Local User	Maximum Syslog folder space	1	GB 🛩	
SNMP Settings	When Syslog folder is full	Overwrite oldest log. Stop logging		
Management	RouterName	DrayTek		
TROE9 Settings	Primary Syslog Server			
Webbook				
Systog Settings	Server IP Address / Hostname			
Mail Alert	Destination Port	514		
Internal Service User Test	Secondary Syslog Server			
Panel Control				
	Server IP Address / Hostname			
	Destination Port	514		
	Mail Syslog	02		
	Collect Syslog About	Pirewall Log		
		VPN Log		
		User Access Log / Hotspot User Information		
	Clear			Saye

These parameters are explained as follows:

ltem	Description
Enable	Click to enable or disable the Syslog function.
Syslog Save to	Select Syslog Server and / or USB Disk.
Maximum Syslog folder space	Set a space (unit GB/MB) to store event logs.
When Syslog folder is full	Overwrite oldest logs - If selected, the action of overwriting the olderest logs will be executed.
	Stop logging - If selected, the action of stopping logging will be executed.
Router Name	Display the name for this router.
Primary / Secondary Syslog Server	Server IP Address / Hostname - Enter the IP address of the Syslog server. Destination Port - Enter a port for the Syslog protocol.
Mail Syslog	Click to enable or disable the function. If enabled, it will record the mail event on Syslog.
Collect Syslog About	Select the type of log to send the corresponding message to syslog.
Save	Save the current settings.

9.4.17.11 Mail Alert

This page allows to configure settings for Mail alert.

	2927ac_1449BC30C3F0 / Con	figuration / System			
Settings	Enable				
w		Send A Test E-Mai			
Account			-		
Local User	Interface	Апу	~		
Settings	SMTP Server				
ement	SMTP Port	25			
Selling	Май То				
ok	Sender Address				
Settings					
	Connection Security	Planintext	×		
		g plain text If the StartTLS conner (the Start(TLS connection fails	tion fails.		
l Service User List. Iontrol	StartTLS: Accept usin Force StartTLS: Sinp ii		tion fails.		
	StartTLS: Accept usin Force StartTLS: Sinp A Authentication		tion fails.		
	SartTL5: Accept usin Force StartTL5: Size # Authentication Username		ston fails.	2	

These parameters are explained as follows:

ltem	Description
Enable	Click to enable or disable the mail alert function. Send Test E-Mail - Make a simple test for the e-mail address specified in this page.
Interface	Specify an interface.
SMTP Server	Enter an IP address of the SMTP server.
SMTP Port	Enter the port number of the SMTP server.
Mail To	Specify a mail address for receiving the mail.
Sender Address	Specify a mail address for sending mails out.
Connection Security	 Select a method (Plaintext, SSL, StartTLS or Force StartTLS) to ensure the connection security. SSL means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. Accept using plain text if StartTLS connection failed.
	• Force StartTLS. Stop if StartTLS connection failed.
Authentication	Click to enable or disable the function. If enabled, the authentication will be activated while using an e-mail application.
Username	Enter the user name for authentication.
User Password	Enter the password for authentication.
Enable E-Mail Alert	Select the item(s) to send the alert message to the e-mail box while the router detecting the item(s) you specify here.
Save	Save the current settings.

9.4.17.12 Internal Service User List

This page allows you to turn on or turn off security authentication service (offered by internal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.

	2927ac_1449BC30C3F0 / Cont	figuration / System			
e Settings	Enable				
How		Send A Test E-Ma			
sin Account		Send A Test E-Ma			
n Local User	Interface	Алу	~		
Settings	SMTP Server				
gement	SMTP Port	25			
9 Salung-	Maii To				
eok	Sender Address				
ng Settings					
	Connection Security	Planintext	*		
luuri 1al Service User List	Note:	The search of th			
nal Service User List	Note: * StartTL5 : Accept using	g plain test if the StartTLS conne			
al Service User List	Note: StartTLS: Accept using Force StartTLS: Stop #	The search of th			
al Service User List	Note: * StartTL5 : Accept using	g plain test if the StartTLS conne			
aal Service User List	Note: StartTLS: Accept using Force StartTLS: Stop #	g plain test if the StartTLS conne			
aal Service User List	Note: • Start 11.5 : Accept usin • Force Start 11.5 : Stop # Authentication	g plain test if the StartTLS conne		ė-	
aal Service User List	Note: • Start115 : Accept usin • Torce Start112; Stop A Authentication Username User Password	g plain text II the StartTLS conne the StartTLS connection Tails	ction fails.	5	
	Note: • Start115 : Accept usin • Force Start1125 Shop A Authentication Username	g plain test if the StartTLS conne		÷	

These parameters are explained as follows:

ltem	Description
Username	Display the name of the existed user profile.
Internal Services RADIUS	Click to enable (turn on) or disable (turn off) the security authentication service offered by the internal RADIUS server for the user profile.
Internal Services Local802.1X	Click to enable (turn on) or disable (turn off) the security authentication service offered by the Local 802.1X server for the user profile.
Apply	Save the current settings.

