Operation and Configuration Guide 2.15.2

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 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.

Other trademarks are the property of their respective owners.

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 6:00 am to 5:00 pm PT
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1	October 28, 2016	Updates for AMM 2.15.2

➤➤| Contents

1: Introduction

This document provides instructions for using the AirLink® Mobility Manager (AMM) user interface, reports, and optional applications. The AMM can be hosted by Sierra Wireless or purchased as a standalone server appliance. Note that the hosted version offers fewer administrative functions and does not support ALEOS devices.

Note: the AMM was formerly known as the oMM in versions prior to 2.15.2; this document references those older versions as "oMM" where applicable

1.1 Who Should Read This Guide

AMM users typically include fleet dispatch operators, fleet managers, IT support staff and vehicle maintenance staff.

1.2 What is the AMM

The AMM is a powerful browser-based software application that enables users to configure, monitor, and analyze Sierra Wireless gateways and associated applications/accessories (such as Asset Manager WiFi tags).

As of Version 2.15, ALEOS devices in addition to oMGs, are supported. The main difference between oMGs and ALEOS devices with regards to how they work with the AMM is that oMGs have constant two-way communication with an AMM when an Internet connection is available, where as ALEOS devices only check in with the AMM at schedule intervals (e.g. Heartbeat).

This means that oMG devices can transmit data to the AMM in near real time and commands can be sent from the AMM to the oMG immediately. For ALEOS devices, data can only be collected when a device checks in with the AMM, and any commands issued to the ALEOS device (e.g. a schedule software upgrade) will not be initiated until the check in occurs.

Each oMG collects operational data in a log (e.g. connection status, data transmitted/ received, temperature of the unit, voltage of the vehicle, GPS location data, etc.). The data logs from the gateways are transmitted over a wireless data network to an AMM server. The AMM uses these data logs to present current and historical activity.

The AMM is highly configurable to enable great flexibility between customer situations. Business intelligence-style data presentation and reporting enable users to leverage the large amount of data available from the gateways.

The AMM is available both as a "Hosted" version which is operated by Sierra Wireless, and as a standalone appliance which can be purchased and administered by a customer as an on-premise solution.

In this document an oMG and/or ALEOS gateway is often just referred to as a gateway. The gateway hardware is typically installed in a vehicle but it can also be installed in offices or depots to take further advantage of the system's capabilities. Note that since a gateway is often installed in a vehicle, the term is often also used in place of the word "vehicle".

1.3 AMM Hardware Appliance Requirements

1.3.1 Appliance Requirements

The AMM hardware appliance is to be installed in a shelf rack within a secure, climate-controlled space such as a data center that can provide 120 AC power and access to the Internet (or your external network of oMGs) as well as the enterprise network. Dell factory-supplied rails are included for this installation.

For oMG fleets of 200 gateways or less and 10 concurrent interactive users, the Dell specification is:

- PowerEdge R220 or equivalent chassis
- Quad Core Processor 2.4 GHz or higher
- Minimum 8GB RAM Memory
- 500GB storage minimum (2GB/oMG/year recommended)
- Gbit Ethernet[1]

For oMG fleets larger than 200 gateways, the Dell specification is:

- PowerEdge R630 or equivalent chassis
- 2xQuad Core Processor (8 cores) 2.4 GHz or higher
- Minimum 16GB RAM Memory
- 1TB storage minimum (2GB/oMG/year recommended)
- Gbit Ethernet

Since, the AMM is designed to operate 24x7, an uninterrupted power supply (UPS) should be used.

For installation purposes, you will need to supply:

1. VGA cable and local monitor.
2. USB keyboard.
3. Ethernet network interface cable.
4. Ethernet network interface cable to internal network.
5. AC power (connected via included power cord).

1.3.2 VM Requirements

The AMM VM virtual machine has the following requirements:

---

1. The AMM only supports one network interface card.

- VMware ESXi 5.0 or higher.
- For fleets consisting of less than 200 gateways and 10 concurrent interactive users, Sierra Wireless recommends a VM instance with at least 8GB of memory and four virtual processors.
- For larger fleets, Sierra Wireless recommends a VM instance with at least 16 GB memory and eight virtual processors.
- For storage requirements, space should be provided for a minimum of 2GB per gateway per year of data retention, with provisions to increase capacity as fleet requirements grow.

1.3.3 External Network Access

The AMM must be network-accessible to the gateways it manages.

1.3.3.1 Simple AMM Networking Method

For gateways that employ standard data plans that communicate over the Internet, the AMM must have a publicly accessible fully qualified domain name (FQDN) and corresponding unique public IPv4 address.

For example, an AMM hosted by Sierra Wireless uses:

omm01.inmotionsolutions.net

1.3.3.2 Advanced AMM Networking Method

For gateways that employ a private networking cellular service from a carrier and optionally employ a second WAN interface such as Wi-Fi, network access to the AMM must still be provided. The network design and implementation for this method is outside the scope of this document. However the end result is that the AMM is typically assigned a private address and host name within the enterprise.

1.3.3.3 Firewall Considerations

The AMM has an integrated firewall that defends against unauthorized access and therefore it may be installed with direct access to the Internet. However the AMM may also be installed behind a firewall provided that certain ports are made accessible through the firewall.

Refer to Firewall Considerations for IP ports required by AMM.

1.3.3.4 oMG Re-Homing

oMGs can be configured to home in onto a particular AMM explicitly. However, Sierra Wireless recommends that the default oMG behavior be relied upon to perform an automatic location look-up of a unit's designated AMM via DNS.

Note: this requires that access to an external DNS service is available and therefore may not work for private-only networks.

The DNS-based location method uses a high-availability DNS service managed by Sierra Wireless. This DNS service is the authority for the *omgservice.com* domain. oMGs that use automatic lookup discover their AMM by resolving their serial number within the omgservice.com domain. For example:

H1301111G0001.omm.omgservice.om

would refer to omm01.inmotionsolutions.net.

The target AMM should be determined prior to deploying oMGs by contacting Support and requesting DNS redirects for the units in question.

If the recommended DNS-based method is anticipated, it may affect where you physically locate the AMM (so it connects to the appropriate network segment within your enterprise) and influence your naming and addressing choices. For example, your AMM may need to be explicitly included in your APN configuration by your service provider.

1.3.3.5 Internal Network Access

In order for operations staff to use the management functions of the AMM, their workstations must be able to access the server.

If operators reside outside the facility where the AMM is installed, this section may not apply.

If your operators reside within the same facility (i.e. on the same enterprise network) as the AMM, the AMM server will be directly connected to the enterprise network. In this case the AMM must be assigned a unique internal name and IP address to the AMM.

This may require two measures:

1. The internal DNS server should be changed so that user workstations can locate the AMM.
2. The second network interface of the AMM may be connected to provide internal network access.

1.3.3.6 Operator Station Requirements

The AMM provides a graphical user interface for operators to access management functions via a web browser.

The AMM is certified to operate with PC workstations running various browsers listed below in Supported Browsers.

The AMM user interface is not designed to operate on tablets or smart phones.

The web browsers must have cookies and Javascript enabled.

Some features of the AMM such as maps, integrate local data produced from the server with remote web based data. Maps are used primarily for location-based coverage reports and require that user desktops be able to access the following map services:

- For oMM versions below 2.12: Microsoft Maps (dev.virtualearth.net)
- For oMM 2.12 and above: Google Maps (maps.googleapis.com)

1.4 Supported Gateways

AMM works with the following gateway versions:

- oMG 3.14.1 and above[1].
- AirLink devices with ALEOS software versions 4.4.x and higher. Note that ALEOS devices are not supported in hosted versions of the AMM.

Note: the AMM generally handles oMG 500/2000 and MG90 devices in a similar manner, with the exception of the Software Repository and Software Distribution features where the MG90 is managed differently. Where appropriate, all references to "oMG" in this document refer collectively to oMG 500, 2000, and MG90 devices.

1.5 Supported Browsers

oMM 2.15 and above has been tested on Internet Explorer 11.0. Other supported browsers include Chrome and Firefox. The AMM application requires the use of browser "cookies". Ensure that this option is enabled on your browser before logging into the AMM.

Other types of workstations (e.g. Linux Desktop, Mac) may also work but have not been certified to operate with the AMM.

1.6 Supported Features for ALEOS Devices.

Support for ALEOS devices was added to the oMM starting in version 2.15. See Features Supported for ALEOS Devices for a full list of AMM features that are supported/available for ALEOS devices.

Note: when a fleet of mixed ALEOS and oMG devices is selected, additional menus applicable only to oMG devices may also be shown. For customer fleets consisting of only ALEOS devices, these additional menus will be disabled. If oMG devices are added and selected, these menus will become enabled.

Note: only AMM appliances that are purchased by customers can support ALEOS devices. AMMs hosted by Sierra Wireless currently don't support ALEOS devices.

1.7 Determining the Version Number

The version number is displayed on the login page, under the user name and password fields. The version number can also be obtained when logged in by selecting the *Help->About* menu.

---

1. All oMGs must be upgraded to 3.14.1 or later prior to upgrading to AMM 2.15+.

Table 1-1: oMM Version Numbers

Version	Details
oMM 2.15	May 5, 2016
oMM 2.14	August 21, 2015
oMM 2.13	October 8, 2014

1.8 Related Publications

Table 1-2: Related Publications

APP-ED-101101 - Tracker User Guide	Provides information for the Tracker application.
oMG-ED-100801 - Four Port oMG Telemetry Configuration Guide	Provides information for the Telemetry application.
APP-ED-110301 Asset Manager Configuration and User Guide R1.6	Provides information for asset tags and the Asset Manager.
oMM-ED 101001 Nav Operation and Configuration Guide	Provides information for the Nav application.
APP-ED-101102 Passenger WiFi App Config Guide	Provides information for the passenger WiFi (aka "web portal") application.
4118618 oMG Operation and Configuration Guide for R3 3.9	Provides information about operating the oMG.
4119940 - AMM Report Guide 2.15.2.pdf	Provides information about the reports that can be run from the AMM.

All related documentation is available from http://source.sierrawireless.com.

2: Overview

The AMM enforces security by requiring each user to login with a name and password. When purchased as a standalone appliance, an administrator user account is provided which can be used to grant permissions to other users. Once logged in, users are presented with a sophisticated web user interface consisting of a hierarchy of gateways, graphical icons and links. The following sub-sections describe these features in more detail.

2.1 Logging In

A user name and password is sent to customers for their first log in. To change this password, or to add more users, contact Support.

To safeguard your login credentials, ensure that your browser does not store your user name and password unless you are confident that no one can access your computer.

Note that the version of the AMM is shown below the login fields.

Figure 2-1: AMM Login Screen

Note: the system will log out the current user after 30 minutes of browser inactivity.

2.2 General Layout

The main user interface used throughout the AMM consists of the following key features:

Gateway Tree: displays a hierarchical view of the gateways and groups of gateways currently managed by the AMM.

Filter Field and Nav Icons: provides tools for filtering the list of gateways and refreshing the list.

Main Tabs: displays the available views for both built-in applications/features and any optional applications which are installed.

Option Tabs: provides tools for filtering items and information.

User Name: displays the name of the user currently logged into the AMM.

These features are described in more detail in the following sub-sections.

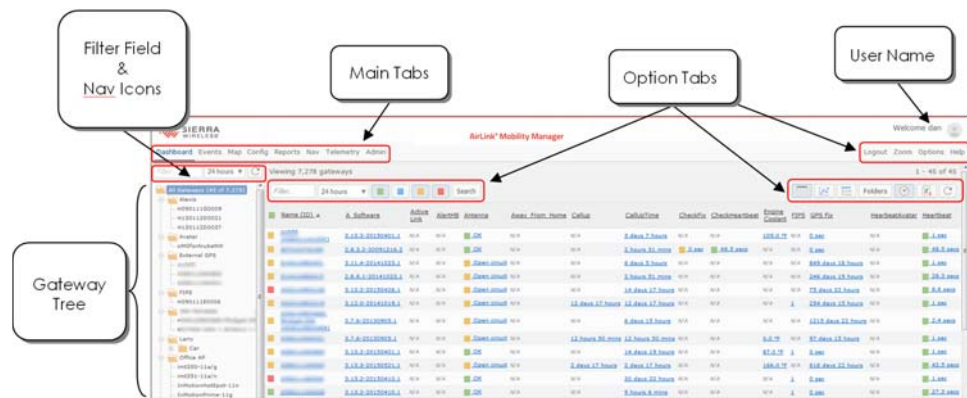The Dashboard view, shown below, is the default view.

Figure 2-2: General Layout of the AMM

2.3 Tabs

The main tabs located at the top left of the screen are used to select different presentations of available information.
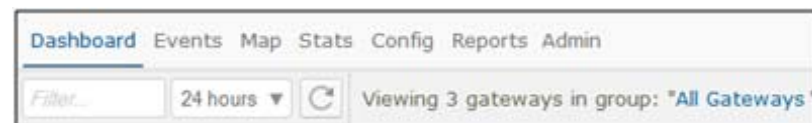

Figure 2-3: AMM Tabs

For more details for the individual tabs, see Chapter 3 - Main Tabs.

2.3.1 Option Tabs

The option tabs located at the top right of the screen, are used to select one of the following actions:
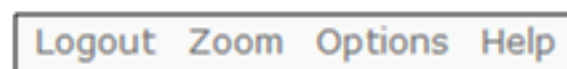

Figure 2-4: Option Tab

Logout: logs the current user out of the AMM and displays the login screen.

Zoom: hides/shows the navigation tree and heading information (AMM title, Sierra Wireless logo and currently logged in user) to provide additional screen real estate for use by the current view.

Options: display menus for configuring maps, showing/hiding advanced report options by default (same as clicking *Show Advanced Config* on a report's configuration screen), and setting preferences.
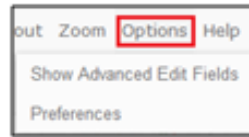

Figure 2-5: Menu items under Options Tab

Show advanced edit fields: Provides the ability to display advanced edit fields primarily in report set up.

Preferences: Select to modify the user preferences, including Dashboard items. Some or all of the following settings are available for modification depending on your user security level:

- *Identification parameters*:
  - **Name***: enter the new user name
  - **Email**: enter the email address to associate with the user.
  - **Customer group**: use the drop-down menu to select the group for which the ID is being created.
  - **Password & Confirm**: enter the password in both fields. Used when the AMM performs authentication.
  - **Remote Authentication**: will be available for selection when a Customer Group is selected which has been configured with LDAP authentication (see LDAP for more information). Enabling this field will hide the *Password* and *Confirm* fields and will authenticate using the LDAP authentication configuration which has been configured for the Customer Group.
  - **Expiry**: if an expiry date is required for the ID, click in the expiry field and a calendar will open. Select the expiry date for the ID.
- *Privileges*:
  - **AMM**: select the privilege - None, Read or Read/Write.
  - **Tabs**: select the tabs for which the user will have access. Note that the tabs available depend upon the optional packages purchased.
  - **Reports**: select which reports will be available to the user.
  - **Stats**: check All to enable Stats (default).
- *Preferences*:
  - **Measurement units***: select Imperial (default) or Metric.
  - **Position Format**: select the GPS coordinate format to use for reports: decimal degrees (default) (e.g. 49.206052, -122.91309), or degrees minutes-decimal minutes (e.g. 49:012.363 N,122:054.785 W).
  - **Format CSV output values same as HTML**: forces the exported Excel output to be in the same format as specified by the Position Format option. When this option is not selected, the format outputted to CSV will default to decimal degrees.
  - **Dashboard Timespan**: specifies the default timespan for which to display items in the dashboard.
  - **Tracker refresh***: enter the refresh rate, in seconds, for the tracker refresh.

- **Dashboard refresh***: enter the refresh rate, in seconds, for the dashboard refresh.
- **Oldest report***: enter the number, in days, for the oldest report available.
- **Max concurrent logins**: enter the number of maximum concurrent login connections. By default, there are no restrictions (blank implies no restrictions).
- **Restricted IP**: limits logins from a range of IP addresses.
- **Maximum threshold emails per day**: enter the maximum number of threshold emails the user will receive per day (blank implies unlimited).
- **Nav Stop List**: determines the order that the Nav stops are displayed (only available when the Nav package has been purchased).
- **Time zone**: use the drop-down to change the time zone for the user. The default is the server's time zone. For a list of time zones supported by the AMM see: Supported Time Zones.
- **Dashboard items**: specifies the dashboard items available to the user. Deselect to create a custom list of items to be made available. For default items see Parameters.
- **Telemetry Dashboard**: limits the telemetry stats available to the user. Deselect to create a custom list of items to be made available.

- Click **Save** to create the user ID.

Users can be deleted from the gateway by clicking in the checkbox next to the user label and then on **Delete**.

* denotes a required field

Help: displays menus for help and information related to the AMM.

- **Help**: opens the online help feature for the AMM.
- **About**: displays information about the version number of the currently running AMM.

2.4 Gateway Tree

The gateway tree located on the left side of the screen, allows users to select vehicle groups, sub-groups and individual gateways. The look and feel is similar to traditional file management systems with folders and files.

Click on the group/sub-group/individual gateway to select it. This selection will remain active when toggling between the main tabs (e.g. Dashboard to Map). Additionally, when running reports, the gateway field is automatically populated and can be changed by clicking on another group/sub-group/gateway. Multiple items can be selected by holding down the Control (Ctrl) key while clicking.
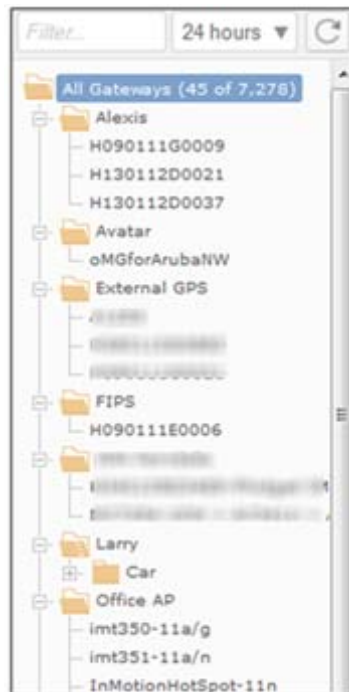
Figure 2-6: Gateway Tree

2.4.1 Filter Box and Searching

The Filter field for the gateway tree, as well as many other search boxes throughout the AMM, allows users to enter the full or partial name of a gateway to search for.

The search is not case sensitive and performs wildcard searches by recognizing the following patterns from the keyword entered in the search box:

- **!<keyword>**: if the keyword starts with '!' (e.g. "!abc"), gateways with no fields containing the sub-string will be returned.
- **0-10**: if the keyword contains two numbers separated by "-", gateways with numerical fields which fall in the range enclosed by these two numbers inclusively, will be returned.
- **Regular Expression**: the keyword will be used as regular expression, if the two patterns above don't match on any fields.

