MGOS 4.1.2 Release Notes

MGOS 4.1.2 is for MG90 Series routers.

Note: This release supersedes MGOS 4.1.1. Sierra Wireless recommends that customers who have MGOS 4.1.1 installed upgrade to MGOS 4.1.2 at their earliest convenience.

New Features

Radio Modules

Updated radio module firmware:

- MC7430—02.24.05.06 (Telstra)
- MC7455—02.24.05.06 (Verizon)

Addressed Issues

Advanced Routing Rules

Resolved issue where the postLinkState script (General > Advanced Routing Rules) would fail to insert a route on MC7354/MC7355 variants when the device boots.

LEDs

- Resolved issue with MC7354 variants where the signal strength LED would always indicate poor signal strength (red). LED now indicates correct signal strength.
- Resolved issue where LEDs would not ‘chase’ (blink in sequence) during a firmware update. LEDs will now display a blue chase while a firmware update is in progress.

Important: *Do not turn off the power while the update is in progress.*

AMM

- Resolved issue where MG90 would report incorrect boot time to AMM.
- Resolved MG90 event reporting issue that caused some AMM reports (e.g. Link Utilization) to be incorrect.

Logging

Eliminated unnecessary logging to prevent premature media wear.

12 Lead Transmission Devices

Resolved issue where Physio Control LIFEPAK device would not synchronize time with the LIFENET server.

VPN

Resolved VPN reconnection issue when the MG90 has multiple WAN connections that have different VPN configurations.

Resolved Security Issues

Bluetooth

Bluetooth is now disabled by default; password will be user-specified when Bluetooth is enabled. (This does not affect the MG90's current configuration; the new default configuration takes effect if a factory reset is performed.)

Wi-Fi Radio

Upgraded Wi-Fi radio firmware to address Krack vulnerability.

Common Vulnerabilities and Exposures (CVE)®

Addressed potential Bluetooth vulnerabilities ("BlueBorne") related to:

- CVE-2017-1000250
- CVE-2017-1000251

Addressed potential Wi-Fi vulnerabilities ("KRACK") in the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) standard related to:

- CVE-2017-13077
- CVE-2017-13078
- CVE-2017-13079
- CVE-2017-13080
- CVE-2017-13081
- CVE-2017-13082
- CVE-2017-13084
- CVE-2017-13086
- CVE-2017-13087
- CVE-2017-13088

Vulnerability Impact: Affected when Wi-Fi is operating in client mode.

Sierra Wireless Contact Information

Sales information and technical support, including warranty and returns:

Web: sierrawireless.com/company/contact-us/

Global toll-free number: 1-877-687-7795

Corporate and product information: sierrawireless.com