9.4.17.13 Panel Control

This page allows you to customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

Configuration	2865ac_001DAA000000 / Configu	ration / System			
intenance	LED				
e Settings	and the second				
nin Account	Enable LED	C			
sin Local Uses	Enable Sleep Mode	D			
IP Settings	Turn off LED after (Minutes)	1			
geneni					
ð Settings	Button				
og Settings	Wirefess	•			
	and the second se				
	Factory Reset	C			
mal Service User List	Note:	inctions of "Wireless Button" and "Fa	actory Reset Button" on the front panel as below: LED On	LED Off	
mal Service User List	Note: Enable the Sleep Mode will make the fu	inctions of "Wineless Button" and "Fa	LED On Wreless On/Off/WPS		
mal Service User List	Note: Enable the Skeep Mode will make the tw LED Status Wireless Button Factory Reset Button	unctions of "Wireless Builton" and "Fo	LED On	LED ON Turn LED On*	
mal Stavice User List	Note: Enable the Sacep Mode will make the tw LED Status Windess Button	unctions of "Wireless Builton" and "Fo	LED On Wreless On/Off/WPS and: Turn LED off Immediately*		
mal Service User List	Note: Enable the Sleep Mode will make the hu LED Saltus Winkes Button Factory Reset Button *308 functional even the buttons are di	unctions of "Wireless Builton" and "Fo	LED On Wreless On/Off/WPS and: Turn LED off Immediately*		
Alert Annak Service Liner Line Al Longend	Note: Enable the Skeep Mode will make the hu LED Saturs Workless Button Factory Reset Button "Soil functional even the buttorn are dh USB	Inctions of "Wheeless Button" and "Fo W Prios 1 seco Prios 1 seco Prios to the Prios to the Prio	LED on Windess On,/Off/WPIS On Erun LED off Internediately* ACT light flashing: Reset router		
mal Service User List	Note: Enable the Skeep Mode will make the hu LED Saturs Workless Button Factory Reset Button "Soil functional even the buttorn are dh USB	Incisions of "Whreless Buttion" and "Fa W Protos 1 seco Press till the sabled.	LED on Windess On, Off, WPS On Charn LED off Internediately* ACT light flashing: Reset router Status		

ltem	Description
	LED
Enable LED	Click to enable or disable the LEDs to function according to the configured settings.
Enable Sleep Mode	Click to enable (turn on) or disable (turn off) the LEDs after the specified number of minutes has elapsed.
Turn off LED after (Minutes)	Enter a number.
	Button
Wireless	Click to enable or disable the ability of the Wireless button to control WLAN and WPS functions.
Factory Reset	Click to enable or disable the reset function of the factory reset button.
	USB
Enable	Click to enable or disable the USB port.
	LAN Port
Enable	Click to enable or disable the LAN port.
Status	Displays the status of the USB port.
Speed	Displays the negotiated speed of the LAN port.
Cancel	Discard current modification.
Save	Save the current settings.

9.4.18 Switch

9.4.18.1 Status

It displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch connected to Vigor router.

Switch Status

Switch Status	Switch Hierarchy					
Status						
Group	Switch Name	IP Address MAC /	Address Model	System Up Time Port In Us	e Clients	Firmware Version
			No data available			
New Switch List						
Index	Switch Name	IP Address	MAC Address	Model	Firmware Ver	sion
0 1	G2280	• 192.168.1.1	0 00:1D:AA:22:80	0:AA G2280	2.5.1_RC5	
0 2	P2500	• 192.168.1.1	2 00:1D:AA:4C:1	8:83 P2500	2.6.0_RC1	
		-				

ltem	Description
Status	Displays the switch which is managed by Viogr router.
	Group - Displays the name link of the group. You can click the link to modify the group settings if required.
	Switch Name - Displays the name link of VigorSwitch. You can click the name link to access into the switch profile.
	IP Address - Displays the IP address of VigorSwitch.
	MAC Address - Displays the MAC address of VigorSwitch.
	Model - Displays the model name of VigorSwitch.
	System Up Time - Displays the time accumulated since this Vigorwitch is powered up.
	Port in Use - Displays how many devices connected to VigorSwitch.
	Clients - Displays the number of LAN ports used in VigorSwitch.
	Firmware Version - Displays the firmware version that VigorSwitch current used.
New Switch List	The one under New Switch List is allowed to be managed under current used group.
	+Add Device - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status.

