NO:AP1101-2 V.1

Release Note for Vigor2136 Series

Firmware Version:	5.3.5
Release Type:	Critical - Upgrade immediately to address urgent security issues or major system risks
Applied Models:	Vigor2136 / Vigor2136ax

Vigor2136 features advanced bandwidth control mechanism such as IP-layer, QoS, NAT Session Limitation, Bandwidth Borrowed, etc., to allow easy, flexible, reliable access control and bandwidth management.

New Features

- Support IKEv2 cookies for preventing DoS attack.
- Add a new CLI command to adjust the NAT service priority.
- Add a new tab of Notification under Monitoring>>Log Center.
- Add IGMP Accept List in Configuration>>IGMP>>General Setup.
- Support SafeSearch feature for Google/ YouTube under Configuration>>DNS.
- Add "Client Config Generator" for WireGuard VPN protocol in VPN>>Teleworker VPN.
- Add the "More Subnets" setting under More Remote Subnets in VPN>>Site-to-Site VPN.
- Add new fields of Status and Last Update Time in Configuration>>WAN>>Dynamic DNS.
- Add a new link to configure Let's Encrypt Certificate in Configuration>>Certificate>>Local Certificate.
- Add the option related to DSCP/802.1p QoS in Configuration>>Bandwidth Management>>Traffic Shaping Policy.
- Allow the users to select an External RADIUS Server Profile in Configuration>>LAN>>LAN Port 802.1x.
- Provide certificate-related parameters to VigorACS for effective management.
- Support special characters (e.g., ' = + ,) for admin password.
- Support for IPv6 for the DrayDDNS service in Configuration>>WAN>>Dynamic DDNS.
- Support for specifying a customized IPv6 DNS server for a WAN interface in Configuration>>WAN>>WAN Connections.
- The active IPv6 LAN DNS can be displayed on the main LAN Status Dashboard.
- The Subject Alternative Name (SAN) of the certificate can be viewed by clicking 'View' in Configuration >> Certificate >> Local Certificate.

Improvement

- Improved: Improve the WiFi Driver Security (CVE-2025-20710, CVE-2025-20711, CVE-2025-20715, CVE-2025-20716, CVE-2025-20720, CVE-2025-20724, CVE-2025-20729, CVE-2025-20731, CVE-2025-20732, CVE-2025-20733, CVE-2025-20734, CVE-2025-20735, CVE-2025-207337, CVE-2025-20738, and CVE-2025-20739).
- Improved: Set the default DHCPv6 WAN IAID to 0.
- Improved: Optimize the VPN Protection Rules window layout.
- Improved: Add Auto APN data profile for the French ISP Orange.
- Improved: Support Phase2 network ID option for DoS protection for VPN.
- Improved: Expand the Hostname text input field in Utility>>Network Tools.
- Improved: Support unlimited quota in Configuration>>Notification Services.
- Improved: Support for special characters (e.g., ' = + ,) used in the PPPoE password.
- Improved: Modify "OSPFv2" / "RIP" wording in Configuration>>OSPF>>General Setup.
- Improved: Add an option that allows users to enable or disable the SMS Quota feature.

- Improved: Expand the DHCPv6 Server "Start Address" and "End Address" text input fields.
- Improved: Add "Hostname" to be specified as the Source IP for NAT rules (in Configuration>>NAT).
- Improved: Hide the message of "dhcp6_send_web_syslog" in the Content field in Monitoring>>Log Center.
- Improved: Add "Seconds" legend for the Key Renewal Interval field in Configuration>>Wireless LAN>>SSID.
- Improved: Add a search tool box (for security reports) in Security>>Security Defense Status>>IP Reputation.
- Improved: Add new links of Auto General Update and Auto Critical Update in the System section on the Dashboard.
- Improved: Enhance the device notes displayed in the Add New Switch window in Virtual Controller >> Switch >> Device.
- Improved: Improve the Teleworker VPN (IKEv2 EAP) connections when a user inputs the wrong username/password.
- Improved: Modify and provide more detailed information for the error message related to configuration restoration.
- Improved: Modify the name of the button from "Download zip file" to "Download file" in the OpenVPN Config Generator window.
- Improved: Adding a checking mechanism to detect whether the LTE module is in the correct mode and switch it to QMI mode if necessary.
- Corrected: An issue with WAN IPv6 DHCPv6 Client.
- Corrected: An issue with incorrect IGMP behaviour.
- Corrected: A typo issue in the IP Reputation log message.
- Corrected: An issue with the failure to set the hostname in LAN DNS.
- Corrected: An issue with unabling to send SMS with a specific SIM card.
- Corrected: An issue with the failure to establish IPsec VPN with Zyxel router.
- Corrected: An issue with the failure of connecting to the selected time server.
- Corrected: An issue with the failure of working with QLD310 with the DHCP mode.
- Corrected: An issue with the failure to change the username of a Teleworker VPN profile.
- Corrected: An issue with the failure of the DDNS Client update when "used in the password.
- Corrected: An issue that the Ethernet WAN would disconnect if Ethernet Port 1 was disabled.
- Corrected: An issue with the failure to establish IKEv2 VPN (NAT mode) with the Juniper router.
- Corrected: An issue with the failure to show the correct DDNS Log in Monitoring>>Log Center.
- Corrected: An issue that the Fiber WAN for the fiber model was shown incorrectly with Ethernet WAN.
- Corrected: An issue with the failure of checking/updating the router firmware when using the IP alias.
- Corrected: An issue that "Clear Session when Schedule is On" in Security>>Firewall Filters>>IP Filters didn't work.
- Corrected: An issue with failure to apply the bandwidth limit to the WLAN clients via the Hotspot Web Portal.
- Corrected: An issue with the RX Bytes count for the LAN port was incorrect when the TX traffic exceeded 1TB.
- Corrected: An issue that the router didn't send out the correct Local ID when dialing out the IKEv2 VPN with NAT mode.
- Corrected: An issue that a VPN interface would remain on the failover WAN even after the primary WAN came back online.
- Corrected: An issue with the failure of displaying Category information for a Site in Security>>URL/IP Lookup>>History.
- Corrected: An issue with missing "Cellular WAN Bridge mode" and "Cellular WAN SMS" information in Monitoring>>Cellular WAN Status.
- Corrected: An issue with the failure of applying a certificate signed by a Root CA in Configuration>>Certificates>>Local Services.

- Corrected: An issue of sending User Access Log to Syslog even the "User Access Log" was disabled in System Maintenance>>Device Settings>>Syslog.
- Corrected: An issue with the failure to save the specific SMTP Sender address when the TLD was more than four characters.

Note

- 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.