In Figure 2-7 the image on the left shows the list of gateways displayed when nothing is entered in the *Filter* field (i.e. show all gateways). The image on the right shows only gateway names containing "H0". After entering or changing a value in the filter field, the refresh button to the right of the time dropdown can be clicked to refresh the list. Alternatively the list will refresh on its own after a few seconds.
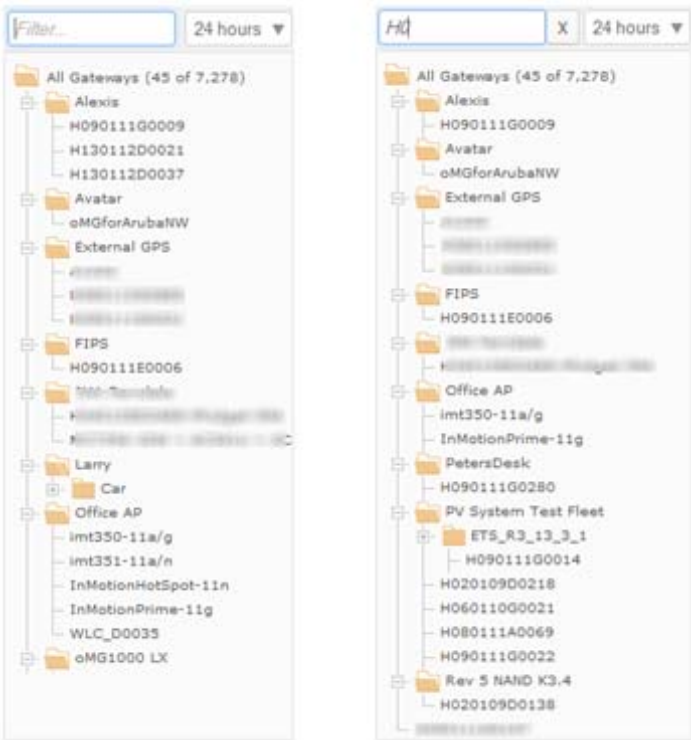
Figure 2-7: Filter Box in Gateway Tree

Text in the *Filter* field can deleted, by clicking on the **X** icon which appears to the right of the field when text has been entered.

2.4.1.1 Gateway Tree Filter Options
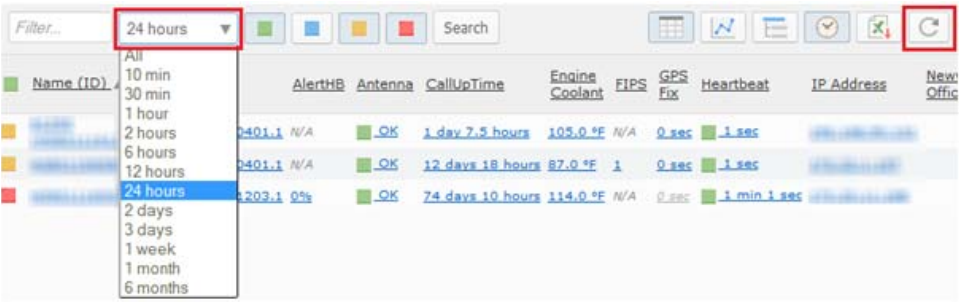
The following fields are also used for filtering:

Figure 2-8: Filter Options

Time Dropdown: click on the drop-down menu to limit the gateways displayed to those which have actively reported data during time period selected. The default value is *24 hours*.

Refresh: click to show the latest available list of gateways/groups. This button must be clicked when entering or changing the filter text or when a new gateway has been deployed.

2.4.2 Groups and Sub-Groups

Groups allow gateways to be categorized and grouped together for organizational purposes. For example, different groups could be created to organize fleets for different departments. Sub-groups can be created under other groups for additional subcategorization.

To manage groups and sub-groups in the gateway tree, right-click on a group name and select one of the options listed below:
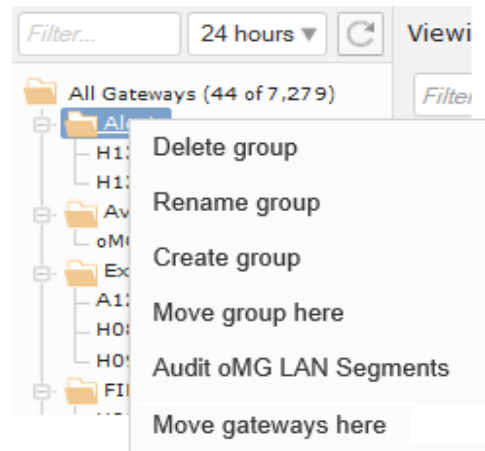

Figure 2-9: Group Context Menu

Delete group: select to delete a particular group.

Rename group: select to rename a group.

Create group: select to create a group of gateways.

Move group here: select to move a group to a particular group.

Audit oMG LAN Segments: select to trigger the AMM to cross reference the LAN segments configured for all the oMGs within the selected group to ensure that there is no conflict/overlap between them. This is useful for managing a fleet that is peering to the same oCM (or VPN server), where overlapping subnets will cause confusion for the VPN server and will be flagged as a configuration error when running the audit.

Move gateways here: click on a gateway to select it. Right-click on a group and select this option to move the gateway to the group.

Note: the menus available will vary depending on whether the node selected represents an oMG, ALEOS device, fleet of devices, or a mixed fleet of devices.

2.4.3 Changing Gateway Details

When setting up a fleet of gateways, several fields exist to help identify and group each gateway. To change these details, right-click on a gateway and select one of the options listed below:
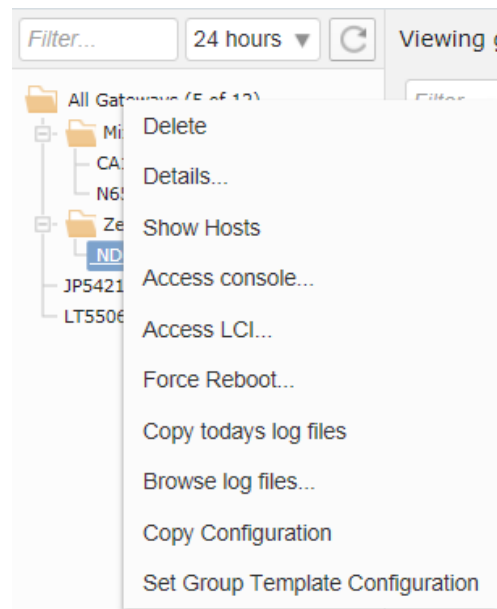
Figure 2-10: Gateway Context Menus.

Delete: select to delete a particular gateway.

Details: opens the *Add or Edit Gateway* panel in a new browser. Users can update gateway details. For more information about the options available in this panel, see Gateways.

Show Hosts: displays a list below the gateway's node, listing the host devices connected to that oMG.

Access Console: provides SSH (shell) access to the selected oMG. The IP address and port are provided which can be copied and pasted for use when connecting using a 3rd party SSH application.

Access LCI: remotely connect to the oMG's Local Configuration Interface (LCI) screens.

Request Reboot: forces an oMG to reboot, or instructs an ALEOS device to reboot next time it checks in with the AMM. Note that a login and password are required for the oMG.

Browse log files (oMG devices only): shows log files that were previously uploaded to the AMM.

Copy today's log files (oMG devices only): forces the oMG to upload all log files generated today. Under normal operation, critical logs are uploaded hourly, while the remaining log files are only uploaded once a day.

Copy Configuration: copies the configuration files from one gateway to another.

Set Group Template Configuration: uses the oMG's configuration as the template configuration for the parent group containing the oMG. This template configuration will used as the starting point for the group's provision configuration which can then be modified and even overridden in sub groups and/or the oMGs contained within the group. Note that the selected oMG must be in the In Sync state. For more information see: Provisioning.

Note: the menus available will vary depending on whether the node selected represents an oMG, ALEOS device, fleet of devices, or a mixed fleet of devices.
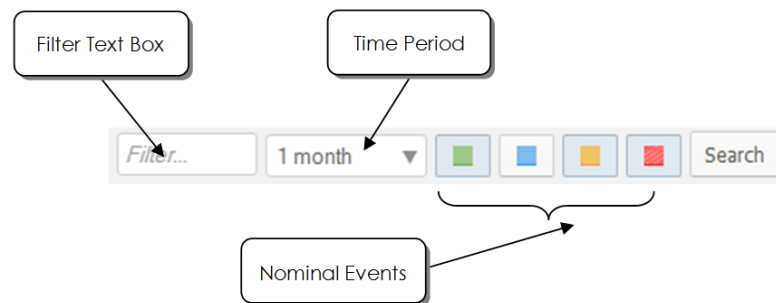
2.5 Main Display: Filtering and Options

Figure 2-11: Location of Filter and Option Fields

2.5.1 Filter Text Field

Filters gateways by name or group name. In addition to selecting a group of gateways from the gateway tree, the Filter Text field allows users to further filter selections by entering part or all of the gateway or gateway group name.

Once the filter text has been entered or changed, click on **Search** to initiate the search request.

2.5.2 Time Period

Select a time period from the drop down list. Only gateways which have reported data to the AMM (over a WAN) within the selected time period will be displayed on the map. This allows users to quickly find and manage only those gateways which are active.

2.5.3 Nominal Events

Nominal events include any event where a threshold is exceeded. See Thresholds for further details.

Use the nominal events icons to display the gateways for the defined thresholds.

The colored circles are defined as follows:
- **Green**: operating normally within the thresholds
- **Blue**: no data available
- **Yellow**: warning level threshold exceeded
- **Red**: error level threshold exceeded

The *Default* setting has the *Green*, *Yellow*, and *Red* events on for all gateways.

3: Main Tabs

Located at the top left of the screen, the main tabs are used to navigate through the various presentations of the information available in the AMM. Click on a tab to select the view.

The tabs available depend upon the purchased options and the overall configuration of the system. The main tabs cannot be altered by individual users. However, administrators can add and remove tabs (go to **Admin > Users**) if they own their own appliances. Clients using hosted services from Sierra Wireless do not have the *Admin > Users* option.

Note: the order of tabs is specified by AMM administrators for each user.
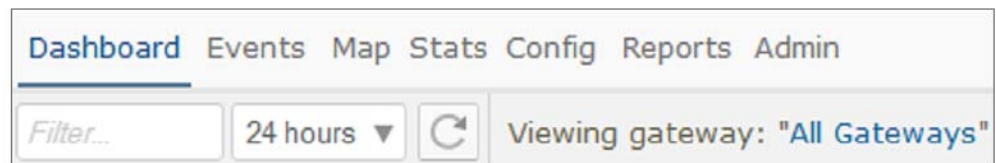
Figure 3-1: View of Main Tabs

3.1 Dashboard

The *Dashboard* provides the main management view of the fleet. There are three views available: *List*, *Graph,* and *Threshold*.
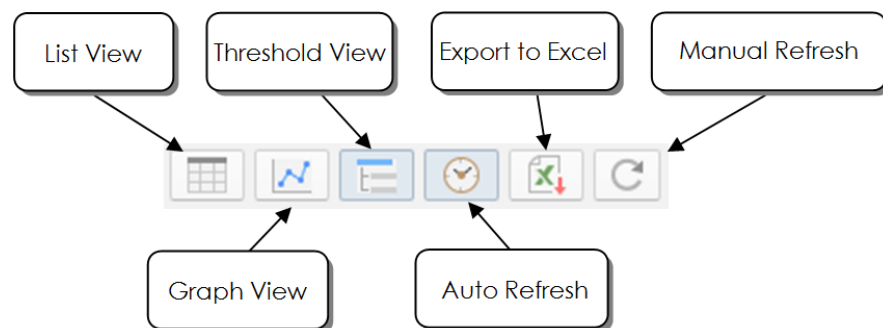
Figure 3-2: Dashboard Buttons

List View: the *List* view is the default view for the dashboard. Each parameter is presented in columns, with each gateway appearing as a single row.

Figure 3-3: List View

Graph View: The *Graph* view displays the same parameters as the List view but represented in graphical form. Gateways are represented on the Y axis, with the parameter value on the X axis.
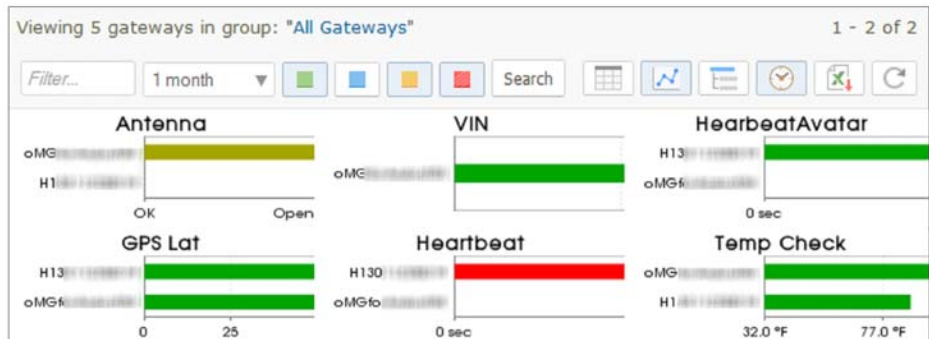

Figure 3-4: Graph View

Threshold View: the *Threshold* view provides a summary for each parameter, including:

- totals of each threshold status for the group of gateways selected.
- a minimum value for each parameter for the group of gateways selected.
- a maximum value for each parameter for the group of gateways selected.
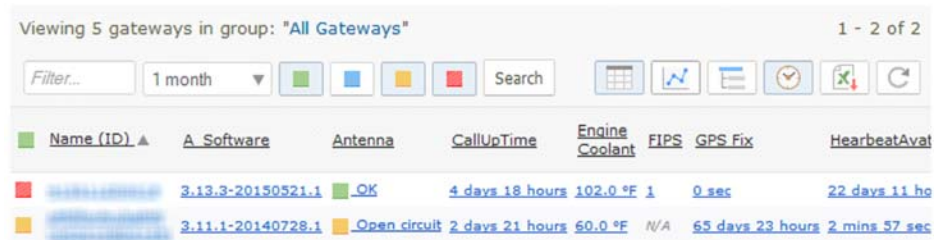

Figure 3-5: Threshold View

This view is beneficial because it provides a quick view of the parameters that are out of threshold. The list of statistics displayed on the dashboard is also configured through **Admin > Thresholds**.

Auto-refresh: clock icon. When enabled, the browser page is automatically updated (default is 30 seconds).

Refresh: manually refresh the AMM with the latest gateway information.

3.1.1 Dashboard: List View

The *List* view is the default view for the dashboard. Each parameter is presented in columns, with each gateway appearing as a single row.

Figure 3-6: List View Showing Various Parameters

3.1.1.1 Parameters

The *Dashboard* items are made available by creating thresholds (see Thresholds for more information). These are listed as parameters in the column headings, and descriptions for each row's fields can be displayed by hovering the mouse over them.

The default parameters are:

Name (ID): displays the gateway's serial number. If a name was given to the gateway during set-up, this field will display the name along with the serial number in brackets.

CallUP Link: the amount of time the call is up for the WAN connection.

Heartbeat: the time since the gateway last sent data to the server. The format is HH:MM:SS.

IP Address: the IP (Internet Protocol) address assigned to the most recent Internet connection made by the gateway.

Battery: the voltage level of the vehicle's battery supplying power to the gateway. The gateway has a built-in voltage meter which monitors voltage and shuts down the unit if voltage levels are too low or too high. Note that voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.

GPS Fix: the time since the gateway last reported its latitude/longitude coordinates.

Satellites: the gateway is equipped with a multi-channel GPS receiver. The number shown is the number of GPS satellites from which the gateway is currently receiving signals.

Temp Check: the temperature of the gateway, measured in Celsius (^{0}C). The gateway has a built-in temperature sensor.

Note: the available parameters may vary depending on the type of device(s) selected in the Gateway Tree.

Note: CallUP Link is not supported for ALEOS devices as of AMM 2.15.2.

3.1.2 List View: Color Coding

Color coded icons indicate the status of parameter values in relation to their defined thresholds:

- **Green**: operating normally, within thresholds
- **Yellow**: warning level threshold exceeded
- **Red**: error level threshold exceeded
- **Blue**: no data available

Note that the colored icon next to the name/serial number in the gateway list panel indicates the overall health of the gateway. The color will be based on the worst case threshold value from amongst the gateways thresholds displayed on the Dashboard.

Figure 3-7: Color Coded Icons

For example, the threshold for the 12V battery in a vehicle is typically set up to generate a warning threshold (yellow) for voltages less than 10.8V or greater than 14.7V. The error threshold (red) is set for voltages less than 10.5V or greater than 15.0V. If all other parameters are within the thresholds set (i.e. green) but the battery falls at 10.7V, then the colored icon next to Battery will be yellow. A yellow icon will also be present next to the gateway name/serial number. Note that voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.

3.1.3 List View: Sorting

Data displayed in the list view columns can be sorted by clicking on the column header. The triangle indicates which column is being sorted. When the triangle is pointing up, data is in ascending order and when pointing down, it is in descending order. By default, rows are sorted by the Name (ID)

Figure 3-8: Column Headings with Arrow Indicating Sort Order

3.1.4 Dashboard: Graph View

The *Graph* view displays the same parameters as the List view but in graphical form. Gateways are represented on the Y axis, with the parameter value on the X axis.

Values within defined thresholds appear green. Any values that are outside of defined thresholds appear as yellow (warning state) or red (error state).
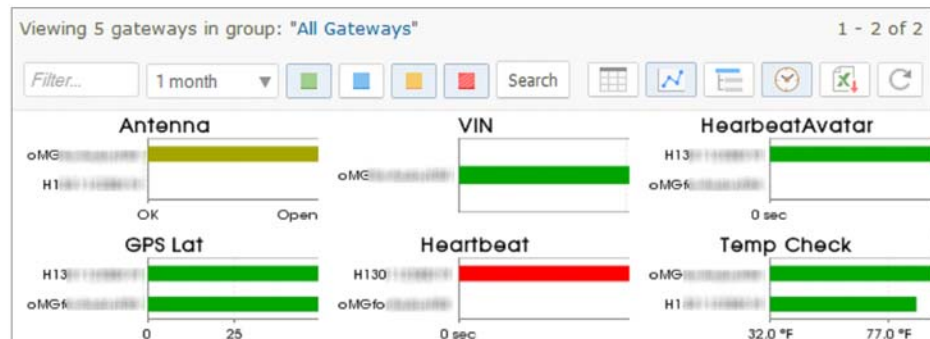

Figure 3-9: Graph View

3.1.5 Dashboard: Threshold View

The *Threshold* view provides a summary for each parameter, including:

• totals of each threshold status for the group of gateways selected.
• a minimum value for each parameter for the group of gateways selected.
• a maximum value for each parameter for the group of gateways selected.

This view is beneficial because it provides a quick view of the parameters that are out of a threshold.

Figure 3-10: Values Exceeding Thresholds

To display additional information about the status of the gateways, click on a numeric value in a column.

Figure 3-11: Additional Threshold Details

To see how a particular parameter is configured, click on the ellipsis (…) beside the parameter name to open the *Edit Threshold* panel. This will open the panel in a new browser window and allow parameter changes to be saved (for more information see Thresholds).

3.2 Events Tab

Gateways record a wide variety of information and diagnostics about their usage, and report this information as "events".

