Release Notes for DrayTek Vigor 2962 (UK/Ireland)

Firmware Version	4.4.3.1 – Mainline branch (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	14th August 2024
Release Date	30th September 2024
Revision	4694_7298_9c7d22d
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

Before upgrading to 4.4.3.1 or later, please upgrade to 4.3.2.7 to avoid configuration compatibility first.

New Features

1. Support for 4 WANs

Improvements

1. Web GUI Security Improvements
2. Fix an issue related to the WCF improvements
3. The RADIUS timeout increased to 120 seconds
4. Support for Auto-check WAN MTU for PPPoE connections
5. Support for multiple untagged PPPoE on the same port
6. The country code in mail alert for VPN connections added
7. The Blocked IP List page displays the unit for Block Time [Firewall] > [Defense Setup] > [Brute Force Protection]
8. Support for unlimited quota for Customized SMS Service Object
9. Support for WAN alias IP for Server Load Balance and Port Knocking
10. Webhook Server URL character limit increased from 64 to 200 characters
11. Support for complete certificate chain for IKEv2 EAP VPN authentication
12. Modify Brute Force Protection due to usage by Smart Action (Suricata)
13. Management/SNMP WUI no longer requires a router reboot
14. A new log alert added: "VPN service is disabled for WANx" when VPN service is not enabled
15. Support for customizing the port in "Vigor Router SMS Gateway" (SMS Service Object)
16. Support for Vigor management from TR-069 servers using either uppercase or lowercase HTTP headers
17. The Port Knocking as Source IP added for [NAT] > [Open Ports] and [NAT] > [Port Redirection] added
18. Improvements to the performance of the User Management feature by eliminating unnecessary HTTPS page redirection
19. The IP search box added to [System Maintenance] > [Management] for Blocked IP List (Brute Force Protection)
20. Improvements to the Port Knocking for Local Service and Brute Force Protection on the [System Maintenance] > [Management] page
21. Advanced notifications added for expiring certificates to Syslog to prevent connection issues

22. A note added about the VPN support for LDAP/AD Authentication on [VPN and Remote Access] > [PPP General Setup]
23. The Port Knocking Tools download link added on the of [NAT] > [Port Knocking] and [System Maintenance] > [Management] pages
24. A local certificate with an expiration date less than or equal to 397 did not get a warning message after modification
25. Improvements to the buffer overflow mechanism for SSL VPN
26. Improvements to the reversed Internet IP for DrayDDNS
27. Improvements to the connect compatibility with third-party ACS
28. Fix an issue with the PPTP VPN failure from Android Phone
29. Fix an issue with failure to set a hotspot with the created API
30. Restore backup NAT configuration did not work
31. Improvements to the Remote Dial-in User's IPsec Peer Identity feature
32. Improvements to the WUI where some NAT-related features would allow to select unused WAN interfaces
33. The router could stop responding after enabling the WCF
34. Improvements to the host display mechanism on [Diagnostics] > [Data Flow Monitor]
35. Improvements to the issues with import/export configuration mechanism related to long integer values
36. The Management option on [WAN] > [Multi-VLAN] was missing
37. After the firmware upgrade, the Firewall Filter Set 1 was empty
38. The router could stop responding while the remote dial-in user profile was edited
39. An issue with failure to open Bandwidth Management >> Quality of Service.
40. The LAN DNS firmware compatibility improvements
41. The router could stop responding when the conntrack table is full
42. The SFP P1 link was up (1Gbps) but no ARP entry was observed after upgrading to 4.4.3 firmware
43. The graphics of Login Page Greeting in WUI when using HTTP is now adjusted
44. The unnecessary character has been removed from [Diagnostics] > [NAT Sessions Table]
45. Network stability improvements for OpenVPN
46. The router did not renew DrayDDNS the WAN IP address changed
47. The Delete and Rename options were missing on the [USB Application] > [File Explorer] page
48. The password and pre-shared key for VPN LAN-to-LAN are hidden on the backup file
49. The Open Port option failed to direct the traffic to a virtual server which had two IP addresses
50. SSL VPN LAN-LAN in NAT mode did not allow to reach the remote network
51. An error message appeared on User Management after enabling Validation Code
52. The CPE device lost Internet access via high availability while using two switches
53. Fix for the WANx first for the DrayDDNS service not working when the Internet IP was used
54. The wrong direction was displayed for VPN Log Details on [Diagnostics] > [VPN Graph]
55. The DDNS could fail to update correctly while HA status was not yet complete during the boot process
56. Correction for the WUI login logs that were displayed under User Access instead of Others on Syslog

