

Release Notes for DrayTek Vigor 3912 (UK/Ireland)

Firmware Version	4.4.3.4 (Formal Release)
Release Type	Regular – Upgrade recommended when convenient
Build Date	27 th March 2025
Release Date	14 th May 2025
Revision	4926_7605_b8950f82bc
Applicable Models	Vigor 3912, Vigor 3912S
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improvements to the wording; “null” is replaced with “empty”
2. Support for TCP protocol for Port Knocking
3. Improvements to the update method for User Management’s data quota
4. BFP (Brute Force Protection) Status added to the Dashboard
5. The CMS profiles that are not enabled on the Main Filter page are hidden
6. The “Product Registration” is renamed to “Registration & Services”
7. New SMS Service Providers added: “sms.mitake.com.tw” and “SerwerSMS.pl”
8. A new TR-069 parameter added for [Applications] > [Radius/TACACS+] > [Certificate]
9. A note added to explain the ‘None’ item for Protocol on the [NAT] > [Port Knocking] page
10. The “Malloc OSPF config fail” error log has been removed when OSPF is enabled but no profiles are configured
11. The Router Policy Name (comment) is displayed in the dropdown menu instead of displaying the “Index number”
12. A prompt added to re-enter the verification code when changing other settings on the [NAT] > [Port Knocking] page
13. The username length increased in [User Management] and [USB] > [User Management] sections to 32 characters (previous limit was set to 11 characters)
14. Enhance of the DPDK Anti-DoS mechanism to reduce high CPU usage caused by UDP broadcast/multicast floods that could lead to instability of the router
15. Fix for the STUN server related issues
16. Buffer management improvements related to SSL VPN service
17. The router could become unresponsive after enabling login with 2FA
18. The all traffic (0.0.0.0/0) through VPN improvements
19. Some of the IGMP Status information was incorrect
20. The WAN IP object/group wasn’t listed in firewall source IP
21. Improvements related to the high CPU usage caused by UDP broadcast/multicast flood
22. Fix for the connection issues related to the IPsec X.509 H2L VPN
23. Fix for sending SMS via MessageBird or custom settings
24. RADIUS Request Interval improvements
25. High Availability Hot-Standby Config Sync was not functioning correctly

26. Improvements to the WANx prioritization for DrayDDNS when using Internet IP
27. Improvements with the log for updating an external device turned into garbled text
28. The Syslog client failed to work when using the WAN Alias IP
29. Improvements to the DoS attack mechanism that could cause high CPU usage and make the router unresponsive
30. Fix an issue where creation of a Let's Encrypt certificate with No-IP domain did not work
31. The router could become unresponsive while establishing the 3rd IKEv2 EAP VPN connection
32. Improvements to the online status showing "Fiber" even when the Ethernet connection was selected
33. The correct icon is displayed for VigorAP 918R, VigorAP 805, and VigorAP 962C via APM
34. Fix for the firewall block issue where a rule was set with WAN->Localhost direction and was ignored by the system after 5 minutes
35. Fix for the issue where router could become unresponsive when login into the WUI with TOTP after downgrading from 4.4.3.2 to 4.4.3.1
36. Improvements to the WAN RX Packet Count that displayed negative values when using the CLI command "show state"
37. Fix an issue where the Gateway setting appeared if WAN/LAN was selected for the Failover to option on [Routing] > [Route Policy]
38. Improvements to the router stability related to dray_dpdk, QEMU and configuration backup job via VigorACS server
39. Fix for the issue where Internal Syslog Server continued to receive Syslog from the WAN, even after the NAT Open Port rule was disabled
40. The IKEv2 VPN was disconnecting when a Peer Domain Name was specified and receiving DNS server responses with a TTL of 0
41. When using the packet capture function on the web interface, P1 was incorrectly set to enabled even after stopping the packet capture function

Known Issues

(None)

Firmware File Types

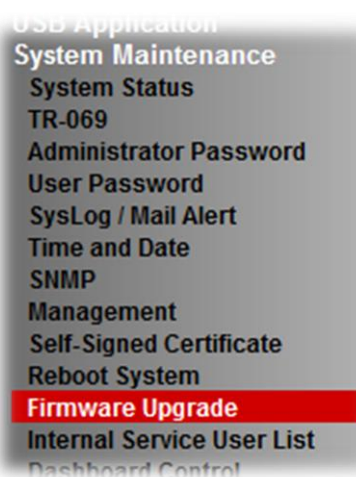
The file name of the firmware controls which upgrade type is performed.

