Software Release Notes V2.16.2

AirLink® Manager and AirLink® Mobility Manager

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 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	Oct 11, 2018	AMM 2.16.2 Release Notes
2	Oct 12, 2018	Corrected latitude to altitude in the first sentence of "Display Altitude in the Gateway Trips Report".

≫ Contents

1: Release Information

AirLink Manager (AM)/AirLink Mobility Manager (AMM) 2.16.2 is a minor release of the AirLink Manager Platform that provides support for the AirLink LX40, includes a series of security-related improvements, and provides new features in support of both MG and ALEOS-based AirLink devices.

After completing an upgrade of the AM/AMM, Sierra Wireless recommends that all users refresh their browser cache after the upgrade before accessing AMM 2.16.2.

These release notes include the details for AM/AMM 2.16.2, AMMER 1.0.3, and Uploadlog 1.0.1.

Officially Released Versions

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

AMM 2.16.2 was officially released to General Availability on October 5, 2018.

Platform Support

AMM 2.16.2 has been tested on Dell R230 and R630 servers and on VMWare ESXi.

Browser Support

AMM 2.16.2 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, AMM 2.16.2 supports up to oMG R3.15.1 and MG90 4.x+. For AirLink gateways, AMM 2.16.2 supports ALEOS firmware version 4.4.3 and higher. Some features of AM/AMM 2.16.2 require later versions of the ALEOS or MG software.

AMM 2.16.2 also supports:
- GNX6: G604.08.01 and higher (limited support)
- GNX3-UMTS: G303.08.83 and higher (limited support)
- AirLink LX40 (new)
- Calamp LMU2631CV model (limited support)

›› |2: Key Features and Enhancements

AM/AMM URL Changes Due to Consolidating All HTTP/HTTPS Access Through the Apache Proxy

In previous releases of the AM/AMM, access to different parts of the system were provided through various services on the AM/AMM. To improve the overall security of the AM/AMM and to simplify the deployment and configuration process, AM/AMM 2.16.2 consolidated all HTTP and HTTPS access through the Apache proxy.

The main impact of this change is that the URL to access the AM/AMM for all users will require a one-time change. All users must update their AMM bookmark to: *http(s)://<AMM URL>/sierrawireless/*

The other benefit is it allows some of the required ports on the AM/AMM to be closed. Ports 8080, 8443, and 51000-51100 will no longer be needed to access the AM/AMM user interface, further improving the security posture of the system.

Support for the AirLink LX40

Sierra Wireless recently launched the AirLink LX40 gateway, our most compact LTE and LTE-M/NB-IoT router for IoT/M2M applications. The LX40 provides "out-of-the box", secure, managed LTE networking for IoT and enterprise applications such as IP Cameras, Security, Point-of-Sale terminals and Smart Lockers. LX40 is also ideally suited for connecting industrial, remote data logging and sensing equipment in protected (indoor) locations and supports processing of IoT data at the edge. The LX40 is also available with Wi-Fi, to act as a local hotspot or to connect to WiFi infrastructure.

AM/AMM 2.16.2 is required to support the AirLink LX40.

New ALEOS Application Framework (AAF) Applications

AMM Event Reporting AMMER 1.0.3

AMMER 1.0.3 is required to support the AirLink LX40 and provides support for new features in AM/AMM 2.16.2. AMMER 1.0.3 has been released as part of the AM/AMM 2.16.2 release and is preloaded with the installation/upgrade of AM/AMM 2.16.2 and is available on the Source to be downloaded independently.
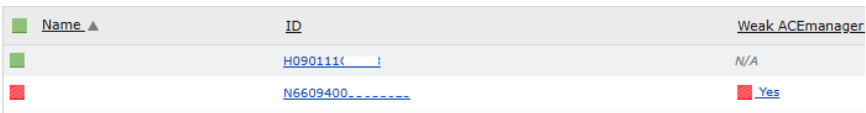
Uploadlog 1.0.1

The uploadlog 1.0.1 AAF application is required to support secure uploads and is pre-installed with AM/AMM 2.16.2. It is also available on the Source to be downloaded independently.

