

Release Notes for DrayTek Vigor 3910 (UK/Ireland)

| | |
|-------------------|---|
| Firmware Version | 4.3.2.8 – Mainline branch (Formal Release) |
| Release Type | Critical – Upgrade recommended immediately |
| Build Date | 7 th August 2024 |
| Release Date | 13 th August 2024 |
| Revision | 369_4221_f4ab312 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(None)

Improvements

1. Web GUI Security improvements
2. Corrected: An issue with the OpenVPN certificate was lost while downgrading the
3. firmware.
4. Corrected: An issue with failure to display correct DMZ host WAN status on the NAT >> DMZ Host page.
5. Corrected: An issue with failure to display the web page for Quality of Service on Bandwidth Management.
6. Corrected: An issue with failure to restore the settings with the backup file for Port Redirection / Open Ports on NAT.

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.
 2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
 3. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
 4. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration
 5. The TR-069 parameters for [Application] > [Smart Action] is not completed yet
 6. To prevent potential errors when upgrading firmware, it is recommended to upgrade firmware sequentially one version at a time (e.g., if the current firmware is 3.9.1, upgrade to 3.9.2 then 3.9.7.2, and then to the latest version)
-

Firmware File Types

The file name of the firmware controls which upgrade type is performed.

If the file name is unchanged (e.g. xxxx.all) then the upgrade will just upgrade the firmware, whereas renaming the firmware to a .rst extension will wipe all settings back to factory defaults when upgrading the firmware.

Upgrade Instructions

It is recommended that you take a configuration backup prior to upgrading the firmware. This can be done from the router's system maintenance menu.

To upgrade firmware, select '*firmware upgrade*' from the router's system maintenance menu and select the correct file. Ensure that you select the ALL file unless you want to wipe out your router's settings back to factory default.



Manual Upgrade

If you cannot access the router's menu, you can put the router into 'TFTP' mode by holding the RESET whilst turning the unit on and then use the Firmware Utility. That will enable TFTP mode. TFTP mode is indicated by all LEDs flashing. This mode will also be automatically enabled by the router if there is a firmware/settings abnormality. Upgrading from the web interface is easier and recommended – this manual mode is only needed if the web interface is inaccessible.

| | |
|-------------------|--|
| Firmware Version | 4.3.2.7 – Mainline branch (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 7 th May 2024 |
| Release Date | 19 th June 2024 |
| Revision | 367_4197_3248cd1 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(None)

Improvements

1. Password mechanism changed to force admin to change the password from the default password
2. Fix for the IPsec X.509 VPN packet size
3. Improvements to the WAN interface selection / WAN IP address shown in the PVC/WAN
4. Web GUI security improvements (jQuery update to 3.5.1)
5. The Let's Encrypt certificate failed to auto-renew
6. In some cases Windows L2TP IPsec VPN could disconnect every 8 hours
7. Login from a VPN subnet or non-directly connected LAN could fail
8. The UDP session over WireGuard VPN wasn't released after the VPN reconnection

Known Issues

7. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.
8. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
9. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
10. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration
11. The TR-069 parameters for [Application] > [Smart Action] is not completed yet
12. To prevent potential errors when upgrading firmware, it is recommended to upgrade firmware sequentially one version at a time (e.g., if the current firmware is 3.9.1, upgrade to 3.9.2 then 3.9.7.2, and then to the latest version)

| | |
|------------------|--|
| Firmware Version | 4.3.2.6 – Mainline branch (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 2 nd January 2024 |

| | |
|-------------------|-------------------------------|
| Release Date | 9 th February 2024 |
| Revision | 354_4126_de9d8a1 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

(None)

Improvements

1. Improvements to the WUI security
2. Fix for the WCF URL Reputation Get [Send Query Failure] & [Abnormal Server Response] errors
3. WCF/DNSF didn't work when the domain name exceeded 63 characters
4. In some circumstances SNMP could stop working after a few days of use
5. Fix for the DrayDDNS WAN IP updates
6. Fix for the use of IP alias with the mail objects
7. IPsec VPN rekeying could cause packet drops
8. In some circumstances firewall settings unexpectedly blocked IPv6 packets
9. The web portal image could not be displayed
10. The Specify Peer IP function didn't work with WireGuard LAN to LAN profile
11. The IKEv2 EAP connection via iPhone built-in VPN client could not be established
12. When HTTP Management Port was changed, port 80 would still respond
13. Remote VPN clients could not ping router's LAN IP when connected via IPsec LAN to LAN VPN tunnel

