Release Notes for DrayTek Vigor 2926 series (UK/Ireland)

Firmware Version	3.9.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	18th July 2023
Release Date	18th August 2023
Revision	17151_1116_ed90019452
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

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. Web GUI security improvements
2. In some circumstances the DHCP relay did not work
3. ACL could not be removed by TR-069 parameter
4. The APP Enforcement function could not block TeamViewer
5. The simplified Central AP Management feature has been restored to full version

Known Issues

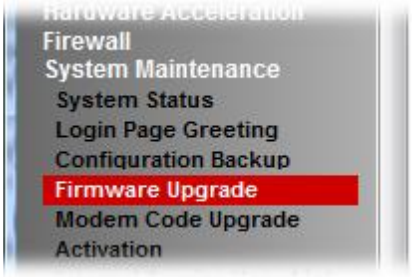
(None)

Firmware File Types

The ZIP file contains the firmware with two different file extensions, .ALL and .RST. The firmware is identical, but the RST file contains factory default settings. If you install the ALL file, your router will retain all existing settings. If you use the RST file, all settings will be wiped from your router.

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	3.9.9.1 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	11th January 2023
Release Date	3rd March 2023
Revision	16792_1066_ee824ddd7e
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improvements to the Web GUI Security (CVE-2023-23313)

Known Issues

(None)

Firmware Version	3.9.9 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	28th November 2022
Release Date	19th December 2022
Revision	16197_1064_5ae179909c
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. Support for Cyren Zero-Day WCF

Improvements

1. Secondary NTP server can now be specified as a backup if the primary is unavailable
2. Improvements to the IPsec IKE buffer used for receiving retransmitted phase2 PFS negotiation
3. System uptime displayed on [Central Management] > [Switch] > [Status] was showing incorrect data
4. The Hotspot Web Portal terms and conditions section exceeding 500 characters could stop the feature showing the page correctly

Known Issues

(None)

Firmware Version	3.9.8.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	26th April 2022
Release Date	20th May 2022
Revision	12433_959_e14180a37
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
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. Improvements to the mesh connection synchronisation mechanism

Known Issues

(None)

Firmware Version	3.9.8 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	08th February 2022
Release Date	07th March 2022
Revision	12497_917_417fa193cd
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. The WAN2 driver update will be installed with this firmware.
   Important Note: downgrading the firmware may disable WAN2 functionality due to incompatibility with older firmware
2. A new email alert message when a VPN login attempt fails "[X.X.X.X] CHAP Login Failed ()", which includes the IP address of the remote client attempting the VPN connection
3. Improvements to the HTTP stack-based buffer mechanism
4. 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

Known Issues

(None)

Firmware Version	3.9.7 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	17th January 2022
Release Date	18th February 2022
Revision	12261_900_11ee60a3db
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improved Ethernet WAN DHCP compatibility with Starlink
2. Resolved an issue that could cause problems with certificate renewal in some circumstances
3. DNS queries going through the router's DNS did not include the CNAME alias
4. NTP and Mail Alert server requests could not be sent when configured to send through a specific WAN IP Alias
5. 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

Known Issues

(None)

Firmware Version	3.9.6 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	24th February 2021
Release Date	23rd March 2021
Revision	4731_511_74a11ac
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Support of new encryption mechanisms for license, network, and MyVigor connections

Known Issues

(None)

Firmware Version	3.9.5 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	23rd December 2020
Release Date	18th January 2021
Revision	3577_418_4bae6b9
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. Brute Force Protection can now be applied to the router's VPN services
2. ['ac' models only] Support for VLAN over Mesh (Bridge VLAN to Mesh) for multi-subnets and isolated guest WiFi without cabling
3. Support for new 4G USB modems including the Huawei E3372h-320
4. Hotspot Web Portal now supports authenticating users with "Receive PIN via Mail" to send out an e-mail with PIN code to a client's e-mail address

Improvements

1. Central AP Management feature-set has been reverted to the previous firmware's functionality, allowing configuration of multiple SSIDs and VLANs. Management of Mesh APs is now managed through the [Mesh] menu on 'ac' model routers
2. WAN IP Alias can now be used with DDNS
3. Improvements to Mesh reconnection mechanism
4. Conditional DNS forwarding can work with a VPN user
5. Corrected an appearance of "DHCP IP Assignment Table" on [Diagnostics] > [View DHCP Assigned IP Addresses]

Known Issues

(None)

Firmware Version	3.9.4.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	11th August 2020
Release Date	2nd September 2020
Revision	92671
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. 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).