If the file name is unchanged (e.g. xxxx.**sfw**) 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 SFW 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	4.4.3.2 (Formal Release)
Release Type	Critical – Upgrade recommended immediately
Build Date	28 th November 2024
Release Date	24 th December 2024
Revision	4859_7498_8085331
Applicable Models	Vigor 3912, Vigor 3912S
Locale	UK & Ireland Only

New Features

1. Support to enable/disable Port 1 to Port 12 via CLI:
`port setting -p [port number] -e [0 for disable; 1 for enable]`
For example, port 11 can be disabled with the following command:
`port setting -p 11 -e 0`
2. Support for TLS 1.3 added to [System Maintenance] > [Management]
3. Support for checking the SSD/eMMC health information on [Linux Applications] > [Storage],
and via CLI command:
`linux dstatus -s`
4. The new tabs for Custom Rules and Rule Exclusion List options added on [Linux Applications] > [Suricata]
5. TOTP 2-factor authentication (Google Authenticator) is now available for authenticating web interface administrator access from the Internet
[System Maintenance] > [Administrator Password]

Improvements

1. Web GUI Security improvements
2. The GeoIP database updated to version 2024-10-01
3. The [Diagnostics] > [Debug log] feature enhancements
4. Support added for responding to ARP Probe packets
5. Improvements to the view sort arrows on the [Firewall] > [Defense Setup] page
6. The syslog output changed to "SMS/Email alert suppressed" when triggered by Notification Object for VPN Tunnel with "Downtime Limit" settings enabled
7. The new pop-up notification added:
"If you have enabled DNS Filter on CSM Profile>>DNS Filter and want to access Vigor router via a specified domain name, type the domain name in [Domain name allowed] on [System Maintenance>>Management>>LAN Access Setup]"
8. The redundant "Clear All" button has been removed from [Applications] > [Dynamic DNS]
9. The "optional" note added for [Objects Setting] > [IP Object] for MAC Address selection
10. A note related to EOL AP-900 was removed in [Central Management] > [AP] > [Load Balance]
11. IPv6 status will be shown in green only when IPv6 interface is enabled
[LAN] > [General Setup]
12. Individual clear buttons added for Restore Backup Firmware/Config on [System Maintenance] > [Configuration Export]
13. BGP over GRE did not work
14. The correct AP906 icon can be displayed in APM
15. Fix for the high packet loss with Starlink connections

16. Improvements to system stability and compatibility with IPTV connections
17. Fix an issue where a wrong port triggering was linked with the defined Smart Action profile
18. Improvements to the IP phones SIP registration being lost when used over VPN LAN to LAN connections
19. Router's stability improvements linked with QEMU system
20. Block list not showing when IP is blocked via Data Flow Monitor
21. Fix an issue with the internet access that could be caused by Fast NAT using incorrect MSS values
22. The [Diagnostics] > [NAT Sessions Table] WUI page did not display all the data
23. Failed to restore V3912S > NAT > Port Redirection/Open Ports .bak file
24. The VPN Traffic Graph H2L traffic accuracy improvements
25. Changing LAN1 IP Address could cause inaccessibility after reboot (ports 9–12 only)
26. VPN Matcher special characters [] () compatibility improvements
27. The client data quota could not be recorded if the router was power cycled
28. The URL Filter did not block HTTPS websites when TLS 1.3 hybridized Kyber was enabled in the browser
29. Vigor 3912S model only: VigorConnect and Suricata did not start after resetting to their default configurations
30. OpenVPN certificate compatibility improvements
31. The system would show two temperature sensor icons when only one sensor was connected [Online Status] > [Physical Connection]

Known Issues

(None)

Firmware Version	4.3.6.2 (Formal Release)
Release Type	Critical – Upgrade recommended immediately
Build Date	29 th October 2024
Release Date	26 th November 2024
Revision	4306_5107_ed63ed3
Applicable Models	Vigor 3912, Vigor 3912S
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Web GUI Security improvements (CVE-2024-46550, CVE-2024-46568, CVE-2024-46571, CVE-2024-46580, CVE-2024-46586, and CVE-2024-46588 ~ CVE-2024-46598)
2. Resolved an issue with DMZ host set for WAN3 Alias IP when P1/P2 port is changed to the LAN port mode

Known Issues

(None)

Firmware Version	4.3.6.1 (Formal Release)
Release Type	Regular – Upgrade recommended when convenient
Build Date	23 rd July 2024
Release Date	13 th August 2024
Revision	4188_5045_109e0bd
Applicable Models	Vigor 3912, Vigor 3912S
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Web GUI Security improvements
2. Description modified for the Fast NAT check box on NAT>>Fast Routing/NAT.
3. Resolved an issue with failure to use the new created Google API via Hotspot.
4. Resolved an issue with HA slave when WCF enabled was enabled
5. Resolved an issue with the lack of the WAN interface setting field on VPN>>VPN Matcher Setup.
6. Resolved an issue with the hotspot HTTPS redirection error by the HTTPS management port being set as non-default.
7. Resolved an issue with the URL filter failed to block HTTPS websites when TLS 1.3 hybridized Kyber was enabled in the web browser and web server used the cipher
8. Resolved an issue with the WUI of Objects Setting>>SMS/Mail Service Object lost connection temporarily after clicking "Send a Test Message"
9. Resolved an issue that the IPsec Peer Identity profile still appeared and was selected on the remote dial-in profile, even if it was deleted or renamed.