The *Events* tab provides a quick way to view events received by the AMM for a specific time period. For advanced users, this feature is useful for testing or troubleshooting gateways.
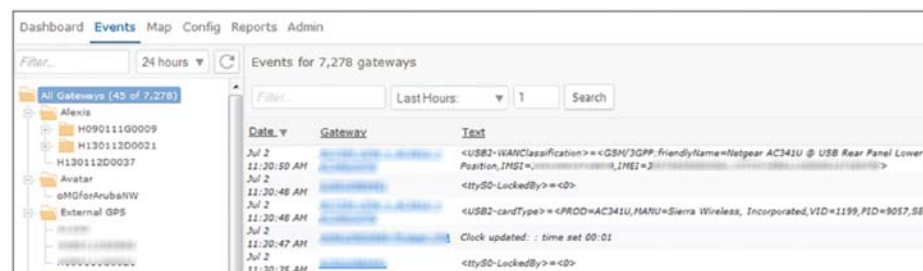
Figure 3-12: Events Tab

To view events:

- select a group, sub-group or individual gateways from the gateway tree.
- enter text in the *Filter* field to help narrow the scope of the search. For more information about searches see: Filter Box and Searching.
- use the time range drop-down box to select the time period for which to display the data. The options are *All, Previous Hours, Previous Days, Previous Months and Range*. Enter the numerical information in the corresponding box. The above image shows data from the previous 1 hour. Click on **Search** to call up the data.

The data can be sorted by clicking on the column header.

Click on the Excel icon to export the list of events to CSV format.

3.3 Map Tab

The *Map* tab provides a geographical view of a fleet using Google Maps. Use the gateway tree to select the group, sub-group or individual gateway to view on the map. Each gateway is shown at a location on the map according to the most recent location data transmitted.
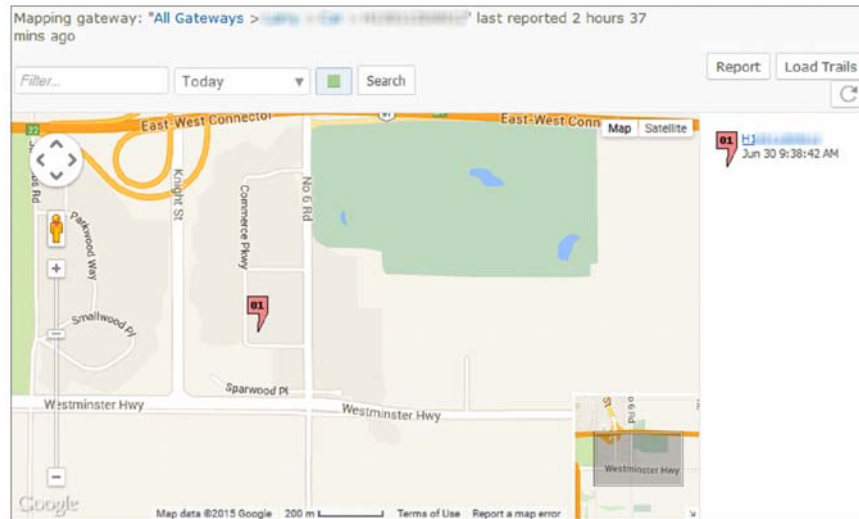
Figure 3-13: Map Tab

Gateways are identified using numerical markers, with a list of details by gateway shown to the right of the map. The color of the marker corresponds to the threshold color next to the gateway's name/serial number shown in the Dashboard. If a gateway has no issues it will be shown with a green marker, otherwise it will be shown in yellow if it has warnings or red if it has errors. To obtain detailed event information, click on a gateway marker on the map to show the information pop-up:

Figure 3-14: Gateway Marker Popup

The popup displays the following primary information:

Gateway ESN: the serial number assigned to the gateway.

Gateway ESN Hyperlink: when clicked, the map will zoom into the marker and also filter out any other markers. Doing so allows the user to focus solely on the current marker. Note that for informational purposes, the hyperlink text also contains the name of the tree folder (surrounded by "[" and "]" characters) in which the unit is contained (e.g. in the screenshot above, the unit is contained within a folder called "SJ oMGs").
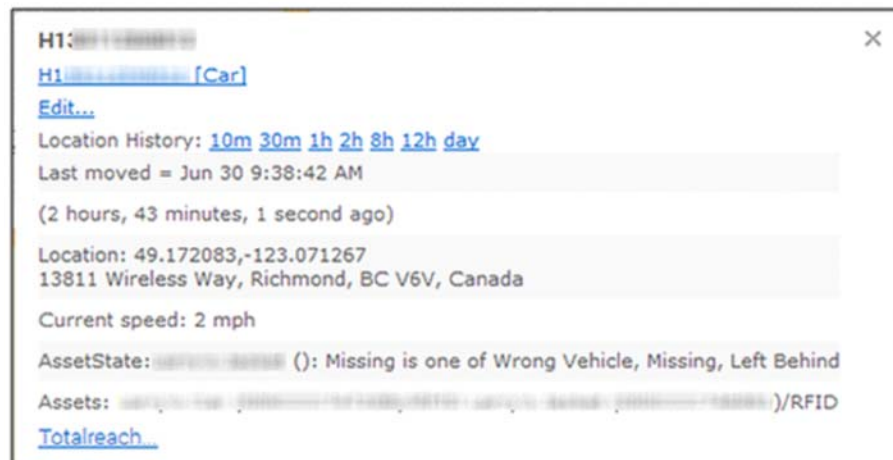
Location History: clicking on one of the time periods draws a path on the map showing where the unit travelled during that time frame in the past (e.g. clicking on *10m* will show where the unit has been travelling for the last 10 minutes). Note that the unit must have been travelling within selected time period. If the unit has been idle (e.g. for the last two days) then clicking on some or all of the time periods will not display a path.

Last Moved: the date and time that movement of the vehicle was last detected.

Location: the current location of the unit including both the GPS coordinates and address.

Threshold information: displays threshold names and values which have been configured for the selected device. Thresholds which have exceeded their defined ranges define the color of the marker (e.g. a red marker will be shown for a threshold that exceeds its range).

Click on the gateway name in the list to the right of the map, to center the map for a single gateway.

Click on **Load Trails** to show the path travelled by the vehicle.

Click on **Report** to generate a Gateway Trips report corresponding to the map.

Note: the Report button is available for ALEOS devices in AMM 2.15.2 and above.

Click on the **Refresh** button to refresh the map.

3.3.1 Navigating Within the Map

The AMM uses Google Maps for all map related screens which can be navigated as follows:

- Zoom in or out using the scroll button of your mouse. Hold the mouse pointer over the map location you wish to remain centered.
- Pan in any direction by clicking and holding the left button of your mouse, and dragging the map.
- To zoom using the map controls, use the (+) and (-) icons (shown in Figure 3-15) to zoom in and out.
- To pan using the map controls, press one of the four arrows in the white circle:

Figure 3-15: Google Map Controls

Additional Controls:

Click on **Map** or **Satellite** to display the respective map detail.

When displaying map level detail, hovering the mouse over *Map* will display a *Terrain* dropdown which when enabled, overlays the map with terrain features:

Figure 3-16: Map Level Detail with Terrain Enabled

Note that the Terrain dropdown will only be available when the map isn't zoomed in too far. Also, when the *Terrain* option is enabled, the level to which the map can be zoomed in to, will be limited.

When displaying satellite level detail, hovering the mouse over *Satellite* will display the following option:

• **Labels**: when enabled, displays map labels such as street names.

Figure 3-17: Satellite Level Detail with Sub Options Enabled

3.3.2 Filtering Gateways

The map view provides a number of options for filtering which gateways are displayed on the map:

Figure 3-18: Map Filter Fields

Filter field: similar to the filter in the gateway tree. Enter part of the name (or other gateway labeling data) in the box to limit the gateways displayed.

Time dropdown: a time period can be specified when viewing the map to show where the selected gateways were located within that time period. The location(s) shown are based on when the gateways last reported data over the WAN to the AMM within the specified time period. To specify a time period, select the desired time period from the dropdown, enter the time range (if applicable) and click **Search**.

The following options are available from the dropdown:

- **All**: displays the last known location(s) of the selected gateways.
- **Today**: displays the last known location(s) of the selected gateways for the current day.
- **Last Hours**: displays the last known location(s) of the selected gateways within the last number of specified hours. Selecting this option displays an edit field where the value can be entered.
- **Previous Days**: displays the last known location(s) of the selected gateways within the last number of specified days. Selecting this option displays an edit field where the value can be entered.
- **Previous Months**: displays the last known location(s) of the selected gateways within the last number of specified months. Selecting this option displays an edit field where the value can be entered.
- **Range**: displays the last known location(s) of the selected gateways within the specified date range. Selecting this option displays two edit fields in which the start and end of the range can be specified. Clicking in these fields displays a date chooser widget. Alternatively the date can be manually typed in.

Nominal Events: represented by the green box icon. When selected, shows all gateways, including those operating within threshold limits (green). When de-selected, only gateways in warning (yellow) or error (red) state are visible.

Search: when clicked, searches for the selected gateways over the specified time period. For more information about searches see: Filter Box and Searching.

Report: displays the *Gateway Trip* report for the selected gateways over the specified time period. For more information see the AMM Reports guide.

Load Trails: displays lines showing where the gateways traveled during the specified period.

Manual Refresh: refreshes the page to show the latest information.

3.4 Tracker Tab

Tracker utilizes the GPS and data transfer capability of the oMG to record location and other related information on the AMM. These locations, along with data such as speed, direction (North, South, etc.) and time are used to show current or historical gateway activity. Tracker provides map and list views of the data, detailed reports, and the ability to export data for further analysis.

Tracker is currently targeted at the following markets:

- EMS
- Fire
- Law Enforcement
- Utilities / Large Commercial Fleets

Tracker is not designed as a full replacement for a Computer Aided Dispatch (CAD) system. It is a location tracking system designed for flexibility across verticals.

Note: as of AMM 2.15.2, Tracker is included as a core app. In oMM 2.15.1.1 and below, Tracker was provided as an optional add-on.

Tracker plots the geographical locations of all units/vehicles in a fleet or selected vehicles within a fleet as shown in Figure 3-19:

Figure 3-19: Tracker Tab Plotting Locations

The following options are available/relevant to Tracker:

Figure 3-20: Tracker Tab Options

Filter: use to filter vehicles by name or group name

Font Size: use this dropdown to select the font size point for Tracker labels on the map. This can be used to facilitate identifying the gateways. The default is 6pt.

Autocenter: by default, the map will automatically center the gateways on the map.

Traffic: displays traffic flow information on the map.

Find: locates an area on the map based on an address or a more general area (e.g. a city). The map will center on the address, but will not mark or indicate a specific location.

Use the drop-down menu to filter vehicles by time since the previous report. Nominal events (those operating within the threshold limits) are displayed by default (green circle icon). De-selecting the green icon displays only those gateways in warning and error states.

Clicking in the purple arrow displays only the gateways that have moved in the last 5 minutes.

3.4.1 Tracker Reports

Reports provide the true power of the AMM. Tracker-related reports are designed to be broad, with data export capability to allow for further analysis.

To generate Tracker reports, navigate to **Reports > Geographic**.

Reports that are related to Tracker include:

- **Geographic: Gateway Trip Trend** - shows the distance traveled per gateway per time unit including time spent moving and (related) average speed. This report is useful in identifying trends in vehicle usage across a fleet of vehicles.
- **Geographic: Gateway Trips** - plots the gateway location as a trail (continuous line) on the map (i.e. the route the vehicle traveled). This report is most useful for a single gateway over a relatively short period of time (e.g. one gateway trip) where the same location is not visited repeatedly.
- **Geographic: Gateway Trip Coverage** - plots a coverage map of locations visited by vehicles and uses color to represent the time spent in the area.
- **Geographic: Trip Replay** - animates a gateway trip over the time period selected. As the gateway (represented by a marker) moves over the map, it is followed by a colored trail which indicates speed and distance covered. The report is a spatial representation of gateway location history that is not available on the Gateway Trip report. It is useful for analyzing how often gateways cross paths with each other.
- **Geographic: Zone Summary** - provides a summary of time spent, as a percentage, in different zones across one or more units.
- **Geographic: Zone Times** - provides a time-based, visual representation of the zones visited by a gateway. The report is best used for a single gateway over a short period of time (one day is optimum) or as an in depth view to the Zone Summary report. It is useful for fleet managers who assign gateways to zones to monitor utilization.
- **Geographic: Zone Map** - reports the locations of a single gateway over a specific time period.

For detailed information on using and configuring reports, see the AMM Report Guide.

3.4.2 Configuring a Tracker User Account

Tracker user accounts are modified AMM user accounts, assigned by AMM administrators. Tracker users are typically only interested in a fraction of the AMM's functionality and the AMM administrator should customize the Tracker account for this purpose. A recommended set of features are:

- **Dashboard tab**: Customize the visible thresholds to display only the Zone indications so that other threshold conditions do not conflict with the zone threshold.
- **Event tab**: Useful to display historical locations.
- **Tracker tab**: Required to use the Tracker feature.

3.4.3 Basic Viewing and Operation

Tracker must be activated for each AMM account to be a visible tab in the AMM. Additionally, each oMG to be tracked must be set up to report GPS and related data at the correct frequency. Contact Sierra Wireless Technical Support for InMotion Solutions (IMS) for further details or to confirm that this has been completed for a particular gateway.

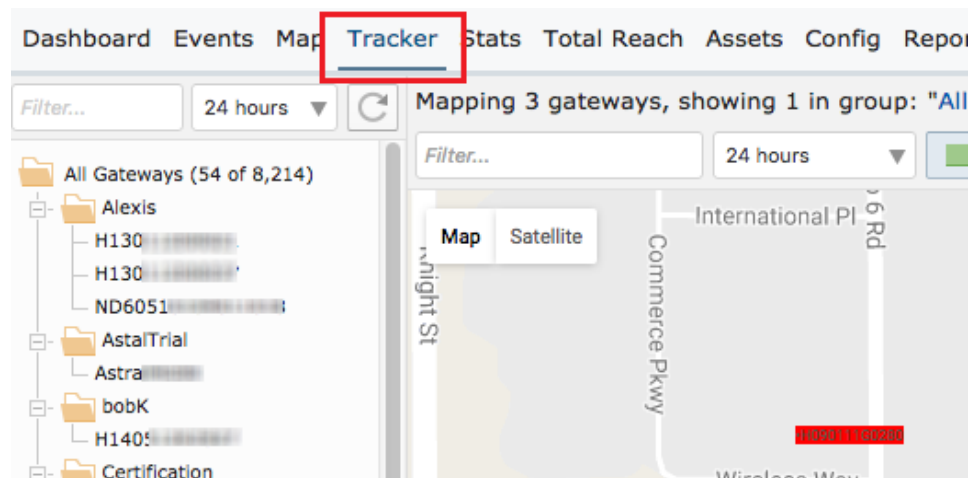To view the Tracker dashboard, click on Tracker in the AMM menu:

Figure 3-21: Location of Tracker Tab

3.4.4 Navigating within Tracker

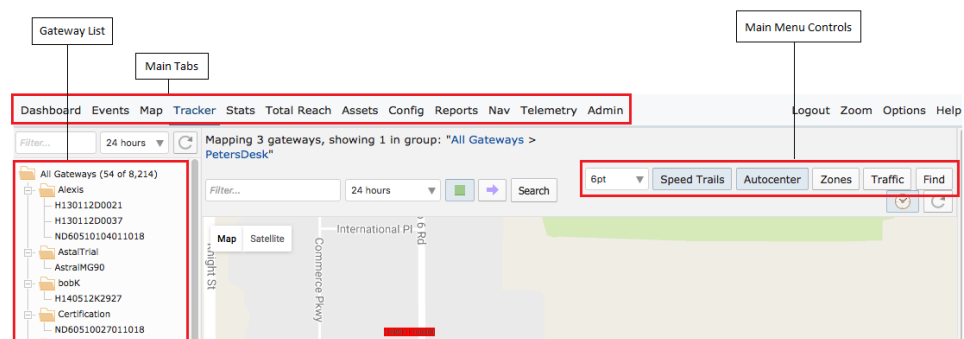The following navigational element's of the AMM are used for Tracker:

Figure 3-22: Main elements of AMM interface used for Tracker

- **Main Tabs**: used for selecting Tracker.
- **Gateway List**: used for selecting and filtering gateways to view with Tracker. For more information see Chapter 2.4 - Gateway Tree.
- **Main Menu Controls**: the following main menu controls are available:
  - **Font size dropdown**: Controls the size of the font for the gateway indicators on the map.
  - **Speed trails**: Toggles whether color-coded lines are shown indicating the speed of each gateway over its journey. When enabled, a legend is also shown at the bottom describing the speeds corresponding to each color.
  - **Autocenter**: Centers the gateway(s) on the map. If the map is set to refresh automatically, or is refreshed manually, the map re-center itself if a gateway reaches the edge of it.
  - **Zones**: Toggles predefined zones on and off. Zones are virtual geofences which track when gateways leave or enter a defined area. See Chapter 3.8.7 - Zones for more information.

- **Traffic**: Some mapping providers supply local traffic information. Check with your preferred mapping provider for more details about traffic information availability in your area.
- **Find**: Used to locate a street address or a general area on the map.
- **Autorefresh** (clock icon): When enabled, the browser page is automatically updated (default is 30 seconds).
- **Refresh**: Manually refreshes the map with the latest gateway location.

3.5 Stats Tab

The *Stats* tab provides a high level of detail about all aspects of a gateway's operations and is recommended for advanced users only.
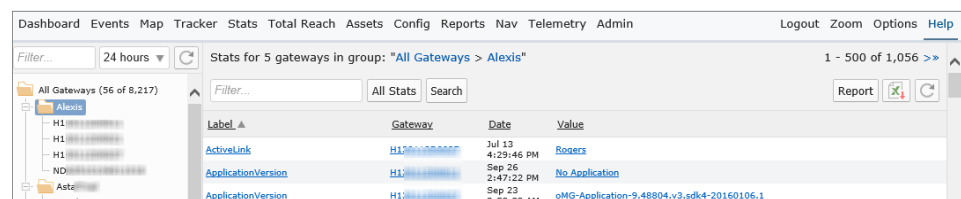
Figure 3-23: Stats Tab

Parameter (statistic) names are listed in the list view on the left of the screen. Results are displayed for the gateway(s) selected - group, sub-group or single gateway. Double-click on items in the list view to filter the corresponding stats (or alternatively, single click an item and then click **Search**). For example, filtering by *All GPS* will display all stats belonging to that type. Filtering by *All* will display each parameter reported.

For more information about searches see: Filter Box and Searching.

3.5.1 Views

The user may choose from several different views of the data found in the Stats tab:

Figure 3-24: Stats Tab View Buttons

Graph: display the Statistics Graph report configuration page where a report can be generated. For more information see the AMM Reports Guide.

Export: export the data to CSV format.

Refresh: manually refresh the information.

The example below shows a sample of data exported to Excel:

Table 3-1: Sample Excel Data

Date	Stat	Gateway	Value
3/21/2009 5:05	Link1-TotalrxBytes	H078	740,069
3/19/2009 17:01	Link1-TotalrxBytes	H078	2,050,218
3/19/2009 16:37	Link1-TotalrxBytes	H078	1,996,618
3/19/2009 16:11	Link1-TotalrxBytes	H078	1,937,808
3/19/2009 15:47	Link1-TotalrxBytes	H078	1,878,855
3/19/2009 15:03	Link1-TotalrxBytes	H078	1,803,895
3/19/2009 14:41	Link1-TotalrxBytes	H078	1,752,574
3/19/2009 14:13	Link1-TotalrxBytes	H078	1,700,738

3.6 Total Reach Tab

Allows users of the AMM to remotely access one or more devices (e.g. laptops, handhelds, etc.) in an oMG LAN or Vehicle Area Network (VAN) via the AMM.

Note: this feature is for oMGs only.

