Software Release Notes V2.15

oMM Management System

SIERRA WIRELESS®

4119199
Rev 2

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless modem **MUST BE POWERED OFF**. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Dell® is a registered trademark of Dell Inc. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales	1-877-687-7795 sierrawireless.com/airlink_sales
Support	sierrawireless.com/support
Technical Documentation and Resources	source.sierrawireless.com
General Information	www.sierrawireless.com

Revision History

Revision number	Release date	Changes
1	May 5, 2016	Used new SWI template.
2	May 11, 2016	Added Browser issues to Outstanding Problems section.

Contents

1: Release Information

Officially Released Versions

These release notes are inclusive of all oMM Management System (oMM) R2.15.x versions.

oMM 2.15 was officially released to General Availability on May 5, 2016.

Platform Support

oMM 2.15 has been tested on Dell R220 and R630 servers and on VMWare ESXi.

Browser Support

oMM 2.15 has been tested on Internet Explorer 11. Other supported browsers include Chrome and Firefox. Users that attempt to use a browser that is not supported will get a warning and may experience some issues.

Sierra Wireless Gateway Support

For oMG gateways, oMM 2.15 supports up to oMG R3.14.3 or later. For AirLink gateways, oMM 2.15 supports ALEOS firmware version 4.4.3 and higher. Support for AirLink gateways is only provided for the Customer Data Center version of the oMM, and is not provided in the Cloud solution.

2: Key Features and Enhancements

Self-Serve Software Update

oMM 2.15 provides the ability for customers to manage the process of updating gateway firmware, radio modules and applications on all supported gateways. This new feature provides a repository of firmware releases, and provides a wizard-style GUI to guide the user through the process. Only software upgrade is supported; downgrade is not supported.

This capability is available for oMG and AirLink gateways. Different capabilities are available on each platform.

Key features of Self-Serve Software Update include:

Software Repository Management User Interface

oMM 2.15 provides a software repository, where users can store and manage copies of gateway firmware, radio modules and applications for all supported Sierra Wireless gateways. For oMG software, the repository can be configured to check for new releases from the Sierra Wireless public software repository. There are configurable options to specify software download actions. Users can then chose to download new versions. For customers that do not allow the oMM to connect to the public Internet, firmware packages can be downloaded from the Source (http://source.sierrawireless.com/) and uploaded to the oMM.

ALEOS firmware for AirLink gateways can be downloaded from the Source (http://source.sierrawireless.com/) and uploaded to the oMM.

The user interface for the software repository provides details on the software that has been uploaded, including file name, version, platform, release date and the current status of the files. Once firmware is no longer needed in the oMM, it can be purged to conserve space or streamline the environment.

Gateway Software Management User Interface

Once the software releases are available in the oMM, a new user interface is provided to assist users with managing the software distribution process. A wizard-based user interface is provided that assists users with distributing the selected software to oMG or AirLink gateway(s). Only software upgrade is supported; downgrade is not supported. For customers that have the FIPS version of the oMG software, only oMGs running the FIPS version can be upgraded to new FIPS versions.

For AirLink gateways, oMM 2.15 supports scheduling of software updates. The user can select the date and time when the update will be applied. Once scheduled, the upgrade process can be cancelled, provided that the AirLink gateway has not checked in to the oMM.

Self-Serve Software Update Limitations

- oMG 1000 is not supported in Software Distribution.
- oMM currently supports an upgrade of up to 1,000 gateways at a time.

AirLink (ALEOS) Device Management

oMM 2.15 provides the ability to register, monitor and deploy configurations from one AirLink gateway to other gateways. Supported AirLink gateways include:

- ES440/450
- LS300
- GX400/440/450
- RV50
- MP70

oMM 2.15 supports ALEOS firmware version 4.4.3 and higher.

Key features of AirLink Device Management include:

Gateway Registration

oMM 2.15 supports the manual registration of one or more AirLink gateways into the oMM. From the Admin->Gateways menu, the user can add an AirLink gateway by providing the device type, its serial number and name. Once added, it will be available for assignment to new or existing device groups in the oMM user interface. This release supports detection of a misconfigured gateway type, to ensure a valid AirLink gateway is being registered.

Devices can be automatically populated in the oMM by changing the server URL in AirLink Management Service (ALMS) or via the AceManager user interface to point to the customer's oMM.

oMM Dashboard

The oMM Dashboard has been updated to display key information about the AirLink gateways, such as Heartbeat, Operational State or IP address.

Supported Stats

AirLink gateways reporting to the oMM report key stats that are presented in the oMM’s user interface. The following stats are supported for AIrLink gateways:

- **Link-based**: ActiveLink, Active, IPAddress, State, CurrentNetworkOperator, NetworkServicetype, WANSignalStrength, ICCID, MobileDirectoryNumber, RadioFirmwareVersion
- RemoteSocketAddress
- ResetCount
- **GPS-based**: longitude, latitude, miles, satellites, speed, zone, antenna, and fix
- ReportIdleTime

- Platform
- ConfigurationState,ConfigSyncStatus
- SoftwareVersion

The stats reported by an AirLink gateway differ from those reported by an oMG gateway. Thresholds are supported for AirLink gateways for all supported stats.

Config Copy/Deploy

oMM 2.15 supports copying the configuration from one AirLink gateway to one or more gateways of the same type. The model supported in this release is to start with a "golden master" configuration, and use that configuration to be copied from one AirLink gateway, to be deployed on one or more target gateways. oMM 2.15 does not support the direct configuration of an AirLink gateway from within the oMM directly.

