NO:AP1101-2 V.1

Release Note for Vigor2136 Series

Firmware Version:	5.4.5
Release Type:	Important – Review release notes and upgrade if the changes affect your system stability, performance, or security
Applied Models:	Vigor2136, Vigor2136ax, Vigor2136ax-4G, Vigor2136F, Vigor2136Fax

Vigor2136 Series is a Dual-WAN broadband and Ethernet VPN security router available in wired and Wi-Fi 6 (IEEE 802.11ax) models. It delivers load balancing, automatic failover, secure VPN connectivity, and integrated cybersecurity for reliable, high-speed business networking.

New Features

- Supported MCP Server (Model Context Protocol) with protocols of HTTP/HTTPS.
- Supported to act as an NTP server for LAN clients.
- Supported Multiple L2 Bridge Domains over a single WAN (for Norwegian ISP).
- Supported WAN AutoHunt in DSL / PON modem mode.
- Added WinNuke attack defense to DoS Defense.
- Added an option to disable the local router admin account while the router is managed by VigorACS.
- Added the virtual WAN option for ACS Server On under TR-069.
- Added the exec provision CLI commands, a fixed command interface for ISP provisioning.
- Supported to export only filter based Syslogs.

Improvement

- Improved: Strengthened Linux kernel security to mitigate CVE-2026-98432.
- Corrected: An issue where improper handling of DHCPv6 options and DUIDs could allow attackers to run code without authentication.
- Corrected: Corrected: An issue which the runtime status values (e.g., last login time, IP address) were not saved in configuration backups or the preset ".def" files.
- Improved: Improved WAN SLA in Load Balance / Failover.
- Improved: Moved the WAN Service VLAN option to Advanced Mode (under Configuration>WAN).
- Improved: Supported to activate Bind IP to MAC without restarting the LAN switch.
- Improved: Added Specified LAN protection to DNS Forwarding.
- Improved: Modified the "Please Select..." option for "Assign IP from" in Teleworker VPN profiles, so OpenVPN no longer fails when no LAN is selected.
- Improved: Added error messages to indicate when an IAM user or Teleworker VPN username already exists.
- Improved: Updated the WUI layout and wording on System Maintenance > System Upgrade > Firmware.
- Improved: Added a note clarifying that 802.11r is not applicable in WPA3 security mode and may be incompatible with certain wireless clients.
- Improved: Updated the Dashboard to display LTE bridge information only when bridge mode is enabled.
- Corrected: An issue where an Independent WAN (not a Failover member) is showing as offline on

the Dashboard.

- Corrected: An issue where the CPE Dashboard's LAN Overview displayed Active Clients only for LAN1.
- Corrected: An issue where the router sent the LAN MAC address over the WAN during boot.
- Corrected: An issue where PPPoE failed to reconnect after the credentials were changed, and the DSL LED remained off.
- Corrected: An issue where PPPoE did not reconnect automatically.
- Corrected: An issue where WAN1 was shown as offline when Ping Detect was enabled and the PPP gateway did not respond to ping requests.
- Corrected: An issue where a Virtual WAN did not display an IP address when the ISP provided routes only through DHCP Option 121 without a default gateway.
- Corrected: An issue where the WAN menu could not be opened from the router's WebUI.
- Improved: Support VLAN tag 1 on WAN.
- Corrected: An issue where SNMP did not work on WAN2.
- Corrected: An issue where Dynamic DNS did not update the WAN2 IP address.
- Corrected: An issue where LAN Port Mirroring did not capture ADSL WAN packets.
- Corrected: An issue where VPN / LAN could not be selected as the interface in Route Policy rules that use Country Objects or APP Services.
- Corrected: An issue where VPN routes took priority over LAN routes.
- Corrected: An issue where Bandwidth Limit did not work as expected.
- Corrected: An issue where Port Redirection displayed the WAN IP as "None" when WAN Interface was set to Any.
- Corrected: An issue where the automatic upgrade schedule for the GeoIP database did not work as expected.
- Corrected: An issue where USB user management did not allow uppercase letters in usernames.
- Corrected: An issue where SMS alert messages were formatted inconsistently across different SMS providers.
- Corrected: An issue where a "Login Succeeded" email alert was sent before the user completed MFA verification.
- Corrected: An issue with failure to import a signed CA certificate for a CSR generated on the router.
- Corrected: An issue where the short-lived certificate status was displayed incorrectly under Configuration > Certificates > Local Certificates.
- Corrected: An issue where the WebUI became unreachable when the ACME client was enabled on two Dynamic DNS profiles.
- Corrected: An issue where IP addresses, such as Google DNS, received incorrect reputation scores and were subsequently blocked by IP Reputation Filters.
- Corrected: An issue where IPsec VPN did not work.
- Corrected: An issue where the router rebooted due to “No IKE buffer available”.
- Corrected: An issue where an "On Demand" Site-to-Site VPN tunnel was established only for the primary remote network and not for additional remote subnets.
- Corrected: An issue where VPN connections failed on WAN2.
- Corrected: An issue where an L2TP/IPsec Teleworker VPN user was converted into a Local User without clicking the 2FA link.
- Corrected: An issue where the router crashed after testing VPN / 2FA features.
- Corrected: An issue where two L2TP/IPsec VPN connections from the same public IP address

could not be established simultaneously.