To use *Total Reach*:

1. Click on the **Total Reach** tab.
2. Select a gateway in the tree.
3. Click on the radio button to the left of the desired device in the list to connect to (see Chapter 3-25 below).
4. Click the button corresponding to the type of connection to use (e.g. VNC):
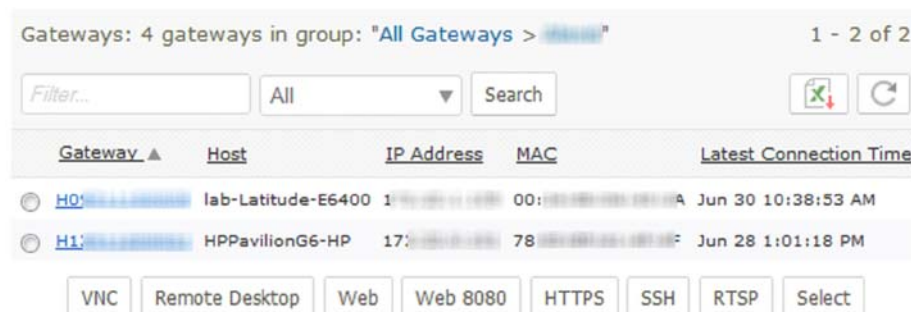

Figure 3-25: Total Reach Tab

Note: to connect to multiple devices, you must select each individually and click the desired connection button for each.

Total Reach provides the following methods of remote access:

VNC: runs a VNC (Virtual Network Computing) session to connect to a VNC server on a host (e.g. laptop) connecting to an oMG.

Remote Desktop: provides access using the RDP protocol. Devices need to have remote desktop enabled.

Web: provides access via the browser to web services/interfaces made available by the device on port 80 (e.g. a device configuration screen).

Web 8080: provides access via the browser to web services/interfaces made available by the device on (alternate) port 8080.

HTTPS: provides secure access via the browser to web services/interfaces made available by the device on port 443.

SSH: provides **a Java based SSH window for running SSH commands on the device.**

RTSP: uses *Real Time Streaming Protocol to view* streaming media. (e.g. if there is a camera hooked up, the video content can be viewed).

Select: provides access via the browser to web services/interfaces made available by the device on a particular port. Clicking Select will allow you to first select the port on which to access and then display the available web service/interface.

Note that AMM users must be granted Total Reach privileges by the AMM administrator in order to use Total Reach. Also, additional software (e.g. VNC software) may need to be installed on each device connected to the oMG for which remote access is to be enabled.

For more information see the *Total Reach User Guide*.

3.7 Config Tab

The *Config* tab provides access to the *Tracker*, *Copy*, *Upload*, *Deploy*, *WLAN WiFi Settings Import/Export*, and *WAN WiFi Security Import/Export* panels which are used for managing oMG configuration remotely. Access to these panels is organized under the *Provisioning, Deploy,* and *CSV Import | Export* sub menus under the *Config* tab.

3.7.1 Provisioning

The *Provisioning* menu allows for the configuration of VPNs and management tunnels on either a single oMG or groups of oMGs. This mechanism is also used by fleet operators to implement PSK rotation for VPNs. On oMM 2.14.x, this feature is supported for oMG versions 3.8 through 3.14. On oMM 2.15 and above, this feature is supported for oMG versions 3.14.1 and above.

Note: if an oMM running version 2.14 detects an oMG with a version greater than 3.14, assistance from Support will be required for provisioning. In this case the system will display a message indicating this condition when provisioning is attempted.

This provisioning system utilizes a hierarchy of configuration settings where by settings can be defined per group and either inherited or overridden by subgroups and/or individual oMGs within those groups.

Note: top level groups don't inherit any settings since there are no parent groups to inherit from.

Provisioning provides fleet operators with the flexibility to provision a fleet of oMGs while retaining the ability to provide unique configuration settings for specific oMGs or groups of oMGs.

3.7.1.1 Setting the Template Configuration

In order to provision a group, at least one oMG must have reported to that group and the configuration from a gateway within the group must be selected as the *template* configuration. Before provisioning a group for the first time, identify an oMG in the group whose configuration should be used as the template. Once identified, right click on that oMG in the Gateway Tree, and select **Set Group Template Configuration**. The settings from the oMG will be used to create a configuration for the parent group and the provision feature can then be used as described in the sub sections below.

3.7.1.2 Provisioning VPNs

VPN configurations are provisioned using the *Config->Provisioning->VPNs* menu.

Note: this functionality is for oMGs only.

In addition, fleet managers who use PSK rotation for VPNs (i.e. regularly change the PSK for VPN access to increase security) can use this provisioning feature to update oMGs or groups of oMGs with the new PSK credentials.

The VPN provisioning screen lists all VPN configurations for the currently selected item(s) in the Gateway Tree:
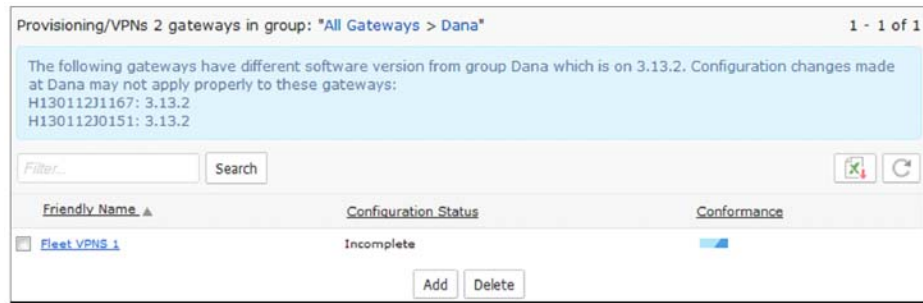
Figure 3-26: VPN Provisioning Listing Screen - Listing for a Selected Group
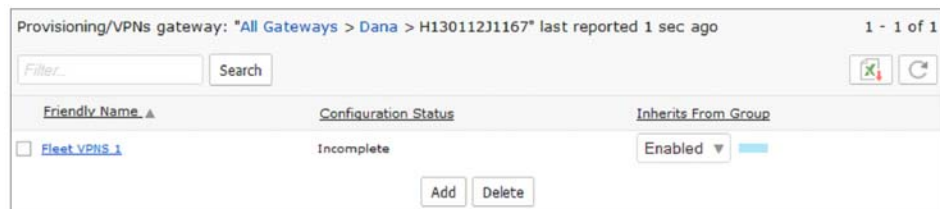

Figure 3-27: VPN Provisioning Listing Screen - Listing for a Selected Gateway

Note: A software version check is performed at the group level and any differences are highlighted as shown in Figure 3-26. A group inherits the software version from the source gateway in the 'set template config' operation (see Setting the Template Configuration), and can be looked up from the Admin->Group menu.

The list contains the following columns:

- **Friendly Name**: the name assigned to the VPN configuration.
- **Conformance** (shown when a group is selected in the Gateway Tree): visually indicates if the configuration assigned to sub groups and oMGs under the selected group conforms to the configuration assigned to the selected group:

Table 3-2:

	All gateway(s) in the group inherit the configuration.
	Some gateway(s) in the group inherit the configuration.
	No gateway(s) in the group inherit the configuration.

Note: at the group level, hovering the mouse over the conformance bar provides details as to which gateways within the group that are not inheriting the VPN.

- **Inherits From Group** (shown when an oMG is selected in the Gateway Tree): provides the two subfields listed below for inheritance:
  - **Enabled/Disabled Dropdown**: when set to Enabled, the oMG will inherit the configuration from the parent group. When set to Disabled, the oMG will have its own configuration that does not inherit from that of the parent group (note though that the parent configuration will be used to create the initial configuration for the oMG). Note that this field is blank (i.e. doesn't say enabled or disabled) when the VPN does not exist at group level and only exists at the gateway.
  - **Conformance Bar**: visually indicates if the configuration assigned to the selected oMG conforms to the group from which it inherits.

Table 3-3:

	Fully inherited from the parent group.
	Partially inherited from the parent group.
	Not inherited from the parent group.

Adding and Editing VPN Configurations

Adding a VPN

To add a VPN configuration to a group or gateway:

1. Ensure the template configuration has been assigned to the group as described above in Setting the Template Configuration.
2. Select the group or gateway in the Gateway Tree.
3. Select the **Config->Provisioning->VPNs** menu.
4. Click **Add**.
5. Enter the required configuration fields:
   a. **Label**: the name of the VPN configuration. The default label is automatically generated by the system. Note that this field cannot be changed once the VPN is created.
   b. **Server**: the IP address of the VPN server.
   c. **Enterprise Network Subnets**: a common-delimited list of enterprise subnets in CIDR notation to include.
6. Optionally click **Show Advanced Config** to display and edit additional VPN configuration fields. Defaults are provided for each advanced field.

7. Optionally override any settings specific to the selected item as described below in *Overriding VPN Settings*. Note that required settings vary between the group level and individual gateway level (e.g. interfaces and PSK). Certain fields may be optional at the group level but may be required at the gateway level for deployment.

Note: at the group level, only links and monitors that are common in all gateways within the group will be displayed as options.

---

8. (Optional) Click **Attach a CSV file for importing**. This allows for PSK credential information stored in a .csv file to be used for configuring one or more oMGs in a group that require different PSKs. Using a .csv file allows these different PSKs to be defined in one file. Note that this option is not available when setting a configuration for a single oMG, nor does it apply settings at the group level.

    If provided, the values defined in the file will override the value in the *Pre-shared Key* field for each oMG listed in the .csv file. The *Attach CSV* dialog provides the following fields:

    a. **Template** (top right corner): generates a blank CSV file which can be populated with VPN PSK information (see VPN CSV).

    b. **Select a CSV file**: allows for a populated CSV file to be selected and attached to the configuration. The values in this .csv file will override those on the configuration screen. Once selected, a list of oMG's will be displayed indicating which gateways will be affected and excluded by the settings being imported. Click on **oMG(s) will be updated** and **oMG(s) excluded** to display the respective list:
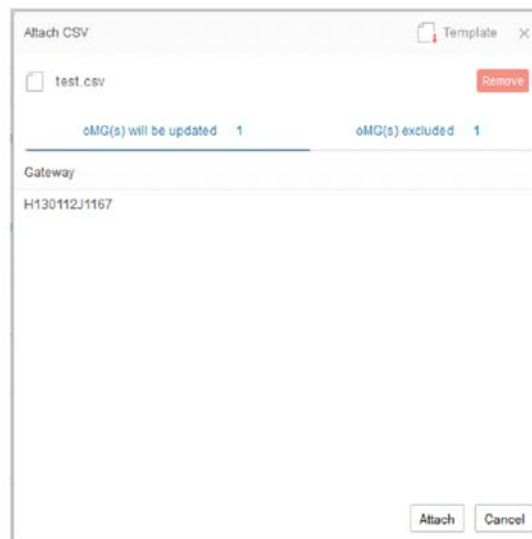
    These lists provide a summary of which oMGs the CSV file contains a configuration for.

    c. **Attach**: attaches the selected .csv file to the configuration.

9. (Optional) Click **Deploy configuration to gateways**. If checked, the configuration will be deployed when the *Save* button is clicked. Be sure to verify the

deploy state by hovering the mouse over the box in the top left corner of the title. This will display a popup indicating if deployment can take place:
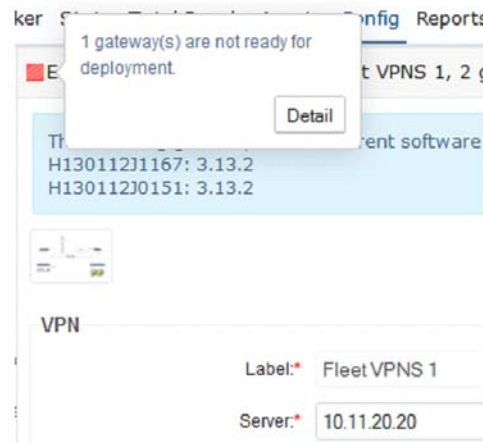
Clicking *Detail* displays additional information about issues impacting deployment.

Note that the *Deploy Configuration to gateways* checkbox will not be available if a CSV was attached and a PSK has not been assigned to the group.

10. Click **Save** to save the configuration to the group or gateway. The new VPN will be listed on the VPN provisioning listing screen. If *Deploy configuration to gateways* is checked, the configuration will also be deployed to the selected oMGs. If a configuration conflict exists (e.g. due to a configuration version mismatch), the *Deploy* screen will be displayed which can be used to rectify the problem (e.g. to update oMGs with the latest configuration files). If a CSV file was attached, any child gateways specified in the CSV file will transition from the *Complete* state to the *Modified* state on save, in which case the *Apply* button on the *Deploy* screen must be used to push the changes to those gateways. For more information see Deploy).

Note: when 'Save' is clicked at the group level, all changes on the group are applied to gateways within the group as long as the fields modified are not overridden at the gateway.

Note that info bubbles are provided beside each field which can be clicked on to display popup help about the respective field:

Figure 3-28: VPN Info Bubbles

Editing an existing VPN

To edit an existing VPN configuration, select the group or oMG whose configuration is to be edited, select **Config->Provisioning->VPNs**, click on the name of the VPN under the *Friendly Name* column and edit the fields as described above for adding a VPN.

Overriding VPN settings

When editing a specific oMG, the left hand column of the configuration editing screen indicates if each value inherits from or overrides the setting from the parent group's configuration:

Figure 3-29: Example of Inheritance Indicators on Configuration fields

To change whether a setting inherits or overrides from the parent group, click on the indicator and select the respective option:

- **Inherit value from parent group:** specifies that the setting from the parent group's configuration should be used.
- **Assign a custom value and override parent group**: specifies that the parent group's configuration setting should be overridden. Selecting this option allows the input field to be modified for some settings, while other settings will be taken from the configuration stored on the selected oMG.

Note: syntax checking is performed by the AMM on most fields before a configuration can be saved.

To obtain contextual information about the meaning of the various field labels, click the diagram icon on the top left corner to display a network diagram:

Once all settings have been made, click **Deploy configuration to gateways** if the changes should be deployed, and then click **Save** to save and deploy the changes.

Multi-VPN Provisioning Restrictions and Behaviours

oMG 3.14 and up allows for the configuration of multiple VPNs per WAN link. The AMM will only allow provisioning of multiple VPNs on oMGs running 3.14 and higher and will enforce the following rules when provisioning VPNs:

1. If a VPN is added/edited at the gateway level on a gateway older than 3.14, and if the WAN link already has an IPsec VPN, then the VPN configuration cannot be saved.

2. If a VPN is added/edited at the group level, some gateways in the group are older than 3.14, and if the WAN link on those gateways already has an IPsec VPN, then the VPN configuration will not be saved on those gateways.

3. Copying a configuration from one gateway to another is not restricted or monitored. This means for example, if a 3.14 VPN configuration (which may or may not have multi-VPN) is copied to a 3.13 gateway, then the VPN behavior on the 3.13 gateway will be undefined/unknown.

3.7.1.3 Provisioning Management Tunnels

Management Tunnel configurations are provisioned using the *Config->Provisioning->Management Tunnel* menu. This allows fleet operators to assign Management Tunnel settings to either a single oMG or group of oMGs.

Note: this functionality is for oMGs only.

To edit a VPN configuration to a group or gateway:

1. Ensure the template configuration has been assigned to the group as described above in Setting the Template Configuration.

2. Select the group or gateway in the Gateway Tree.

3. Select the **Config->Provisioning->Management Tunnel** menu.

4. Edit the *Server* field to specify the fully qualified domain name of Management Tunnel server address.

5. Optionally click **Show Advanced Config** to display and edit the *AMM Tunnel IP* field.

6. Optionally override any settings specific to the selected item as described below in *Overriding Management Tunnel Settings*.

7. (Optional) Click **Deploy configuration to gateways**. If checked, the configuration will be deployed when the *Save* button is clicked.

8. Click **Save** to save the configuration to the group. If *Deploy configuration to gateways* is checked, the configuration will also be deployed to the selected oMG(s). If a configuration conflict exists (e.g. due to a configuration version mismatch), the *Deploy* screen will be displayed which can be used to rectify the problem (e.g. to update oMGs with the latest configuration files). For more information see Deploy).

Note: syntax checking is performed by the AMM on most fields before a configuration can be saved.

Overriding Management Tunnel Settings

When editing a specific oMG, the left hand column of the configuration editing screen indicates if each value inherits from or overrides the setting from the parent group's configuration:

- **Inherit value from parent group**: specifies that the setting from the parent group's configuration should be used.
- **Assign a custom value and override parent group**: specifies that the parent group's configuration setting should be overridden. Selecting this option allows the input field to be modified for some settings, while other settings will be taken from the configuration stored on the selected oMG.

Once all settings have been made, click **Deploy configuration to gateways** if the changes should be deployed, and then click **Save** to save and deploy the changes.

Note that info bubbles are provided beside each field which can be clicked on to display popup help about the respective field:
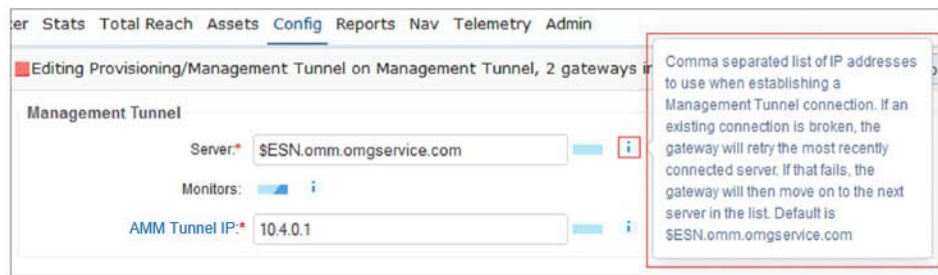
Figure 3-30: Management Tunnel Info Bubble

3.7.1.4 Controlling Configurations when Moving Gateways between Groups

When moving a Gateway to a group, the following options are provided to control how the configuration of the group is applied to the new gateway:

*   **Inherit**: the configuration is copied from the group to the gateway.
*   **Retain**: no change is made to the gateway's configuration.

3.7.2 Deploy

The *Deploy* menu provides access to tools for copying and deploying configuration files to gateways. These are described in the following subsections.

3.7.2.1 Tracker

The *Tracker* panel allows you to inspect and configure the GPS TAIP forwarding groups for the Tracker feature (for more information about Tracker see Tracker Tab). Using GPS TAIP, oMGs can send GPS information at a much higher frequency than via the normal event stream.
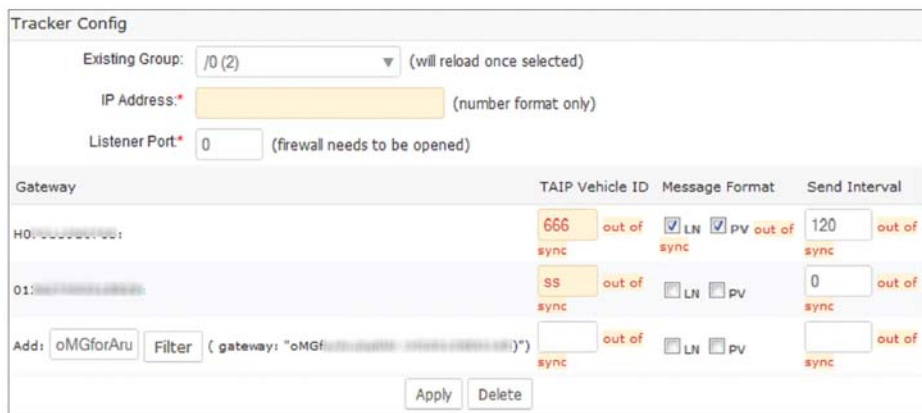
Figure 3-31: Tracker Panel

Tracker configuration fields:

- **Existing Group**: displays the names of the gateway groups to configure TAIP for. The name consists of the IP address and listener port followed by the number of gateways (in brackets) within that group.
- **IP Address & Listener Port**: the IP address and port where you want to send the TAIP data (i.e. the address of the AMM and port that has been opened in the firewall).