Known Issues

1. The 3.9.3, 3.9.3.1, 3.9.4 and 3.9.4.1 firmwares simplify AP Management Profiles for full compatibility with the new Mesh Root functionality. The changes limit AP Profile management to a single SSID only.
   Continue to use the 3.9.1.4 firmware if using Central AP Management with multiple SSIDs or VLANs configured. The 3.9.5 firmware release will re-instate the full AP Management Profile feature-set.

Firmware Version	3.9.4 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	8th July 2020
Release Date	31st July 2020
Revision	91724
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. App Enforcement and App QoS now each support an expanded range of software and services, including Zoom
2. StartTLS is now supported by Mail Alert feature
   [System Maintenance] > [SysLog / Mail Alert Setup]

Improvements

1. App QoS can now apply Quality of Service Class 1, 2 or 3 to more services as individual items
2. DH Group 2 is now supported in Aggressive Mode for IKE phase 1 proposal
3. A new option of "Router generated certificates" on [VPN and Remote Access] > [OpenVPN]
4. New applications (including Anydesk) added on [CSM] > [APP Enforcement Profile] page
5. DNS settings for LTE WAN can now be manually configured with this CLI command:
   wan lte set manual
6. Fixed an issue where VoIP quality was affected by ACS data traffic
7. Improved compatibility with Windows IKEv2 EAP Clients set with a static IP where access to VPN network would fail when IPsec rekey occurred

Known Issues

1. The 3.9.3, 3.9.3.1 and 3.9.4 firmwares simplify AP Management Profiles for full compatibility with the new Mesh Root functionality. The changes limit AP Profile management to a single SSID only.
   Continue to use the 3.9.1.4 firmware if using Central AP Management with multiple SSIDs or VLANs configured. The 3.9.5 firmware release will re-instate the full AP Management Profile feature-set.

Firmware Version	3.9.3.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	6th April 2020
Release Date	16th April 2020
Revision	89435
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Removed SSL Java Tunnel Support because NPAPI Java based Plugins are a deprecated feature and no longer supported by web browsers. Please use SSL Tunnel instead.
2. IPsec Xauth and IKEv2 EAP authentication is supported by RADIUS/LDAP/AD
3. Improvements added to welcome message in [System Maintenance] > [Login Page Greeting] section
4. Improved ACL mechanism for remote management when 0.0.0.0 remote network VPN is established
5. Firmware upgrade mechanism improvements
6. Resolved an issue with SNMPv3 authentication

Known Issues

1. The 3.9.3 and 3.9.3.1 firmwares simplify AP Management Profiles for full compatibility with the new Mesh Root functionality. The changes limit AP Profile management to a single SSID only.
   Continue to use the 3.9.1.4 firmware if using Central AP Management with multiple SSIDs or VLANs configured. The 3.9.5 firmware release will re-instate the full AP Management Profile feature-set.

Firmware Version	3.9.3 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	25th February 2020
Release Date	23rd March 2020
Revision	88735
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. Mesh is now available on Vigor 2926ac routers with 802.11ac dual-band wireless
    a. Set up Mesh initially from the [Wizards] > [Mesh Wizard] menu
    b. Configurable from the [Mesh] menu
    c. Supports Mesh Root mode
2. 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]

Improvements

1. Improved interoperability with Let's Encrypt certificate service with support for ACMEv2
2. IKE Proposals can now be controlled as Basic/Medium/High modes:
    a. Basic: DES/3DES/AES encryption, MD5/SHA1/SHA256 authentication, all DH groups
    b. Medium: AES only, SHA1/SHA256 auth, G5/G14/G19/G20/G21 DH groups
    c. High: AES only, SHA256 only, G14/G19/G20/G21 DH groups
    d. Configured in [VPN and Remote Access] > [IPsec General Setup]
3. Support for using IP-alias address to register with VigorACS
4. Resolved an issue with establishing wireless WAN connection in some configurations
5. Improved handling of Fast Leave with IGMP Proxy when using multiple subnets / VLANs
6. Simplifying the APM and integration with Mesh
7. Fixed an issue with some domain name configuration in TR-069 section.