Known Issues

(None)

Firmware Version	4.3.6 (Formal Release)
Release Type	Regular – Upgrade recommended when convenient
Build Date	7 th June 2024
Release Date	2 nd August 2024
Revision	4091_4929_2bc9d11
Applicable Models	Vigor 3912, Vigor 3912S
Locale	UK & Ireland Only

New Features

1. Support for Vigor 3912S
2. The 'Telegram' and 'Block IP' smart actions added to the [Application] > [Smart Action] page

Improvements

1. VigorConnect can be enabled from the router's WUI in [Linux Applications] > [VigorConnect]
2. Password mechanism changed to force admin to change the password from the default password
3. In some circumstances BGP routing didn't work
4. Support for detailed Port Statistics added in [Diagnostics] > [Port Statistics]
5. Improvements to the DoS defense alerts accuracy
6. Improvements to the VPN mechanism (L2TP over IPsec)
7. The note to copy 2FA token has been added for the VPN Dial-in User WUI profile pages
8. The Port Physical Type selection did not match the [Port Setup] and [WAN] > [General Setup] pages
9. The Port Knocking for Local Service field added to [System Maintenance] > [Management]
10. The display mechanism for [System Maintenance] > [Management] WUI for "Port Knocking for Local Service" and "Brute Force Protection" will show additional option in the same manner
11. The note in [System Maintenance] > [Firmware Upgrade] matches the new firmware file type (".sfw" instead of ".all")
12. The new note added to the [VPN and Remote Access] > [PPP General Setup] page:
"4. AD/LDAP Authentication only supports PPTP / L2TP / SSL / OpenVPN / IPsec XAuth and doesn't support IKEv2 EAP"
13. Simplified time format, and log sorting set from the latest to the oldest (like in Syslog Explorer) will be used by [Linux Applications] > [Log collector] page
14. The Port Knocking Tools download link added on the [NAT] > [Port Knocking] page
15. Redesign of the [System Maintenance] > [Configuration Export] "Restore Backup Firmware / Config", and [NAT] > [Fast Routing/NAT] pages
16. Fix for the DoS Defense alerts linked with the DHCP packets
17. Fix for the DrayDDNS WAN IP updates
18. User data quota in User Management didn't work
19. Fix for the auto timezone option that could not pick the right zone
20. In some circumstances the DHCP Server could not assign over 1000 IP addresses
21. Fix for the NAT Open Port, Port Redirection, and Port Knocking WAN selection where unavailable WAN interfaces were also selectable in the WUI
22. The router could stop responding every few hours after enabling the WCF

23. The first IP/LAN IP in Smart Action did not work
24. The router couldn't send SMS when VPN and TOTP were used
25. Login from a VPN subnet or non-directly connected LAN could fail
26. The get code page showed incorrect model of the router (3910) when the advanced authentication web login from wan was enabled
27. The Log collector did not work after upgrading to a beta firmware
28. The router could stop responding when the conntrack (connection tracking) table is full
29. Fix for the VPN settings inconsistency when accessed via WUI and CLI
30. Hotspot Web Portal - Social login with Google account didn't work
31. In some cases Windows L2TP IPsec VPN could disconnect every 8 hours.
32. When a sudden power off occurred, the router could boot up by using the backup image
33. When turning the Smart Action profile on or off, router could stop responding
34. Improvements to the VPN mechanism (L2TP over IPsec)
35. Improvements to the LAN to LAN Dial-out profiles set with the domain name using uppercase letters (did not work)
36. The router could not detect the USB temperature sensor (TEMPer1F_V3.4) after a normal reboot and power off/on
37. Fix for the issue where router did not boot up on a cold reboot when SFP-10G-T100 was connected to SFP1 interface
38. The UDP session over WireGuard VPN wasn't released after the VPN reconnection
39. Fix for the Advanced Authentication options for Web Login that could disappear after importing a configuration file from Vigor 3910
40. VoIP - Incoming/outgoing calls failed based on "Allow pass inbound fragmented large packets" status
41. In some circumstances, testing ping could cause DNS failure and WAN Offline (WAN Connection Detection failure) issues. Brute Force Protection will exclude some of the well known DNS IP addresses
42. Improvements to the URL reputation mechanism that did not block some specific websites and print the "Get Request Resource Failure" in the syslog
43. Fix for the ping failure issue from LAN P9-P10 (related to the Link Aggregation setting that wasn't cleared completely)

Known Issues

(None)

Firmware Version	4.3.5.2 (Formal Release)
Release Type	Regular – Upgrade recommended when convenient
Build Date	30 th April 2024
Release Date	11 th June 2024
Revision	3733_4582_c35e39d
Applicable Models	Vigor 3912
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. The network connection stability improvements
2. Improvements to the network security related to the password and DHCP functionality
3. Password mechanism changed to force admin to change the password from the default password
4. Fix for the IPv6 firewall functionality
5. Fix for the IKEv2 EAP with the iOS VPN client issue
6. The Configuration Backup button in the top section of the GUI did not work

Known Issues

(None)

Firmware Version	4.3.5.1 (Initial Release Firmware)
Release Type	Initial Release
Build Date	8 th January 2024
Release Date	8 th February 2024
Revision	3694_4567_1a05379251
Applicable Models	Vigor 3912
Locale	UK & Ireland Only

First Firmware Release for this model

New Features

(None)

Improvements

(None)

Known Issues

(None)

[END OF FILE]