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.
2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
3. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above

4. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration
5. The TR-069 parameters for [Application] > [Smart Action] is not completed yet

| | |
|-------------------|--|
| Firmware Version | 4.3.2.5 – Mainline branch (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 28 th September 2023 |
| Release Date | 3 rd November 2023 |
| Revision | 350_4073_196e127 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

1. Support for the new WCF service – URL Reputation. If you have an existing activate licence, then this will be upgraded to the URL Reputation licence

Improvements

1. IP database for country objects updated
2. The [System Resource > Memory Usage] section on the Dashboard is showing DrayOS memory usage only
3. Fix an issue where forcing HTTPS connection to SMS provider did not work
4. Fix for IGMP not working correctly if both WAN1 and WAN2 were online
5. The SNMP settings were not available when SNMPv3 only was enabled
6. MyVigor product registration link could not be opened from router's WUI
7. Port 443 from LAN could be detected despite of disabling all known services
8. Fix for the firmware upgrade mechanism that was likely to be unsuccessful when MAX connection set to 1000K
9. The router could stop responding when IKEv2 re-dialled and the local ID was set to 32 characters
10. Multiple WANs with the same IP could affect services such as Hotspot Web Portal and VPN
11. Improvements to the IPSec multiple SA using phase2 network ID function
12. The TOTP 2FA pop up was not shown on SmartVPN Client if router's LAN DHCP scope was outside of the first 254 addresses of the network

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.

2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
3. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
4. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration
5. The TR-069 parameters for [Application] > [Smart Action] is not completed yet

| | |
|-------------------|--|
| Firmware Version | 4.3.2.4 – Mainline branch (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 25 th May 2023 |
| Release Date | 29 th July 2023 |
| Revision | 342_3979_6e34c6d |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

(None)

Improvements

1. Improvements to the Web GUI Security
2. The “-“ character can be used with the recipient number on the [Applications] > [SMS/Mail alert] configuration pages
3. [LAN] > [Wired 802.1x] new menu item added
4. Fix for the IPsec MultiSA VPN dial-up delay issue
5. VPN remote dial-in clients could not access the local server using the WAN Alias IP
6. 2FA web authentication via Telegram
7. Wrong source LAN IP was displayed by Ping Diagnosis
8. Access to the WUI did not work if an apostrophe was used
9. Sometimes MacOS/iOS VPN Remote Dial-in users could not reconnect over the IPsec protocol
10. Fix for the [Dashboard] > [Security] > [DoS] section displaying correct information when an attack was detected
11. Some Internet traffic was sent via non-existing WAN9 interface
12. The router could stop responding when downloading the debug log
13. Fixed an issue with the special character á in the "Receiving PIN via SMS Content" textbox for Hotspot Web Portal
14. The memory usage bar (Dashboard) was using the wrong (red) colour

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] -

“Restore Firmware with Config” feature, to load the previous configuration file along with the previous firmware.

2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
3. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
4. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration

| | |
|-------------------|--|
| Firmware Version | 4.3.2.3 – Mainline branch (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 29 th March 2023 |
| Release Date | 26 th April 2023 |
| Revision | 333_3924_5ab4adc |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

1. The new [NAT] > [Fast NAT] menu item added to increase the number of sessions established per second

Improvements

1. Improvements to the [WAN] > [Multi-VLAN] port-based bridge performance
2. The default [System Maintenance] > [Max Connection] value is 300K
3. SSL TLS Encryption 1.0 and TLS 1.1 in now disabled by default
4. Improvements to the route policy sent via WAN IP Alias
5. Fixed an issue with Canon printers that could not obtain a DHCP IP address
6. Improvements to the ICMP ping via the BGP route
7. WAN3 and WAN4 did not work simultaneously
8. MyVigor could not be connected after rebooting the router with Wipe Out All
9. Fixed an issue with the user-based firewall where only those users that fulfil the rule would be impacted
10. PIN could not be sent via SMS when the recipient number contained +(country code) character
11. IKEv2 VPN connection could drop every two hours
12. In some circumstances the L2TP over IPsec VPN connection to Synology NAS could disconnect
13. Multiple VPN tunnels could get disconnected due to an invalid server domain entered in the VPN profile 1
14. Remote IP not included in Access List could see the login page when HTTPS remote access and SSL VPN services were enabled
15. The host of the routed subnet was not accessible even when inter-lan routing was enabled
16. The firewall could stop working when the "IP Group (or IPv6 Group or Service Type Group)" contained a large number of IP objects

