MGOS 4.3.1.2 Release Notes

MGOS 4.3.1.2 is a general release for MG90 LTE-A and MG90 LTE-A Pro routers.

Customers are recommended to upgrade to this latest release to take advantage of new features, security updates, and addressed field-reported issues.

Important:

- *LCI local access is restricted to HTTPS only, on routers manufactured on MGOS 4.3.1 or later, or on routers that are reset to factory default on MGOS 4.3.1 or later. The LCI should then be accessed using https://172.22.0.1/MG-LCI/*
- *New routers are provisioned with random factory default passwords printed on the MG90 device label. The default "admin" password will not work for these routers.*
- *SSH access on LAN segments is now disabled by default.*

For details, see New Features/Updated Functionality on page 3.

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

Upgrade Methods

MGOS 4.3.1.2 can be installed using either of the following methods:

- USB stick—Upgrade directly from MGOS 4.2.2 or newer to MGOS 4.3.1.2.
- Over-the-air—Upgrade via AMM subject to the requirements below.

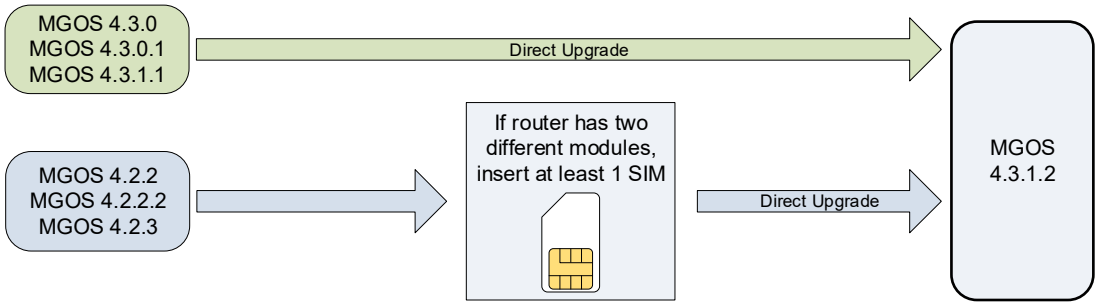
Note: To upgrade from older MGOS versions (i.e. MGOS 4.2.1 or earlier), upgrade first to MGOS 4.3.0.1 and then upgrade to MGOS 4.3.1.2. (Refer to the MGOS 4.3.0.1 Release Notes at https://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/mg-release-notes/.)

AMM Over-The-Air Upgrade Requirements

- AMM 2.16 or newer is required to upgrade over-the-air to MGOS 4.3.1.2.

  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.*

- Upgrade paths—The following upgrade paths to MGOS 4.3.1.2 are supported:



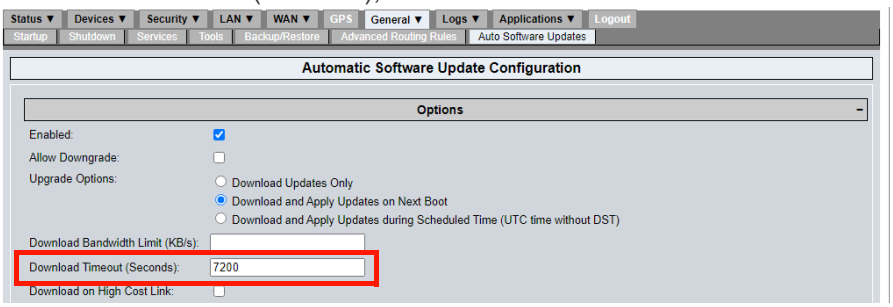
Note: MGOS 4.3.1.2 supercedes MGOS 4.3.1/MGOS 4.3.1.1.

- *Routers with MGOS 4.3.1 installed must upgrade directly to MGOS 4.3.1.2.*
- *Routers with MGOS 4.3.1.1 installed should upgrade directly to MGOS 4.3.1.2 to avoid any potential radio module firmware switching issues when changing carriers.*

- If upgrading from MGOS 4.2.2/4.2.2.2/4.2.3 and the MG90 contains two different Sierra Wireless modules (e.g. MC7354+MC7455, MC7455+EM7511, etc.), a SIM must be inserted for at least one module prior to performing the upgrade. For more information, refer to the AirLink MG90 Software Configuration Guide topic “Installing Software Updates”.
- **Upgrade recommendation—**Before using AMM to upgrade to MGOS 4.3.1.2, Sierra Wireless recommends setting the download timeout value to 7200 s, to ensure the download completes in one attempt. (Otherwise, if the download times out, it will resume at the next opportunity—for example, when the active link changes, the next scheduled update window, when the device reboots, etc.)

  a. In MGOS, go to General > Auto Software Updates.

  b. In Download Timeout (Seconds), enter 7200.



  c. Click Submit.