	tus	Switch Hierarchy				
Status						
Group		Switch Name	IP Address	MAC Address	Model	System Up Time
					No data available	
w Switch Li	st					
Add Device						
	Index	Switch Name	IP Addre	\$\$	MAC Address	
	1	G2280	• 192.1	68.1.10	00:1D:AA:22:80:4	AA
	2	P2500	• 192.1	68.1.12	00:1D:AA:4C:18:8	83
Switch Sta Status	itus	Switch Hierarchy				
itus						
oup		Switch Name	IP Address	MAC Address	Model	Sys
efault		G2280	• 192.168.1.10	00-1d-aa-22-80-	-aa G2280	
Default ew Switch L	lst	G2280	• 192.168.1.10		-aa G2280	
Default lew Switch L +Add Device		62280	• 192.168.1.10		-aa G2280	
/ Switch L		G2280 Switch Name				0:5 ddress

Switch Hierarchy

This page displays the hierarchy of VigorSwitch(es) managed under Vigor router.

	/ Configuration / Switch	8
Profile	Switch Status Switch Hierarchy	
Alert And Log	PI	
Database Settion Group	VigorSwitch G2280 11 192,165,10 G2280	
Maintenance	92	
	19	
	14	
	<i>F</i> 5	

9.4.18.2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor router. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.

Status			····· / Configuratio	n / Switch			
Profile	Profile I	List					
Alert And Log							
Database Setup		Index	Name	Group	IP Address	MAC Address	Model
Group		1	G2280	Default	• 192.168.1.10	00-1d-aa-22-80-aa	G2280
Maintenance							
	New Sw	itch List					
	+Add De	evice					
		Index	Switch Name	IP Address	MAC Address	Model	Firmware Version
		1	P2500	• 192.168.1.12	00:1D:AA:4C:18:83	P2500	2.6.0_RC1

These parameters are explained as follows:

Item	Description
	Profile List
Delete	Click to remove the selected entry from the profile list.
Check box	Click to select the device.
Index	Displays the index number of the switch profile.
Name	Displays the name of the switch profile.
Group	Displays the group name of VigorSwitch(es).
IP Address	Displays the IP address of VigorSwitch.
MAC Address	Displays the MAC address of VigorSwitch.
Model	Displays the model name of VigorSwitch.
	New Switch List
+Add Device	Make the selected VigorSwitch to be managed by Vigor router and be shown under Profile List.
Index	Displays the index number of the switch device.
Switch Name	Displays the name of the switch.
IP Address	Displays the IP address of VigorSwitch.
MAC Address	Displays the MAC address of VigorSwitch.
Model	Displays the model name of VigorSwitch.
Firmware Version	Displays the firmware version that VigorSwitch current used.

To edit profile for the selected switch:

1. Selecting one device from the Profile List. Click on the entry to open the following page.

Switch Profile 1 : G2280		
General VLAN Port		
Index	1	
Switch Name	G2280	
Comment		
Trap Community Name		
Enable Copy configuration	\bigcirc	
Copy configuration from	None •	
Login Password	••••• •	
IP Address	DHCP 192.168.1.10	
Set General to Factory Default		Cancel Save Send to Devi

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the switch profile.
Switch Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Comment	Enter the text in such field if additional explanation for the switch is required.
Trap Community Name	Enter the text in such field as trap community.
Enable Copy configuration	Click to enable or disable the function.
Copy configuration	Check the box to copy configuration from other device. Use the drop down list to choose the one you need.
from	Note, if there is only one VigorSwitch connected and managed by Vigor router, then such field is unavailable.
Login Password	Displays the original login password for the VigorSwitch.
IP Address	Display the dynamic IP address (of the connected switch) assigned by Vigor router.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.
Send to Device	Transfers the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately.