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.
2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management
3. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
4. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration

| | |
|-------------------|---|
| Firmware Version | 4.3.2.2 – Mainline branch (Formal Release) |
| Release Type | Critical – Upgrade recommended immediately |
| Build Date | 10 th January 2023 |
| Release Date | 3 rd March 2023 |
| Revision | 301_3844_df764e0 V400_RD3_432 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

(None)

Improvements

1. Improvements to the Web GUI Security (CVE-2023-23313)
2. SFP module information added to [WAN] > [General Setup]
3. Admin authentication can be linked with the TACACS+ server
4. APPE version updated from 15.27 to 15.29 (able to block AnyDesk)
5. Ports P3/P4 setup includes new selection for the speed drop-down menu:
"Auto, 2.5G_AN, 1G_AN, 100M_AN"
6. In some circumstances DNS forwarding did not work
7. Static route did not work for packets originated from Inter-LAN subnets
8. The VPN config backup did not restore the 'more' remote subnet section of the VPN profile

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.
2. Users logging into the web portal may cause the router to be too busy to respond quickly to the Web UI for management

| | |
|-------------------|--|
| Firmware Version | 4.3.2.1 – Mainline branch (Preview Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 11 th November 2022 |
| Release Date | 20 th December 2022 |
| Revision | 266_3711_ce83dc5 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug fixes and firmware improvements.

Release Candidate - Incorporates new features, bug fixes and firmware improvements.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

1. The [Routing] > [Load-Balance/Route Policy] profiles support "Session-Based" and "IP-Based" modes

Improvements

1. Daylight saving time will be enabled automatically
2. [LAN] > [Bind IP to MAC] comment entries can now have up to 31 characters
3. OpenVPN stability improvements
4. IPv6 NAT throughput improved for all subnets (LAN1 wasn't affected)
5. Fixed an issue where WAN (Static IP mode) reconnects often in HA hot standby mode
6. Router could stop responding when APM profile was sent to APs frequently
7. 2FA authentication code via SMS wasn't working
8. The WAN IP Alias interface selection was missing in Service Status section
9. In some circumstances dial-up NordVPN via OpenVPN LAN to LAN could not connect
10. Hotspot Web Portal settings could disappear after the reboot of the router
11. NAT loopback traffic was blocked wrongly when Firewall Default Rule was set to Block
12. The router's firewall default block rule could stop remote management, VPN access, and other local services
13. The USB thermometer (TEMPer1F_V3.4) could not be detected after the router reboot
14. Let's Encrypt auto renew certificate feature could fail due to the mismatch certificate and router domain
15. In some circumstances access to the router via WUI (http or https) could fail

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.

| | |
|-------------------|--|
| Firmware Version | 4.3.2 – Mainline branch (Preview Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 24 th August 2022 |
| Release Date | 16 th September 2022 |
| Revision | 239_3517_95064ee |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Release Candidate Firmware Branches:

Mainline - Formal releases of firmware incorporating any bug **fixes** and firmware **improvements**.

Release Candidate - Incorporates **new features**, bug **fixes** and firmware **improvements**.

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

1. Added support for multi-language WUI
2. Smart Action task automation feature can be run via CLI to trigger alerts, disable VPN profiles, schedule an NAT policy rule etc.
3. Central Switch Management supports new VigorSwitches including FX2120, PQ2200xb, Q2200x, P1282, and G1282
4. UDP broadcast traffic can be sent over VPN