New Features/Updated Functionality

LCI Secure Access (HTTPS)

HTTPS support for LCI access:

- Added Security Settings option to select supported protocols for LCI access (HTTP+HTTPS, or HTTPS only).
  (i.e. https://172.22.0.1/MG-LCI/ is now supported. http://172.22.0.1/MG-LCI/ can be used only if HTTP+HTTPS is enabled.)
- HTTPS only is enabled by default for new installs
- HTTPS only is enabled on factory reset.
- HTTP+HTTPS is enabled by default when upgrading from an earlier MGOS version. (i.e. HTTP can continue to be used until option is changed or factory reset is performed.)

Note: Any time the protocol is switched from HTTPS only to HTTP+HTTPS, clear the browser cache to allow access via HTTP (i.e. to access http://172.22.0.1/MG-LCI/).

The Advanced Configuration Login (which appeared when accessing some LCI tabs, such as General > Auto Software Updates) has been removed.

Security

Random Factory Default Password—MG90 routers manufactured from February 2021 onward feature a random factory default password to access the LCI that is printed on the bottom label of the router. A separate label is also provided with each new MG90—this label is intended to be applied on a surface near the MG90 for convenient access to important information, including the factory password.

Note: If the router label does not include a password, use "admin" as the password.

Password Complexity (Root and User)—LCI password complexity rules are now applied when adding new users or changing existing passwords.

Password requirements:

- Length: Minimum 8 characters (printable characters only)
- Must include at least one uppercase (’A’–’Z’), one lowercase (’a’–’z’), and one numeric (’0’–’9’)

User Login Name—Login names must be POSIX-compliant

- Length: 2–28 characters
- Supported characters: ’A’–’Z’, ’a’–’z’, ’0’–’9’), period (’.’), underscore (’_’), hyphen (’-’).

Important: *If passwords and login names are to be pushed from AMM to the router, make sure to follow these requirements when setting them up in AMM. If invalid passwords or login names are pushed to the router, the users will not be able to log in to the LCI.*

SSH access on LAN segments (Ethernet and Wi-Fi) is now disabled by default, and can be enabled/disabled from LAN Segment Configuration.

CBRS (Citizens Band Radio Service)

Introduced Cellular WAN Link functionality to configure EM75xx radio modules for use on private CBRS networks.

Note: MG90 LTE-A Pro routers manufactured from February 2021 onward support CBRS.

WAN Link Configuration (Cellular)

Added Custom Band Setting Mode to allow or prevent operation on specific bands (Restrict to Bands, or Exclude Bands).

Status (WAN Links Extended Status)

Updated Cellular Link information to include carrier aggregation data for supporting devices (e.g. EM75xx)

Broadcast (Gateway State Beacon)

Expanded Broadcast Data WAN States option to include additional cellular module data (network type, band number, bandwidth, RSSI, RSRP, RSRQ, SINR).

Radio Module Firmware

SIM-based Switching—Automatic image switching to Bell firmware for EM7511 when a Bell SIM is inserted is now supported.

Automatic Software Update Configuration—Enhanced the process to upload custom radio module firmware.

New radio module firmware for:

- EM7511 (AT&T, Sprint, Bell)—Includes support for B14 carrier aggregation (CA) where applicable
  (Note—New Bell firmware can be downloaded from AMM and manually installed.)
- EM7565 (Generic)
- MC7430 (Generic)
- MC7455 (AT&T, Sprint, Generic)

(Deprecated) Roadside Safety Application

Important notice: Road Safety, the application that forwards data for the ZOLL RS3000 (formally RescueNet) is no longer supported. Please contact your ZOLL sales representative for an up-to-date solution.

Addressed Issues

Firmware update / Network connectivity

Resolved an issue that may cause the device to be unable to connect back onto a specific carrier network.

Wi-Fi

Resolved an issue that caused roaming squelch to occasionally improperly invalidate APs seen during background scanning.

Resolved an issue that caused traffic interruptions on Wi-Fi WAN.

VPN

Resolved issues that could cause an IPsec VPN to disconnect and not automatically reconnect.

WAN

Resolved an issue that could prevent cellular connection from being established on boot up.

Resolved an issue in MGOS 4.3.0.1 (FIPS only) that prevented port forwarding on Host-to-LAN VIPs.

Resolved an issue where Ethernet would not be available on power up.

AMM

Resolved issue where AMM would incorrectly show ConfigState as "Out of sync".