Reports

oMM 2.15 supports limited reporting on AirLink gateways. Only the Event Viewer and Statistics Graph reports are supported for AirLink gateways.

User Interface Changes

Network Availability Trend Report

In previous releases, the Network Availability Trend report did not indicate failed units clearly. Users were advised to schedule the Availability Trend report and examine the "top of the list" for units to investigate. If a unit was performing poorly in relation to others (i.e. a lower connectivity percentage) it was sorted to appear at the top of the list. Units that had not reported at all did not appear in the sorted list. This was misleading and could cause failed units to be easily overlooked.

To address this issue, the user interface has been updated to include a new check box entitled "Discard units that did not report in time period". The check box is selected by default, and non-reporting units are not included in the report. Customers that wish to see all units, irrespective of when they last reported, should uncheck this new check box.

Coverage Trails Report

The link names in the menu at the bottom of the Coverage Trails Report were unclear and could be confusing. The link names have been updated to properly reflect the carrier.

Documentation

On-line User Guide

The on-line user guide has been updated with an overview of the new features from oMM 2.15. A new visual style has been applied that is consistent with Sierra Wireless standards.

Management Tunnel Certificate Upgrade

As part of oMM 2.15, the management tunnel certificates set to expire in November 2016 have been upgraded with new certificates. Only oMGs with the new certificate will be able to successfully establish a management tunnel with the upgraded oMM servers. Note that this is only supported for oMGs running software version 3.14.1 or greater.

3: Addressed Problems

Reference	Problem Description
2166	**Copy->Config** The Config/Copy screen does not filter out groups or multiple nodes as the source. An improvement has been made such that when the user selects multiple nodes using Ctrl+click and then navigates to the Copy page using top-header menu, an alert appears indicating that only one gateway can be selected and the user is blocked from accessing the Copy page.
2511, 2923	**Link Utilization Report** The Link Utilization report shows 'unknown' for last 9 days but displays correctly for the last 10 days. The Link Utilization report now shows a message about the limitations of the report data (account is limited to 90 days of report history).
3521	**Shutdown Reason Report** The Shutdown Reason report gives misleading shutdown times after hard power cut.
2982	**Management Certificates** The management tunnel certificates are set to expire in November 2016 and have been updated in this release.
3040	oMM vulnerable to "Clickjacking" attacks.
3114	Vulnerability on BIND.
3184	Addressed all critical, high and medium priority issues identified by a Nessus scan against oMM 2.14.
3784	Disable TLS 1.0 and TLS 1.1, SSLv3.
3979	Confirm that the user cannot access the rest of the system via HTTP/ Apache (Software Distribution path).
4004	Address 'DROWN' vulnerability (CVE-2016-0800).
3135, 4036	Tomcat Remove context reloadable from Tomcat. Upgrade Tomcat to 6.0.45.
4038	Double-free in DSA code (CVE-2016-0705).
4039	Fix memory issues in BIO_*printf functions (CVE-2016-0799).
4040	Addressed CVE-2016-2842, an OpenSSL vulnerability.
4067	OpenSSH Security Advisory: x11fwd.adv

Reference	Problem Description
4151	Address an issue where the oMM certificate was signed with a weak algorithm.
3037, 3046	**Threshold Email** Improvement to do a field check for threshold email addresses. Addition of validation of user email address.
3843, 3199	**DELS** Enhancement of a new DELS events for Flash Media Life Extension (FMLE). Addressed an issue where the Delsrx receive time is being incorrectly logged.

4: Outstanding Problems

Reference	Problem Description
4041	LS300 disconnects periodically.
4201	**Software Distribution** Can't sync a gateway release after an upgrade from outside of the oMM.
4222	Security update for Java-1.8.0-openjdk available. This issue does not affect the current release.
4219	ALEOS-only banner not shown when node tree filter used.

Browser Cache Interfering with oMM User Interface

After the upgrade to oMM 2.15, some users are experiencing issues in the oMM User Interface where they cannot save changes. To address this issue, the browser history and cache must be cleared using the instructions below for each browser.

Chrome:

1. Press **Ctrl + Shift + Delete** to display the **Setting/Clear browsing data** window.
2. In the dropdown: **Obliterate the following items from**, choose **The beginning of time**.
3. Check **Cached images and files** to enable the option.
4. Click **Clear browsing data** at bottom of the window.

Firefox:

1. Press **Ctrl + Shift + Delete** to display the **Clear All History** window.
2. In the dropdown: **Time range to clear**, choose **Everything**.
3. Check **Cache** and **Offline Website Data** to enable the options.
4. Click **Clear Now** at the bottom of the window.

Internet Explorer:

1. Close all Internet Explorer windows and tabs, and open a blank page. This must be done in order to clear the cache.
2. Press **Ctrl + Shift + Delete**, to display the **Delete Browsing History** window.

3. Uncheck **Preserve Favorites website data**. This option must be unchecked, otherwise the oMM cache cannot be cleared if the oMM was saved to the bookmarks.
4. Check **Temporary Internet files and website files** and **Cookies and website data** to enable the options.
5. Click **Delete** at the bottom of the window.

If this process is unsuccessful, and the same issue is still being experienced, then cached Internet Explorer files must be manually removed:

- Navigate to **C:\Users\<YOUR NAME>\AppData\Local\Microsoft\Windows\INetCache** and delete all files.

If the above location does not exist, identify the location where Internet Explorer is saving cached files:

1. Navigate to **Tools -> Internet Options**.
2. Click **Settings**.
3. Look for the path under **Current location**.
4. Navigate to that location and delete all files.