Improvements

1. The APPE module upgrade from 15.25 to 15.27
2. Router's local services such as NTP and Mail Alerts did not work via WAN IP Alias addresses
3. MSS value will automatically change according to the MTU value (MSS = MTU - 140)
4. Mail Service Objects username and password fields accept up to 128 characters
5. In some circumstances there was high CPU usage and high VPN ping
6. Improved compatibility with SUMITOMO modems
7. VPN clients could obtain a duplicated IP address when DHCP relay was enabled
8. The router could stop responding when SSL VPN dial-out failed in linking state
9. WUI did not render some pages as expected after upgrading to 4.3.1.1 firmware
10. Router could stop responding when a Load Balance Policy was configured for VPN Trunk
11. Central Switch Management is now compatible with more than 15 LANs/VLANs
12. Remote dial-in users could not access LAN after changing VPN protocols between PPTP and SSL VPN
13. Virtual WAN traffic improvements
14. [WAN] > [Multi-VLAN] interfaces were unable to establish the PPPoE connections
15. Improvements to the LAN DNS functionality
16. OpenVPN generated certificate is valid for 10 years (previously 1 year only)
17. Improvements for WireGuard VPN stability
18. WireGuard MacOS clients can now use "Set VPN as Default Gateway"
19. TR-069 socket management improvements
20. Some DrayDDNS logs were incomplete

21. SFP LEDs did not work as expected
22. IKEv2 VPN users were disconnected during the rekey process
23. Improved compatibility with DHCP relay and VLAN tagged traffic
24. SSL VPN stability improvements
25. In some circumstances untagged PC could obtain an IP from a VLAN tagged subnet
26. Router could stop responding when WAN/LAN IPv6 option was enabled
27. An SNMPv3 agent could not get any data when using AES algorithm
28. Intermittent packet loss when routing through load balance policy that was set with an IP Alias (High Availability configuration)

Known Issues

After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.

Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.

| | |
|-------------------|--|
| Firmware Version | 4.3.1.1 – Mainline branch (Preview Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 19 th April 2022 |
| Release Date | 26 th May 2022 |
| Revision | 146_3126_869f846 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

To change firmware from one branch to another as a precaution take a configuration backup before performing the firmware upgrade

New Features

(None)

Improvements

1. Improved Web GUI Security
2. Updated HTTPS mechanism to address the CVE-2022-0778 (OpenSSL)
3. Central AP Management WLAN profiles support 802.11ax and 160 MHz options
4. Improved the CPU usage with multiple VPN connections
5. Router would become inaccessible when rebooted in some circumstances
6. A warning message will appear for reused IP object / IP Group profile that has already been used by other applications
7. OpenVPN dial-in users could not obtain an IP address
8. BGP compatibility between Vigor and Juniper improved
9. Some ARP frames did not meet the minimum expected size

Known Issues

After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.

Instead, we recommend using the [System Maintenance] > [Configuration Export] - "Restore Firmware with Config" feature, to load the previous configuration file along with the previous firmware.

| | |
|-------------------|--|
| Firmware Version | 4.3.1 – Mainline branch (Preview Release) |
| Release Type | Regular – Upgrade recommended when convenient Note: A previous firmware (3.9.6.3) was a critical release. This f/w includes all changes/improvements that were in 3.9.6.3. |
| Build Date | 08 th March 2022 |
| Release Date | 08 th April 2022 |
| Revision | 140_3094_04ec693 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

Mainline and Stable Firmware Branches:

Stable - Formal releases of firmware incorporating any bug **fixes** and firmware **improvements**.

Mainline - Incorporates **new features**, bug **fixes** and firmware **improvements**.

To change firmware from one branch to another; as a precaution take a configuration backup before performing the firmware upgrade

Stable - 3.9.7.2 - Latest release

Mainline - 4.3.1 - Adds new features including SD WAN, Wireguard VPN features and USB thermometer/storage support

New Features

1. Support for WireGuard VPN protocol, for both LAN to LAN and Remote Dial-In User VPN tunnels.
This service and its listening ports can be configured from the [VPN and Remote Access] > [WireGuard] menu, and enabled in [VPN and Remote Access] > [Remote Access Control]
2. SD-WAN is now supported in conjunction with VigorACS 3
3. TOTP 2-factor authentication (Google Authenticator) is now available for authenticating Remote Dial-In User VPN connections
4. USB Thermometer support added
5. PIN Generator facility is now available for Hotspot Web Portal
6. Objects can now be exported / imported in bulk, in .csv format from the new [Objects Setting] > [Objects Backup/Restore] menu
7. Webhook feature can now be enabled in [System Maintenance] > [Webhook] to send updates to the monitoring server

