

## Release Note for Vigor3910 Series

Firmware Version:	4.3.2.3
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor3910

### Read First

Due to the WebGUI security issue (fixed in 3.9.6.3), we recommend **changing the passwords** for admin login and password/PSKs for VPN profiles after upgrading the latest firmware from 3.9.6.2 or earlier.

### New Features

- Add a new menu item (NAT>>Fast NAT) to increase the number of sessions established per second.

### Improvement

- Improved: Improve WAN >> Multi-VLAN port-based bridge performance.
- Improved: The default setting for System Maintenance >> Max Connection will be 300K.
- Improved: Disable SSL TLS 1.0 and TLS 1.1 in the default settings of TLS/SSL Encryption.
- Corrected: An issue with the route policy sent via WAN IP Alias.
- Corrected: An issue where Canon printer could not get DHCP IP.
- Corrected: An issue where ICMP ping via the BGP route did not work.
- Corrected: An issue where WAN3 and WAN4 did not work simultaneously.
- Corrected: An issue where MyVigor could not be connected when rebooting the router with Wipe Out All.
- Corrected: An issue with the user-based firewall where only those users who fulfill the rule would be impacted.
- Corrected: An issue where PIN could not be sent via SMS when the recipient number contained +(country code).
- Corrected: A VPN issue where the IKEv2 connection dropped every two hours.
- Corrected: A VPN issue with frequent disconnection occurred in L2TP over an IPsec connection to Synology NAS.
- Corrected: A VPN issue where multiple VPN tunnels might get disconnected due to an invalid server domain in VPN profile 1.
- Corrected: An issue with an IP not in Access List could see the login page when enabling HTTPS remote access and SSL VPN service.
- Corrected: An issue where the host in the routing subnet was not accessible even when

inter-lan routing was enabled.

- Corrected: An issue with the firewall problem which caused when the "IP Group (or IPv6 Group or Service Type Group)" contains a large number of IP objects beyond the system memory capacity.

## Known Issue

- The web portal may cause the router to be too busy to respond quickly.
- The encryption method for OpenVPN will be factory defaulted if firmware upgrading is performed from v3.9.7 to v4.3.1 or above.
- When the firmware is downgrading via "System Maintenance >> Firmware Upgrade", one might have a chance to experience a config compatibility error, which causes the config of a certain function to return to the default setting. To avoid this error, "System Maintenance >> Configuration Export >> Restore Firmware with config" is the preferred way for firmware "downgrading". We suggest backup the config file before upgrading any firmware as well.
- To prevent potential errors when upgrading firmware, it is recommended to upgrade firmware sequentially one version at a time. (e.g., if the current firmware is 3.9.1, upgrade to 3.9.2 then 3.9.7.2, and then the latest version).
- Inter-LAN routing setting exported/backed up from firmware 4.3.2 release might be incorrect, please check inter-LAN routing settings.