Identify Weak ACEmanager Passwords in the Dashboard

Updating the default passwords on ALEOS devices is a critical component of overall system security. Sierra Wireless recommends that all users update their passwords on their AirLink routers and gateways on a regular basis, and provides tools in the AM/AMM to make this process easy.

AM/AMM 2.16.2 introduces a new column in the AM/AMM dashboard titled *Weak ACEmanager Password* that indicates whether the ACEmanager login password for an ALEOS device is weak.

Name ▲	ID	Weak ACEmanager
🟩	H090111(!	*N/A*
🟥	N6609400_____	🟥 Yes

Figure 2-1: Identify Weak ACEmanager Passwords from the AM/AMM Dashboard

The values that can be displayed are:

- **Yes**: the ALEOS password is one of the top 1,000,000 known weak passwords.
- **No**: the password is not set to one of the weak passwords and is therefore considered strong.
- **HTTP**: if the device is configured to communicate to the AMM over HTTP, rather than HTTPS, the column will be set to HTTP to indicate that the password state cannot be determined.

Secure Communication Between an AirLink Gateway and AM/AMM

In past releases of the AM/AMM, communication between ALEOS gateways and the AM/AMM was required to happen over HTTP in an insecure fashion. With the release of AM/AMM 2.16.2, customers can configure their AM/AMM with a certificate signed by Sierra Wireless that will allow the ALEOS devices to communicate securely with the AM/AMM over HTTPS if the customer configures their devices with the *TLS Verify Peer Certificate* option enabled from ACEmanager.

This feature requires AM/AMM 2.16.2 and ALEOS 4.11.+

Set Device Location Manually in AM/AMM

Most AirLink routers and gateways come equipped with GPS, allowing the devices to be identified in the *Map* and *Tracker* features of AM/AMM. In some situations, where the device has not been provided with a GPS antenna, or when a device is deployed in an indoor location where GPS signals cannot reach, the device cannot provide AM/AMM with its location.

In these situations, AM/AMM 2.16.2 includes a new feature that allows a user to provide a location for the device, ensuring it will display in the *Map* and *Tracker* screens.
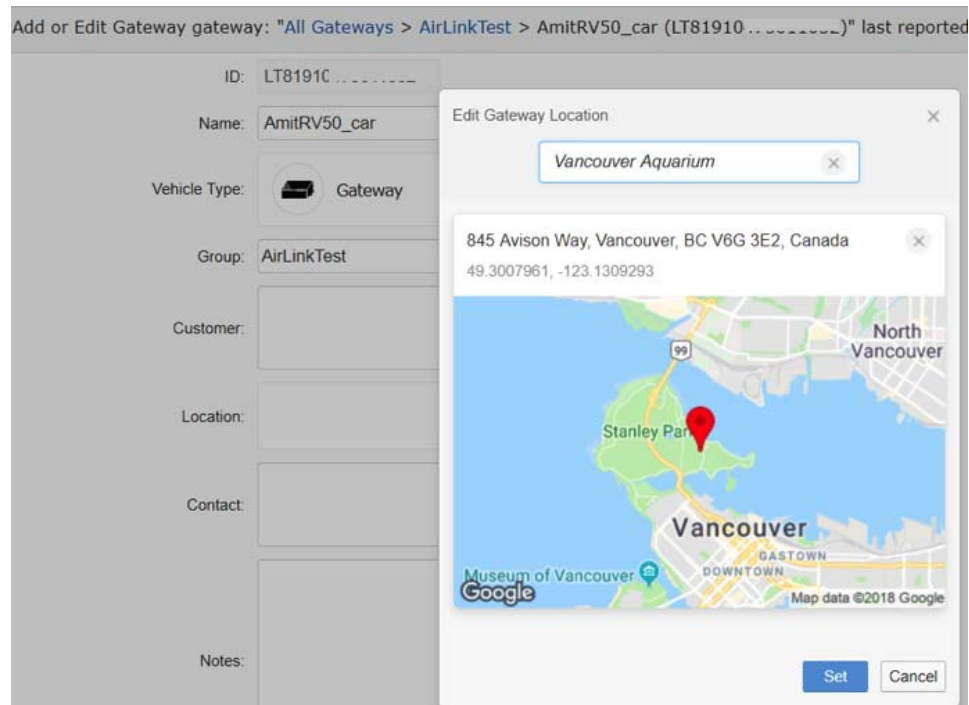