Below the main configuration options, the following fields are presented for the list of gateways which are part of the group:

- **Gateway**: the name of the gateway.
- **TAIP Vehicle ID**: a 4-digit number used to identify the gateway within the group. Numbers must be manually entered and failure to do so will show "Duplicate" beside blank TAIP Vehicle ID fields.
- **Message Format**: the type of TAIP response message format to use – LN or PV.
- **Send Interval**: the frequency (in seconds) at which to send messages. Note: "Out of sync" will be displayed if the gateway is using a different configuration than that defined on the AMM.

Adding a group:

Select **** New **** from the Existing Group dropdown, enter an IP address and port. Click **Apply** to create the group.

To add a gateway to the group, select a gateway from the *Gateway Tree* and click **Apply**. Note: individual gateways cannot currently be removed from the group.

To find a specific gateway to add, click **Filter** and enter a search string to filter by. A drop down will appear with gateways matching that filter:

Figure 3-32: Filtering by Gateway

To further refine the search, enter values for one or more of the following fields which correspond to the information stored for gateways (Note: the search will be invoked after clicking on another field):

- **Version pattern**: filters on version numbering information (e.g. r3).
- **Name pattern**: filters on the gateway names and ESNs.
- **Customer, Contact, Location**: filters on customer name, contact information, or location.

- **Notes**: filters on the notes entered for the gateways.
- **Reporting Within**: filters on those gateways which have reported within the specified number of days.
- **Matching vehicles**: shows the gateways found as a result of the filter. From this list a gateway can then be selected.

To delete a group, click **Delete** and then click **OK** on the confirmation popup.

3.7.2.2 Upload

The *Upload* tab is used to apply saved configuration file(s) to the gateways.

Figure 3-33: Upload Tab

Uploading the configuration file:

- **Apply to***: the gateways to which the file(s) will be copied to. Enter the gateway's ESN or alias, or locate it in the *Gateway Tree.*
- **Configuration file***: click on **Browse** to locate the appropriate file(s) to copy. Up to four files can be uploaded at a time, by locating a file for each of the four *Configuration File* fields provided.
- Click on **Upload** to upload the file.

3.7.2.3 Copy

The *Copy* panel is used to copy the configuration file from a gateway to be used as a *template* for other gateways. This panel is used in conjunction with the Deploy panel when copying configurations. For more information on this procedure see: Copying Configurations Between Gateways.

*Figure 3-34: Copy Panel*

Copying the gateway's configuration file:

- **Source***: the gateway from which the configuration files are being copied.
- **Copy config to***: the gateway to which the files are to be copied to. Enter the gateway's ESN, alias or locate it in the *Gateway Tree*.

Note: users can enter more than one gateway in this field for mass configuration.

- **Configuration Files** options:
  - **All files**: enabled by default, this will display all files with a checkmark beside each. Clicking *Copy* will therefore copy all files to the gateway.

To copy specific files from the source gateway, uncheck **All Files** to deselect all files and place a checkmark beside each file to copy:

☑ All Files
    ☑ 802dot1x.yaml
    ☑ access.yaml
    ☑ aptracker.yaml
    ☑ assetTracker.yaml
    ☑ bl.yaml
    ☑ bt.yaml
    ☑ dbcleand.yaml
    ☑ globals.yaml
    ☑ gps.yaml
    ☑ hdobd.yaml
    ☑ lan-segments.yaml
    ☑ lan.yaml
    ☑ mcu.yaml
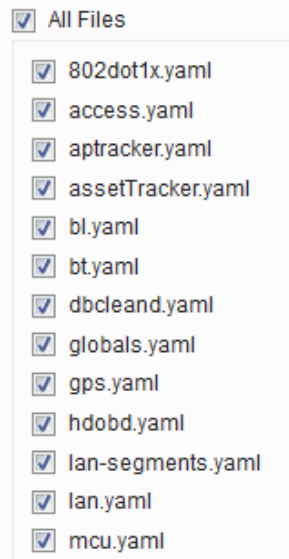
Figure 3-35: Selecting configuration files to copy

Note: the files available for selection may vary depending on the selected device type

- **Skip version check**: by default, configuration files can only be copied to gateways running the same software version. Version check therefore verifies that both the source and destination gateways have the same software version and ensures compatible configuration files. To override this restriction, enable this option.
- **Skip platform check** (applicable to ALEOS devices only): by default, configuration files can only be copied to gateways of the same type. The platform check verifies that both the source and destination gateways are of the same type and ensures compatible configuration files. Enabling this option, overrides this restriction.
- **Reboot automatically after changes are applied** (applicable to ALEOS devices only): when selected, the device will be rebooted after the copy operation has completed.
- **Copy**: click to copy the file(s); this opens the *Deploy* panel.

Note: this panel is also available by locating the source gateway in the Gateway Tree*, right-clicking on it and selecting Copy Configuration.*

---

* denotes a required field

3.7.2.4 Deploy

The *Deploy* panel aids administrators during mass configuration deployment of their gateways. The deploy feature maintains current gateway configurations and stores them on the AMM. This allows administrators to easily copy configurations from one gateway to another, to a group of gateways, or to an entire fleet.

This panel is used in conjunction with the Copy panel when copying configurations. For more information on this procedure see: Copying Configurations Between Gateways.
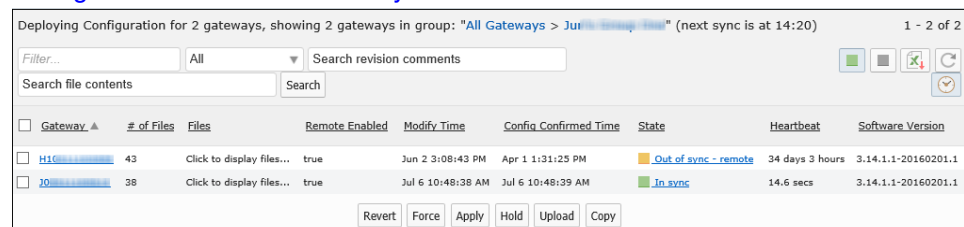
Figure 3-36: Deploy Panel

The list of gateways displayed can be filtered by using the following filter fields:

- **Filter edit box**: filters the list on part or all of a gateway name. For more information about searches see: Filter Box and Searching.
- **Range dropdown**: can be used to select a date/time range of previous deployments to filter on. Selecting an option from the dropdown will display a field where the range can be input.
- **Search revision comments**: filters the list to include only those units which participated in a deployment where the specified comment was attached. Revision comments are used for identifying units which participate in PSK rotations (see Section Deploying PSK Rotation through the AMM for more information).
- **Search file contents**: filters the list based on the contents of script files. This is useful for filtering on script content where specific changes (e.g. additions) have been made and uploaded to gateways.

Information is provided in the following columns:

- **Gateway**: lists the gateways connected to the AMM. The list is based on those gateways which are organized under the folder (and its subfolders) currently selected in the Gateway tree.
- **# of Files**: indicates the number of configured files.
- **Files**: when clicked, displays links to the individual files, each of which can be clicked on to edit the content.
- **Remote Enabled**: indicates if the gateway is accessible remotely to verify if a deploy action was performed.
  - *True* = Yes, an action was performed

- *False* = No action was performed

- **Modify Time**: the date and time when the gateway's configuration was last modified.

- **Config Confirmed Time** (ALEOS only): the time when the configuration of an ALEOS device was synchronized with the AMM. This field is applicable when the State (see below) is *Config Confirmed* or *Config Confirmed with Warnings*.

  This time value is provided for ALEOS devices because changes made to ALEOS devices in ACE Manager result in a notification that must be delivered to the AMM. Therefore the time value indicates the time when the configuration was received and confirmed to be in sync by the AMM. For oMG devices, this field does not apply and will display the same value as the *Modify Time* column.

- **State**: using green, yellow and red circle icons, this information allows administrators to see the state of each gateway's configuration in relation to the configuration stored on the AMM. The possible states are listed below, and various functions can be initiated depending on the state (see Functions below).

  - **In sync** (oMG only): the configuration of the oMG is synchronized with the AMM, which means that the repositories of the oMG and AMM are an exact copy of each other. The following functions/state transitions can be initiated:

    - Revert: the oMG's configuration state will transition to Awaiting rollback.

    - Copy: the gateway's configuration state will transition to Modified.

    - Upload: the gateway's configuration state will transition to Modified.

  - **Config Confirmed** (ALEOS only): the configuration of an ALEOS device was synchronized with the AMM. The following functions/state transitions can be initiated:

    - Revert: the gateway's configuration state will transition to Awaiting rollback.

    - Copy: the gateway's configuration state will transition to Modified.

  - **Config Confirmed with warnings** (applies to ALEOS devices only): indicates the device has been synchronized but rejected a subset of the configuration elements. Clicking on the warnings will display a summary of items rejected. The following functions/state transitions can be initiated:

    - Revert: pulls all of the configuration settings from the gateway and overwrites any invalid values that were introduced from the AMM's configuration. The gateway's configuration state will transition to Config Confirmed. Using Revert is the recommended action because it corrects all invalid values where as other actions may cause future invalid values to end up back on the gateway putting the device back into the Config Confirmed with warnings state. Alternatively, the Config hyperlink can be clicked to identify invalid values after which they can be manually corrected.

    - Copy: the gateway's configuration state will transition to Modified.

    - Upload: the gateway's configuration state will transition to Modified.

  - **Awaiting rollback**: the configuration is waiting to be rolled back from that on the AMM. The following functions/state transitions can be initiated:

    - Revert: the oMG's configuration state will remain as Awaiting rollback.

- Copy: the gateway's configuration state will transition to Modified.
- Upload: the gateway's configuration state will transition to Modified.
- **Awaiting rollforward**: the configuration is waiting to be rolled forward to that on the AMM. The following functions/state transitions can be initiated:
  - Revert: the gateway's configuration state will transition to Awaiting rollback. This feature should be used in cases where a change of decision has taken place (e.g. after the Force button was used to overwrite the gateway's configuration with the AMM's version) such that the AMM's configuration should now be overwritten with the gateway's configuration.
  - Copy: the gateway's configuration state will transition to Modified.
  - Upload: the gateway's state will transition to Modified.
- **Conflict**: the config on the AMM and on the gateway have both been modified. To manually resolve this, choose the desired configuration to use, and overwrite the other configuration with it. The following functions/state transitions can be initiated:
  - Force: selects a configuration from the AMM. The gateway's configuration state will transition to Awaiting rollforward.
  - Revert: selects the gateway's configuration. The gateway's configuration state will transition to Awaiting rollback.
  - Copy: the gateway's configuration state will transition to Modified.
  - Upload: the gateway's configuration state will transition to Modified.
- **Incomplete** (applies to oMG devices only): a gateway configuration has been detected that is missing mandatory fields. The issue must be rectified in the configuration before trying to deploy again. Issues are typically due to mandatory configuration fields which have not been filled in. Note that mandatory fields are visually indicated on the configuration screen via red asterisks. Navigate to *Config->Provisioning->VPNs* to identify which VPN is incomplete. The following functions/state transitions can be initiated:
  - Force: tells the AMM to ignore the issues causing the incompleteness. The gateway's configuration state will transition to In Sync.
  - Revert: the gateway's configuration state will remain as Incomplete.
  - Copy: the gateway's configuration state will transition to Modified.
  - Upload: the gateway's configuration state will transition to Modified.
  - Hold: the gateway's configuration state will transition to Out-of-sync-local or Out-of-sync-remote.
- **Modified**: changes have been made on the AMM but are waiting for a user to review and apply them before they will be pushed out to the gateway. Therefore the gateway and AMM are not in sync. The following functions/ state transitions can be initiated:
  - Apply: commits the changes. The gateway's state will transition to In sync.
  - Revert: the gateway's state will transition to Awaiting rollback.
  - Copy: the gateway's configuration state will transition to Modified.
  - Upload: the gateway's configuration state will transition to Modified.
- **Configuration Reset Completed**: the device has successfully reset its software back to the factory default configuration. The following functions/ state transitions can be initiated:

- Force: the gateway's configuration state will transition to Awaiting rollforward. This should be used to restore the oMG to its previous configuration if the oMG reset on its own.

- Revert: the gateway's configuration state will transition to Awaiting rollback. This should be used to accept (reset to) the factory settings.

- Copy: the gateway's configuration state will transition to Modified.

- Upload: the gateway's configuration state will transition to Modified.

- **Out of sync - local**: changes were detected in the AMM's configuration repository. The changes will be automatically pushed to the oMG. The following functions/state transitions can be initiated:

  - Sync Now: manually pushes the changes to oMG. The gateway's state will transition to In Sync.

  - Revert: the gateway's state will transition to Awaiting rollback. This feature should be used to "cancel" the request to push AMM changes to the oMG.

  - Copy: the gateway's configuration state will transition to Modified.

  - Upload: the gateway's configuration state will transition to Modified.

- **Out of sync - remote**: changes were detected on the oMG. The changes will be automatically pulled from the oMG by the AMM. The following functions/state transitions can be initiated:

  - Sync Now: manually pulls the changes from the oMG to the AMM. The gateway's state will transition to In Sync.

  - Revert: the gateway's state will transition to Awaiting rollback.

  - Copy: the gateway's configuration state will transition to Modified.

  - Upload: the gateway's configuration state will transition to Modified.

- **Remote Config failure**: a previously attempted sync action has failed. In this state, one of the functions below must be invoked. The following functions/state transitions can be initiated:

  - Force: sends the AMM's configuration to the gateway.

  - Revert: attempts to recover the configuration from the oMG. The gateway's state will transition to Awaiting rollback.

  - Copy: the gateway's configuration state will transition to Modified.

  - Upload: the gateway's configuration state will transition to Modified.

- **Software Version**: the current software version of the gateway listed.

Functions

There are seven functions for deployment:

Figure 48 - The Seven Deployment Function Buttons

- **Sync Now**: use this function to initiate synchronization between the gateway and the AMM. Always ensure that the configuration is in sync before making any changes to configuration files or pushing a new configuration to the gateway. Note: this button is only available when a single gateway is selected and is only available for oMGs. To select a single gateway, click on a gateway's link in the *Deploy* list, or select the gateway in the *Gateway Tree*.

- **Revert**: pulls the gateway's copy of the configuration into the AMM regardless of the *Sync State*.
- **Force**: pushes the AMM copy of the configuration out to the gateway regardless of the *Sync State*. This button is only applicable for certain states (see States listed above).
- **Apply** (available for oMGs only): applies changes made on the AMM to the oMG. Note that when the state is *Incomplete*, the *Apply* button cannot be used. However, advanced users such as Sierra Wireless personnel, can use the *Force* button to ignore the incomplete state and apply the configuration.
- **Hold**: cancels all changes pending synchronization.
- **Copy**: copies configuration files from one gateway to another or to a group of gateways.
- **Upload**: applies configuration files that have been previously backed up to a PC.

3.7.3 CSV Import | Export

3.7.3.1 WLAN WiFi Settings and WAN WiFi Security

In order to minimize intrusion opportunities when using pre-shared keys, it's common for fleet operators to change or "rotate" login credentials on a regular basis. The *CSV Import | Export* menu allows fleet operators to perform this rotation by exporting credentials to user-friendly CSV files, which can then be updated with new credentials using spreadsheet software, and then re-imported back into the oMG(s).

oMM 2.9 and above in combination with oMG 3.8 and above, support the "rotation" of PSK credentials for WiFi WAN access points. WiFi WAN PSK rotation works by switching between access point profiles, each of which contains different PSK credentials. oMM 2.11 and above also includes WLAN export which allows fleet operators to provision LAN access point configurations and perform PSK rotation for WLAN's. Note that as of oMM 2.14, PSK rotation for VPNs is done through provisioning (see Provisioning VPNs - for more information).

The *WAN WiFi Security* and *WLAN WiFi Security* menus under the *Config->CSV Import | Export* tab allow fleet operators to easily deploy PSK rotation changes to a fleet of configured oMG's.

WEP encryption is not supported for credential rotation.

oMG PSK Rotation Requirements and Assumptions

For WiFi WAN PSK rotation, at least two WiFi access point profiles need to exist on the oMG's for which rotation is to be used, and those profiles must be assigned to at least one WAN link. The use of two access points ensures that WAN access remains uninterrupted during latency or other delays that may occur when transitioning oMG's to the new PSK credentials. This is accomplished by allowing oMG's to gradually transition to using the new access point while still allowing access through the old access point. Once all oMG's have transitioned to the new access point, the credentials of the old access point can then be

changed thereby leaving WAN service uninterrupted. Access points are configured through the oMG's LCI screen as described in the oMG Operation and Configuration Guide.

WiFi WLAN PSK rotation doesn't have a similar, dual-access point requirement, in part because there is only a single access point per LAN device on the oMG and because WLAN access should be interrupted when credentials change (i.e. to increase security by preventing devices which previously had access from being able to connect to the WLAN). This means that all devices currently connected to the oMG will be immediately disconnected, and users will need to be provided with new login credentials either prior to the rotation, or very soon thereafter.

Deploying PSK Rotation through the AMM

Rotation deployment is accomplished by exporting the configuration of one or more oMG's to a CSV file, modifying the settings in that CSV file using third party spreadsheet software (e.g. Microsoft Excel), re-importing the CSV file back into the AMM and deploying the settings to the fleet of oMG's. Information about the CSV file is available in CSV File Information.

The detailed steps to accomplish this PSK rotation deployment are as follows:

1. Select the oMGs in the Gateway Tree whose credentials are to be updated.

2. Navigate to **Config->CSV Import | Export->WLAN WiFi Settings->Export** or **Config->CSV Import| Export->WAN WiFi Settings->Export** to access the export screen for the respective PSK credentials.

3. Click **Export** and then save the CSV file when prompted.

4. Modify the credentials in the CSV file using spreadsheet software and then save the CSV (see CSV File Information for information about the CSV file format). In the case of WAN rotation, be sure to also update WiFi Network Name to rotate the oMGs to use the new access point.

5. Navigate to **Config->CSV Import | Export->WLAN WiFi Settings->Import** or **Config->CSV Import| Export->WAN WiFi Settings->Import** to access the import screen for the respective PSK credentials.

6. Click **Browse**, locate the modified CSV file and click **Import**. The credentials will be imported to the AMM and checked for any errors which will be displayed. If no errors were found, proceed to the next step.

Note: configuration settings will be deployed to all oMG's which are both selected in the Gateway Tree *and are listed in the CSV file. Be sure to verify which oMG's will be updated before moving onto the next step, by checking that each oMG listed in the CSV is also selected in the Gateway Tree.*

7. Enter a descriptive comment in the *Deploy Comment* field if desired. Attaching a comment to a deployment allows for gateways participating in deployments to be easily identified on the *Config->Deploy* page via the *Search revision comments* field (as described in Deploy).