- Corrected: An issue where firewall IP filters were not applied to L2TP/IPsec Teleworker VPN traffic.
- Corrected: An issue where L2TP/IPsec Teleworker VPN clients did not receive DNS server addresses from the LAN.
- Corrected: An issue where EasyVPN (WireGuard) clients did not receive the DNS server address from the router.
- Corrected: An issue where the source IP address was changed to the router's LAN IP address when an OpenVPN client accessed a LAN PC.
- Corrected: An issue where the L2TP option became unchecked and disabled in VPN > General Setup > Access Control.
- Corrected: An issue where VPN LAN-to-LAN and Teleworker profiles could not be imported from a Vigor2927 .cfg file when the profile name, username, or password contained spaces or unsupported characters.
- Corrected: An issue where disconnected devices continued to appear in the ARP Table.
- Corrected: An issue where the Sessions page displayed "Peak Sessions" data for a port configured as LAN.
- Corrected: An issue where SMB file sharing services (ports 137/138/139/445) were missing from the Running Services list.
- Corrected: An issue where Syslog reported WAN information for WAN1 only.
- Corrected: An issue where Ping in Network Tools failed when a "Ping from" interface was selected.
- Corrected: An issue where Packet Capture failed to capture WAN2 PPPoE packets.
- Corrected: An issue where the TR-069 service stopped running.
- Corrected: An issue where the CPE configured an incorrect Connection Request URL when STUN was set to Auto or Disabled.
- Corrected: An issue where TR-069 Auto STUN did not work with CGNAT addresses.
- Corrected: An issue where the PCB serial number was not displayed in VigorACS.
- Corrected: An issue where TR-369 DSL_Status reported "DSL" instead of the actual DSL mode.
- Corrected: An issue where the IPv4 / IPv6 WAN access management options were missing after a firmware upgrade.
- Corrected: An issue where the MyVigor serial number was not displayed on the Registration page when the PCB serial number was 000000000000.
- Corrected: An issue where the CPE crashed intermittently.
- Corrected: An issue where the router took an excessively long time to boot.
- Corrected: An issue where the "[DrayOS5 CGI] Error: 2021: Couldn't find the input column in config file" error occurred in System Maintenance>Account & Permission>Role & Permission.
- Corrected: An issue where Wi-Fi clients connected to the same SSID on different bands were isolated from each other.
- Corrected: An issue where traffic was blocked between a wireless SSID and an untagged VLAN port within the same VLAN.
- Corrected: An issue where the port status of managed switches was displayed incorrectly under Virtual Controller > Switch > Device > Port Profile.
- Corrected: An issue where the LTE WAN connection on LTE models dropped intermittently.
- Corrected: An issue where LTE WAN bridging did not work on LTE models.
- Corrected: An issue where LTE PPP mode did not function as expected.

Note

- To prevent potential errors after the firmware upgrade, if you are currently using version 5.3.0 or 5.3.1.1, please upgrade to 5.3.2.1 first before proceeding to later versions.
- Please ensure that you use the ".rst" firmware file when recovering the router. Note that uploading the ".rst" file will reset the router to factory default settings.
  For certain models, a separate ".rst" (reset) firmware file may not be provided. If the ".rst" version is not available, please manually rename the file extension of the ".all" or ".sfw" firmware file to ".rst" to create an equivalent RST firmware file.
  Example:
  Rename Vigorxxxx_1.2.3.4.sfw → Vigorxxxx_1.2.3.4.rst
  Please ensure you back up your configuration before applying a ".rst" firmware, as all settings will be erased during the process.
- The Vigor router system now offers automatic firmware upgrade feature (optionally, default is disabled), making it convenient for users to stay updated on crucial firmware changes, security issues, and significant bugs that necessitate immediate firmware update. With this feature, there is no need to download the latest firmware version yourself. The Vigor system will automatically detect the latest release, download it, and upgrade the router. This option is particularly beneficial for addressing critical security issues and fixing major bugs.

Known Issue

- None.