57. Incorrect values were displayed when editing a filter rule with the direction set to WAN-> LAN/RT/VPN
58. The URL Filter did not block HTTPS websites when TLS 1.3 hybridized Kyber was enabled in the browser
59. Improvements to the Hotspot HTTPS redirection not working when Vigor HTTPS management port was set to a non-default value
60. Fix an issue where NAT Port Redirection Rule (e.g., index 2) was disabled automatically when modifying rules on other pages

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).

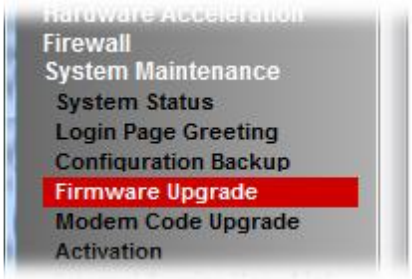
Firmware File Types

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	4.4.3 – Mainline branch (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	28th June 2024
Release Date	28th August 2024
Revision	4299_6922_734d159
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

Before upgrading to 4.4.3, please upgrade to 4.3.2.7 to avoid configuration compatibility first.

New Features

1. Support for [NAT] > [Server Load Balance]
2. Support for Port Knocking (for local service)
3. Support for TLS 1.3 added to [System Maintenance] > [Management]
4. TOTP for Remote Web Management added on the [System Maintenance] > [Administrator Password] page
5. New VPN features: VPN Isolation, VPN packer capture, Active Directory and 2FA for VPN users, IPSec AES-GCM and SHA-512 authentication

Improvements

1. The VPN Traffic Graph added to [Diagnostics] > [VPN Graph] section
2. The Primary router can synch Time & Date settings for High Availability
3. The VPN Peer IP country info added into the VPN Connection Status section
4. Enhancements for Brute Force Protection, DoS and Firewall
5. A new notification object added for Fail login and Brute Force Protection Alerts
6. The number of supported Radius clients increased from 30 to 200
7. Support for the new Fast NAT option to skip the DNS packet inspection to reduce the CPU load in a specific environment
8. Fix an issue with the VPN Log Details WUI that showed wrong direction
9. The DoS Defense could fail to stop TCP SYN flood attacks
10. The User data quota in User Management did not work
11. The LAN port traffic information could not be reported by PRTG software
12. Fix to the firewall that did not block incoming ICMP packets from VPN LAN to LAN
13. Improvements to the SMS customized object
14. Fix an issue where 200 IPsec dial-out VPNs (neither NordVPN nor IP Vanish) could not go online after the system reboot
15. The inbound/outbound VoIP traffic could fail when the “Allow pass inbound fragmented large packets” was disabled/enabled
16. Improvements to the URL Reputation mechanism where some website could not be blocked and the "Get Request Resource Failure" showed in the syslog
17. An issue with failure to dial-up IPsec VPN to the server with Domain Name when the server changed to a new IP

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. The encryption method for OpenVPN will be factory defaulted if firmware is upgrading from v3.9.7 to v4.3.1 or above
3. Configuration backup settings restored from 4.3.2 firmware may be incorrect. Please check inter-LAN routing settings after uploading the configuration
4. The TR-069 parameters for [Application] > [Smart Action] is not completed yet
5. 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	4.3.2.7 – Mainline branch (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	7th May 2024
Release Date	19th June 2024
Revision	2781_4197_802d887
Applicable Models	Vigor 2962
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

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 Version	4.3.2.6 – Mainline branch (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	2nd January 2024
Release Date	9th February 2024
Revision	r2646_4126_565148c
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

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	28th September 2023
Release Date	3rd November 2023
Revision	2538_4073_ddbd6db
Applicable Models	Vigor 2962
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.

