

Release Note for Vigor2865 Series

Firmware Version:	4.4.3.1
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor2865 / Vigor2865ac / Vigor2865Vac Vigor2865L / Vigor2865Lac / Vigor2865ax

Vigor2865 Series is a VDSL2/ADSL2+ Security Firewall router integrating a DSL modem which is compatible with variants of ADSL and VDSL, including profile 35b Super Vectoring.

New Features

- Support new WCF suppliers.
- Support a new feature Wireguard VPN.
- Support VPN interface on NAT>>Open Port.
- Support HTTP compression to reduce the TR-069 payload size.

Improvement

- Improved: Improve the web GUI security.
- Improved: Support more SMS commands.
- Improved: Support more LTE SNMP OIDs.
- Improved: Improve Auto APN for Gamma SIM.
- Improved: Improve SIM1/SIM2 failover mechanism.
- Improved: Support writable/read-only notes for TR-069 parameters.
- Corrected: Issues with DNS PTP records.
- Corrected: An issue with WAN2 L2TP not working.
- Corrected: An issue with the DHCP relay not working.
- Corrected: An issue that IPsec Hardware Acceleration enabled.
- Corrected: An issue with the router rebooting after WAN IPv6 renew.
- Corrected: Add a new option to enable/disable the individual SIM slot.
- Corrected: An issue that the Bridge VLAN over mesh network not working.
- Corrected: An issue with empty .json response for CPE when using VigorACS API.
- Corrected: An issue that the router rebooted while using LTE module for a long period.
- Corrected: An issue with the firmware was damaged when upgrading from VigorACS.
- Corrected: An issue with the router rebooting after restoring the config from Vigor2862.
- Corrected: An issue with gaps appeared on the graphs displayed on the VigorACS page.
- Corrected: An issue with failure to enable/disable the wireless bands via the WPS button.

- Corrected: An issue that strange data used information shown on the WUI when using SIM budget.
- Corrected: An issue that the Let's Encrypt certificate could not be renewed automatically but manually.
- Corrected: An issue that failure to disconnect the VPN tunnel between VPN server (Vigor router) and client.
- Corrected: An issue that the router rebooted after saving L2TP with IPsec (LAN to LAN) VPN profile.
- Corrected: An issue that OpenVPN to Pfsense connected but could not get the push route from the server.
- Corrected: Issues related to authentication on External Hotspot Server and the External RADIUS Server.
- Corrected: An issue with the key data loss for OpenVPN client config file when exported from VigorACS.
- Corrected: An issue with an error message of HTTP Content Error appeared while trying to import ovpn file.
- Corrected: An issue that the router rebooted when IKEv2 re-dialed and the local ID was set to 32 characters.
- Corrected: An issue with staying in the Firmware Damage state after uploading the wrong firmware (file size was 0).
- Corrected: An issue that VPN 2FA Windows was not popped-up when a SmartVPN client dialed with IKEv2 EAP and the router's LAN IP used not the 1st setting.

File and Modem Code

- "Vigor2865_v4.4.3.1_STD.zip" provides Annex A modem code 8B0F07_8B0701 and 8B2607_8B0B01, and Annex B modem code 8B2607_8B0B02 and 8B2817_8B0812.
- "Vigor2865_v4.4.3.1_MDM1.zip" provides Annex A modem code 8B1117_8B0701 and 8B0F07_8B0701, and Annex B modem code 8B2817_8B0812 and 8B2607_8B0B02.
- "Vigor2865_v4.4.3.1_MDM2.zip" provides Annex A modem code 8D1917_8D0C11 and 8D1507_8D0901, and Annex B modem code 8D1917_8D0C12 and 8B2817_8B0812. Recommended for Australia.
- "Vigor2865_v4.4.3.1_MDM3.zip" provides Annex A modem code 77C717_8D0C11 and 8D1507_8D0901, and Annex B modem code 77C717_8D0C12 and 8B2607_8B0B02.
- "Vigor2865_v4.4.3.1_MDM4.zip" provides Annex A modem code 8D1C17_8D0E11 and 8D1B17_8D0E11, and Annex B modem code 8D1C17_8D0E12 and 8D1917_8D0C12.
- "Vigor2865_v4.4.3.1_MDM5.zip" provides Annex A modem code 8D1F17_8D1011 and 8D1917_8D0C11, and Annex B modem code 8D1F17_8D1012 and 8D1917_8D0C12.

Known Issue

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

Note

- IPsec HMAC (MD5) is no longer supported.