

Release Note for Vigor3912 Series

Firmware Version:	4.3.6
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor3912, Vigor3912S

New Features

- Add a new model, Vigor3912S.
- Add two new actions (Telegram and Block IP) in Application>>Smart Action.
- Add new menu item, Linux Applications>>VigorConnect.

Improvement

- Improved: Password mechanism changed to force admin to change the password from the default password.
- Improved: BGP routing improvement.
- Improved: Support Detailed Port Statistics.
- Improved: Improve the DoS defense alerts accuracy.
- Improved: Improve the remote dial-in (L2TP over IPsec) stability.
- Improved: Add a note in WUI when setting up 2FA Secret for VPN Dial-in User.
- Improved: Unify the Port Physical Type between "Port Setup" and "WAN > General Setup".
- Improved: Support Port Knocking for Local Service field in System Maintenance>>Management.
- Improved: Modify the note in System Maintenance >> Firmware Upgrade (".all" firmware was not available, instead by ".sfw").
- Improved: Unify "System Maintenance >> Management" WUI for "Port Knocking for Local Service" and "Brute Force Protection".
- Improved: Add a note in "VPN and Remote Access >> PPP General Setup" WUI about VPN supported for LDAP/AD Authentication.
- Improved: For Linux Applications >> Log collector, use simple time format, logs sorting from the latest to the oldest like in Syslog Explorer.
- Improved: Add the Port Knocking Tools download link on the pages of NAT>>Port Knocking and System Maintenance>>Management.
- Improved: Redesign the web page, System Maintenance>>Configuration Export >> Restore Backup Firmware / Config, and NAT>>Fast Routing/NAT.
- Corrected: An issue with DoS Defense alerts on the DHCP packets.
- Corrected: An issue with failure to update WAN IP for DrayDDNS.
- Corrected: An issue that user management's data quota did not work.
- Corrected: An issue with failure to set the correct timezone by Auto.
- Corrected: An issue with the DHCP failure due to waiting for a long time.

- Corrected: An issue that some NAT WUIs showed unused WAN interfaces.
- Corrected: An issue with rebooting every few hours after enabling the WCF.
- Corrected: An issue that first IP/LAN IP in Smart Action seemed not to work.
- Corrected: An issue that the router did not send an SMS when the VPN was up.
- Corrected: An issue with login Failure from VPN or non-direct connected LANs.
- Corrected: An issue with the wrong model display on the Web Advanced Login page.
- Corrected: An issue with failure to work for Log collector after upgrading new beta.
- Corrected: An issue with a router reboot problem caused by the contrack table being full.
- Corrected: An issue with inconsistency on VPN from LAN configuration via WUI vs CLI.
- Corrected: An issue that Hotspot Web Portal - Social login with Google account didn't work.
- Corrected: An issue that a Windows L2TP over IPsec VPN disconnected every 8 hours problem.
- Corrected: An issue that a sudden power off might cause the router to boot up by using the backup image.
- Corrected: An issue with a reboot problem resulting from turning on or off the Smart Action profile.
- Corrected: An issue with L2TP over IPsec connected with phase2 none hash when IPsec security method is high.
- Corrected: An issue that the LAN to LAN Dial-out profile did not work if the domain name was set with uppercase letters.
- Corrected: An issue with failure to detect USB temperature sensor (TEMPer1F_V3.4) after a normal reboot and power off-on.
- Corrected: An issue that the router did not boot up on a cold reboot when SFP-10G-T100 was connected to SFP1.
- Corrected: An issue that no traffic on the UDP port until rebooting the device when the WireGuard VPN dropped and came back.
- Corrected: An issue that Advanced Authentication options for Web Login disappeared after importing a customer's 3910's config file.
- Corrected: An issue with incoming/outgoing calls failure (VoIP) based on "Allow pass inbound fragmented large packets" status.
- Corrected: An issue that attackers in LAN network could cause general Internet access problems (DNS Failure) and WAN Offline (WAN Connection Detection failure).
- Corrected: An issue with failure to block specific websites by using URL reputation and the "Get Request Resource Failure" shown in the syslog.
- Corrected: An issue with failure to ping from LAN P9-P10 (related to the Link Aggregation setting that wasn't cleared completely).

Known Issue

- None.