Figure 2-2: Set a Location Manually in AM/AMM

This new feature is available from the **Admin->Gateways** screen for individual devices, or users can update many devices at one time using the spreadsheet upload feature. The multiple device feature only supports latitude/longitude for input.

User Creation and Management for Hosted AMM Customers

AM/AMM 2.16.2 provides the ability for hosted AMM customers to create, edit, and manage their users in the **Admin->Users** section of the AMM interface. In the past, all user creation and management had to be done by the Sierra Wireless Customer Support team. Users can now manage this process themselves. There is no change for customers with on-premise AM/AMMs.

Remote Access to ACEmanager

There are many times when it is advantageous to be able to remotely connect directly to the AirLink router or gateway and access the ACEmanager interface directly (e.g. some settings in ACEmanager can only be managed directly on the device).

AM/AMM 2.16.2 introduces the ability to access the ACEmanager interface directly, by right-clicking on the *Access ACEmanager* link from the device in question on the Device Tree (left-hand panel in the AM/AMM user interface).
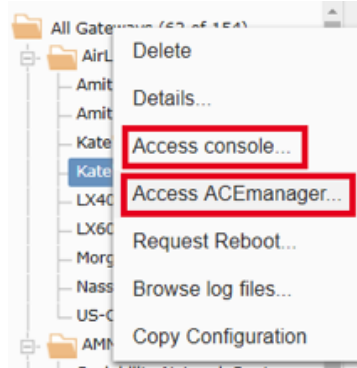

Figure 2-3: Access ACEmanager Directly from the AM/AMM

This feature requires the AirLink routers and gateways to be running ALEOS 4.11.0+ and to have AMMER 1.0.3+ installed. This will enable a management tunnel between the device and the AM/AMM. Please note that enabling the management tunnel by installing AMMER 1.0.3 will increase the data usage on your devices. This feature can be disabled in the AMMER 1.0.3 configuration.

There is also a requirement for the server certificate for the AM/AMM to be signed by Sierra Wireless. Please contact the Sierra Wireless Customer Support team for more information. Certificates signed by other CA's will not work.

Improvements to the WAN Wi-FI Spreadsheet Upload

The configuration feature is improved to add support for Custom Hostnames and Static IP settings in the spreadsheet upload feature. This feature requires release 3.14.5+ on the oMG and is supported on all software versions of the MG90.

Browse Log Files Support for ALEOS Devices – Secure Access

AM/AMM 2.16.1 introduced the ability to access log files on ALEOS-based devices, through the installation of the uploadlog AAF application. Once installed on the ALEOS devices, the device will upload ALEOS log files from the device to the AMM. In 2.16.1, the files were uploaded in the clear.

AM/AMM 2.16.2 includes a new version of the uploadlog AAF application that can leverage AMMER 1.0.3 and its management tunnel to upload the log files securely. If the management tunnel is not present, the log files will continue to be uploaded in the clear.

Secure access to this feature requires ALEOS 4.11.0+, AMMER 1.0.3+ and uploadlog 1.0.1+.

New Gateway Stats

AM/AMM includes support for a series of new Stats from AirLink devices.

Stats for MG Devices

- **UpTime**: This new stat is updated when the AM/AMM receives a heartbeat event from the device.

Stats for ALEOS Devices

- **UpTime**: This new stat is updated when the AM/AMM receives a heartbeat event from the device.
- **RAP ID**: Displays the RAP ID set for the device as configured in ACEmanager.
- **IMEI**: Provides the IMEI from the AirLink device.
- **CallUp**: Indicates if the cellular WAN interface is active.
- **GPSFix**: Indicates if there is a GPS fix.
- **OperationalState**: Identifies the operational state of the device.