Before changing firmware from one branch to another, as a precaution, take a configuration backup.

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. In some circumstanced the router could stop responding when Always On / Backup WAN settings were selected
4. Fix an issue where forcing HTTPS connection to SMS provider did not work
5. Fix for IGMP not working correctly if both WAN1 and WAN2 were online
6. The SNMP settings were not available when SNMPv3 only was enabled
7. MyVigor product registration link could not be opened from router's WUI
8. Port 443 from LAN could be detected despite of disabling all known services
9. Fix for the firmware upgrade mechanism that was likely to be unsuccessful when MAX connection set to 1000K
10. The router could stop responding when IKEv2 re-dialled and the local ID was set to 32 characters
11. Multiple WANs with the same IP could affect services such as Hotspot Web Portal and VPN
12. Improvements to the IPSec multiple SA using phase2 network ID function
13. 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	25th May 2023
Release Date	29th June 2023
Revision	2404_3979_cc9de1a
Applicable Models	Vigor 2962
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. Improved throughput stability
4. In some circumstances WAN failover configuration could not be completed
5. 2FA web authentication via Telegram
6. Wrong source LAN IP was displayed by Ping Diagnosis
7. Access to the WUI did not work if an apostrophe was used
8. Sometimes MacOS/iOS VPN Remote Dial-in users could not reconnect over the IPSec protocol
9. Fix for the [Dashboard] > [Security] > [DoS] section displaying correct information when an attack was detected
10. Some Internet traffic was sent via non-existing WAN9 interface
11. The router could stop responding when downloading the debug log
12. Fixed an issue with the special character á in the "Receiving PIN via SMS Content" textbox for Hotspot Web Portal
13. The pop-up 2FA authentication page could not appear if VPN interface on [System Maintenance] > [Management] > LAN Access Setup was disabled

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	16th March 2023
Release Date	26th April 2023
Revision	2321_3914_165f608
Applicable Models	Vigor 2962
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. SSL TLS Encryption 1.0 and TLS 1.1 in now disabled by default
3. Improvements to the route policy sent via WAN IP Alias
4. Fixed an issue with Canon printers that could not obtain a DHCP IP address
5. Improvements to the ICMP ping via the BGP route
6. MyVigor could not be connected after rebooting the router with Wipe Out All
7. Fixed an issue with the user-based firewall where only those users that fulfil the rule would be impacted
8. PIN could not be sent via SMS when the recipient number contained +(country code) character
9. IKEv2 VPN connection could drop every two hours
10. In some circumstances the L2TP over IPsec VPN connection to Synology NAS could disconnect
11. Multiple VPN tunnels could get disconnected due to an invalid server domain entered in the VPN profile 1
12. Remote IP not included in Access List could see the login page when HTTPS remote access and SSL VPN services were enabled
13. The host of the routed subnet was not accessible even when inter-lan routing was enabled
14. 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	11th January 2023
Release Date	3rd March 2023
Revision	2230_3844_ef2dd6a
Applicable Models	Vigor 2962
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. In some circumstances DNS forwarding did not work
6. Static route did not work for packets originated from Inter-LAN subnets
7. The VPN config backup did not restore the 'more' remote subnet section of the VPN profile

Known Issues

1. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the 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. 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	4.3.2.1 – Mainline branch (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	12th November 2022
Release Date	20th December 2022
Revision	2118_3711_ecabcef
Applicable Models	Vigor 2962
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. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the 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. 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 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	9th June 2022
Release Date	16th September 2022
Revision	1832_3397_d13b317
Applicable Models	Vigor 2962
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. Support for Wired 802.1x for LAN
3. Support for Link Aggregation (LAG) for selected LAN ports
4. Smart Action task automation feature is now available [Application] > [Smart Action] to trigger alerts, disable VPN profiles, schedule an NAT policy rule etc.