2. After finished the settings, click VLAN tab to open following page.

Blank page due to LAN>>VLAN not configured previously:

itch Profile General	1 : G228 VLAN		rt																			
uter VLAN																						
roup S	ubnet	VID	Priority	P1		P2	P3		P4	P5	SSID1	SSID2	SSID	3 1	SSID4	ss	ID1 5G	SSID2	5G	SSID3 5G	SSI	ID4 50
										No data ava	lable											
										NO Gata ava	nabre											
						10		13				17 16	10	20	24	22		24	24	26	37	
ernal Switc 1		- Port Mer 3 4	nbers 5 6	7	8 5	10	11	12	13	14 15	16	17 18	19	20	21	22	23	24	25	26	27	28
				7	8 5	10	11	12	13		16	17 18	19	20	21	22	23	24	25	26	27	21
	2	34							13	14 15 No data avai	16 Ilable	17 18	19	20	21	22	23	24	25	26	27	2

Setting page with LAN>>VLAN configured previously:

iroup	Subne	t	VID	Prie	ority	P1		P2	P3		P4		P5	SS	ID1	SSID2		SSID3	2	SID4	SSID	1 5G	SSID2 5	5	SSID3 5G	SSI	04 5G
LAN0	LAN1		0	0									2							3							
LAN1	LAN2		10	0							\boxtimes							\boxtimes		0						\boxtimes	
LAN2	LAN3		20	0	0						\boxtimes								Ð	\boxtimes						\boxtimes	
ternal Sw	itch Vl	AN - F 2	ort Mei 3	nbers 4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
					5	6	7	8	9	10	11	12	13	14	15	16 💟	17	18	19	20	21	22	23	24	25	26	
ternal Sw lan0 [0] lan1 [10]	1	2	3	4							11 🖸		13 🖸	14	15 🖸												27

3. Click Save to save VLAN configuration. Then, click Port tab to access the following page:

General VLAN Por	t			
ort Description	Port Control	Schedule	Ingress Rate (Kbps)	Engress Rate (Kbps)
	Enable Port	•	•	0
	Enable Port	• 0 , 0	•	0
	Enable Port	▼ 0 , 0	•	0
Uplink	Enable Port	• 0 , 0	•	0
	Enable Port	▼ 0 , 0	•	0
s	Disable Port	• 0 , 0	•	0
j	By Schedule	• 0 , 0	•	0
	Enable Port	▼ 0 , 0	•	0
	Enable Port	▼ 0 , 0		0
	Enable Port	▼ 0 , 0	•	0
0	Enable Port	· 0,0		

These parameters are explained as follows:

ltem

Description	If required, enter a brief description to explain the device connected to VigorSwitch via the LAN port.
Port Control	Disable Port – The port (e.g., Port 3 in this case) which is used to connect VigorSwitch and Vigor router will not be shutdown by Vigor router.
	Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Save, the network connection between that device and VigorSwitch will be terminated.
	By Schedule – Two schedule profiles can be specified here to force Vigor router executing specific action to VigorSwitch.
Ingress Rate	Check the box for entering the ingress rate for the selected VigorSwitch. After clicking Save, the value modified in this page will be written to VigorSwitch and enabled.
Egress Rate	Check the box for entering the egress rate for the selected VigorSwitch. After clicking Save, the value modified in this page will be written to VigorSwitch and enabled.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings.
Send to Device	Transfers the configuration change (e.g., login password, switch name, etc.) to the VigorSwitch immediately.

4. Click Save to save the changes and then click Send to Device. Settings will be sent to VigorSwitch immediately.

9.4.18.3 Alert And Log

Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly.

Alert Setup

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

ke -	Enal	ble Alert a	nd Log	2						
lich and Port Setup	Alert	Levels	and Action							
rtLogs	index	Enable	Level Name	Color	Create Log	send Notification	object 1	object 2	object a	Object 4
base Setup	4		No Alert	No Color	No Log	No Notification				
	2		Minor Alert	0	Enable	No Notification				
enance	2		Moderaté Alert	- @ c			sms 1-777 ~	sms1-777 ~	sms 1-777 🗢	sms 1-777
	4		Major Alert	000		13	sms 1-777 ~	sms 1 ??? •	suns 1.777 ~	sms 1-77
	5	¢,		0.00	Ð	13	sms 1-777 ~	sms 1-??? ~	sms 1-??? ~	sms 1-77
	6	п		0	TT.	17	sms 1-777 ~	sms 1-??? ~	sms 1-??? 😒	sms 1-771
	7	a		000		10	sms 1-??? ~	sms 1-??? ~	sms 1-??? 👻	sms 1-777
	6	a		000	0	10	sms 1-777 😒	sms 1-??? 🗸	sms 1-??? 👒	sms 1-???