These new Stats require AMMER 1.0.3.

Software Distribution Enhancements

Start a Software Download to the Device Immediately Triggering an Upgrade in the AMM

In previous releases of the MG/AM/AMM software, MGOS would not poll the AMM for changes in related to the upgrade request, and as a result, the software download would only start when there was a link state change, system reboot, or forced LCI/tool/software-download.

This release of the AMM introduces the ability for the device to self-trigger a software download without additional intervention from the AMM. This is supported for both on-demand and scheduled software updates.

This feature is specific to the AirLink MG90 and requires MGOS 4.2+. This behavior is not supported on the oMG2000.

Purge Software no Longer Needed in the AM/ AMM

With this release, users are able to remove selected package(s) from the list to prevent the software package screen from becoming cluttered. Now all the software packages can be purged except when they are in *Downloading* state.

The purged packages can be viewed using the **Show Purged** button

Verify that AAF is Enabled for ALEOS Devices When Installing an AAF Application

AAF applications can be installed by AM/AMM but only when AAF has been enabled on the device. If AAF is not enabled, the AM/AMM will put the targeted device in the *Unaffected Gateways* list with reason *ALEOS Application Framework is not enabled, or its state cannot be detected*.

3: AM/AMM User Interface Enhancements

AM/AMM 2.16.2 includes a series of enhancements to existing reports.

Redesign of the Vehicle Diagnostics Report (Telemetry)

In previous releases of the AM/AMM, the *Vehicle Diagnostics* report was hard-coded to support a limited number of specific vehicle Stats for reporting. There was no ability for the user to change those values.

AM/AMM 2.16.2 introduces a new report design that improves the value and flexibility of this report. Instead of being hard coded for specific Stats, the report now provides the user with the ability to customize the parameters to report on any Telemetry stats that are available in the system. Stats can be added or removed as required.

Figure 3-1: Vehicle Diagnostics Report - Report Input

Figure 3-2: Vehicle Diagnostics Report - Report Output

Display "Band 14" Separately on the Cellular Technology Reports

With the release of FirstNet in the United States, many customers want to understand the state of availability of Band 14 in their region. To support this, the *Cellular Technology Map* and *Cellular Technology Trails* reports have been updated to allow the user to separately identify Band 14.