8. Click **Show Gateways** (optional) to show the gateways that will be affected by the import operation.

9. Click **Deploy Configuration**. The configuration deployment screen will be shown and all units targeted for deployment will transition to a *File generating* state and then a *File pending* state.

10. Click **Apply** to perform the deployment. Once the sync cycle completes the state will change to *In Sync* for each affected oMG, assuming that the oMG is online during the sync cycle.

11. For WiFi WAN PSK rotation: after all oMG's have transitioned to the new access point, repeat the above steps to change the credentials of the old access point. This will prevent WAN access via the old access point which will eventually become the new access point on the next PSK rotation.

When exporting a long PSK containing all numerics (e.g. 77667766776677667766776677) using Excel 2010, Excel will automatically convert the value to the "General" format (e.g., "7.76678E+25"). When saving back to csv, the value will be saved as "7.76678E+25" instead of the original number.

To properly edit a file with these kinds of values you must use a text editor. This ensures that the PSK values remain in their proper numeric format.

3.8 Admin Tab

The *Admin* tab provides users with admin privileges to access a number of administrative panels.

3.8.1 Software

The AMM can store gateway software packages (e.g. gateway firmware) and provides facilities for updating gateways with these packages.

Obtaining packages and updating gateways is a two-step process. This involves using the *Admin->Software* menu which provides access to the *Repository* screen where gateway software packages can be downloaded to the AMM and administered, and the *Admin->Distribution* screen, which allows administrators to update gateways with these downloaded software packages.

Both of these screens are described in the following sub sections.

3.8.1.1 Repository

The *Software Package Repository* (aka "Repository") screen, shown in Figure 3-37 below, allows administrators to check for and download available software packages, upload packages from other sources, set up automatic checks, and purge packages.

Acquiring packages using this screen is the first step in the two-step process for obtaining packages and updating gateways.

oMG packages are hosted by Sierra Wireless and can be downloaded to the AMM using the Repository screen's download facilities. ALEOS packages are hosted on Sierra Wireless' "Source" website at http://source.sierrawireless.com/

and must be manually acquired from that website and then uploaded to the AMM using the Repository screen's *Upload* button. These controls are discussed in further detail below.

In order for a customer's AMM appliance to access Sierra Wireless' repository, the corporate firewall be configured to allow the AMM to access *repo.inmotiontechnology.com* over HTTP.

Figure 3-37: Software Package Repository Screen

Figure 3-37 shows the following key features:

• **Check Now**: checks the Sierra Wireless servers to see if any new oMG software packages are available for download to the AMM. The status on when the last check was performed is shown below the button. A list of selectable software packages, if available, is shown in the grid.

• **Edit**: displays the *Auto Update* popup in which automatic checks for software can be configured:
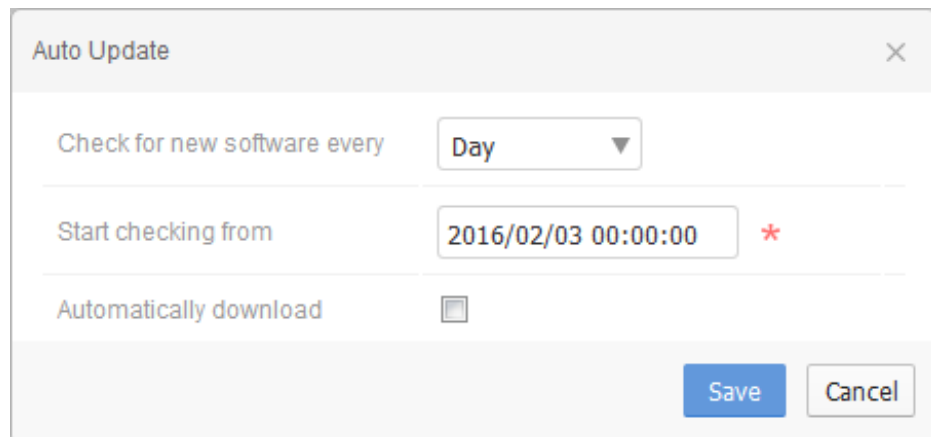
Figure 3-38: Auto Update Popup

- **Check for new software every**: can be set to *Day*, *Week*, or *Month*. To disable this feature, select *Do not check*.
- **Start checking from**: specifies the date and time from which to start performing automatic checks.
- **Automatically download**: select this option to automatically download new software packages to the AMM. Leave this option deselected to perform the check without automatically downloading the package. Note that customers using their own AMM appliance must first ensure that their firewall has been configured to allow the AMM to access the Sierra Wireless package repository (see Repository for more information).

- **Download**: downloads the selected oMG software packages to the AMM. Note that only those packages with a status of *New* or *Available* can be downloaded.

- **Purge**: removes the selected software packages from the AMM. Note that only those packages with a status of *Downloaded* can be purged.

Working with the Software Package List

The following controls are available:
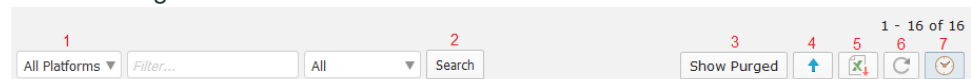
1. **Filter Fields**: filters the list by device type, name, and date (selectable options are *Release Date* and *Available Since*).

2. **Search**: executes the filter. For more information about searches see: Filter Box and Searching.

3. **Show Purged**: enable this option to include purged software packages in the list.

4. **Upload**: allows a software package stored on the local PC to be uploaded to the AMM. This button must be used for ALEOS firmware packages which must first be manually acquired from Sierra Wireless' "Source" website at http://source.sierrawireless.com/. This button can also optionally be used to upload oMG software packages.

Note: for customers running their own AMM appliance who have not configured their firewall to allow the AMM to access Sierra Wireless' package repository, the Upload button will be the only method for transferring oMG packages to the AMM. In this case, oMG packages (e.g. firmware) must also be downloaded from Sierra Wireless' "Source" website.

5. **Export to CSV**: exports the list of software packages to a .CSV file.

6. **Refresh**: refreshes the list of software packages. Used mainly to update software package statuses.

7. **Last Update**: toggles whether the date/time of the last update is to be automatically updated and displayed.

The software package grid displays the following fields:

Name	Version	Platform	Release date ▼	Status	Available since
☐ oMG-Core-Software	3.14.1.1-20160201.1	oMG-2000	Feb 1	New	N/A
☐ ALEOS-Core-Software	4.4.2.006	ES440	Dec 14	Available	2015/12/15 09:53:50

1. **Name**: the filename of the software package.

2. **Version**: the version number of the software package.

3. **Platform**: the Sierra Wireless gateway for which the software package applies.

4. **Release Date**: the date when the software package was released.

5. **Status**: the current status of the software package. Can be set to one of the following statuses:

    a. **New**: the software package was added to the repository since the last check and is available for download.

    b. **Available**: the software package is available for download.

    c. **Failed**: the last attempt to download the software package failed. An error message will be included to describe the error.

    d. **Downloading**: the software is being downloaded to the AMM.

    e. **Downloaded**: the software was successfully downloaded to the AMM.

    f. **Pending**: a request was made to download the software, but the download hasn't started yet (e.g. due to a batch download).

6. **Available Since**: indicates that the software has been available since the specified date/time.

3.8.1.2 Distribution

The *Software Distribution* screen allows administrators to push downloaded software packages to selected gateways. This is the second step of the two-step process for obtaining software packages and distributing those packages to gateways.
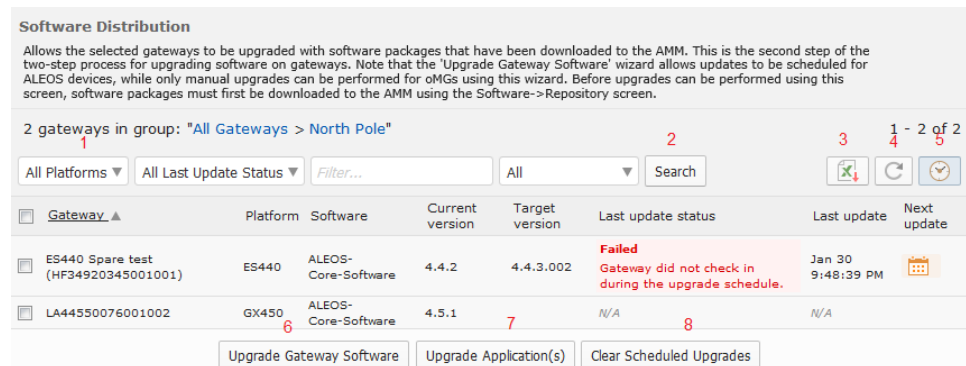
Figure 3-39: Software Distribution Screen

Figure 3-39 shows the main features of the Software Distribution screen:

1. **Filter Fields**: filters the list by device type, last status, name, and date/time range. For more information about searches see: Filter Box and Searching.

2. **Search**: executes the filter.

3. **Export to CSV**: exports the list of software packages to a .CSV file.

4. **Refresh**: refreshes the list of software packages. Used mainly to update software package statuses.

5. **Last Update**: toggles whether the date/time of the last update is to be automatically updated and displayed.

6. **Upgrade Gateway Software**: displays the *Upgrade Gateway Software* wizard to perform firmware upgrades to a selected gateway. If multiple gateways are selected, the wizard will require that a single gateway platform be selected (see Upgrading Gateway Software below).

7. **Upgrade Applications**: displays the *Upgrade Application(s)* wizard to perform application upgrades to a selected gateway. If multiple gateways are selected with differing platforms, the wizard will require that a single gateway platform be selected (see Upgrading Applications below).

8. **Clear Scheduled Upgrades**: removes any upgrades which are scheduled to automatically run. Upgrades can be scheduled using the *Upgrade Gateways Software* and *Upgrade Application(s) wizards*.
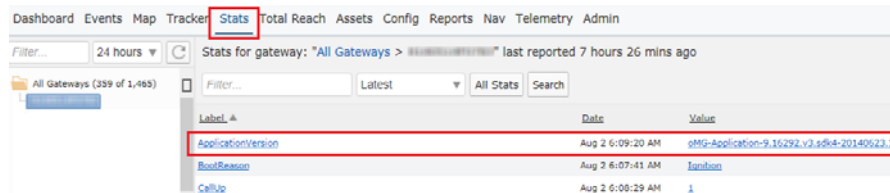
Note that an application package's date indicates whether it contains the latest build, as opposed to package version numbers which may change for various reasons unrelated to versioning.

As of oMM 2.15.1.1, the Software Distribution screen compares the build dates of downloaded application packages to determine if they are newer than that installed on the selected oMG. Packages which have a newer date are then made available by the Software Distribution screen for a potential upgrade.

For example, if an application package listed on the Software Distribution screen contains a software package with version 9.48804.v3.sdk4-20160106.1, the AMM will compare its date ("20160106") to that of the package installed on the selected oMG, and make it available as an upgrade if that date is newer than the oMG's installed version.

oMM Version 2.15 and below compares packages based on version numbers instead of dates, and may therefore show older versions of packages. Care must therefore be taken when viewing packages on the Software Distribution screen of oMM version 2.15 and below to ensure that the date of a given package is greater than that of the selected oMG.

The software version of a selected oMG can be viewed in the AMM, by clicking on the **Stats** menu and looking for the value of the **ApplicationVersion** stat:
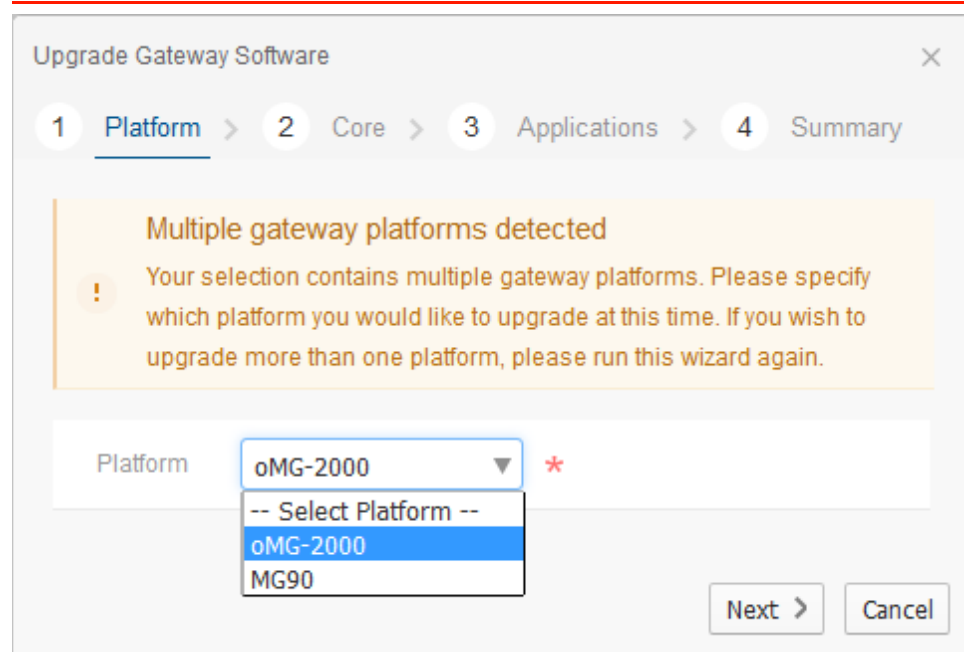
Figure 3-40: Application Version Stat

Upgrading Gateway Software

The *Upgrade Gateway Software* wizard is activated using the *Upgrade Gateway Software* button and allows administrators to apply firmware to a selected gateway via the following screens.

As of oMM 2.15.1.1, the *Upgrade Gateway Software* wizard provides the ability to update application software in addition to firmware for oMG devices. This is useful for cases when a firmware upgrade requires an application software package for repository preparation.

Note: if multiple devices are selected from different platforms, the wizard will require that a specific platform be selected. Only those devices which run on the specified platform will be upgraded, as shown here:

Select a platform from the *Platform* dropdown and click **Next**.

The *Upgrade to version* dropdown lists the software which is available on the AMM:

Upgrade Gateway Software   ✕

1   Platform   >   2   Core   >   3   Applications   >   4   Summary

ℹ   Please select the core software version you would like to upgrade to. Radio firmware releases are included and will be installed along with your selected core software version.

Upgrade to version   oMG-Core-Software-3.14.0.1-20150930.3   ▼   *

-- Select Version --
oMG-Core-Software-3.14.0.1-20150930.3
oMG-Core-Software-3.7.6.1-20141001.1
oMG-Core-Software-3.14.3-20160308.1.fips
oMG-Core-Software-3.13.4.1-20160201.1

Cancel

Select the version of the software to upgrade to and click **Next**.

For ALEOS Devices Only: the following *Schedule* screen will be displayed for ALEOS devices allowing an upgrade to be scheduled. This scheduling can be set by clicking **Yes** to display the scheduling options.

Note: the scheduling capability can only be used for ALEOS software.

Select the *Attempt upgrade* frequency (day, week, or month), the *Starts from* date, and the *During time* (the time during the day to perform the upgrade) and click **Next**, or select **No** and click **Next** to advance to the next screen without scheduling.

For oMG Devices Only: the following *Applications* screen will be displayed for oMG devices only. This screen provides the ability to select any applications that should also be upgraded at the same time as the firmware.

To perform an application update along with a firmware upgrade:

- click **Yes** for the *Would you like to upgrade applications?* field.
- click the checkbox beside an application in the list to select it for upgrade.
- select the version from the dropdown, and click **Next**:.

If there are no applications to be upgraded, then the following message will be displayed instead:

On the *Summary* screen, verify the upgrade information and click **Apply** to schedule or start the upgrade process:

Note that ALEOS device upgrades occur when the devices are scheduled to check in next, and therefore upgrades may not initiate immediately after completing the upgrade wizard. The upgrade will start when the device's next scheduled Heartbeat occurs (the default is once per day). Upon exiting the upgrade wizard, the "Last update status" for the ALEOS devices will be set to *Pending* until the next scheduled Heartbeat occurs and an upgrade is initiated.

Upgrading Applications

The *Upgrade Applications* wizard is activated using the *Upgrade Application(s)* button and allows administrators to apply software to a selected gateway via the following screens.

Note: if multiple devices are selected from different platforms, the wizard will require that a specific platform be selected. Only those devices which run on the specified platform will be upgraded as shown here:

Note: oMM 2.15.1.1 and above provides the ability to update applications at the same time as the firmware which is useful for situations where the firmware depends on a particular version of an application. See Upgrading Gateway Software for more information.

Click on the checkbox beside the application that is to be applied to the gateways and select the version from the *Version* dropdown and click **Next** to continue:

Review the upgrade information and click **Apply** to perform the application upgrade:

Note: the Affected Gateways and Unaffected Gateways titles can be clicked on to display lists of devices that will be upgraded or not upgraded by the process.

3.8.2 Gateways

The *Gateways* panel is used to add, modify and delete gateways.

Figure 3-41: Gateways Tab

Adding a new gateway

Click on **Add** to open the *Add* or *Edit* Gateway panel.

Enter the following fields:

- **ID***: electronic serial number (used to uniquely identify the gateway).
- **Name**: enter the name or alias for the gateway.
- **Group**: use the drop-down menu to select the group to which the gateway will belong.
- **Update DNS Servers** (applicable only for oMG devices): use the drop-down menu to select the DNS server to which updates will be sent. Note: before a DNS server can be assigned to a gateway, it must first be created. See DNS Servers. Click on **+** to add additional DNS servers and - to remove them.
- **Customer**: enter the customer information for the gateway.
- **Location**: enter the location information for the gateway.
- **Contact**: enter the contact information for the gateway.
- **Notes**: enter additional information regarding the gateway. This can be used to segment a fleet. For example, when using search filters, entering "Laptop equipped" or "Winter Tires" will only display vehicles equipped with laptops or winter tires.
- **Icon URLs**: leave empty - reserved for future use.

Click **Save** to create the new gateway.

For additional methods of adding gateways see:

- Adding Multiple Gateways to an AMM
- Transitioning AirLink Gateways from ALMS to the AMM

Deleting a Gateway

Gateways can be deleted by clicking in the checkbox next to the gateway label and then on **Delete**. Deleting a gateway removes it from the AMM's Gateway Tree. After deletion, the gateway will no longer report to the AMM and existing information about the gateway will no longer be available.

Editing a Gateway

To edit an existing gateway, click on its gateway link in the Label column to open the Editing panel (or click on **Edit**). Gateways can be moved from one group to another from this panel.

* denotes a required field

Note: administrators can add gateways before they go online. When a gateway boots up, the AMM matches it based on the ESN. This enables administrators to pre-assign gateways to a fleet and to configure additional properties.

3.8.3 Users

The *Users* panel is used to add, modify and delete user IDs for the AMM and is available only to customers who own an AMM appliance.

Figure 3-42: Users Panel

Figure 3-43: New User Screen

Adding a new user:

- Click on **Add** to open the *Adding new user* panel.
- Enter the user options. For a description of each field see Preferences under Option Tabs.
- Click **Save** to save the new user.