Known Issues

1. The 3.9.3 and 3.9.3.1 firmwares simplify AP Management Profiles for full compatibility with the new Mesh Root functionality. The changes limit AP Profile management to a single SSID only.
   Continue to use the 3.9.2 firmware if using Central AP Management with multiple SSIDs or VLANs configured. The 3.9.5 firmware release will re-instate the full AP Management Profile feature-set.

Firmware Version	3.9.1.4 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	24th December 2019
Release Date	03rd January 2020
Revision	87483
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improved WebGUI security

Known Issues

(None)

Firmware Version	3.9.1.3 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	23rd October 2019
Release Date	07th November 2019
Revision	85718
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improved SSL VPN compatibility with Apple devices. Self-Signed certificate's Valid To date is now 2 years from date of generation. Regenerate the router's Self-Signed Certificate to meet the new trusted certificate requirements of Apple iOS 13 & macOS 10.15.
   Longer Valid To periods can be specified by generating a Local Certificate and self-signing it with the router's internal Root CA.

Known Issues

(None)

Firmware Version	3.9.1.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	23rd September 2019
Release Date	11th October 2019
Revision	85041
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Support the new DrayTek MAC Address OUI beginning with "14:49:BC" and improved the firmware downgrade compatibility.

Known Issues

1. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.
   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2] by changing the Enable setting of WAN2 to "No".

Firmware Version	3.9.1.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	19th August 2019
Release Date	9th September 2019
Revision	84162
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Hotspot Web Portal PIN codes could not be sent correctly through SMS text message
2. SSID1(All) schedule option in [Wireless LAN] > [General Setup] added
3. Receiving SMS messages would not work in some circumstances
4. The router would stop responding when the SSH session from a LAN PC times out
5. Some configuration backup files could not be properly restored
6. WAN2 Wireless mode would not work when connecting to a hidden SSID
7. IPsec Xauth VPN connection could not be established
8. A wireless client could still connect via WLAN 2.4G even though the time expired according to the profile schedule.
9. Detection of other DrayTek devices from [External Devices] was limited to LAN1
10. Improved router's handling of Central AP and Central Switch Management with many VigorSwitches and VigorAPs connected
11. Hotspot Web Portal could not be used with some network configurations

Firmware Version	3.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	8th July 2019
Release Date	18th July 2019
Revision	83262
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. Support for IPTV diagnostics using the [Applications] > [IGMP] > Enable IGMP Syslog option
2. Service activation status can now be verified from [MyVigor Services] > [Service Status]
3. Configure Exceptions from load balancing in [WAN] > [General Setup] > Advanced
4. IP Groups can now be allowed as Source IPs for [NAT] > [Port Redirection] & [Open Ports]