These parameters are explained as follows:

ltem

Description

Enable Alert and Log	Click to enable or disable the function.
	Exadite Alert And Log
	Alert Levels and Action
	index Dadde Level Name Calor Create ing Send NorthCalor Object 2 Object 3 Object 4
	2 De Meur Alus De Endre Na Nestalation
	a 🗴 Maasaa Aast 2 🗗 🖬 🕬 waa 1977 - waa 1977 - waa 1977 - waa 1977 -
	4 🖬 Major Alem 🚱 🔹 - anno 6777 • anno 6777 • anno 6777 • .
	Alert Levels and Action
Index	Displays the index number of alert profile.
Enable	Check it to enable this feature.
Level Name	Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined.
Color	Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed.
Create Log	Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default.
Send Notification	If it is checked, Vigor router's system will send notification to specified phone number via SMS.
Send Notification Object 1 ~ 4	

Switch and Port Setup

This page defines enabling switch alert and/or port alert for each switch.

Status	2927ac_1449BC30C3F0 /	Configuration / Swite	ch			e
Profile	Index Switch Name	IP Address	Model	switch Alert	Port Alert	
			No data available			
Alert Setup						
Alert Logs						
Database Setup						
Group						
Maintenance						

ltem	Description
Index	Displays the index number of the alert profile for switch(es).
Switch Name	Displays the name of the switch.
IP Address	Displays the IP address of the switch.
Model	Displays the model name of the switch.
Switch Alert	Displays the switch alert status.
Port Alert	Displays the port alert status.

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

Index	1		
Switch Name	G2280		
IP Address	192.168.1.10		
Model	G2280		
Switch Alert	Enable Disable		
Port Alert	Enable Disable		
Cold Start	4-Major Alert	•	
Warm Start	4-Major Alert	•	
Disconnect	4-Major Alert	•	
Reconnect	2-Minor Alert	*	
Port Alert			
Port Description	Device Disconnects	Device Reconnects	Schedule On/Off
1	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻
2	1-No Alert 👻	1-No Alert 👻	1-No Alert 👻
Set to Factory Default			

These parameters are explained as follows:

ltem	Description
Index	Displays the index number of the alert profile for switch(es).
Switch Name	Displays the name of the switch.
IP Address	Displays the IP address of the switch.
Model	Displays the model name of the switch.
Switch Alert	Enable - Click to enable the switch alert function.
	Cold Start, Warm Start, Disconnect, Reconnect - When VigorSwitch encounters the alert events, alert mechanism will perform corresponding actions based on the servity level of the incident encountererd. Specify the severity level (Minor, Major, or No) for each incident.
	Disable - Click to disable the switch alert function.
Port Alert	Enable - Click to enable the port alert function. Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this page. Each port can be confgiured with different alert level for diffent alert event. Disable - Click to disable the port alert function.
Port Alert table	Port – Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this table. Each port can be confgiured with different alert level for different alert event.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

Alert Logs

The system administrator can get the information by filtering the collective information based on the conditions specified in this page.

Status	2927ac_1449BC30C3F0 / Configurat	ion / Świtch				0
Profile	Select Columns to Filter Logs			*		
Alert Sidup	Level					
Switch and Port Setup	Туре	Switch Alert Port Alert				
	Switch		4			
latabase Setup	Time Period	Last 24 Hours Last 7 Days				
тонр				_		
lainterance				Apply		
	Alert Logs					
	OLugs				ia 🤟 🚹	70 % N
	Index. ¹⁴ Level Name	те ут туре	switch	Port	incident	-24
		Ne	data available			
	-					

These parameters are explained as follows:

ltem	Description
Select Columns to Filter Logs	Level – The alert can be divided into several levels, Minor Alert, Moderate Alert and Major Alert. Check the one(s) you want to check in Alert Logs list.
	Type – Select the type (switch / port) of the log to be displayed in Alert Logs list.
	Switch – Switch(es) connecting to Vigor router will be shown in this area. Select the one you need.
	Time Period - Select Last 24 Hours or Last 7 Days as time period.
	Apply – Click to save the configuration.
	Log related to the items selected above will be shown in Alert Logs list.
Alert Logs	This area displays logs (level name, time, type, switch, port, and incident) related to VigorSwitch managed by Vigor router.

9.4.18.4 Database Setup

The database of the switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of the switch.