Improvements

1. Firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests
Important Note: The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading

VPN:

1. Improvements to the LAN to LAN VPN profile layout, with the TCP/IP Network Settings simplified to display relevant settings for the selected VPN types
2. “Change default route to *VPNx / None*” added to [VPN and Remote Access] > [LAN to LAN]
3. Support for More Local Network (Multiple SA) in IPsec LAN to LAN profiles
4. VPN services can now be bound to only selected WAN interfaces from the new [VPN and Remote Access] > [Remote Access Control] – Bind to WAN tab
5. Fixed VPN IKE buffer leakage when the VPN peer (Google Cloud) used AES_GCM as the phase1 proposal
6. Corrected an issue with high CPU usage when running many IPsec tunnels

Other Functionality:

1. Switch Management now supports these additional VigorSwitch models:
 - a. VigorSwitch P2100
 - b. VigorSwitch G2100
 - c. VigorSwitch P2540x
 - d. VigorSwitch G2540x
2. [Port Control] now supports specifying “100M Full Duplex fixed” rate for LAN/WAN ports
3. “Bypass” option added to Hotspot Web Portal profiles
4. New reboot options added to [System Maintenance] > [Reboot System]
 - a. Using current configuration (Fast reboot) – Restarts DrayOS for minimal downtime
 - b. Using current configuration (Normal reboot) – Fully restarts the Vigor 3910
5. Support for either “restore config” or “restore config with specific firmware” added to [System Maintenance] > [Configuration Export]
6. Improved handling of IPTV / Multicast traffic passed by IGMP Relay
7. Increased number of Object profiles:
 - a. IPv4 Object profiles increased to 500
 - b. IPv6 Object profiles increased to 200
 - c. Service Type Object profiles increased to 500
8. Resolved an issue with DNS security

Known Issues

1. After upgrade, downgrading firmware from [System Maintenance] > [Firmware Upgrade] is not recommended. This is because the new features / config for 4.x.x firmware will not be compatible with the 3.9.x firmware.
Instead, we recommend using the [System Maintenance] > [Configuration Export] - “Restore Firmware with Config” feature, to load the previous configuration file along with the previous firmware.

| | |
|-------------------|--|
| Firmware Version | 3.9.7.2 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient Note: A previous firmware (3.9.6.3) was a critical release. This f/w includes all changes/improvements that were in 3.9.6.3. |
| Build Date | 21 st December 2021 |
| Release Date | 13 th January 2022 |
| Revision | 63_662_dbe6d00 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(None)

Improvements

1. Improved LAN-to-LAN throughput for OpenVPN tunnels
2. PPPoE dial-in facility now supports up to 200 concurrent connections, up from 20
3. Performance improvements for packet captures in [LAN] > [Port Mirror / Packet Capture] and debug log data in [Diagnostics] > [Debug Logs]
4. Resolved an issue that could cause problems with certificate renewal in some circumstances
5. DNS queries going through the router's DNS did not include the CNAME alias
6. Conditional DNS Forwarding did not work correctly through a VPN tunnel
7. Improved handling of BGP routing with Cisco routers using a 4-Byte AS number
8. The router will automatically re-generate its self-signed certificate prior to the original expiring, so that the router's self-signed certificate cannot expire while in use
9. VigorAP access points managed through the router's [Central Management] > [AP] > [Status] would show as offline if a Management VLAN was set up on the VigorAPs

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.7.1 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient Note: A previous firmware (3.9.6.3) was a critical release. This f/w includes all changes/improvements that were in 3.9.6.3. |
| Build Date | 11 th October 2021 |
| Release Date | 26 th October 2021 |
| Revision | 54_625_7ce12ae |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Support for IKEv2 fragmentation to improve IKEv2 EAP compatibility
2. Email notifications can be sent when a VPN remote dial-in user tunnel is established

Improvements

1. Area ID 0 for OSPF is now supported
2. Increase IGMP proxy and IGMP snooping table

Connectivity and System stability:

3. In some circumstances WAN failover feature would not work
4. Current System Time would not display correct time
5. An issue of probable leakage caused by VPN CGI
6. Router would not respond when IPsec was used in some circumstances
7. IKE buffer mechanism improvements for IPsec Peer ID configuration
8. Fixed high CPU usage caused by blank gateway WAN IP address
9. Improved compatibility with IKEv2 Google Cloud
10. Local hosts could not access the Internet via WAN IP (configured with an Alias IP)