Improvements

1. WAN2 port is now set to operate as LAN5 by configuring the [WAN] > [General Setup] > [WAN2] Enable setting to "No"
2. Station Control settings can be specified in [Central Management] > [AP] > [WLAN Profile]
3. Note added to indicate router's certificate isn't included as part of the configuration backup
4. Show button added to [Switch] > [Group] management page to check group password
5. TR-069 parameters added to allow configuration of VoIP QoS through VigorACS
6. Support for "Dynu" DDNS provider added to [Applications] > [Dynamic DNS]
7. IPsec EAP option added to IKEv2 LAN to LAN VPN to use X.509 for authentication
8. VigorACS STUN server settings for [System Maintenance] > [TR-069] is automatically filled in from the ACS Server URL hostname/ip
9. VigorACS CPE registration could fail when registering over a VPN using LAN2 – LAN8
10. IKEv2 EAP VPN connection could not be established from Windows 10 when using a self-signed CA on the router
11. VPN Profile Backup from other DrayTek router models couldn't be restored to Vigor 2926
12. VPN Remote Dial-In Users could not connect to the router when using a LAN to LAN VPN tunnel with "Change default route to this VPN tunnel" enabled
13. In some scenarios, it was not possible to resume watching IPTV services through the router after pausing the IPTV video service for 5 minutes or more
14. SSL VPN Clients could receive the router's WAN DNS servers instead of the DNS servers specified through DHCP Relay
15. CLI commands can now be issued through VigorACS with the "CLIcmd" TR-069 parameter in the VigorACS Parameter Tree
16. TFTP Firmware Upgrade notes removed from [System Maintenance] >> [Firmware Upgrade]. The TFTP Firmware Upgrade method is supported as usual.
17. ACS RMM Health Server communication improved
18. USB Printer Server disabled by default

19. Disabled Captive Portal Detection would still pop-up on Android and Windows 10 clients
20. Unable to authenticate VigorACS server certificate (issued by Let's Encrypt)

Known Issues

1. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.
   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2] by changing the Enable setting of WAN2 to “No”.

Firmware Version	3.9.0 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	30th November 2018
Release Date	2nd January 2019
Revision	78123
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. OpenVPN is now supported as a Remote Dial-in User VPN protocol.

   Important Note: The router's OpenVPN server is automatically enabled on the router upon upgrade to 3.9.0 firmware, which listens on TCP & UDP ports 1194 by default and will take precedence over port forwarding to a LAN server using these ports.
   This service and its listening ports can be configured from the [VPN and Remote Access] > [OpenVPN] menu, or disabled in [VPN and Remote Access] > [Remote Access Control]

2. The router's Switch Management can now manage the VigorSwitch G1080, P1092 & P2121
3. Let's Encrypt certificate support added
4. Hotspot Web Portal can now support IPv6 clients
5. Support for dial-out IPsec VPN with XAuth to Cisco EZ VPN Server

Improvements

1. Hotspot Web Portal Database stored on USB can now be encrypted by enabling "Database Encryption" in [Hotspot Web Portal] > [Users Information] > [Database Setup]
2. Wireless LAN SSID is now displayed for each SSID in [Wireless LAN] > [Security] settings
3. Added support for data compression of VigorAP management
4. Support user management on the client authentication by the RADIUS server
5. IPsec EAP option added to IKEv2 LAN to LAN VPN to use X.509 for authentication
6. Hotspot Web Portal logs for user connection & disconnection can now be sent via syslog
7. Support NAT mode for IKEv2 LAN to LAN dial-out connection and IKEv2 NAT mode with EAP MSCHAPv2 authentication
8. SNMPv1 and SNMPv2 can now be enabled / disabled separately from SNMPv3 operation in [System Maintenance] > [SNMP]
9. Added TR-069 parameters for enabling/disabling [Data Flow Monitor] function
10. SNMP monitoring clients can now read out the CPU load and memory usage percentages as part of the router and firmware details in the sysDescr.0 (OID 1.3.6.1.2.1.1.1) value
11. The router's SSL VPN server port can now be set via the CLI command "mngt sslvpnport"
12. TR-069 login message no longer displays model information from the router
13. USB Thermometer was not detected in some configurations
14. Wrong IP address for the subnet mask "/15". Correct IP address should be "255.254.0.0"
15. In HA Hot-Standby mode, DHCPv6 Sync Status failed in the Secondary router