3.8.4 Stats

A *stat* defines a parameter value collected by the AMM. The *Stats* panel is used to add, delete, and modify the many parameters that are monitored and tracked by the AMM.
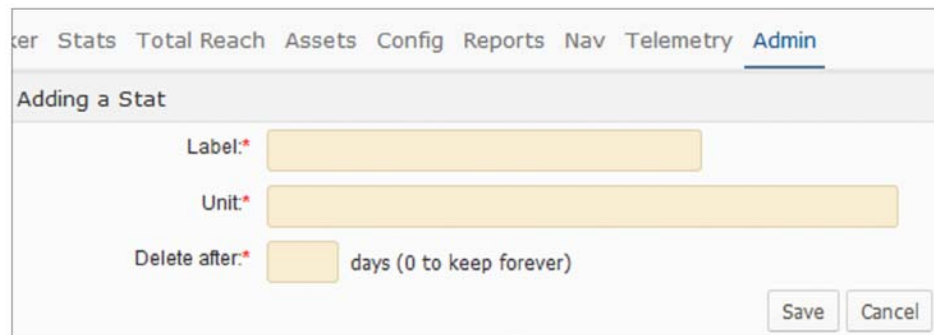
Figure 3-44: Adding a Stat

Important: do not modify these parameters unless under direct consultation with Sierra Wireless personnel.

3.8.5 Groups

A *group* is a named collection of gateways which allows for groups of gateways to be managed throughout the AMM. Groups of gateways are shown in the AMM's *Gateway Tree*:
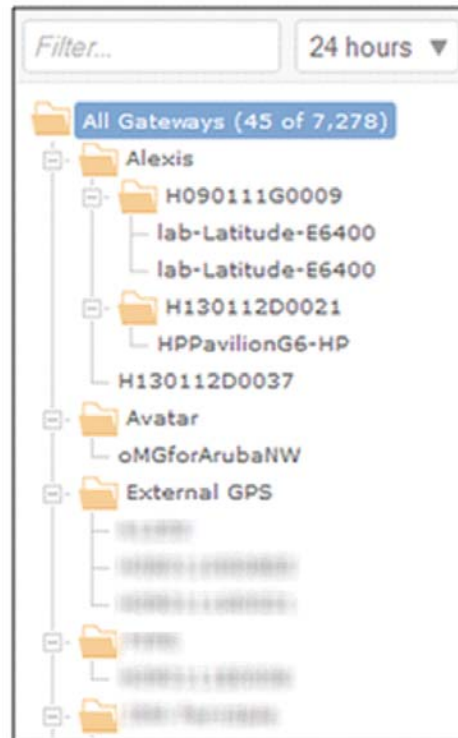
Figure 3-45: Groups in the Gateway Tree

Groups can also be organized under other groups to form a hierarchical organization of gateways.

Adding a new Group:

Figure 3-46: Group Administration Screen

Click on Add to open the *Add a Group* panel and set the following fields:

*   **Name**: enter a descriptive name for the Group in the Name field.
*   **Parent Group** (optional): select a Group from the Parent group dropdown to make the new group a child of that parent.
*   **Group Software Version**: defaults to the master gateway software version that is copied to the group when *Set group template configuration* is selected. This field can be used to change the default value.
*   **Authentication Type**: select the authentication type for user login:

- **Local authentication**: uses passwords defined on the AMM.
- **LDAP**: uses an authentication server for LDAP authentication. When selected, the following fields are available:
  - **Server Address**: specifies the URL of the LDAP server (e.g. ldap://yourcompany.com) which will be used for authentication.
  - **Search Base**: the distinguished name of the search base object which defines the directory location to begin the LDAP search.
  - **Domain**: identifies the domain to which the user belongs.
- When selected, any users which are assigned to the group will have the option to select remote authentication to use this LDAP authentication configuration (see Remote Authentication);

3.8.6 Thresholds

The *Thresholds* panel allows users to specify threshold settings that can be applied to one or multiple gateways. A threshold is configured for a Stat (e.g. a battery voltage level) and triggers an event when the threshold criteria is met. Thresholds can be created without warning or error conditions. Once created a threshold is available for display on the *Dashboard*.
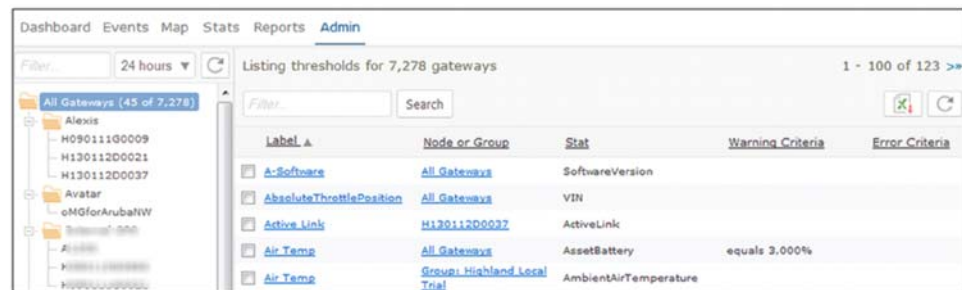
Figure 3-47: Thresholds Panel

Adding a new threshold:

Click on **Add** to open the *Add a Threshold* panel.

Configure the *Properties*:

- **Label***: the name of the threshold.
- **Group** or **Gateway***: the group or gateway listed will be the one selected in the gateway tree.
- **Stat**: use the drop-down to select the stat. The available items will vary depending on the type of device (oMG or ALEOS) selected in the Gateway tree, or on the *Stat for gateway type* selection when a mixed fleet is selected.
- **Default value**: specifies a value for which reporting is not expected.
- **Display Filter**: controls what is displayed for the threshold's value on the dashboard using regular expressions.
- **Matching Labels**: some stats use sub-keys (e.g. AssetTemperature) and the sub-key is the asset tag ID. This provides a way to limit the threshold to a specific asset (e.g. AssetTemperature: 1234567890 > 50C = error).

- **Dashboard group***: select the group on the dashboard where the threshold is to appear. Groups are displayed from left to right depending on their number. To avoid showing the group select **Do not show on dashboard**.
- **Threshold owner**: allows a threshold to output using the settings of the specified user.
- **Show value as obsolete when**: determines when to grey out a value to indicate that it is "stale" (obsolete). This can be set to go obsolete when the unit is powered off or a heartbeat is over an hour old.
- **Email warning and error actions to owner**: sends an email containing error and warning information related to the threshold to the user specified by the Threshold owner field. The information included is dependent on the definition of a threshold but can include the ESN, timestamp, description, location and other information.
- **Only show warning and alert values on dashboard**: when enabled, overrides the dashboard settings and only shows the threshold's value when it meets the criteria for a warnings or error.
- **Do not trigger actions on clear**: when enabled, actions are not sent for "clear" events (i.e. events indicating that a previously crossed threshold is no longer occurring).
- **Notes or instructions**: enter the instructions that will be included in alerts and email messages.

Set the *Warning Conditions*

- **Warning Criteria***: sets the criteria required for the stat's value to trigger a warning (e.g. selecting greater than and then entering a value of 10 will generate a warning when the stat's value exceeds 10). The meaning of the value is specific to each stat and its units of measurement.
- **Extra Criteria**: enter up to four additional criteria (i.e. stats) that must be satisfied in order for a warning to be sent. Upon selecting a stat for each criteria, the condition and value fields will become visible for configuration.
- **Actions***: select the actions to be taken to report a warning:
  - **Log Event**: default action. It is recommended that this remain enabled so that all warnings are written to a log file.
  - **Send Email**: select to enter the email address(es) to which an email will be sent, advising of the warning condition. Up to two email addresses can be entered, separated by a comma.
  - **SNMP Trap**: when enabled, an SNMP Trap is sent by the AMM when a threshold is crossed. Enter the IP address to which the SNMP Trap is sent.
  - **Trigger on all events**: enable to set the threshold to trigger every time a value is reported to the AMM.

Important: *this option triggers the threshold to report each and every value to the stats selected. Therefore, it is recommended that it only be used for PNDError with the optional Nav application.*

- **Hold time***: enter a value between 0 and 600. This state will be held even if the value clears for the specified number of minutes.
- **Delay Time**: specifies an amount of time (in minutes) during which an error threshold whose criteria has been met, should be ignored (e.g. if driving at a

certain speed should trigger a speeding threshold error, but the user wants to allow a vehicle to be able to travel at that speed to pass other vehicles (e.g. for up to 1 minute), then setting a delay time allows that threshold to be ignored for the specified amount of time, without triggering the threshold error).

Set the *Error Conditions*

- **Error Criteria***: sets the criteria required for the stat's value to trigger an error (e.g. selecting greater than and then entering a value of 10 will generate an error when the stat's value exceeds 10). The meaning of the value is specific to each Stat and its units of measurement.

- **Extra Criteria**: enter up to four additional criteria (i.e. stats) that must be satisfied in order for an error to be sent. Upon selecting a stat for each criteria, the condition and value fields will become visible for configuration.

- **Actions***: select the actions to be taken to report a warning:
  - **Log Event**: default action. It is recommended that this remain enabled so that all warnings are written to a log file.
  - **Send Email**: select to enter the email address(es) to which an email will be sent, advising of the warning condition. Up to two email addresses can be entered, separated by a comma.
  - **SNMP Trap**: when enabled, an SNMP Trap is sent by the AMM when a threshold is crossed. Enter the IP address to which the SNMP Trap is sent.

- **Trigger on all events**: enable to set the threshold to trigger every time a value is reported to the AMM.

Important: *this option triggers the threshold to report each and every value for the stats selected. Therefore, it is recommended that it only be used for PNDError with the optional Nav application.*

- **Hold Time***: enter a value between 0 and 600. The state will be held even if the value clears for the specified number of minutes.

- **Delay Time**: specifies an amount of time in minutes during which a warning threshold whose criteria has been met, should be ignored (e.g. if driving at a certain speed should trigger a speeding threshold error, but the user wants to allow a vehicle to be able to travel at that speed to pass other vehicles (e.g. for up to 1 minute), then setting a delay time allows that threshold to be ignored for the specified amount of time, without triggering the threshold warning).

Click on **Save** to create the new threshold.

Thresholds can be deleted from the gateway by clicking in the checkbox next to the threshold label and then on **Delete**.

* denotes a required field

3.8.7 Zones

The *Zones* panel can be used to identify, add, and delete zones (e.g. virtual boundaries or geofences). Zones allow administrators to monitor vehicles in different ways. For example, if a vehicle is expected to only travel within a certain area, a threshold can be set up that triggers an alert when the vehicle leaves a zone.

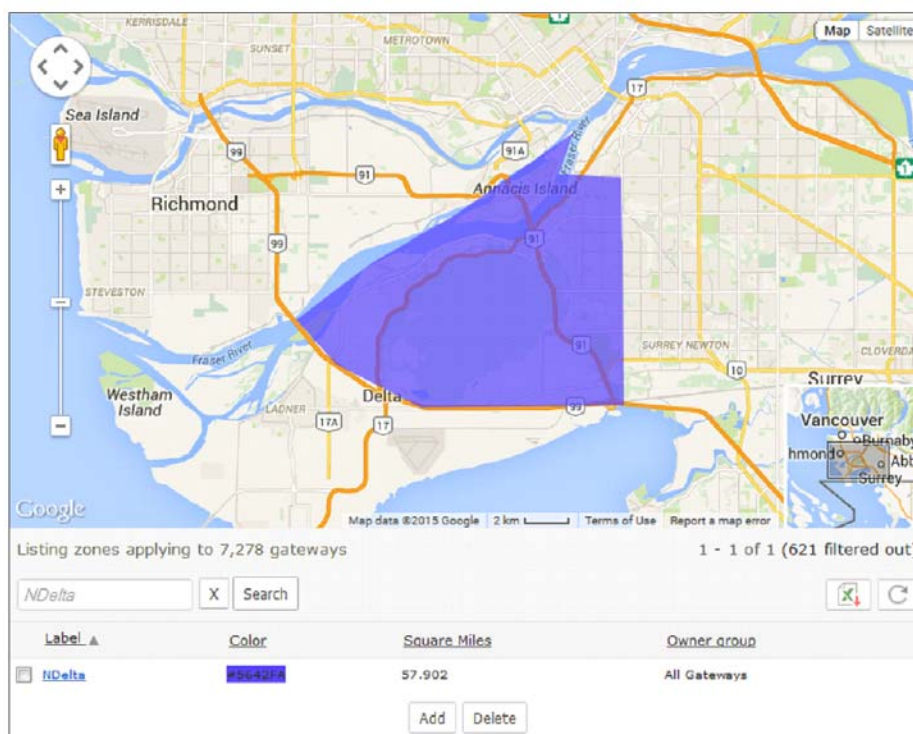*Note: for ALEOS devices, the communication frequency with the AMM determines the accuracy of threshold triggers with respect to zone boundaries.*

Figure 3-48: Zones Panel

Adding a new zone

1. Click on the **Add** button (located at the bottom of the zone list) to open the *Adding a Zone* panel and edit the following:
    *   **Label***: enter the name for the new label.
    *   **Owner group**: use the drop-down menu to select the preferred group.
    *   **Color***: click on the field to open the color picker or enter the 5-digit code (if known). Select a color and then click the *OK* button.
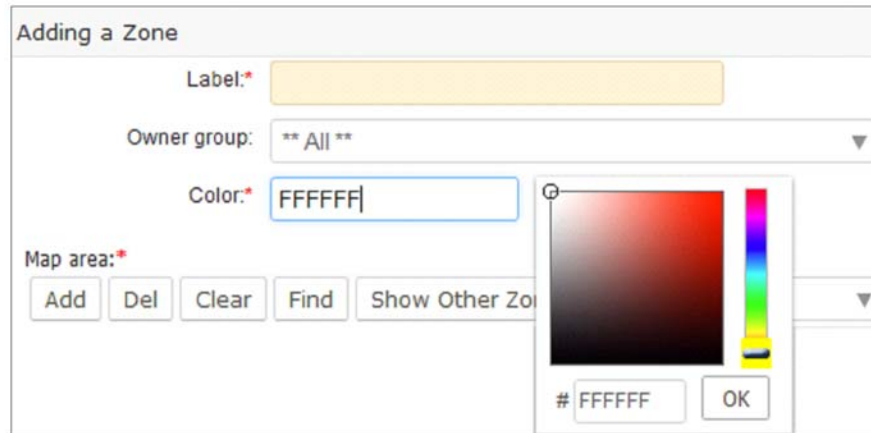
Figure 3-49: Zone Configuration Screen

2. The default map is a view of the world. Zoom in on the map to the area in which to create the new zone.

- Under *Map area*, click on **Add** to add a four-point rectangle on the map (the color will be the one chosen above)

Figure 3-50: Map Area Controls

Figure 3-51: Map Bounding Box

Each point is labeled; the top-left point is *point1*. Click and drag it to the first boundary for the zone.
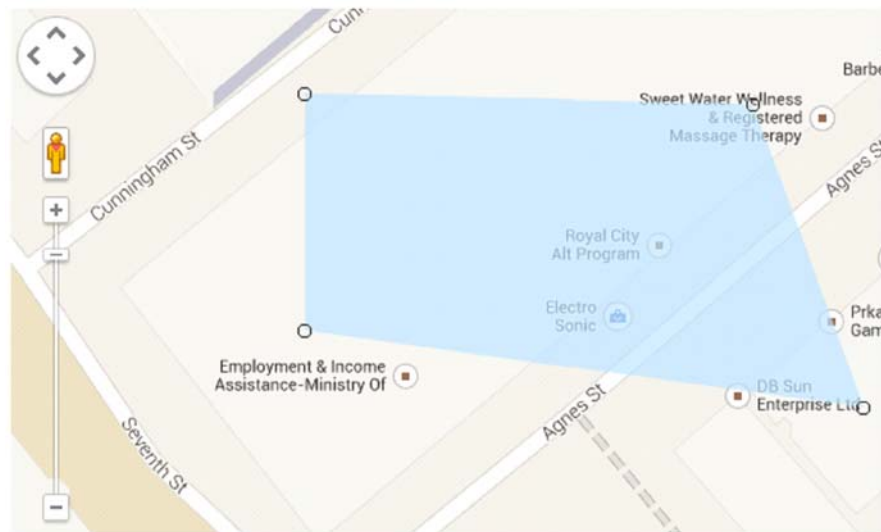
Figure 3-52:   Dragging a point on the bounding box

• Click and drag the remaining points to define the boundary.
• To refine the boundary, click on **Add** (in the Map area toolbar) to add additional points. The new points will be labeled in numeric order.
  · Adding more points results in a better-defined boundary, especially if there is a curve in the boundary.
  · Use the zoom in/out controls and drag the map to achieve the best views of the boundary areas.
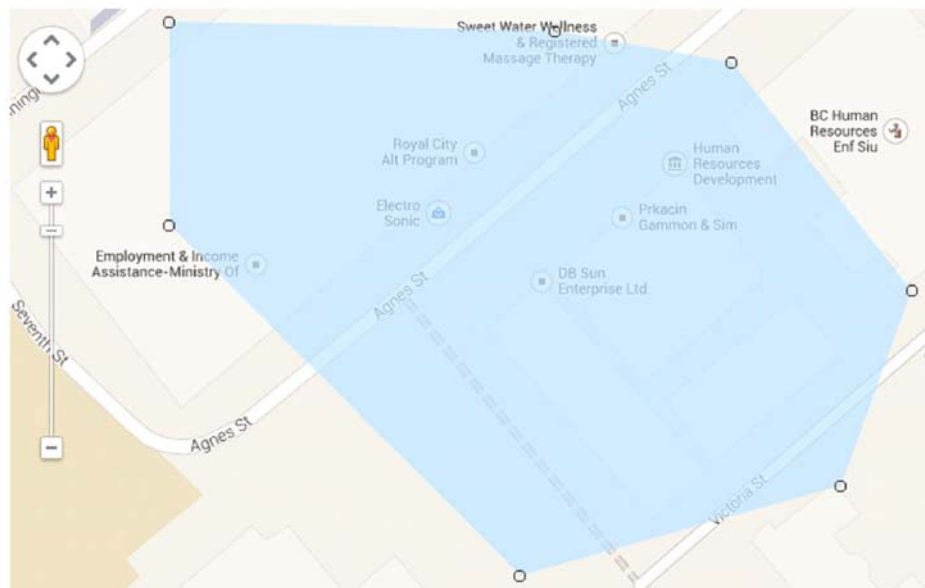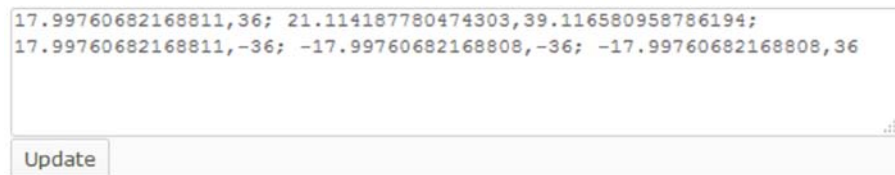
Figure 3-53: Adding more points to the bounding box

• To remove the most recently added or edited point, select the point, and click on **Del**.

- To clear the zone from the map, click on **Clear** (note that once cleared, there is no way to retrieve the zone).
- Click on **Find** to locate a location on the map.
- To display other zones on the map, click on **Show Other Zones**.
- To import an existing zone into the new zone, use the drop-down menu to select it. Using an existing zone provides a starting point and can facilitate quicker zone creation.
- Click on **Advanced** to define the zone using raw point text in latitude/longitude position pairs. Click on **Update** when complete.

```
17.99760682168811,36; 21.114187780474303,39.116580958786194;
17.99760682168811,-36; -17.99760682168808,-36; -17.99760682168808,36
```

Update

Figure 3-54: Raw Latitude/Longitude Pairs Used to Define a Zone

3. Click on **Save** to save the new zone.

Editing an existing zone

1. From the main *Zones* panel, click on an existing zone name in the list of zones, to open the editing panel.
2. From this panel, the zone's properties can be changed including the name, color, and owner group. Points can also be moved, added, and deleted to redefine the boundary.
3. Click on **Save** to save the changes.