VPN:

11. Improved IKEv2 VPN with a static virtual IP configuration (My WAN IP / Phase 2 Network ID)
12. Remote VPN Gateway can be defined by a Domain Name (previously only a static IP address was accepted)
13. SSL VPN stability improvements
14. IKEv2 EAP Host to LAN VPN connection stability improvements
15. RADIUS authentication is bypassed for connections matching VPN LAN to LAN profile
16. Configuration of the VPN mOTP could cause unexpected errors
17. Route policy didn't bypass default VPN route
18. IPsec multiple SA VPN compatibility improvements (e.g. Juniper vSRX)
19. IKEv2 EAP rekey failed when the Limit Connection option was in use
20. Sending DNS queries to the router via VPN (OpenVPN, IKEv2 EAP) improvements
21. The VPN Dial-out profile type was changed to IKEv2 when importing the IKEv2 EAP profile
22. VPN trunk (failover) did not send packets when one of the WANs is down
23. Remote Dial-In IKEv2 EAP couldn't connect if VPN profile specified the Remote VPN Peer IP

24. LAN access to the router did not work when a dial-out IKEv2 VPN active profile was set with remote network 0.0.0.0

Others:

25. IP database for country objects updated
26. VPN Mail Alert log will include Source IP and the total connected time information
27. RADIUS authentication log improvements
28. For LAN to WAN topology OSPF did not exchange the routing LAN subnets details
29. Clients could not access Internet if Gateway was located on BGP peer network
30. Brute Force Protection for VPN (IKEv2 EAP/SSL) was not applied to invalid VPN usernames
31. PPPoE client could not access the Internet when PPPoE server was set with a VLAN tag
32. The local user account in [System Maintenance] > [Administrator Password] login failed if another local user account was deleted
33. NAT loopback could fail when LAN in routing mode or IP routed subnet were enabled
34. Routed streaming traffic could stop after 10 minutes

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|---|
| Firmware Version | 3.9.6.3 (Formal Release) |
| Release Type | Critical – Upgrade recommended immediately |
| Build Date | 06 th July 2021 |
| Release Date | 08 th July 2021 |
| Revision | 9_454_3f658b8 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(none)

Improvements

1. Improve the WebGUI security.

Please see the security advisory on <https://www.draytek.co.uk/support/security-advisories/kb-advisory-jul21>

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.6.2 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 14 th May 2021 |
| Release Date | 08 th July 2021 |
| Revision | 1644_436_312e1ad |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Routed subnet traffic can be load-balanced

Improvements

1. Improved the ping response time
2. Weight and Prepend options for BGP added in [Routing] > [BGP] > [Neighbour Setup]
3. “Downtime Limit” for VPN Tunnel notifications added for [Objects Setting] > [Notification Object]
4. Username and password for both LAN-to-LAN and Remote Dial-In VPN profiles are increased to 26 characters
5. Router did not route VPN traffic correctly if dial-out WAN IP is used in IP routed subnet
6. Default rule with WCF DNS Filter was not applied after firmware upgrade to 3.9.6
7. In some circumstances route policy could not bypass the VPN default route
8. An active IPsec tunnel to a 3rd party VPN endpoint would reconnect every 60 minutes
9. Ping Detect option on [Diagnostics] > [Traffic Graph] page did not display any data
10. In some circumstances RADIUS server authentication would fail
11. Wake on LAN sent from WAN did not work if the router was rebooted
12. VPN traffic stopped working after reconnecting PPPoE (WAN interface)
13. Accessing the WUI via mOTP by local administrator improvements
14. Fixed configuration of TR069 and Time and Data settings when using WAN IP Alias
15. DMZ host could not access the Web server in another LAN
16. Packets would still reach LAN DMZ host after disabling DMZ setting from WUI
17. VPN LAN-to-LAN traffic was incorrectly classified as VoIP traffic in Quality of Service
18. Traffic of LAN host were not sent to NATed IPsec Xauth tunnel when the policy-route rule was enabled
19. WAN’s static IP can be set without specifying a gateway
20. RADIUS VPN authentication timeout interval can be manually configured
21. A remote VPN gateway can be specified by Domain Name
22. Mail Service Object supports StartTLS
23. A static virtual IP can be configured for IPsec IKEv2 NAT on LAN to LAN VPN