Improvements

1. OpenVPN generated certificate is valid for 10 years (previously 1 year only)
2. Improvements for WireGuard VPN stability
3. WireGuard MacOS clients can now use “Set VPN as Default Gateway”
4. Mail Service Objects username and password fields accept up to 128 characters
5. Increased number of characters from 32 to 64 for CN and email fields in [VPN and Remote Access] > [IPsec Peer Identity]
6. Some DrayDDNS logs were incomplete
7. Improvements to the LAN DNS functionality
8. In some circumstances there was high CPU usage and high VPN ping
9. Improved compatibility with DHCP relay and VLAN tagged traffic
10. SSL VPN stability improvements
11. The router could stop responding when SSL VPN dial-out failed in linking state
12. WUI did not render some pages as expected after upgrading to 4.3.1.1 firmware
13. Improved functionality of the ‘Ping to Keep Alive’ in IPsec NAT mode
14. Router could stop responding when a Load Balance Policy was configured for VPN Trunk
15. In some circumstances untagged PC could obtain an IP from a VLAN tagged subnet
16. Router could stop responding when WAN/LAN IPv6 option was enabled
17. VoIP RTP traffic was sent with an incorrect VLAN tag if route policy was with Force Routing
18. [WAN] > [Multi-VLAN] interfaces were unable to establish the PPPoE connections
19. An SNMPv3 agent could not get any data when using AES algorithm

20. Intermittent packet loss when routing through load balance policy that was set with an IP Alias (High Availability configuration)
21. Remote dial-in users could not access LAN after changing VPN protocols between PPTP and SSL VPN
22. WUI responsiveness improved for [System Maintenance] > [Mac Connection], [VPN and Remote Access] > [Wireguard], [Applications] > [Dynamic DNS] and other pages

Known Issues

1. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the firmware.
2. 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 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	24th August 2022
Release Date	02nd September 2022
Revision	239_3517_95064ee
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

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. Hostnames are also supported in the remote management ACL
5. Improved the CPU usage with multiple VPN connections
6. Updated the time graph for CPU usage
7. Router would become inaccessible when rebooted in some circumstances
8. A warning message will appear for reused IP object / IP Group profile that has already been used by other applications
9. OpenVPN dial-in users could not obtain an IP address
10. Some domains fail to resolve when DNS Security was enabled
11. Firewall ignored rules 84 and above
12. BGP compatibility between Vigor and Juniper improved
13. Cipher and HMAC algorithm in OpenVPN would change when .all firmware file was used
14. Some ARP frames did not meet the minimum expected size
15. When downgrading the firmware, some firewall rule directions would become “undefined”
16. Connection speed improvements for NordVPN (IKEv2 EAP)
17. If L2L tunnel can’t be established due to authentication errors, other VPN users (IKEv2 EAP) could not connect unless services were restarted

Known Issues

1. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the firmware.
2. 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 to use 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 (Formal Release)
Release Type	**Optional** – Upgrade to make use of new features 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	4th January 2022
Release Date	8th February 2022
Revision	1269_3000_72fac4a
Applicable Models	Vigor 2962
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

Other Functionality:

1. Support for up to 4 WANs, with at most 2 active WANs at any one time. The additional WAN interfaces can be used for failover
2. Switch Management now supports these additional VigorSwitch models:
    a. VigorSwitch P2100
    b. VigorSwitch G2100
    c. VigorSwitch P2540x
    d. VigorSwitch G2540x
3. [Port Control] now supports specifying "100M Full Duplex fixed" rate for LAN/WAN ports
4. "Bypass" option added to Hotspot Web Portal profiles
5. 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 2962
6. Support for either "restore config" or "restore config with specific firmware" added to [System Maintenance] > [Configuration Export]
7. Improved handling of IPTV / Multicast traffic passed by IGMP Relay

Known Issues

1. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the firmware.
2. 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 to use 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	23rd December 2021
Release Date	13th January 2022
Revision	1030_663_32d512d
Applicable Models	Vigor 2962
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. NAT Loopback failed when the IP routed subnet was enabled
8. Improved handling of BGP routing with Cisco routers using a 4-Byte AS number
9. 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
10. 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. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the firmware.

Firmware Version	3.9.7 (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	3rd September 2021
Release Date	26th October 2021
Revision	905_616_d7774eb
Applicable Models	Vigor 2962
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

Connectivity and System stability:

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

VPN:

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

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

Known Issues

1. If the firmware is updated via TFTP, the loader version displayed on the Dashboard may be incorrect, the actual loader version is correct for the firmware.