Figure 3-3: Report generation of the Cellular Technology Map report allows the user to run the report on Band 14.
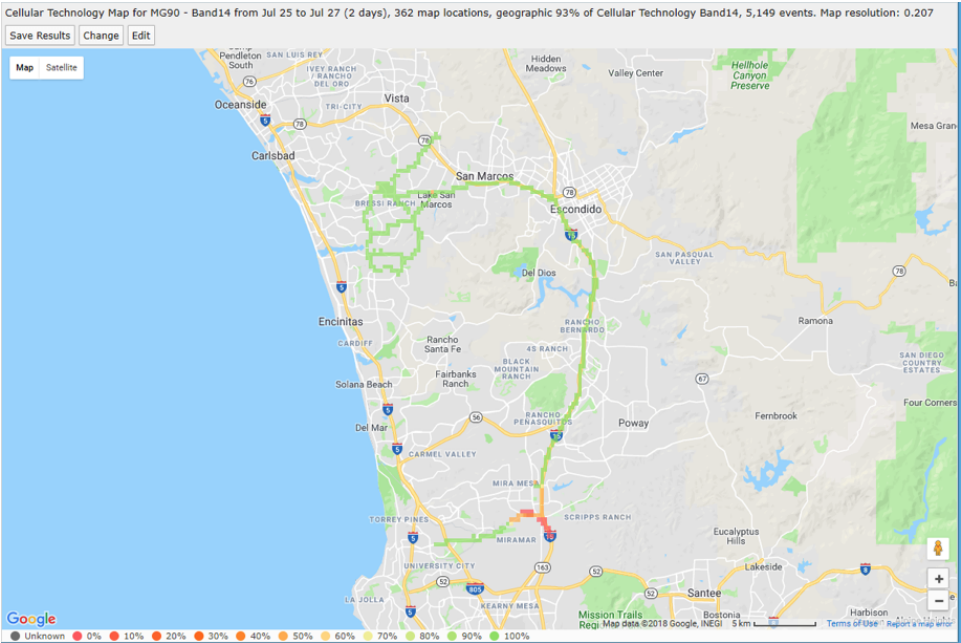
Figure 3-4: The Cellular Technology Map report can display the coverage on Band 14.
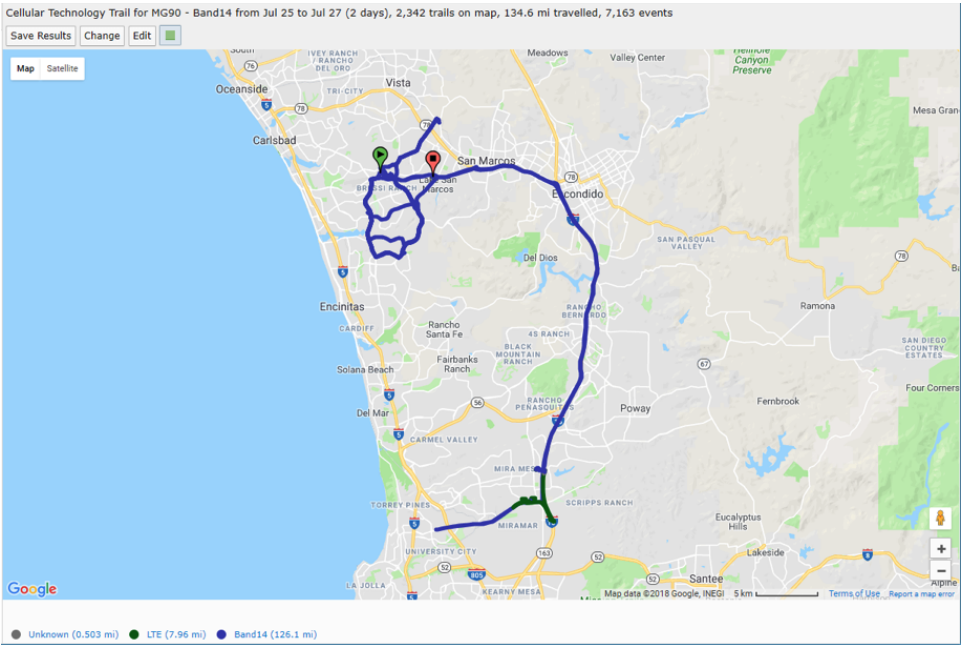
Figure 3-5: The Cellular Technology Trails report can show where a driver has had coverage on Band 14.

Link Utilization Report: Move "Show Detailed Info" out of Advanced Configuration

Show detailed info allows additional information to be displayed when hovering the mouse in the *Link Utilization* report. In previous releases, this feature was inside the *Advanced Configuration* menu. It has now been moved out into the main report generation screen to make it easier to enable.

Figure 3-6: The "Show detailed info" Check box has been Moved onto the Main Link Utilization Report Generation Screen.