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.6 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 17 th February 2021 |
| Release Date | 23 rd March 2021 |
| Revision | 1540_314_3fbf1a1 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Increased the router's capabilities:
 - a. Firewall: Increased firewall filter sets from 12 to 50
 - b. LAN Subnets: Increased from 50 to 100 total subnets
 - c. WAN IP Alias: Increased from 32 per-WAN to 300 per-WAN
2. Add IGMP proxy/snooping, IPv6 to fast path
3. Add USB support (storage only, e.g., Syslog to USB disk, web portal)
4. Support WAN Budget
5. Support Port-based Bridge for [WAN] > [Multi-VLAN]

Improvements

1. Updated MyVigor authentication method used for Web Content Filter license validation
2. Support for SNMP monitoring of VPN Tunnels
3. Added RADIUS with 802.1x authentication
4. ICMP ping performance improved (to local router only)
5. Changed the DHCP server pool size from 1K to 4K
6. Support NAT/routing table/load-balance for virtual WAN
7. Support for multiple untagged subnets on the same physical port
8. Schedules can now be applied to profiles for VPN Remote Dial-In
9. Added an option to limit concurrent Remote dial-in user connections allowed per profile

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|---|
| Firmware Version | 3.9.2.5 (Formal Release) |
| Release Type | Critical – Upgrade recommended immediately |
| Build Date | 16 th December 2020 |
| Release Date | 26 th January 2021 |
| Revision | 1497_94184 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Brute Force Protection can now be applied to the router's VPN services

Improvements

1. Improved precision of System Uptime counter
2. OpenVPN WUI error fixed
3. Corrected: private keys used in the RSA certificate
4. Improved mechanism of memory management
5. Improved operation of bandwidth limit auto-adjust
6. WANs 5-8 could not use prefix MAC address other than "00-1d-aa-"
7. Improvements to L2TP protocol VPN server

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.2.4 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 8 th October 2020 |
| Release Date | 3 rd November 2020 |
| Revision | 1456_93809 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Support for BGP prepending

Improvements

1. LAN to LAN VPN profile improvements: “Enable PING to keep IPsec tunnel alive” option for all LAN subnets added
2. OpenVPN WUI error fixed
3. Corrected: rekey for IPsec XAuth connection
4. TX/RX display improvements for virtual WANs
5. Router did not respond to SNMP requests when SNMP Host IP subnet was larger than /32
6. In some conditions with High Availability, config sync could cause the secondary router to restart more frequently than necessary
7. Router’s Mail Alert compatibility improved with Office365, Hotmail, and Outlook mail servers
8. VLANs 15 to 19 did not appear properly on **[Central Management] > [Switch] > [Profile]**
9. Improved VoIP connections and Ping response time on WAN/LAN interfaces while VPN is established
10. The new firmware upgrade process required an additional reboot to update

Known Issues

1. Firmware downgrade affects Route Policy rule’s “Failover” and “To” settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router’s configuration and make a note of the “To” and “Failover” settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.x firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.2.3 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 11 th August 2020 |
| Release Date | 17 th September 2020 |
| Revision | 1332_90943 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(none)

Improvements

1. Ports P1 and P2 support 1G_AN mode that can be selected in [Port Setup] section
2. The Router's self-signed certificate will change upon upgrade for compatibility with new browser certificate requirements.
Starting from September 2020, many client OS & browsers will limit publicly trusted TLS server certificate lifetime to 398 days or less, and connections will be rejected if certificates exceed this. This firmware patch will automatically re-sign all self-signed certificate lifetimes to 395 days (was 2 years or longer in older versions)
3. Improved fragments/buffer handling mechanism
4. LAN to LAN IPsec VPN would drop in some circumstances
5. Improved stability of WAN connection
6. An issue of DHCP obtaining wrong gateway address

Known Issues

3. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
4. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.1 or 3.9.2.2 to firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.2.2 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 3 rd June 2020 |
| Release Date | 25 th June 2020 |
| Revision | 1332_90943 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(none)

