

MGOS 4.3 Release Notes

MGOS 4.3 is for MG90 Series routers.

Important: Customers using FIPS mode must upgrade to MGOS 4.3 to stay current with security bug fixes.

Upgrade Requirements

MGOS 4.3 can be installed:

- Directly via USB stick, or
- As an over-the-air upgrade subject to the requirements below

AMM Over-The-Air Upgrade Requirements

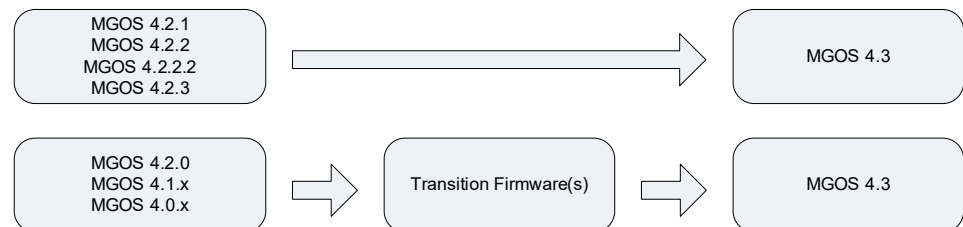
- OTA upgrades must be performed by AMM 2.16 or newer

Important: Upgrading using older AMM versions will result in MGOS firmware upgrade failures, and can require a USB-stick install to recover. For more information, refer to [Product Bulletin: AMM 2.16 Prerequisite to MG90 firmware upgrade](#).

The following requirement must be met if using AMM to upgrade the MG90 OTA:

- Upgrade path—A minimum version of MGOS 4.2.1 is required to upgrade directly to this release. For MG90s installed with MGOS 4.2.0 (or earlier), transition releases are required before upgrading to this release. The required transition releases depend on the MG90's currently installed firmware.

To identify the transition firmware required, refer to [Product Bulletin: Upgrading to MGOS 4.2 or Later—Updated 26 Nov 2018](#).



Important: “Transition Firmware(s)” (MGOS 4.1.2.2 and MGOS 4.2.0.2) are only intended as stepping-stone firmware in the upgrade path to MGOS 4.3 and are not intended for long-term use. Failure to install the required transition firmware prior to upgrading to MGOS 4.3 via the AMM will result in an upgrade failure, and can require a USB-stick install to recover.

New Features/Updated Functionality

GNSS

Turn-based GNSS information forwarding and reporting thresholds added to allow reporting during vehicle turns where speed and distance thresholds are not met.

Added support for reporting altitude information provided by GNSS.

LAN

Serial LAN interface added to provide WAN link access for Sierra Wireless GenX-series devices operating in passthrough mode.

Certificates

Certificate management process enhanced to support AMM certificate distribution.

Important: *Certificate management supports signed certificates containing only specific X.509 standard fields (Distinguished Name and Subject Alternative Name). Existing certificates with unsupported fields are converted for MGOS 4.3 and continue to be operational, however the converted data may not render cleanly in the LCI.*

Customers are encouraged to use the new certificate create method going forward since it uses only the supported attributes.

For details of the enhanced process, refer to the AirLink MG90 Software Configuration Guide (Doc #4118700, rev 7) section 11 Certificate Configuration.

VPN

WAN link VPN support extended to allow either multi-VPN tunnels, or single VPN tunnels with failover to alternate VPNs.

WAN Networking Rules

New policy-based 'Routing Rules' networking rule type added. This rule allows specific traffic to be routed separately from the active WAN interface's standard routing.

Automatic Software Update Configuration (Firmware Upgrades)

Firmware upgrade options expanded to manage upgrades at the MG90 and module level, and allow end-user selection of repository-managed and user-managed firmware images.

FIPS

AES128CCM16 and AES256CCM16 encryptions are no longer supported in FIPS mode.

NTP Servers

NTP server configuration options added to Device Service Configuration.

Status Broadcast

Added option to generate status broadcasts based on WAN state changes.

Added firmware version to broadcast data.

Factory Reset

Added two factory reset options—reset all, and reset configuration and preserve core credentials.

Radio Modules

Updated module firmware:

- EM7511—01.08.04.00 (Generic)
- EM7565—01.08.04.00 (Generic), 01.11.00.00 (Telstra)
- MC7354—05.05.58.05 (Verizon)
- MC7430—02.30.03.00 (DoCoMo/Telstra/Generic)
- MC7455—02.30.01.01 (Sprint/Verizon), 02.33.03.01 (Generic)

Addressed Issues

GPS

GPS jitter reduced when vehicle is stationary.

Resolved issue where TAIP messages were not forwarded at the interval specified in the Remote Forwarding Server List.

Resolved issue where MG90 would lose GPS fix and require a reboot before signal could be reacquired.

Resolved issue where location data was occasionally not being reported until reboot.

