

Release Note for Vigor2926 Series

Firmware Version:	3.9.1
Release Type:	Normal
Applied Models:	Vigor2926, Vigor2926n, Vigor2926ac, Vigor2926L, Vigor2926Vac, Vigor2926Ln, Vigor2926Lac

Vigor2926 series is a broadband router which integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth. The state-of-art routing feature, VPN security, and Dual-WAN provide integrated benefits for professional users and small offices.

New Features

- Support IPTV diagnosis.

Improvement

- Improved: Adjust the setting method for P5/WAN2.
- Improved: Add the MyVigor Services>>Service Status page to display the service activation information.
- Improved: Add the Station Control field in Central Management>>AP>>WLAN Profile.
- Improved: Support Exception list for load balance in WAN>>General Setup.
- Improved: For telnet command setting, give full parameter names for getting/setting all TR-069 parameters.
- Improved: Add a note to notify the user that the Vigor router certificate is not part of the configuration file.
- Improved: Add a check box to hide Group Password in Central Management >> Switch >> Profile page.
- Improved: Support the IP Group as Source IP on Port Redirection/Open Ports.
- Improved: Add a TR-069 parameter of VoIP QoS for configured by VigorACS.
- Improved: Add search bar to Left Menu.
- Improved: Remove the TFTP note from System Maintenance >> Firmware Upgrade.
- Improved: Add the Dynu DDNS provider as a Provider Host selection.
- Improved: Support IKEv2 EAP LAN to LAN tunnel for using with NordVPN server.
- Improved: Improve the timing of sending the RMM information.
- Improved: Support "Use ACS Server" as the STUN server on System Maintenance>>TR-069 Setting.
- Improved: The USB printer server is disabled in default.

- Corrected: Unable to register to VigorACS.
- Corrected: Failed to create IKEv2 EAP connection from Windows 10 when using self-signed CA.
- Corrected: Unable to restore VPN backup profile from other router to Vigor2926.
- Corrected: Android or Windows10 OS built-in detection page still popped up even if Captive Portal Detection was disabled for the web portal setup.
- Corrected: Unable to accept VPN remote dial-in users when "change default route to this VPN tunnel" was enabled for the LAN to LAN.
- Corrected: Unable to authenticate VigorACS server certificate (issued by Let's Encrypt).
- Corrected: Unable to resume IPTV after pausing for more than 5 minutes.
- Corrected: SSL VPN client obtained DNS server address via router's WAN instead of DHCP Relay server.

Known Issue

- None.