Status	2927ac_1449BC30C3F0 / Configuration / S	witch	C
Proite Alest And Log	Enable Database to Record alert logs and traffic history	2	
pelanarikaitan Graup Maintenance	Database Usage N Notification Sc Email Notification Object 1: SMS Notification Object 9	s USB Disk Desected /A end notification ~ 777 ~ Custom 1 ~	
	Action	ackup and clean up all user info, ar \vee	Save

These parameters are explained as follows:

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

Enable Database to Record alert logs and traffic history	Click to enable or disable the function. If enabled, it will make the database (in USB disk) record the alert logs and traffic history.
File Path	Displays the file path for storing the logs.
Database Usage	Displays the used capacity.
Notification	Send notification - A notification will be sent out when there is no capacity for storage in USB.
	 Email Notification Object - Choose an email notification object profile.
	• SMS Notification Object - Choose a SMS notification object profile.
	Don't send notification - No notification will be sent out when there is no capacity for storage in USB.
Action	Choose an action.
	Backup and clean up all user info, and start a new record - Only the newest events will be recorded by the system.
	Stop recording user information - When the capacity of log is full, the system will stop recording.
Save	Save the current settings.

9.4.18.5 Group

Different switches can be classified into different group(s). There are ten switch groups available for configuration.

Status	2927ac_1449BC30C3F0 / Configuration / Switch		C
Profile	Index Group Name	Member Switch	
Alert And Log	1 Default		
Database Setup	1		
Mantenanor	5		
Mantenance	6 T		
	8. 9		
	10		
	2		

To configure the group settings, move the mouse cursor to any entry and click to open the following page.

2865ac_001DAA000000 / Configuration / Switch	h		C
Index	1		
Profile Name	Default		
Enable Group Password			
Group Password	Φ		
Member Switch			
		Cano	cel Save

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

Index	Displays the index number of the profile.
Profile Name	Enter a name as the group name.
Enable Group Password	Click to enable or disable the group password.
Group Password	Enter a password that the system administrator can use to access into the managed VigorSwitch connecting to Vigor router.
Member Switch	Choose the switches you want to group.
Cancel	Discard current modification and return to previous page.
Save	Save the current settings and return to previous page.

9.4.18.6 Maintenance

This page is able to execute configuration backup, restore, reboot or reset the VigorSwitch devices remotely.

	2865ac_001DAA000000 / Configurat	tion / Switch			
Status	Action Type	Config Backup	÷		
Profile	Select Device				
Nert And Log	Select Device				
Database Setup	Switch Name	MAC	P	Download Config	
	52280	00-10-49-22-80-49	192.168.1.10	Â.	
					Sec

ltem	Description
Action type	Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor router to perform on VigorSwitch.
	Config Backup - Perform the configuration backup.
	Config Restore - Perform the configuration restoration.
	• Restore Config From - Select Local File or Shared Folder.
	• File/Path - Click Browse to locate a file.
	Remote Reboot - Reboot the VigorSwitch devices remotely.
	Factory Reset - Reset the VigorSwitch devices with factory default settings.
	Select Device
Switch Name	Displays the name of the switch.
MAC	Displays the MAC address of the switch.
IP	Displays the IP address of the switch.
Download Config	Click to download the configuration file and store on the host.
Save	Save the current settings.

9.5 Advanced

(7)	Advanced	
000	Parameter Tree	
<u></u>	Exclude Parameters	
	Common UI Status	
~	Test Inform	
I E		

9.5.1 Parameter Tree

All control parameters of the selected CPE will be presented on this page with a tree view that is convenient for the administrator/user to view and select.

Dray Tek VigorACS 3	2917Lac_)4499C023768 🗸 🔍		16:30 mk_carrie M 75/74 System Administrator
2927Lac_1449BC023768 / Advanced / Parameter Tree			2
Name		Value	DataType
 Ø InternetGabewayDevice. 			
C LANDeviceNumberOIEntries		9	
WANDeviceNumberOfEntries		6	
p 🐼 Deviccinfo.			
D 🔕 ManagementServer.			
p 🐼 Time.			
D Q Layer3Forwarding.			
1 🐼 LANDevice.			
D 🐼 WANDevice.			
p. 🐼 X_00507F_InternetAcc.			
P @ X_00507F_LAN			
X_00507F_LoadBalancePolicyNumberDfEntries		14	
X_00507F_LoadBalancePolicy.			
) @ X_00507F_NAT.			
₽			
0 🐼 X_00507F_Bandwidth			
p 🐼 X_00507F_Applications.			
b ⊗ X_00507F_VPN.			
b 🐼 X_00507F_WirelessLAN.			

