# Release Note for Vigor3910 Series

| | |
|---|---|
| Firmware Version: | 3.9.7.1 |
| Release Type: | Normal |
| 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

- Support Area ID 0 for OSPF.
- Support IKEv2 fragmentation.
- Increase IGMP proxy and IGMP snooping table.
- Support using a static virtual IP for IKEv2 VPN.
- Support Specify Remote VPN Gateway by Domain Name.
- Support notifying the VPN up event per VPN remote dial-in User profile.

## Improvement

Connectivity and System stability:

- Corrected: An issue of the WAN failover function.
- Corrected: A display issue of Current System Time.
- Corrected: An issue of probable leakage caused by VPN CGI.
- Corrected: An issue of unexpected reboot caused by IPsec state.
- Corrected: An issue of IKE buffer leakage caused by IPsec Peer ID.
- Corrected: An issue of high CPU usage if the WAN gateway IP not existed.
- Corrected: An issue of system reboot after receiving IKEv2 connection from Google Cloud.
- Corrected: An issue of the LAN host accessing the Internet through the main WAN IP (configured with an Alias IP).

VPN:

- Improved: Improve the SSL VPN stability.
- Improved: Improve the IKEv2 EAP Host to LAN VPN connection stability.
- Improved: When L2TP/IPsec VPN has matched to the VPN LAN to LAN profile with Peer IP, it is not necessary to execute RADIUS authentication.
- Corrected: An issue of VPN mOTP config error.
- Corrected: An issue of route policy bypassing VPN default route.

- Corrected: An issue of IPsec multiple SA VPN unstable (with Juniper vSRX).
- Corrected: An issue of IKEv2 EAP rekey failure when the Limit Connection option was in use.
- Corrected: An issue of sending DNS query to the Vigor router via VPN (OpenVPN, IKEv2 EAP).
- Corrected: An issue of VPN Dial-out type was changed IKEv2 when importing the IKEv2 EAP profile.
- Corrected: An issue of stop passing packets to VPN network after WAN1 dropped (VPN failover via WAN2).
- Corrected: An issue of the IKEv2 EAP connection failed when the VPN profile specified the Remote VPN Peer IP.
- Corrected: An issue of LAN Access to Vigor stopped working when a dial-out IKEv2 VPN with remote network 0.0.0.0./0 was up.
-

Others:

- Improved: Update Country IP Database.
- Improved: Add VPN Source IP and the total connected time information in VPN Mail Alert.
- Corrected: An issue of RADIUS authentication (not enabled) log display.
- Corrected: An issue of OSPF failing to exchange the routing LAN subnets.
- Corrected: An issue of routed client failed to surf Internet well if the default route went to the gateway was BGP peer.
- Corrected: An issue of Brute Force Protection for VPN (IKEv2 EAP/SSL) did not work if using an invalid VPN username.
- Corrected: An issue that the PPPoE client could not access the Internet, if the PPPoE server was set with a VLAN tag.
- Corrected: An issue of a local user (set on System Maintenance>>Administrator Password) login failure after deleting another local user account.
- Corrected: An issue of NAT loopback failure when IP routed subnet was enabled.
- Corrected: An issue of routed IPTV stopped streaming after 10 minutes.

# Known Issue

- Once upgraded to 3.9.2.2, configuring route policy settings and then get downgraded to 3.9.2.1 or older, route policy “to” and “failover” to settings are likely to be wrong. Always backup your config before firmware up(down)grading.

- Once upgraded to 3.9.2.x, configure IP Bind MAC settings and then get downgraded to 3.9.1 again. The IP Bind MAC settings will disappear. So make sure the IP Bind MAC settings is backed up before downgrading.