Resolved issue where GPS source was incorrectly identified as “obd” in the LCI.

Resolved issue where enabling built-in GPS and Dead Reckoning at the same time would not enable Dead Reckoning.

Corrected date field in NMEA RMC sentence for dead reckoning.

Software Upgrade

Resolved USB upgrade installation issue that could cause upgrade to fail due to space limitations.

Improved efficiency and reliability of OTA upgrade.

Resolved issue where a radio module firmware downgrade could leave the MG90 in low power mode.

Resolved issue that could cause USB stick upgrade or over-the-air upgrade to stall and retry.

Resolved issue where management tunnel instability could lead to an over-the-air upgrade download failure or a management system sync-up delay or failure.

WAN Link Status

Resolved issue where WAN Link Status page would display without link information.

Captive Portal

Resolved issue where web portal would not work with customized web content after software upgrade.

WAN Link

Resolved issue where, following AMM upgrade where the AMM IP address changed, the management tunnel would not reconnect to AMM after a ping monitor failure.

Removed unused "Network Carrier" field from Cellular WAN Link Configuration screen.

Resolved issue causing instability in cellular link connections.

Resolved issue affecting always-on routers where an out-of-memory error could result in loss of connectivity.

Resolved issue where an unrecognized SIM ID would not result in a switch to the Generic radio module image.

Resolved intermittent issue that prevented cellular interface from obtaining an IP address and passing traffic.

Advanced Routing Rules

Resolved issue with Advanced Routing Rule scripts, which required absolute paths to be used when invoking certain system utilities.

VPNs

Resolved intermittent issue that could cause VPN connections to be brought up and down on a cell link.

Resolved timing-related issue that could cause Host-to-LAN VPN to sometimes not pass traffic.

Resolved issue where Host-to-LAN VPN without MOBIKE would stop passing traffic after extensive WAN link switching.

Access Points

Access Point Configuration screen "Encryption" field now defaults to WPA2/CCMP when the "Enabled" field is selected.

AMM

Resolved issue that could leave the MG90 configuration unsynchronized with AMM.

Resolved issue where the MG90 would not report LAN client absences to AMM.

Resolved issue that could cause AMM link utilization-related reports to display events out of sequence.

Resolved issue that could cause AMM to incorrectly report status of the MG90's VPNs.

Resolved issue where router was not properly notifying AMM of radio module firmware switch.

Resolved issue that could cause location updates to stop when dead reckoning calibration was lost.

Added reporting of dead reckoning configuration status to AMM.

Resolved issue that could cause AMM to incorrectly report the status of VPNs on the router.

Wi-Fi

Improved Wi-Fi connectivity reliability and increased maximum number of connected clients.

Resolved issue with deleting private zones.

GPIOs

Improved GPIO management to reduce impact on CPU resources.

Logging

Resolved issue where the Wi-Fi access point report would temporarily be full.

Added system log to indicate over-the-air download condition not met.

Resolved issue where radio module inventory information was not reporting to AMM.

Status Broadcast

Resolved issue where WAN signal strength was missing from gateway state broadcast output.

Corrected state broadcast VPN status format.

Security Updates

Security

Tightened access to system log files.

Added additional controls to limit remote access operations.

User account is no longer available by default and must be specifically created in order to be enabled

Updated internal web server to address security issues.

FIPS

Resolved issue where ESP traffic was not using the correct crypto module for encryption.

Diagnostic/Service Tools (General > Tools)

Increased controls for diagnostic and device management commands.

Common Vulnerabilities and Exposures (CVE)[®]

Addressed following CVEs:

- CVE-2015-1395
- CVE-2015-6837
- CVE-2016-3627
- CVE-2016-4614
- CVE-2016-5131
- CVE-2016-8615
- CVE-2016-8620
- CVE-2016-9318
- CVE-2016-9594
- CVE-2017-5932
- CVE-2017-9023
- CVE-2017-16932
- CVE-2018-6952
- CVE-2018-14526
- CVE-2019-13986
- CVE-2015-5224
- CVE-2015-6838
- CVE-2016-4447
- CVE-2016-4615
- CVE-2016-6252
- CVE-2016-8617
- CVE-2016-8623
- CVE-2016-9401
- CVE-2016-9952
- CVE-2017-7376
- CVE-2017-11185
- CVE-2018-0732
- CVE-2018-7738
- CVE-2018-1000121
- CVE-2019-13988
- CVE-2015-5312
- CVE-2015-8710
- CVE-2016-4449
- CVE-2016-4616
- CVE-2016-6318
- CVE-2016-8619
- CVE-2016-8625
- CVE-2016-9586
- CVE-2017-5130
- CVE-2017-9022
- CVE-2017-12424
- CVE-2018-6951
- CVE-2018-14404
- CVE-2018-1000301

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