16. The “Block DNS” option in an APP Enforcement profile could be automatically enabled upon upgrade to 3.8.9.x firmware, resulting in App Enforcement blocking DNS unintentionally
17. Unable to allocate static IP address to IKEv2 VPN client
18. The router did not clear routes added via BGP when removed through BGP
19. CLI command “ip bandwidth del <IP>” did not work
20. When selecting Internet IP in Determine WAN IP, DrayDDNS did not update with correct IP, or an error message of “WAN IP not present” appeared
21. Unable to block a static route by the firewall when a remote dial-in user is connected
22. Improved interoperability with Xbox One and UPnP / DMZ host
23. Data quota set on [User Management] > [User Profile] would be reset to zero after re-login
24. Vigor router ignored Don't Fragment flag in IP header
25. Custom local admin user account could not log in from WAN when “Admin Login from Internet” option is disabled
26. Wireless clients would be disconnected from a VigorAP (e.g., VigorAP910C) when adding a new MAC address to Access Control List on [Central Management] > [AP] > [WLAN Profile]
27. SNMP data could be different from the readings on the router's dashboard
28. WDS security key configured in [Wireless LAN] > [WDS] could not be saved
29. Improved PPPoE ISP interoperability by adding support for configurable PPP LCP Echo Request options

Known Issues

1. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.
   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2] by changing the Enable setting of WAN2 to “Set as LAN”.
2. See New Features entry #1 for notes on OpenVPNs impact on Port Redirections for TCP/UDP port 1194

Firmware Version	3.8.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	16th July 2018
Release Date	10th August 2018
Revision	75315
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Firewall filter rules were not correctly applied to Routed LAN subnets
2. Improved interoperability with Hotspot Web Portal and Facebook authentication service
3. Web interface could not be accessed via HTTPS from in some network environments
4. A new Self-signed certificate could not be generated from [System Maintenance] > [Self-Signed Certificate] > Regenerate
5. NAT loopback could not operate with port forwards configured using ports 768 to 1023
6. Wireless clients connecting to 2.4GHz wireless SSID and disconnecting could not connect to 5GHz wireless SSID, receiving an invalid security key error
7. Entering a speech mark character i.e. " in the Pre-Shared Key for wireless SSID 2, 3 or 4 would result in the wireless security settings for SSID 2, 3 and 4 being inaccessible from the web interface
8. The "Analyse a single packet" mode of [Diagnostics] > [Route Policy Diagnosis] could not be displayed correctly in Google Chrome browser

Known Issues

1. The IP Filter does not apply to traffic using [Routing] > [Static Routes] in firmware 3.8.9 and later.
2. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.
   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2] by changing the Enable setting of WAN2 to "Set as LAN".

Firmware Version	3.8.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.8.2) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.8.2.
Build Date	12th June 2018
Release Date	9th July 2018
Revision	74522
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

Security Advisory

1. Check your DNS and DHCP settings on your router.
   https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks
   If you have a router supporting multiple LAN subnets, check settings for each subnet. Your DNS settings should be either blank, set to the correct DNS server addresses from your ISP or DNS server addresses of a server which you have deliberately set (e.g. Google 8.8.8.8). A known rogue DNS server is 38.134.121.95 - if you see that, your router has been changed.

New Features

1. WAN2 (Ethernet) port can now operate as a LAN port when disabled in [WAN] > [General Setup] > [WAN2], for a total of 5 LAN ports, by selecting "No-Set as LAN" as the Enable option
2. Firewall Filter rules can now be linked to specified LAN and WAN interfaces by selecting a Direction then clicking Advanced and selecting the interfaces that the Filter rule will affect
3. ISO 3166 Country objects configured in [Objects Setting] > [Country Object] menu can be applied as Source / Destination IP ranges in Firewall Filter rules
4. LAN IP Alias added to [LAN] > [General Setup] to define which WAN is used for outbound traffic by sending to a different Gateway address for the router
5. Support DrayOS IKEv1 IPsec XAuth as a VPN protocol for Remote Dial-In User VPN tunnels
6. Support for EAP Tunnelled Transport Layer Security (EAP_TTLS) security method added to [Applications] > [Local 802.1X General Setup].
7. Configuration backup / restore is now available for Remote Dial-In User and LAN-to-LAN profiles to back up all VPN profiles configured, separately from the main router configuration file
8. Larger certificate files now supported in [Certificate Management] > [Local Certificate] making it possible to include additional certificates required to complete a certificate chain
9. Support for mOTP and 2FA (two factor authentication) via e-mail/SMS added for remote management in [System Maintenance] > [Administrator Password]
10. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected

Improvements

1. Fixed the App Enforcement profile issue in 3.8.9 firmware
2. Fixed the Web UI Issue if Bandwidth Limit and Data Flow Monitor were enabled in 3.8.9 firmware
3. Support for VigorACS 2 version 2.3.0
4. Improved device compatibility with router's 5GHz WLAN and AES encryption
5. Layout of [WAN] > [Internet Access] > [Details Page] improved to group essential settings in the left pane, with additional / advanced options grouped in the right pane
6. Subnet Mask settings in the web interface now use a drop-down box for selection
7. The number of characters allowed in a text box, such as a username or password field, is now displayed in the web interface when no text is entered in that text box
8. Layout of [VPN and Remote Access] > [Connection Management] improved with separate tabs for active LAN-to-LAN and Remote Dial-In User VPN tunnels
9. Layout of [Bandwidth Management] > [Quality of Service] improved
10. DoS Defence moved to [Firewall] > [Defence Setup]
11. Anti-Spoofing Defence settings for IP and ARP spoofing added to [Firewall] > [Defence Setup]
12. Certificate import can now be performed via CLI using "mngt cert_import" command via URL
13. Removed deprecated CLI commands "ip dmz" and "ip aux [Join to NAT pool]"
14. Added "IPv6 Address Random Allocation" option for DHCPv6 Server settings
15. IKEv2 LAN to LAN VPN tunnels can specify these new Proposal options:
    a. Diffie-Hellman (DH) Group 19 (256-bit Elliptic Curve)
    b. Diffie-Hellman (DH) Group 20 (384-bit Elliptic Curve)
    c. Diffie-Hellman (DH) Group 21 (512-bit Elliptic Curve)
16. The Router Name set in [System Maintenance] > [Management] can be used as L2TP Client's Host name
17. Central AP Management profiles now have options to configure AP-assisted Client Roaming parameters
18. Support Channel Width selection on [Central Management] > [AP] > [WLAN Profile]
19. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected
20. Improvements to WAN Budget scheduling
21. Inter-LAN Routing table in [LAN] > [General Setup] now allows routing between LAN1 and DMZ when VLANs are not enabled
22. Improved load balancing algorithm for VoIP – STUN and SIP connections will now remain on the same WAN interface by default
23. Session timeout values for SSH and Telnet can now be adjusted with "mngt telnettimeout/sshtimeout" CLI commands
24. Improved Bandwidth Limit operation when used in conjunction with QoS
25. If TR-069 was configured with STUN, the resulting UDP connection request address would still be sent to the TR-069 server after disabling STUN for TR-069
26. Unable to pass traffic through VPN when VPN Trunk Backup connection was resumed
27. The web interface did not accept IPv6 Object IP addresses ending with "::"
28. Improved warning notifications given when disabling LAN ports, USB ports, LEDs and buttons in [System Maintenance] > [Panel Control]

