Firmware for OnCell G4308-LTE4 Series Release Notes

Version: v3.18.0	Build: 25062612
Release Date: Aug 07, 2025	

Applicable Products

OnCell G4308-LTE4 Series

Supported Operating Systems

N/A

New Features

• Added Traceroute CLI command.
• Introduced multi-language support for MX-ROS, including Traditional/Simplified Chinese, Korean, and Japanese.
• Added GRE interface on Network Interface.
• Added OSPF support to Routing.
• Added serial interface support for integration with ITS SCATS systems.
• Added support for MRC Quick Link Ultra v4.1.0.
• Added support for displaying the cellular carrier in MRC Quick Link Ultra.
• Added support for MRC-related logs in the system log.

Enhancements

• Added support for “Route Mode” in IPsec Startup Mode. In Route Mode, the VPN tunnel initiates only when routing packets are generated, relying on traffic to trigger the tunnel.
• Added support for CLI commands to configure MXsecurity port settings.
• The "Ping Response" function has been moved from the "User Interface" (MX-ROS v3.12.1 to v3.13) and "Trusted Access" (MX-ROS v3.6) pages to the dedicated "Ping Response" page.
• Added IP display on the Querier Connected Port in the IGMP Snooping Group Table.
• Added Passive Mode to OSPF.
• Added Object types: Secure FTP and SYSLOG (TCP 514) to Object Management.
• Added trap and syslog support for IPS/DPI/ADP to Advanced Protection - Configuration.
• Optimized IPsec reconnection time.
• Reduced the data usage of the MRC service when monitoring the status of devices.
• Optimized RGMII interface reliability by increasing the default Rx Delay parameter, reducing intermittent web access issues.

Bugs Fixed

• When exporting the configuration, the Object IP Range setting is saved incorrectly, causing importing the configuration to fail.
• MXview 1.4.1 does not receive encrypted SNMPv3 Trap/Inform packets from the routers.
• ARP Reply packets are being unintentionally dropped in Bridge mode.
• Email Settings cannot be disabled.
• After changing the Management VLAN, the router is unreachable when pinged.
• When configuring Bridge members, the system unintentionally creates two untagged VLANs under the access port.
• Multicast traffic is not filtered correctly, causing forwarding to ports that have not joined the IGMP group.
• IPsec Startup Mode - Initiate Automatically does not function properly.
• CVE-2024-9138, CVE-2024-9140 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-241155.
• CVE-2025-0415 vulnerability issue(s). For more details, search the Security Advisories section on

the Moxa website for the following Security Advisory ID: MPSA-259491.
• CVE-2025-0676 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-251431.

Changes

• Supervisor and user accounts are no longer created by default, and must be added manually. Existing accounts are not affected.
• In compliance with the EU Radio Equipment Directive (RED), users must change the password on first login.

Notes

• Due to an issue, using an identical pre-shared key to set up multiple site-to-any IPsec VPN tunnels with IKEv1 mode requires a workaround. Please contact Moxa Technical Support for assistance.
• Using an MRC Gateway key with a different gateway model may cause connection issues with the MRC service.