

## Release Note for Vigor2962

Firmware Version:	4.4.3.2
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor2962, Vigor2962P

### 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.
- Before upgrading to 4.4.3, please upgrade to 4.3.2.7 or after to avoid configuration compatibility first.

### New Features

- None.

### Improvement

- Improved: Improve the Web GUI Security.
- Improved: Add handling for raw data without a "Year" field.
- Improved: Remove unused WAN interfaces from NAT WUI.
- Improved: Add the IP Filter name in Syslog for improved logging.
- Improved: Enhance the dashboard to display Link Aggregation status.
- Improved: Ensure the client data quotas persist after the router reboot.
- Improved: Update "Traffic Graph" terminology to prevent user confusion.
- Improved: Changed "Dray DDNS" to "DrayDDNS" in Service Status Log.
- Improved: Update DNS Filter note when "Domain name allowed" is enabled.
- Improved: Update warning messages about firmware damage for better clarity.
- Improved: Increase the ASCII Character Data limit for WAN DHCP Client Options to 127.
- Improved: Add an ARP Probe response to prevent WAN disconnection with ISP Proximus.
- Improved: Add an "optional" note on Objects Setting>>IP Object for MAC Address selection.
- Improved: Add the hyperlink to link to "Configuration Export" on System Maintenance>>Firmware Upgrade.
- Improved: Customers are no longer required to clear the checkbox "Decline VRRP MAC into ARP table" in Firewall > Defense Setup before one can successfully establish a Starlink connection.
- Corrected: An issue with session limit for Meraki VPN.
- Corrected: Issues related to WireGuard VPN access to WUI.
- Corrected: An issue with auto reboot time schedule functionality.
- Corrected: An issue with duplicate USB temper icons in Online Status.
- Corrected: An issue with router reboot and IPTV stopping unexpectedly.

- Corrected: An issue with incorrect VPN log direction display in the web interface.
- Corrected: An issue with lock list not displaying on Diagnostics>>Data Flow Monitor.
- Corrected: An issue with the router reboot and external device password disappearance.
- Corrected: An issue with incorrect session display for non-LAN IPs on Data Flow Monitor.
- Corrected: An issue with some sessions were missing on Diagnostics >> NAT Sessions Table.
- Corrected: An issue with failure to restore configuration for NAT Port Redirection/Open Ports.
- Corrected: An issue with PPPoE dialing failure due to conflicting static and dynamic IP settings.
- Corrected: An issue with misaligned columns in VPN and Remote Access Connection Management.
- Corrected: An issue with removing redundant "Clear All" button on Applications>> Dynamic DNS.
- Corrected: An issue with the router rebooted when External Device contained % in the password field.
- Corrected: An issue with addressing IPsec VPN dialing failure via domain name due to DNS cache time.
- Corrected: An issue with the wrong firmware information displayed when pressing the "Preview" button in "System Maintenance > Firmware Upgrade".

## Known Issue

- This version (4.4.3.2) introduces support for admin password hashing. If the router is upgraded to this version and later downgraded to a previous firmware version, the admin password will reset to its default value. It will be necessary to log in using the default password and reconfigure it. Other settings will remain unaffected.
- TR-069 parameters for Application >> Smart Action is not completed.
- The web portal may cause the router to be too busy to respond quickly.
- The encryption method for OpenVPN will be returned to the factory default settings if upgrading the firmware version from V3.9.7.x to V4.3.1.
- 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).
- 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.
- Inter-LAN routing setting exported/backed up from firmware 4.3.2 release might be incorrect, please check inter-LAN routing settings.