Link Utilization Report: Add Color Coded Events for Clean and Unclean Shutdown

In previous versions of this report, the *Link Utilization* report would only identify shutdown events. This enhancement now displays separate colors for clean and unclean shut down events.
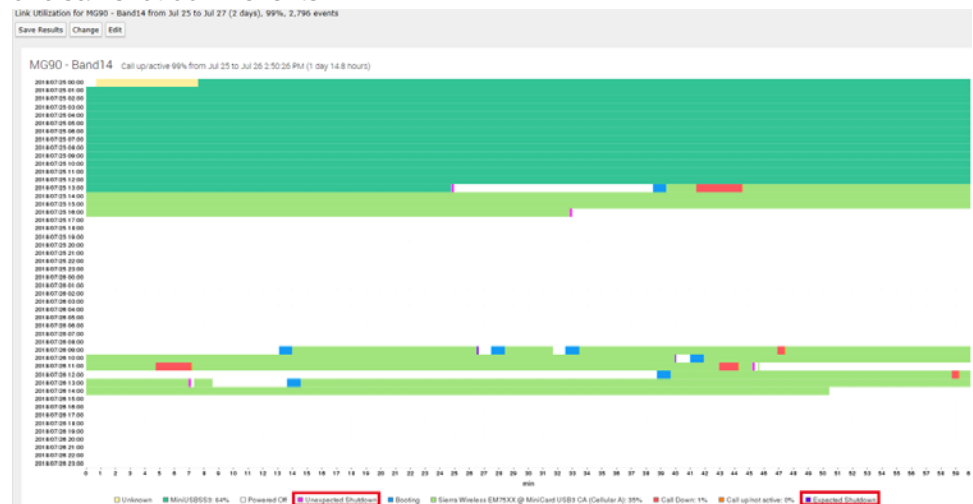
Figure 3-7: Shutdown Events are now Categorized as Either a Clean or Unclean Shut Down

Display Altitude in the Gateway Trips Report

The MG90 AirLink mobile router is able to record the altitude of the device. On the *Gateway Trips* report, enabling *Directions* displays triangles to identify the gateway's direction of travel at a location. Clicking the triangle displays a popup showing the gateway's name, speed, and altitude at that location

The altitude display requires MGOS software version 4.3+. This field will not be shown for gateways that do not support this feature.

Figure 3-8: Altitude is Shown on the Direction markers.

Dashboard: Separate Name and ID Columns

AM/AMM 2.16.2 improves the *Dashboard* by separating the *Name* (name assigned to the device) and *ID* (device serial number) columns, allowing each to be sorted and filtered separately. In previous releases these values were concatenated into a single value.

Figure 3-9: The Name and ID fields can now be Sorted and Filtered Individually.

Remove the "Folders" Button from the Dashboard

This feature was rarely used and was removed to streamline the user interface.

Map View: Added the Ability to Collapse/Hide/Resize the Device Pane

AM/AMM 2.16.2 introduces the ability for the user to Collapse/Hide/Resize the *Device Pane* (right-hand panel in the user interface). This panel now acts in a similar fashion to the panel with the *Device Tree*.

4: Addressed Problems

Reference	Problem Description
Customer Reported Field Issues	
6587	Addressed an issue where a customer was not able to run the *Network Availability Trend* report on a large fleet.
6415	Addressed an issue where the AM/AMM was unable to retrieve the MG90 yaml spec from MG90 software packages, resulting in incorrect error messages.
5962	Updated the AM/AMM to disregard some MSCIID's that were creating error messages in the configuration management process.
6155 6343	Older GX440 devices had a serial number format that was preventing the AM/AMM from registering and properly recognizing the devices. This issue was preventing some devices from being registered and other devices from being moved between folders in the AM/AMM. These issues have been addressed.
5732	Addressed an issue where the AM/AMM user interface will generate an error when the user name has space character " ". The user can successfully log in after closing the error message window. In AM/AMM 2.16.2 the AM/AMM will not allow a space characters when a new user is created. For existing users that are already created with spaces, users may still encounter this issue.
5571	Updated the Configuration Audit report to address an issue that was caused by the report being out of sync with the new YAML specs.
4794	Addressed an issue where the AMM was not correctly reporting the value of a GPIO input.
3914	Addressed a long-standing issue where the *Change* button in the report was not working between the *Shutdown* report and the *Link Utilization* report.
2974	Addresses a series of inconsistencies with the *Odometer* report.
General Issues	
6217	Addressed an issue where the RV50X was displayed as *unknown*.
6580	Addressed an issue where the device was incorrectly reporting cell link up after MSCI configuration changes were applied to the device.
6320	Improved the rendering of the *Options* ->*Preferences* menu.
6098	Implemented a process to purge the M3DA debug logs periodically.
5257	Improved the display of the Telemetry Dashboard headers.
6493	Addressed an issue where icons were not rendering properly in the UI.