ltem	Description
Name	Lists the name of the parameter.
Value	Displays the setting value (true/false, numbers, selections and etc.) of the selected parameter. Sometime, It might be null.
DataType	It means the data type (e.g., string, boolean or unsignedInt) of the parameter. However, the corresponding information will be displayed in this field only if the parameter allowed to be written.
Сору	Copy the selected parameter with the value. The copied parameter can be added onto the XML template downloaded from Provisioning>>Global Parameters. After that, the completed XML template can be saved as a sampling profile which will be selected and applied to Provisioning>>Global Parameters.

9.5.2 Exclude Parameter

The firmware version of the managed CPE might be different from the data stored on VigorACS database. Therefore VigorACS will compare the available parameters of the selected CPE with the one stored in the VigorACS database automatically. When some of the parameters not supported by the CPE, those parameters will be listed on this page.

Dray Tek VigorACS 3	7927Lac_14498C023758 V Q	Di 16-32-02 mk_carrie
2927Lac_1449BC023768 / Advanced / Exclude Parameter	ters.	c
Ill Deleter All		
Parameter		
InternetGatewayDevice X_00507F_Status.CPUTemperature		
InternetGatewayDevice X_00507F_Status.MonitoringDevicesStat	stics.Chent562.Chent.	
InternetGatewayDevice.ManagementServer.AliasBasedAddressin	e,	
InternetGatewayDevice ManagementServer.InstanceWildcardsSa	pported	
InternetGatewayDevice.X_005071_VPN.ConnStatusNumberOfEn	mes	
InternetGatewayDevice X_00507F_MaxNumberDfLoadBalanceFe	licy	
InternetGatewayDevice-X_00507F_InternetAcr_MultiPVCs.Genera	L(x) WARL(y).	
InternetGatewayDevice.X_0050/F_InternetAcc.WAN.(x).InternetF	hysical Type	
internetGatewayDevice.X_00507F_InternetAcc.WAN.(a).MTU		
InternetGatewayDevice X. 00507F_LTE LTEStatus ModernICCID1		
internetGatewayDeviceX_00507F_LTE.LTEStatus.ModemICCID2		
internetGatewayDeviceX_00507F_Operation_Mode_AP		
InternetGatewayDevice.X_00507F_VPN.ConnStatus.JxJ.Phs2Netv	rorkidi.	
InternetGatewayDevice X_00507F_Wirelessi AN,General LongPre	amble	
InternetGatewayDevice.X .005071 WirelessLAN AP,General.Mod	eList	
InternetGatewayDevice.X_00507F_WirelessLAN_SG.General.TxBu	vst	
InternetGatewayDevice-X_00507F_WirelessLAN_5G_AP.General.M	fodeList	
InternetGatewayDeviceX_005071_USBApplication.GeviceStatus	Modem.1xi.SignalStrength	
hternetGatewayDevice.X_00507F_WirelessLAN.General.SSID.(x).	RateCsrt	
InternetGatewayDevice.X_00507F_WirelessLAN,General.SSID,(x).	Uplyad	
InternetGatewayDevice.X_D0507F_WirelessLAN.General.SS(D.(x).	Download.	
InternetGatewayDevice.X_00507F_WirelessLAN_5G.General.SSI0	(p).RateCrt	
InternetGatewayDevice.X_005071_WirelessLAN_5G.General.SSI0	(x)-Upiead	
InternetGatewayDeviceX_00507F_WirelessLAN_5G.General.SSIG	(x) Download	
InternetGatewayDevice.WANDevice.ix1.WANCommonInterlaceCo	nlig.WANInfName	

ltem	Description
Delete All	Click to remove all parameters listed in this page.

9.5.3 Common UI Status

This page allows the user to check if the UI file has been uploaded to VigorACS. If not, the VigorACS server can send a command to the CPE to prompt the upload of the UI file to VigorACS.

Dray Tek VigorACS 3	2927Lac_14498C023768 😪 🔍	Pcap	Q.	16:33:14 8/5/24	mk_carrie	М
2927Lac_1449BC023768 / Advanced	/ Common UI Status					¢
Device Name	2927Lac_L44960023768					
Model Name	Vigor2071_ar					
Firmware	4.4.2.3					
TR069 Support Status	Firmware Version is not supported					
	Upload Common UI File					

These parameters are explained as follows:

ltem	Description
Upload Common UI File	Click to request the selected CPE to upload the UI file to VigorACS. Once completed, the corresponding settings will be displayed on this page.