29. Syslog incorrectly displayed the password setting for WAN DHCP Client Identifier
30. The router could sent incorrect DNS queries if Syslog / Mail Alert was enabled
31. Improved VLAN Tag Insertion layout for [WAN] > [General Setup]
32. Schedule entries are now selected from a drop-down box which displays each schedule entry number and configured Comment fields
33. Schedule entries configured to operate overnight did not work correctly
34. Improved handling of Firewall filter rules configured to operate on a schedule
35. Enabling Session Limit could block Internet connectivity for Remote Dial-In User VPN tunnel connections from VPN clients sending Internet traffic through the VPN tunnel
36. NAT Port Redirection entries configured through the CLI did not take effect unless disabled and re-enabled
37. NAT Port Redirection entries configured with TCP protocol could not be enabled
38. Improved USB storage handling, to better handle USB storage being unplugged while reading data from the USB for a user connected to the router's FTP server
39. Improved interoperability of the DHCP Relay function with Windows Server's DHCP server
40. DHCP Relay did not work with Remote Dial-In User VPN tunnels
41. Enabling "Allow management from the Internet" option for IPv4 could also enable this option for IPv6 Internet connections
42. Entering a Pre-Shared Key(PSK) containing " in [Wireless LAN] > [Security] would cause that settings page to display incorrectly
43. [Central AP Management] > [WLAN Profile] could not set TX Power for 5GHz WLAN
44. USB Disk could not be detected upon reconnection after disconnecting via WUI
45. Improved compatibility with "freedns.afraid.org" and "UBDDNS" Dynamic DNS providers
46. Log information could not be displayed for DtDNS Dynamic DNS hostname updates
47. The Domain Name "ddns.net" could not be selected when using No-IP.com Dynamic DNS
48. Added support for EntryDDNS Dynamic DNS provider
49. Unable to get DrayDDNS domain name after registering and activating the DrayDDNS license
50. TR-069 Packet Counters for LAN ports could still increment when the port was not in use
51. The "Don't Fragment" flag of an IP header was not processed correctly in all scenarios
52. Could not register Avaya phone [H.323] to IPPBX server through router's NAT
53. Multiple objects can now be selected configuring an object group
54. Added "Next" and "Previous" links on each object profile editing page
55. DHCP Broadcast packets from LAN clients could incorrectly be sent out through the WAN2 interface in some circumstances, affecting WAN2 connections using DHCP for IP allocation
56. DHCP server state of LAN Subnets could be displayed incorrectly on the [Dashboard]
57. Auto VoIP QoS is now applied to routed LAN subnets
58. Wireless clients could not communicate with wired clients in the same VLAN with a VLAN tag
59. Incoming RDP sessions cannot authenticate with Firewall configured for User-based mode
60. QoS LED could be incorrectly lit if QoS was enabled then disabled
61. Restart is no longer required for changes to [Applications] > [RADIUS/TACACS+] > [Internal Server] when enabling/disabling Internal Radius Server or modifying the Authentication List
62. Remote Dial-In User VPN connections could not access the Internet through the VPN tunnel if Hardware Acceleration was enabled on the router
63. Some IPv6 packets were incorrectly blocked by the IP Filter with rules configured to pass these IPv6 packets

64. Resolved display issue with Bind IP to MAC enable/disable setting in VigorACS 2
65. When the Interface - LAN section is expanded on the [Dashboard], click on Host ID/Comment text to switch between ARP Table's Host ID and Bind IP to MAC's Comment
66. Added switching between viewing All Users and Online Users view in [User Management] > [User Online Status] by clicking on the text in the upper right
67. Bind IP to MAC was incorrectly limited to 300 entries instead of 1024
68. Increased Hotspot Web Portal profile Terms and Conditions Content field length to 1360 characters
69. Idle timeout value was not applied to Remote Dial-In User tunnels using SSL VPN
70. ARP Table displayed Comments incorrectly for some IP addresses i.e. x.x.x.10 would display the same comment as x.x.x.101
71. "CN" and "cn" values (Common Name Identifier) for LDAP now operate in the same way
72. PPPoE status messages were not displayed in [Physical Connection] > [Online Status]

Known Issues

(None)

Firmware Version	3.8.9 (Not Released)
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.8.2) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.8.2.
Build Date	21st May 2018
Release Date	-
Revision	73984
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(See Firmware 3.8.9.1)

Improvements

(See Firmware 3.8.9.1)

Known Issues

1. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.

   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2].
   Set the Enable setting of WAN2 to "Set as LAN" and click OK. The WAN2/LAN5 port will operate as LAN5 once it has restarted.

2. The router cannot be managed from the Web UI if Bandwidth Limit is enabled on the router. This will be corrected in the next firmware release.

Firmware Version	3.8.8.2 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	18th May 2018
Release Date	18th May 2018
Revision	73953
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

None

Improvements

1. This firmware includes improvements to harden the web interface against attacks. We have become aware of specific attacks against router, including DrayTek models where hackers have altered specific settings relating to your DNS servers and DHCP settings. You should urgently check those settings on your router. If they appear to have been tampered with, correct them and change your admin password and for any other config anomalies. Restore a config backup if you have one (from prior to the attack). We continue to investigate this issue but the first priority was to issue updated firmware.

