oMG 3.15 Release Notes

oMG 3.15 is for oMG2000 and oMG500 gateways.

Upgrade Note

When upgrading to oMG 3.15, the application package (oMG-Application-9.48804.v3.sdk4-20171116.1) must be installed twice on the oMG, as per the instructions below.

Note: Applicable to customers using AMM versions AMM 2.16 and prior, and upgrading to oMG 3.15 from oMG 3.14.5 or oMG 3.14.6.
This issue will be resolved in AMM 2.16.1.

Please install oMG 3.15 as follows:

1. From AMM Admin/Software Distribution, choose Upgrade Gateway Software and follow the instructions to select:

   oMG-Core-Software-3.15.0-20180206.2
   and
   oMG-Application-9.4.8804v3.sdk4-20171116.1

2. Choose Upgrade Application and follow the instructions to select:

   oMG-Application-9.4.8804v3.sdk4-20171116.1

3. The oMG will automatically start downloading the software on the next boot, or the download can be started immediately from the oMG LCI by selecting General > Tool > download-new-software-updates.

New Features

Software Upgrade

Enhanced software upgrade feature to automatically check the repository for new updates, if an installation schedule is configured and no downloaded updates are waiting to be applied.

GPS

Added feature to enable forwarding of GPS data to a local or remote server at tunable reporting intervals.

VPN

Enhanced Multi-VPN support to allow both Host-to-LAN and LAN-to-LAN VPNs.

Enhanced IPSec IKEv1 support to allow multiple local subnets.

LCI

Updated user configuration (System > Users) to enable Administrators to change User password without entering the original password.

Added IMSI field to Extended WAN Link Status page for GD Band 14 Radio module. This field is reported to AMM.

Added private zone configuration fields in WAN Link Configuration (WAN > Links) and Wi-Fi Network Configuration (WAN > WiFi Networks) screens.

PPPoE WAN

StarTech USB2100 USB-Ethernet adapter can be connected to an available USB slot to support PPPoE WAN Link to a connected Land Mobile Radio (LMR)

Addressed Issues

Installation

Existing DNS private zone configuration is automatically imported and converted for use with oMG 3.15.

3rd-party Product Support

Resolved issue where ZOLL devices were losing connection with ZOLL applications running on Microsoft Windows 10 PCs.

Updated default Physio Control configuration to use Physio Control’s new Server URL.

Addressed security issue with Physio Control application.

AMM Support

Resolved issue that caused erroneous reports (e.g. Link Utilization) on the AMM.

Resolved issue where the AMM would not detect the gateway booting up.

Resolved issue where the gateway would not send known laptop name to the AMM.

Resolved issue where oMG500 was incorrectly reported as oMG2000 to the AMM.

Added details for AMM’s cellular network inventory report.

Network Connection

Improved connectivity with AC340U cellular radio adapter.

Resolved issue where the radio module failed to read the SIM, resulting in connection not being made.

Improved Sprint network coverage.

Resolved issue where signal strength was not being reported when connected to WCDMA networks.

VPN

Removed support for IKE and ESP Diffie-Hellman key length DH16 and DH17.

Resolved issue where the VPN would not connect when one WAN link was configured to use MOBIKE while another link was not.

Resolved user authentication issue when Radius server is inside VPN.

Resolved issue to allow support for perfect forward secrecy (PFS).

Resolved issue where the gateway would stop passing traffic over the VPN after many (1000s) WAN interface switches.

Network Policy

Resolved issue with Advanced Routing Rules not applying consistently for post-link state.

Resolved issue affecting traffic flow with WAN link split access configuration.

Resolved issue where certain network rules caused the gateway to lock up.

Resolved issue where Wi-Fi WAN link would disconnect due to abnormal ping monitor failure.

Resolved issue where AMM data was sent in the open network instead of the management tunnel when the event server was specified by IP address.

GPS

Fixed error caused by lower-case TAIP response such as “pv” being accepted from LCI.

LCI—Access Points

Resolved issue where Wi-Fi host encryption could not be changed.

Resolved Security Issues

Common Vulnerabilities and Exposures (CVE)®

Addressed python vulnerability: CVE-2008-1887

Addressed bind vulnerability: CVE-2016-2776

Addressed openvpn vulnerability: CVE-2017-7520

Addressed libxml2 vulnerabilities:

- CVE-2016-5131
- CVE-2016-3627
- CVE-2015-5312

Addressed expat vulnerability: CVE-2016-4472

Addressed linux kernel vulnerabilities:

- CVE-2017-1000364
- CVE-2017-1000365
- CVE-2016-5195 “Dirty Cow”

Addressed glibc vulnerabilities:

- CVE-2012-4412
- CVE-2014-4043
- CVE-2015-5180
- CVE-2016-3075

Addressed glibc vulnerabilities:

- CVE-2007-1659
- CVE-2015-5073

Addressed vim vulnerabilities:

- CVE-2017-6349
- CVE-2017-5953
- CVE-2016-1248
- CVE-2008-3075
- CVE-2008-3074

Addressed large number of tcpdump vulnerabilities by updating to tcpdump 4.9.2.

Addressed openssh/openssl vulnerabilities

- CVE-2012-6689
- CVE-2015-8325
- CVE-2016-2177
- CVE-2016-6210
- CVE-2016-7055
- CVE-2016-3115
- CVE-2017-3732
- CVE-2016-2183
- CVE-2016-6306
- CVE-2016-6304
- CVE-2016-6302
- CVE-2016-6303
- CVE-2017-3731
- CVE-2016-2182
- CVE-2015-8325
- CVE-2016-1908

Addressed libcurl vulnerabilities:

- CVE-2016-5419
- CVE-2016-5420
- CVE-2016-5421

Addressed glibc vulnerability: CVE-2015-7547

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