9.5.4 Test Inform

To test the bidirectional connection between the selected CPE and the VigorACS server, click on Scan Test.

Later the test result will be shown below.

Dray Tek VigorACS 3	29771 ac_144980073768	× •	Ptap	0	16:18:06 0/5/24	mk_carrie System Administrator	М
2927Lac_1449BC023768 / Advanced / Test.inform							C.
	Device Name	2927Lac_14498C023765					
	Model Name	Vigor2937Lac					
	Firmware	4.4.2.3					
		Start Tost					
	0-0	0-0					

Dray Tek VigorACS 3	2927L×_14498C023768		Peap	A	10.62.01. 3/5/28	mk_carrie	М
27Lac_1449BC023768 / Advanced / Test Inform 165353 (MF 165353) (MF 165353) (MF 165353) (MF 165353) (MF 165353) (MF 165354) (MF 165355) (MF 165355) (MF 165355) (MF 165355) (MF 165355) (MF 165355) (MF 165355) (MF 165355) (MF) 165355) (MF)							12
	Device Name	.7927f.ac_1449BC021768					
	Model Name	Viggar 29271.as:					
	Firmware	4.4.7.3					
		Start Tess					
	0-0	0 0					
19632 21632 21632 21653 216555 216555 216555 216555 2165555 2165555 2165555555555	3) JIVI 0) ACS GT Hug-/102 168 105.140306 JIVI0 3) Sep 2 ++ JIVI0 3) JIVI0 3) GT + Heppone HTTP/L1.200 GK HIVI0 3) JIVI0 3 GT + Heppone HTTP/L1.200 GK HIVI0 3) JIVI0 3 GT + Heppone HTTP/L1.200 GK HIVI0 3) JIVI0 3 GT + Heppone HTTP/L1.200 GK HIVI0 3) JIVI0 4 GT + HEPPONE HTTP/L1.200 GK HIVI0 4 GT + HEPPONE H	stewbyDeviceADeviceInt6. Manulacturer + DrayTek, Manulacturer01 = 14496C MaddName + Vggor307Lac Becrigtion = ThayFek Vggar Robinen ProductDas; + Vggr707Lac Sethalthumber + Id496C033768 HardwareVersion + 4 SoftwareVersion + 2 Wolfman + 4238 CWI = 14499C X, 0557F, ManagementUscename + 3dmin X, 0557F, ManagementUscename + 300 K, 0557F, ManagementUscename + 300 K, 0557F, ManagementUscename + 300 K, 0557F, ManagementUscename + 300 K, 0557F, ManagementUscename + 300					

This page is left blank.

Chapter 10 DrayTek Chatbot

DrayTek chatbot server offers a platform for the user account to check general information of the VigorACS server through the web-based browser.

10.1 Installation

DrayTek Chatbot will be installed in accompany by VigorACS software, refer to the section 2.1.3 Installation for VigorACS 3 for detailed information.

10.2 Overview

Login DrayTek Chatbot by entering the URL "https://(domain name or IP address):18443" on a web browser. Note that the port number defined for Chatbot is 18443.

Later, enter the user-defined user name and the password used for login VigorACS server. If not, use the default username/password (root/admin123) to login DrayTek Chatbot.

VigorACS Chatbot 🕰 Check Server Information 🕄 Server Maintenance 🗘 Diagnostic **Dump CPU Status** TCP/UDP Port Status Network Information Support & News ! Latest Alarms

The main screen of VigorACS Chatbot will be shown as follows:

Menu Items	Submenu
Check Server Information	Click the category to display the following submenu for viewing the server information.
	 Current CPU
	ACS Uptime
	 License Information
	 Login History

	 Disk SPACE Disk Usage For EMS Disk Usage For Log Top Disk Usage MySQL Table Current ACS Version Latest ACS Version
Server Maintenance	Click this item to display the history/log of Previous server maintenance.Backup DatabaseDownload Server Log
Diagnostic	 Click this item to display the result of the diagnostic. Dump Memory Status Dump CPU Status TCP/UDP Port Status
Network Information	Click this item to display information on the current network list. Show Network List
Support & News	 Click this item to get the news related to the VigorACS server. Knowledge Base Articles Security Advisory Show Latest News
Latest Alarms	This item will list the latest alarms related to VigorACS and/or CPE devices.Latest Alarms