Known Issues

1. Current Time values on the [Dashboard] are not displayed correctly in Internet Explorer web browser
2. If Hardware Acceleration is enabled then Dial-In Users are unable to route to the Internet via the VPN tunnel using 'Use default gateway on remote network'

Firmware Version	3.8.8 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	14th February 2018
Release Date	14th March 2018
Revision	72017
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. LAN ports, Wireless LAN button and Factory Reset button can now be enabled or disabled from [System Maintenance] > [Panel Control]
2. Router's status LEDs & port LEDs can be turned off or put into "LED Sleep Mode" when inactive, configured in [System Maintenance] > [Panel Control]
3. Wireless Pre-Shared Key can now be viewed when logged into the router's admin account. Click on the "****" text to reveal the password currently in use
4. EAPOL Key Retry Enable/Disable setting added to [Wireless LAN (2.4GHz/5GHz)] > [Security] Disabling this setting can prevent WPA2 Key Reinstallation Attack (KRACK) attack vectors, for more details please read this security advisory: https://www.draytek.co.uk/information/our-technology/wpa2-krack-vulnerability (EAPOL Key Retry is set to Enabled by default and in previous firmware)
5. Anti-Spoofing Defence settings for IP and ARP spoofing added to [Firewall] > [Defence Setup]
6. ISO 3166 Country objects added to [Objects Setting] menu for use with Firewall Filter rules and Route Policy rules
7. Dashboard layout can be configured with the Customise Dashboard link at the bottom of the [Dashboard] page

Improvements

1. Speed and duplex settings manually configured for WAN1 / WAN2 ports could display incorrect status information
2. TR-069 parameters added for Bind IP to MAC configuration and comments
3. Disabling Bind IP to MAC with a specific configuration could block access to the router
4. DoS Defence moved to [Firewall] > [Defence Setup]
5. "None" option for Syslog in CSM (UCF/WCF/DNSF) profile is no longer used
6. Default WAN Connection Detection mode for PPPoE connections is now named "PPP Detect" instead of "ARP Detect"
7. Syslog & SMTP Server fields in [System Maintenance] > [Syslog/Mail Alert Setup] now allow up to 63 characters for longer hostnames
8. Web Syslog in [Diagnostics] > [Syslog Explorer] can now be used when "Syslog Server" is not enabled or configured in [System Maintenance] > [Syslog / Mail Alert]
9. User Management could not authenticate users with RADIUS when the RADIUS server was accessed through a VPN tunnel
10. The "IP Routed Subnet" option could not be enabled in [Bandwidth Management] > [Bandwidth Limit]
11. Bandwidth Limit's effect on LAN to LAN VPN tunnels is toggled on/off with the "IP Routed Subnet" option

12. Bandwidth Limit was not applied to VPN traffic correctly in some configurations
13. MyVigor DrayDDNS service status could incorrectly be displayed in red after updating information
14. [NAT] > [Open Port] settings could not be saved if a UDP port was specified that conflicted with a TCP management port
15. Failback setting option in [Routing] > [Load Balance/Route Policy] rules could not be saved in some configurations
16. Remote Dial-In Users connecting via PPTP protocol were not assigned DNS addresses configured for the LAN subnet
17. Improved DNS caching behaviour with Web Content Filtering and DNS Filtering enabled
18. Firmware could only be upgraded through Firmware Upgrade Utility 3.6.6 when router was manually put into TFTP mode

Known Issues

1. Current Time values on the [Dashboard] are not displayed correctly in Internet Explorer web browser
2. If Hardware Acceleration is enabled then Dial-In Users are unable to route to the Internet via the VPN tunnel using 'Use default gateway on remote network'

Firmware Version	3.8.7 (Formal Release)
Release Type	**Initial Release**
Build Date	27th October 2017
Release Date	15th January 2018
Revision	69532
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

First Firmware Release for this model

New Features

(None)

Improvements

(None)

[END OF FILE]