

Release Note for Vigor2136 Series

Firmware Version:	5.3.3
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

- Comply with EN 18031 cybersecurity requirements.
- Support an option to enable/disable the IKEv1 setting in VPN>>General Setup>>IPsec.
- Support Hotspot Web Portal bandwidth control for specific destination IPs and domains.

Improvement

- Improved: Improve the WiFi Driver Security (CVE-2025-20674).
- Corrected: An issue of display error for the IPv6 PPP online status.
- Corrected: An issue with the failure of firmware upgrade via WUI.
- Corrected: An issue with the failure to load the hotspot authentication page.
- Corrected: An issue with the failure to apply the route policy correctly to Teleworker VPNs.
- Corrected: An issue that VigorACS was unable to manage the router due to the TR-069 service.
- Corrected: An issue with the failure to establish a WAN connection after rebooting the router with VoIP enabled.
- Corrected: An issue that an IP address locked by SSH brute force protection could not be unblocked from the WUI.
- Corrected: An issue that the firmware update initiated from VigorACS failed when the device used an LTE WAN connection.
- Corrected: An issue that a route policy using the virtual WAN setting would fail if the static IP of the virtual WAN was changed.
- Corrected: An issue with configuration backup failed if the "Device Name" contained special characters, such as spaces or brackets.
- Corrected: An issue that an error message 'The "CPE_URL" field value is empty' appeared when configuring TR-069 settings via Telnet/CLI.

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 Vigorxxx_1.2.3.4.sfw → Vigorxxx_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.