Software Release Notes V2.15.1.1

oMM Management System

4119798
Rev 3

SIERRA WIRELESS®

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	Aug 19, 2016	oMM 2.15.1 Release Notes

Contents

1: Release Information

oMM 2.15.1.1 is a minor release of the oMM Management System (oMM) that introduces a number of minor new features, finalizes compatibility with the Airlink MG90 vehicle router, features user interface improvements, and addresses a number of outstanding problems that have been identified in previous releases.

Officially Released Versions

These release notes are inclusive of all oMM R2.15.x versions.

oMM 2.15.1.1 was officially released to General Availability on August 19, 2016.

Platform Support

oMM 2.15.1.1 has been tested on Dell R220 and R630 servers and on VMWare ESXi.

Browser Support

oMM 2.15.1.1 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 2.15.1.1 supports up to oMG R3.14.4. For AirLink gateways, oMM 2.15.1.1 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

Gateway List Import

The oMM allows users to pre-register gateways and routers, and define where in the organizational structure they will reside once they start communicating with the oMM. In previous releases, users had to manually register individual devices, which could prove challenging for large fleets.

oMM 2.15.1.1 introduces a new feature that allows for users to create a .CSV file with their device details, and automatically pre-register and place them into the appropriate folders when they communicate with the oMM. This allows users to avoid the requirement to manually assign large numbers of gateways to the correct structure. This feature can also be used to re-organize a fleet of devices.

Airlink MG90 Vehicle Router Support

oMM 2.15.1.1 provides complete support for the Airlink MG90 High Performance Multi-Network Vehicle Router.

SHA2 Support

The release of 3.14.4 for the oMG 2000/500 and 4.0.1 for the MG90 introduce support for SHA2 (Secure Hash Algorithm 2), specifically SHA-256 and SHA-512, and also provides support for Diffie-Hellman (DH) Groups 14,15,16,17,18. oMM 2.15.1.1 is updated to provide support for these features for the IPsec VPN Tunnels in our products.

Note: Diffie-Hellman (DH) Group 18 is supported by the oMM, but is not yet supported by the 3.14.4 and 4.0.1 software releases.

Global Time Zone Support

Previous releases of oMM only provided support for U.S. time zones. oMM 2.15.1.1 introduces global time zone support.

User Interface Changes

Software Distribution Workflow Improvements

oMM 2.15 introduced Self-Serve Software Update capabilities in the oMM. Over the past few months we have received feedback on the usability of this new feature that has been used to improve the product. As a result, there are a number of user interface changes in Self-Serve Software Update.

Display the Latest Version in the Software Package Repository

Feedback was provided from the user community that it was often difficult to understand which version of the software and/or applications was the latest release. The “Version” information in the Software Package Repository has been improved to expose the date of the package, improving ease of identification.

Allow Core and Application Software Upgrade in One Step

In the original release of the Software Distribution feature, the user was required to update either the Core or Application software independently. The user interface wizard has been improved to allow core and application upgrades in one step.

Support for Engineering Software Builds

On occasion, we need to release engineering builds to customers to help with troubleshooting issues in the field. Previous oMM releases did not support Engineering builds, which prevented customers from managing this process themselves. oMM 2.15.1.1 supports Engineering software builds, and puts control of managing this process back with our customers.

Improvement of User Interface Messages

A number of improvements have been made to the messaging within the user interface to better explain error messages and provide detailed guidance on managing the software distribution process.

Disable Admin->Remote Session Menu for ALEOS Devices

The Admin -> Remote Sessions feature in oMM is not compatible with ALEOS devices that are managed by the oMM. When a device or folder of devices is selected that include ALEOS devices, the Admin -> Remote Sessions selection is now greyed out and inaccessible.

Configuration Audit Report Name Change

oMM 2.15.1.1 changes the name of the *R3 Configuration Audit* report to *Configuration Audit*. No other changes are made to the functionality of the report.

3: Addressed Problems

Reference	Problem Description
Security Vulnerabilities	
4267	Upgraded MySQL to address security vulnerabilities in v5.6.22.
4247	Addressed all critical, high, and medium priority issues identified by Nessus scan against oMM 2.15.
4241	Addressed git security vulnerabilities - CVE-2016-2315 and CVE-2016-2324.
4222	Implemented a security update for java-1.8.0-openjdk.
Copy> Config	
4435	The Copy>Config feature was incorrectly identifying gateways as not in sync.
VPN Stats Accuracy	
4223 4418 4397 4227	There were a number of problems reported with VPN stats not correctly displaying on the oMM. Specific problems included the *VPNIndividualUptime* stat not resetting after an unclean gateway shutdown; the *VPNIndividualTunnelUpTime* stat not always being reset after gateway reboot; and the *VPNTunnelUpTime* threshold not restarting when the oMG is restarted.
Software Distribution	
4403	Corrected a problem where a null pointer exception is triggered after canceling an application upgrade.
4364	oMG 500 devices are now able to use oMG 2000 software packages for upgrades.
VPN Config Provisioning	
4398	On the VPN Config Provisioning page, the *IKE Transform* field shows a wrong value.
4367	oMM 2.15.1.1 requires an update to support oMG spec version 112.
4259	In VPN Config Provisioning, errors were found when the VPN friendly name contains an apostrophe symbol – “ ‘ “.
Admin->Gateways	
4363	The topmost checkbox used for “selecting all” did not work when the page was scrolled down.
4339	Corrected a duplicate title at the top of the Admin->Gateways page.

Reference	Problem Description
DELS	
4388	Added support for decoding DELS events for AceTech Application (69889-69894) in oMM, in support of the MG90.
4385	Corrected a problem where the Event Viewer was not handling event ID 372.
4384	Corrected a problem where the Event Viewer was not handling event ID 337.
4297	Corrected a problem where the *Vehicle Asset* report was displaying a Java error.
4295	oMM does not report the *ResetCount* stat when the system sees this stat for the first time.
4294	Add self-changing cfg elements to the *msciblacklist* when performing config comparison for the purposes of conflict checking.
4246	Addressed a problem where oMM 2.15 was occasionally not able to create users.

4: Outstanding Problems

Reference	Problem Description
Security Vulnerabilities	
4443 4440 4419	A number of security vulnerabilities were identified after our code freeze for oMM 2.15.1. These issues will be addressed in 2.15.2. **OpenSSH Vulnerabilities**: CVE-2015-5352, CVE-2016-3115, CVE-2014-2653, CVE-2014-2532. **Linux Kernel Vulnerabilities**: CVE-2016-4997. There were a number of vulnerabilities identified by Nessus scan against oMM 2.15.1 that were discovered after our code freeze and will be addressed in 2.15.2.
4509	The user cannot upgrade an Application when the oMG gateway is running an engineering build of Core software.