Improvements

1. VPN connections can now be sorted in [VPN and Remote Access] > [Connection Management]
2. Improved handling of large DHCP packets
3. Resolved a socket issue that could affect connectivity when TR069/STUN DNS lookups failed
4. In some specific scenarios, some IPsec VPN tunnels could not pass traffic when many IPsec VPN tunnels were active
5. VPN connections from Windows IKEv2 EAP clients with static IP assignments could lose VPN network access after IPsec rekey
6. Web interface could sometimes display lower CPU usage than real CPU usage

Known Issues

1. Firmware downgrade affects Route Policy rule's "Failover" and "To" settings:
If downgrading from 3.9.2.2 to firmware to 3.9.2.1 or earlier, take a backup of the router's configuration and make a note of the "To" and "Failover" settings for Route Policy rules configured on the router. These settings may be changed to incorrect values once the firmware has been downgraded. Verify the Route Policy configuration is correct after downgrading.
2. Firmware downgrade affects Bind IP to MAC:
If downgrading from 3.9.2.1 or 3.9.2.2 to firmware to 3.9.1, take a backup of the Bind IP to MAC settings. These settings will be cleared during the downgrade process. The Bind IP to MAC configuration can then be imported back into the router.

| | |
|-------------------|--|
| Firmware Version | 3.9.2.1 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 10 th April 2020 |
| Release Date | 17 th April 2020 |
| Revision | 1330_89655 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Increased maximum number of sessions supported, up to 1 million. To adjust the settings, go to [System Maintenance] > [NAT Sessions] section.
2. Router can now be managed by VigorACS 2 (latest version)

Improvements

1. Improved mechanism for VPN connections

Known Issues

1. If you need to downgrade the firmware to 3.9.1, take a backup of the Bind IP to MAC settings

| | |
|-------------------|--|
| Firmware Version | 3.9.2 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 21 st February 2020 |
| Release Date | 2 nd March 2020 |
| Revision | 1300_88674 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

1. Support for DrayTek VPN Matcher service:
 - a. Helps VPN clients and routers connect to a DrayTek VPN router, which connects to the Internet through a firewall or additional NAT router without port forwarding, which would not otherwise be able to accept VPN connections
 - b. Suitable for usage with Cone NAT environments
 - c. Supports LAN to LAN and Remote Dial-In User VPN connections
 - d. Accessible from [VPN and Remote Access] > [VPN Matcher]
2. Support for interchangeable LAN/WAN interfaces
3. Added [Central Switch Management] > [Switch Management] to manage compatible VigorSwitches; up to 30 devices
4. Added [Central AP Management] > [AP Management] to manage compatible VigorAPs; up to 50 devices
5. Support added for LAN port mirror and WUI packet capture
6. Support for console menu under LAN

Improvements

1. Increased DHCP pool from 1021 up to 4K
2. Improved PPTP acceleration up to 320Mbps
3. Improved SSL VPN acceleration up to 1.6Gbps
4. Improved VPN Trunk (GRE over IPsec) acceleration
5. Mail Alert function now supports StartTLS
6. Added APP QoS for Bandwidth Management

Known Issues

(None)

| | |
|-------------------|--|
| Firmware Version | 3.9.1.3 (Formal Release) |
| Release Type | Regular – Upgrade recommended when convenient |
| Build Date | 6 th February 2020 |
| Release Date | 14 th February 2020 |
| Revision | 1286_88265 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

New Features

(None)

Improvements

1. WAN port status mechanism improved
2. Handling of incorrect router configuration improved
3. Dial-in IPSec Aggressive VPN connection could not reconnect after a reboot
4. SSL VPN LAN to LAN did not forward packets with MTU 1395-1400
5. Improved MSS (Maximum Segment Size) for SSL VPN
6. Improved management of Hardware Accelerated sessions when WAN disconnects

Known Issues

(None)

| | |
|-------------------|------------------------------------|
| Firmware Version | 3.9.1.2 (Initial Release Firmware) |
| Release Type | Initial Release |
| Build Date | 4 th December 2019 |
| Release Date | 11 th December 2019 |
| Revision | 1217_87018 |
| Applicable Models | Vigor 3910 |
| Locale | UK & Ireland Only |

First Firmware Release for this model

New Features

(None)

Improvements

(None)

Known Issues

(None)

[END OF FILE]