GNSS

Resolved an issue that, in certain cases, caused infrequent loss of GPS/GNSS fix.

Resolved an issue that caused GNSS to stop reporting after device was upgraded from MGOS 4.0.x/4.1.x to MGOS 4.3.1 using the USB stick method.

Telemetry Status

Resolved an issue that intermittently displayed erroneous speed information.

Security Enhancements

Common Vulnerabilities and Exposures (CVE)®

Addressed the following CVEs:

- CVE-2009-1190
- CVE-2010-1622
- CVE-2011-2730
- CVE-2011-2894
- CVE-2012-1833
- CVE-2013-4152
- CVE-2013-6429
- CVE-2013-6430
- CVE-2013-7315
- CVE-2014-0054
- CVE-2014-0225
- CVE-2014-1904
- CVE-2014-3578
- CVE-2014-3625
- CVE-2015-0201
- CVE-2015-3192
- CVE-2015-3310
- CVE-2015-5211
- CVE-2016-3189
- CVE-2016-5007
- CVE-2016-7798
- CVE-2016-9878
- CVE-2016-1000027
- CVE-2017-3136
- CVE-2017-3145
- 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
- CVE-2017-16808
- CVE-2018-0732
- CVE-2018-0734
- CVE-2018-1199
- CVE-2018-1257
- CVE-2018-1258
- CVE-2018-1270
- CVE-2018-1271
- CVE-2018-1272
- CVE-2018-1275
- CVE-2018-5407
- CVE-2018-5741
- CVE-2018-10103
- CVE-2018-10105
- CVE-2018-11039
- CVE-2018-11040
- CVE-2018-14461
- CVE-2018-14462
- CVE-2018-14463
- CVE-2018-14464
- CVE-2018-14465
- CVE-2018-14466
- CVE-2018-14467
- CVE-2018-14468
- CVE-2018-14469
- CVE-2018-14470
- CVE-2018-14879
- CVE-2018-14880
- CVE-2018-14881
- CVE-2018-14882
- CVE-2018-15756
- CVE-2018-16227
- CVE-2018-16228
- CVE-2018-16229
- CVE-2018-16230
- CVE-2018-16300
- CVE-2018-16301
- CVE-2018-16451
- CVE-2018-16452
- CVE-2018-19325
- CVE-2018-19519
- CVE-2019-1547
- CVE-2019-1551
- CVE-2019-1552
- CVE-2019-1559
- CVE-2019-1563
- CVE-2019-5061
- CVE-2019-5062
- CVE-2019-8936
- CVE-2019-9494
- CVE-2019-9495
- CVE-2019-9496
- CVE-2019-9497
- CVE-2019-9498
- CVE-2019-9499
- CVE-2019-11555
- CVE-2019-12900
- CVE-2019-13377
- CVE-2019-15166
- CVE-2019-16275
- CVE-2019-1010220
- CVE-2020-1968
- CVE-2020-8597

NOTICE—Upcoming TLS Support Changes

Be advised that MGOS 4.3.1.2 is the final release to support the following TLS versions/features:

Version/Feature	Change	Customer Requirements
TLS 1.0/1.1	Not supported after MGOS 4.3.1.2	Customers must use up-to-date browsers that do not use the unsupported features.
TLS1.2	Following cipher suites not supported after MGOS 4.3.1.2 • TLS_DH_anon_WITH_3DES_EDE_CBC_SHA • TLS_DH_anon_WITH_AES_128_CBC_SHA • TLS_DH_anon_WITH_AES_128_CBC_SHA256 • TLS_DH_anon_WITH_AES_256_CBC_SHA • TLS_DH_anon_WITH_AES_256_CBC_SHA256 • TLS_DH_anon_WITH_RC4_128_MD5	
3DES cipher suites	Not supported after MGOS 4.3.1.2	Non-FIPS customers must check/modify VPN configurations to ensure 3DES cipher suites are not used.

Known Issues

LCI—Applications Tab

A significant delay (up to 20 seconds) may occur when moving between an application's configuration tab (e.g. Telemetry) and the corresponding status tab (e.g. Telemetry Status).

AMM—OTA Upgrade from MGOS 4.3.0/4.3.0.1 to MGOS 4.3.1.2

If user accounts have been deleted from an MG90 while running MGOS 4.3.0/4.3.0.1/4.3.1.1, OTA upgrade from MGOS 4.3.0/4.3.0.1/4.3.1.1 to MGOS 4.3.1.2 may result in AMM incorrectly showing the State (in Configuration > Deployment > Configuration Control) as "Error (configuration has been reset)".

To clear this error, select the affected device(s) and click Revert, then wait for the State to return to "In Sync".

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