Reference	Problem Description
Software Distribution Issues	
6584	Addressed an issue where the MG90 FIPS gateway upgrade was showing a false failure status.
6378	Addressed an issue where multiple attempts to initiate the gateway software download were required from the AM/AMM before the download successfully occurred.
Map and/or Tracker Issues	
6571	Addressed a rare occurrence where in some instances when the user tries to load location history data for a device from the Map tab, the screen indicates AM/AMM is "Loading data..." but this action never completes.
6387	Addressed an issue where the device icons were overlapping instead of forming the cluster icon.
6386	We have temporarily removed the *Full Screen Mode* button for the Map and Tracker screens due to an incompatibility between AM/AMM and the Google Maps APIs. The feature is not currently working, so we have removed the icon to reduce confusion.
6229	Addressed an issue where the cluster icons were not shown when the map area is zoomed out.
5798	Addressed an issue where not all vehicle icons are being shown on both the Map and Tracker screens.
AMMER Issues	
125	Addressed an issue where repeated ignition events are sent shortly after device startup.
173	Addressed an issue where AMMER can generate an invalid unclean shutdown event.
169	Addressed an issue where AMMER should only send data to serial port if the user had reserved the serial port in their AAF configuration.
168	Addressed an issue where an ignition on event was reported when the CANBus was enabled but no vehicle was connected to the device.
Security Vulnerabilities	
6510 6194 6148	Addressed kernel vulnerabilities as identified in CVE-2018-5390, CVE-2017-18270, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2016-7913, CVE-2017-9242, CVE-2018-6927
6509	Addressed GIT vulnerabilities as identified in CVE-2018-11235
6507	Addressed HTTPD vulnerabilities as identified in CVE-2017-9788, CVE-2017-7679, CVE-2017-9798
6447	Addressed TOMCAT vulnerabilities as identified in CVE-2018-8037, CVE-2018-1336

Reference	Problem Description
6185	Addressed TCPDUMP vulnerabilities as identified in CVE-2016-7930
6147	Addressed GLIBC vulnerabilities as identified in CVE-2018-1000001

5: Outstanding Problems

There are a number of known issues discovered after code freeze that will be addressed in a future AM/AMM release.

Reference	Problem Description
6526	There is a known issue where the user cannot generate the foreground *Vehicle Diagnostics* report in Excel format.
6200	There is a known issue where the editing buttons available for *Read Only* users on the *Gateways* and *Groups* screen.
6635	There is a known issue where the bottom part of the *Network Availability Trend* report displays blank in the Internet Explorer 11 browser. The report works as expected in Google Chrome or Firefix.
6645	There is a known issue where the vehicle icon will not show on occasion when clicking devices in the *Map* view. This rare occurrence can be reproduced by clicking the *Map* tab and then selecting different devices in the node tree one after another. At times, the icon is not populated.
6590	There is a known issue where non-admin users created with read-only access can add a device from the *Gateway* screen. To mitigate this issue, it is recommended that non-admin users be restricted from accessing the *Gateway* page in the AM/AMM.
6648	There is a known issue where the icons in the AM/AMM interface may not render correctly. A refresh of the page will restore the correct icons.
6653	There is a known issue that when the Map tab is clicked and a selected device does not have any GPS location reports within the specified time range filter, it should default to displaying the manually defined location (if available). However, it has been noticed that in some situations the manually defined location is not shown at all.
EVMS-7287 EVMS-6650 EVMS-8780 EVMS-8801 EVMS-8044	The following security issues were identified after code freeze on the AM/AMM 2.16.2 release – CVE-2016-7913, CVE-2018-1000001, CVE-2018-13410, CVE-2018-13405, CVE-2018-8781 For most of these issues, the impact to AM/AMM is considered low and/or RedHat has not provided a fix in time for inclusion with AM/AMM 2.16.2. This will be included in the next AM/AMM release.
AMMER	
171	There is a known issue where data queue persistence can incur excessive flash wear when connectivity to AMM is not established.
159	There is a known issue where AMMER is not reliably sending a shutdown event on an AirLink MP70 (4.9.0.040) when the ignition is off.