Firmware Version	3.9.6.3 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	06th July 2021
Release Date	08th July 2021
Revision	544_437_95ac18c96
Applicable Models	Vigor 2962
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

(None)

Firmware Version	3.9.6.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	18th May 2021
Release Date	14th June 2021
Revision	544_436_95ac18c
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. The number of WAN IP Alias increased to 254
2. "Downtime Limit" for VPN Tunnel notifications added for [Objects Setting] > [Notification Object]
3. Username and password for both LAN-to-LAN and Remote Dial-In VPN profiles are increased to 26 characters
4. Fixed an issue with ARP that could clear the ARP cache table in some circumstances
5. Default rule with WCF DNS Filter was not applied after firmware upgrade to latest version
6. In some circumstances route policy could not bypass the VPN default route
7. Let's Encrypt Certificate and IPsec X.509 could not be displayed properly
8. In some circumstanced RADIUS server authentication would fail
9. Wake on LAN sent from WAN did not work if the router was rebooted
10. VPN traffic stopped working after reconnecting PPPoE (WAN interface)
11. A routing issue of the traffic selector matching correct IPsec IKEv2 VPN profile
12. DMZ host could not access the Web server in another LAN
13. Traffic of LAN host were not sent to NATed IPsec Xauth tunnel when a policy-route rule was enabled
14. RADIUS VPN authentication timeout interval can be manually configured
15. A static virtual IP can be configured for IPsec IKEv2 NAT on LAN to LAN VPN

Known Issues

(None)

Firmware Version	3.9.6.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	26th March 2021
Release Date	05th May 2021
Revision	492_360_bd7d76c
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

New Features

1. Routed subnet traffic can be load-balanced

Improvements

1. Improved the ping response time
2. "Downtime Limit" for VPN Tunnel notifications added for [Objects Setting] > [Notification Object]
3. Router would not accept LAN packets over 1514B when VLAN Tags were enabled
4. Copying a file between LAN ports could fail under some specific and uncommon conditions
5. GUI did not respond when many SSL VPN dial-in clients were connecting simultaneously
6. VPN LAN-to-LAN traffic was incorrectly classified as VoIP traffic in Quality of Service
7. A remote VPN gateway can be specified by Domain Name

Known Issues

(None)

Firmware Version	3.9.6 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	16th February 2021
Release Date	23rd March 2021
Revision	395_314_bf84f78
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

New Features

1. Add IGMP proxy/snooping, IPv6 to fast path
2. Add SFP module information displayed on [WAN] > [General Setup]
3. Add USB support (storage only, e.g., Syslog to USB disk, web portal)
4. Support WAN Budget
5. Support for VigorACS 2.5.6
6. NAT sessions can now to be configured up to 300K (default 150K)
7. Support Port-based Bridge for [WAN] > [Multi-VLAN]

Improvements

1. Updated MyVigor authentication method used for Web Content Filter license validation
2. Increased the number of firewall filter sets from 12 to 50
3. Support for SNMP monitoring of VPN Tunnels
4. Added RADIUS with 802.1x authentication
5. Add P2 SFP 100Mbps support on Port Setup
6. ICMP ping performance improved (to local router only)
7. Changed the DHCP server pool size from 1K to 4K
8. Support NAT/routing table/load-balance for virtual WAN
9. Support for multiple untagged subnets in the same physical port
10. Schedules can now be applied to profiles for VPN Remote Dial-In
11. Added an option to limit concurrent Remote dial-in user connections allowed per profile
12. Added an option named “primary” to define which port is used in preference when both the SFP and Ethernet WAN combo ports are connected

Known Issues

1. Vigor router doesn’t accept LAN packets over 1514B. Max. accepted MTU is 1496 when VLAN Tags are enabled

Firmware Version	3.9.3.1 (Initial Release Firmware)
Release Type	**Initial Release**
Build Date	16th December 2020
Release Date	20th January 2021
Revision	559_94194
Applicable Models	Vigor 2962
Locale	UK & Ireland Only

First Firmware Release for this model

New Features

(None)

Improvements

(None)

Known Issues

(None)

[END OF FILE]