Deleting a Zone

To delete a zone, select it from the main *Zones* panel and click on **Delete**. Alternatively, click on **Delete** from the editing panel.

Adding a Zone Alert

A zone alert can be used to detect when one or more gateways leave a zone. To create a zone alert, define a threshold as described in Chapter 3.8.6 - Thresholds, set the Group or gateway to the devices which are to be monitored for the zone, and set the **Stat** field to **GPS Locaiton Zone**.

3.8.8 Sessions

The *Sessions* panel provides the list of the users logged into the AMM. Information provided includes the IP address of the login host, the time the user logged in, the last page visited, the time at which the last page was visited, the time spent on the last page and the number of pages visited.

Information can be filtered by text and time and date. Use the drop-down menu to select a time period: *All (default)*, *Last Hours*, *Previous Days*, *Previous Months* and *Range*.

Figure 3-55: Sessions Panel

3.8.9 Remote Sessions

For appliance AMMs only (i.e. AMMs hosted by customers), the *Remote Sessions* panel provides a mechanism for administrative users to monitor and terminate remote LCI sessions that were initiated via the *Total Reach* tab (see Total Reach Tab for more information).

The information provided includes the port number, the gateway, the LAN host address, the host port, the date and time the session started and the user ID of the users connected.

Figure 3-56: Remote Sessions Panel

Sessions can be filtered by text and time and date. Use the drop-down menu to select a time period: *All (default), Last Hours, Previous Days, Previous Months and Range*.

The Remote Sessions panel will only be populated with sessions that have been initiated via the Total Reach tab (see Total Reach Tab for more information).

To terminate a session, select the session by clicking its checkmark box and then click on **Stop**.

3.9 User Activity

On appliance AMMs only (i.e. not hosted AMMs), the *User Activity* panel provides information about user activities. Information includes the date and time of the activity, the user who performed the activity (user ID), the host address, the node/ group ID and the action performed.

Activity can be filtered by text and time and date. Use the drop-down menu to select a time period: *All, Last Hours (default), Previous Days, Previous Months and Range.*

Figure 3-57: User Activity Panel

3.9.1 DNS Servers

The AMM can update a configured name server with the address of the currently active WAN link for an oMG. When a change of active link is reported to the AMM, the name server is updated with the address of the new active link. Before assigning a DNS server to the oMGs, it must first be created.

Note: this feature is not available for ALEOS-only deployments.

Figure 3-58: Panel Listing DNS Servers

Adding a new DNS server:

Figure 3-59: Add or Edit DNS Server Panel

- Click on **Add** to open the *Add or Edit DNS Server* panel
  - **Server name***: enter the name of the DNS server.
  - **Lifetime***: represents the amount of time that a DNS record for a certain host remains in the cache memory of a DNS server after the DNS server has located the host's matching IP address. The default is 300 seconds.

  By specifying this setting for a particular domain's DNS records, webmasters define the frequency of website content updates. A higher value allows for faster domain resolution times. The value can be set to several hours if no changes to the domain's DNS records are planned for the specified amount of time. When changes are required, decrease the outdated website data.
  - **IP address***: enter the IP Address or qualified name of the DNS Server to which DNS updates are sent when a Gateway's IP Address changes.
  - **Domain***: enter the domain of the name service of the DNS Server to update.
- Click on **Save** to save the new DNS server.

It is possible to define multiple server names with the same IP Address/hostname but with different domain names.

To delete a DNS server, select it from the main DNS Server panel and click on **Delete**. Alternatively, click on **Delete** from the editing panel. **Note: a DNS server cannot be deleted if there are oMGs associated with it.**

* denotes a required field

3.9.2 Debug

Debug is an administrative panel showing all of the actions which were performed on an oMG. The output can be used when contacting support to diagnose issues.

4: Optional Packages

4

The following subsections list some of the optional AMM add-on packages and the resulting tabs that will be available in the AMM. More information about the optional packages can be found in their respective user guides.

Note: the add-on packages listed are not supported for ALEOS devices. For more information on supported features see: Features Supported for ALEOS Devices.

Note: the order of tabs is specified by AMM administrators for each user.

4.1 Nav

The *Nav Application* is an optional package requiring installation on the oMG. It works in conjunction with a Garmin PND connected to the oMG to provide vehicle dispatch functionality on the AMM and two way messaging capabilities between a fleet of vehicles and a control center. When the package is installed, a Nav tab will be available in the AMM.
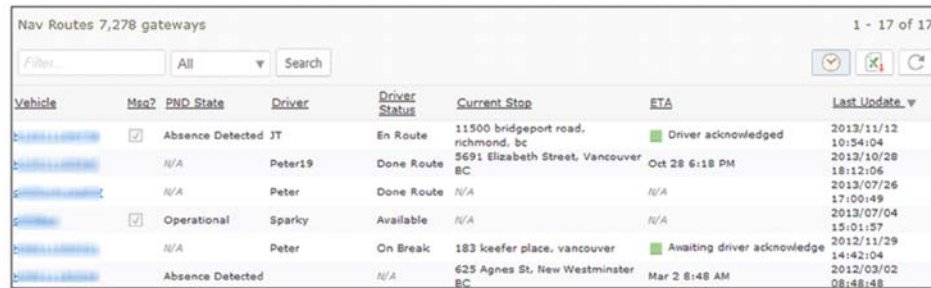
The Garmin PND and the oMG are physically connected via a serial cable and are installed in a vehicle. The PND automatically reports its location via the oMG to the AMM using the oMG's onboard application and wireless WAN connection.

At the control center, administrators can view real-time vehicle locations on a map displayed on the AMM and can dispatch vehicles to their next and future destinations using a simple user interface. Dispatching includes the ability for administrators to add and delete stops on the PND directly from the AMM.

Administrators are able to send and receive messages to one or more vehicles in the fleet at any time, and drivers are able to respond to incoming messages as well as send messages to dispatchers. Messages are received in the vehicle directly on the Garmin PND. Vehicle operators send or response to messages using the PND's message option which features an on screen keyboard. Administrators have the option to send "open ended" questions requiring the vehicle operators to type a response, or multiple choice questions in which vehicle operators can choose from a series of answers.

4.1.1 Nav Panel Overview

The *Nav* panel displays the status for the gateways:

Figure 4-1: Navigator Panel

The following information is available:

Vehicle ID: the ESN of the gateway in the vehicle.

Msg?: notification of messages from drivers.

- **PND state of the vehicle**: can be one of the following values: *Offline, Presence Detected, Absence Detected, Operational, Not Operational.*
- **Driver**: a value identifying the driver that has been programmed into the Garmin PND.
- **Driver Status**: can be one of the following values: *Available, On Break, En Route, Done Route, Unavailable.*
- **Current Stop**: the location currently being provided by the Garmin PND.
- **ETA**: the estimated time of arrival.
- **Last Update**: the last time the AMM received information about Nav.

4.1.2 Dispatching

To add a stop on a Garmin PND connected to a Gateway:

Locate the gateway from the list of gateways on the *Nav* panel and click on the unit's link:

Figure 4-2: Gateway Selection List

Enter a new address into the *New Destination* field, click **Add** to add it to the list of destinations and then click **Send** when the list is ready to be sent to the vehicle:
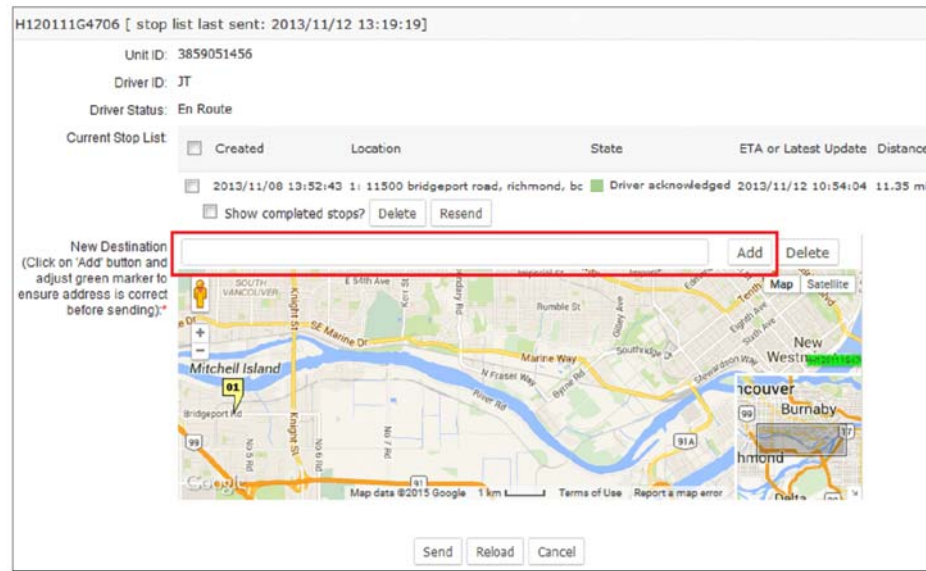
Figure 4-3: Adding a New Destination

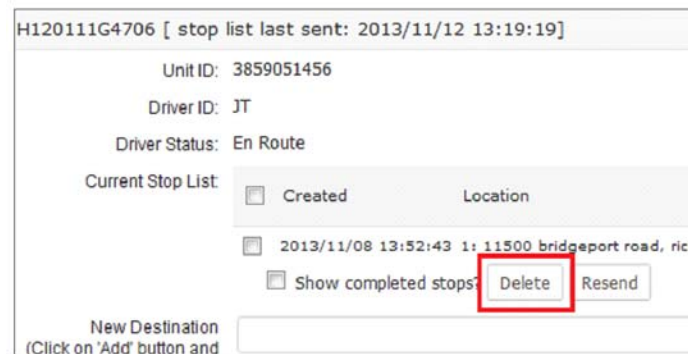To delete a stop, locate the destination in the list of stops and click **Delete**:

Figure 4-4: Deleting a Destination

4.1.3 Send Message

The *Send Message* panel allows administrators to send messages to the gateways.

Figure 4-5: Send Message Panel

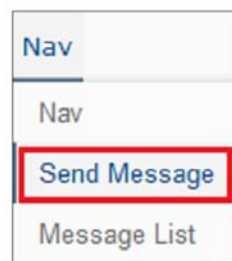To access the *Send Message* panel select **Nav->Send** Message:

Figure 4-6: Displaying the Send Message Panel

The following input fields are available:

Vehicle(s)*: under *Available Items*, click on the vehicle(s) and on the right-arrow to move it to *Selected Items*. The message is sent to the vehicle(s) in this field.

Email a copy to: an optional set of comma delimited email addresses to send the message to.

Message text: type the message to be sent to the gateway.

Response choices: type the response choices for the gateway. This field is optional and can be used to facilitate a response. Enter one response per line.

Click on **Send** to send the message.

* denotes required information

4.1.4 Message List

The *Message List* panel displays the messages sent by both administrators and gateways for the specified time period. Multi-cast messages (i.e. messages sent to more than one oMG) include hyperlinks for additional details.

Figure 4-7: Message List

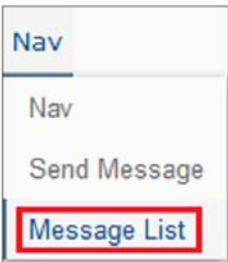To access the Message List panel select **Nav->Message List**:

Figure 4-8: Displaying the Message List Panel

Clicking on a message link opens the original message, along with the response(s) from the gateway(s):

Figure 4-9: Text Message Screen

To send a message:

1. Select the gateways from the Vehicle(s) list to which the message should be sent to.

2. Enter a text message in the Message field.

3. (Optional) Enter multiple responses that the recipient can select from.
4. Click **Send** to send the message. The recipient will receive it on their Garmen GPS device.

4.2 Telemetry

The *Telemetry* package displays data for vehicle performance and maintenance.

Note: as of AMM 2.15.2, the Vehicle Telemetry and Asset Manager applications are bundled together in the AirLink® Mobility Manager Operations Pack.

Using compatible scanner hardware connected to the vehicle's data bus (OBDII and HDODB), vehicle diagnostic information, such as odometer, fuel level and warning lights, is interpreted and presented. When the package is installed, a *Telemetry* tab will be available in the AMM.

Not all Dashboard items are applicable to the Telemetry panel. To select the items to be displayed, go to **Options > Preferences** and uncheck the *Dashboard Items* checkbox. This will display the items which can be selected and shown on the *Dashboard*.

Figure 4-10: Telemetry Tab

4.3 Asset Manager

The *Assets Manager* package displays data about the fleet's optional equipment and to which gateway the equipment is assigned and detected.

Note: as of AMM 2.15.2, the Vehicle Telemetry and Asset Manager applications are bundled together in the AirLink® Mobility Manager Operations Pack.

The information displayed allows users to track the equipment in transit but also warns when it is no longer in the vehicle (*State* column). Additionally, the last known location is available which makes for easy retrieval if the equipment is left

out of the vehicle. This package requires that small electronic devices called *asset tags* be attached to the devices to be tracked. These devices are then in turn, tracked by one or more oMGs.

When this package is installed, an *Assets* tab will be available in the AMM.
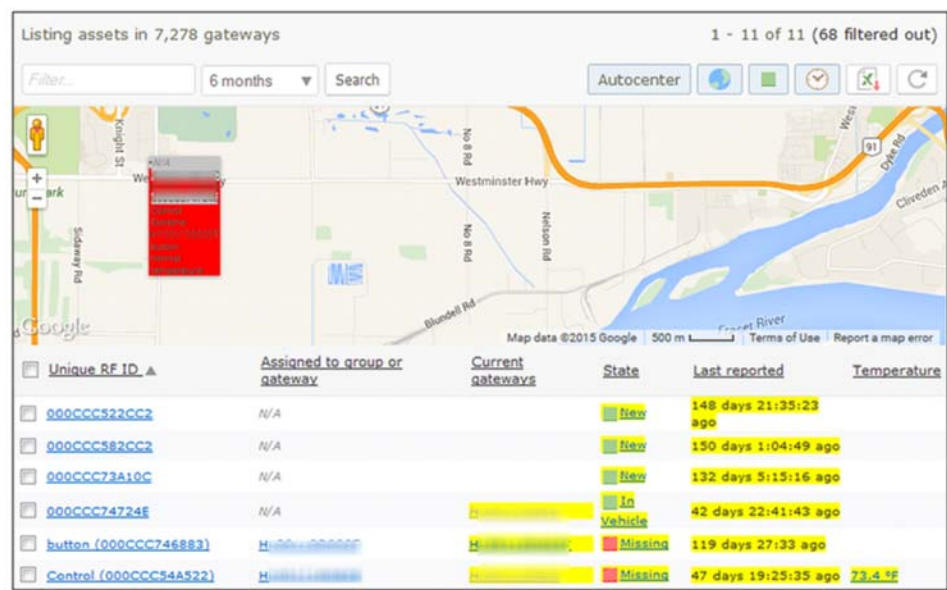
Figure 4-11: Assets Tab

The default name for the assets is their unique ID. To add a new asset, click on **Add**. Enter the information and click on **Save**.

Figure 4-12: Screen for Adding/Editing an Asset

To edit an asset, click on the individual asset, in the *Unique RF ID* column, to open the *Editing* panel. Update the information and click on **Save**.

Note: entering a single ESN or gateway name into the *Assigned to group or gateway* field will cause that unit to track the asset. Entering a predefined group name will allow all oMGs in the group to track and report on the asset.

The *Editing* panel can also be used to delete assets from the AMM. Select the asset from the main panel and click on **Delete**. The asset will return the next time the unit reports it.

5: Reports

Reports provide the true power of the AMM. In addition to reports for the core AMM functionality, reports are also available for optional applications which must be purchased separately. Details for these reports can be found in the separate Reports Guide.

Note: the majority of available reports only work with oMGs and not ALEOS devices.

To generate a report, select **Reports -> <Category> -> <Specific Report>**

Each report contains basic and advanced configuration options which are used for configuring the reports.

To show advanced configuration options, click on **Show Advanced Config** to display the advanced edit fields. The option will turn orange when enabled. Click on the orange button to disable the advanced edit fields.
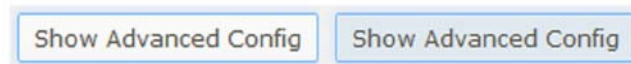
Figure 5-1: Toggling the Show Advanced Config Button

The option to show or hide the **Show Advanced Config** button is found in *Options > Show Advanced Edit Fields*:
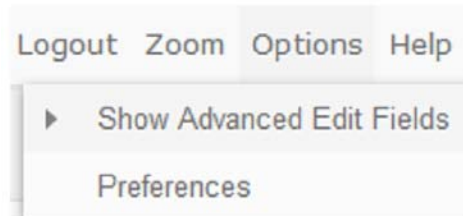
Figure 5-2: Menu to Show or Hide the Show Advanced Config Button

Click on **Run Now** to generate the report immediately. Click on **Run in Background** to run the report in the background and to save the report on the server (go to **Results** for the report). Click on **Save** to save the report for future use without immediately generating it.

Reports also provide the following functions:

Figure 5-3: Additional Report Functions

Save Results: Allows the report to be saved on the AMM. To view the report, navigate to **Reports >Generated Reports** (also be sure to specify the day that the report was run on the selection criteria of the Generated Reports listing screen).

Excel: Open and/or save the report in Excel.

Change: Change the report but retain the same gateway(s) and information in the input fields.
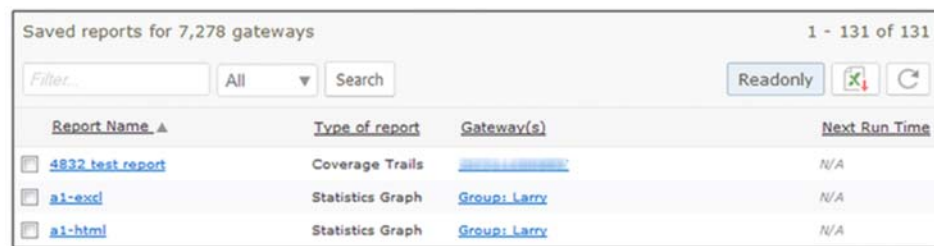
Edit: Edit the existing report input fields to generate different results.

For information on the various reports available, see the AMM Reports Guide.

5.1 Saved Templates

Saved Templates are scheduled reports to be run in the future. Users can configure the report to run on a scheduled day at a specific time.

The example below shows that the *Statistics Graph* was scheduled for one gateway on two different days, while the Event Viewer Reports were scheduled for 3 different gateways.

Figure 5-4: List of Saved Templates

To edit a report, click on its name. To delete a report (or several), checkmark it and click on **Delete**.

5.2 Generated Reports

The *Generated Reports* panel contains the list of all saved reports. When generating reports, users can save the report to the server.

Reports are listed with the most recent at the top. Click on a report name to view it. Click on a column header to sort the list. To delete a report, select it and click on **Delete**.

To filter the list, select a time period from the dropdown, enter a value into the filter box and click **Search**. This will list only those reports which were generated within the specified time period.

Figure 5-5: List of Generated Reports

Upon clicking on a generated report in the list, the report will be displayed and the following options will be available:
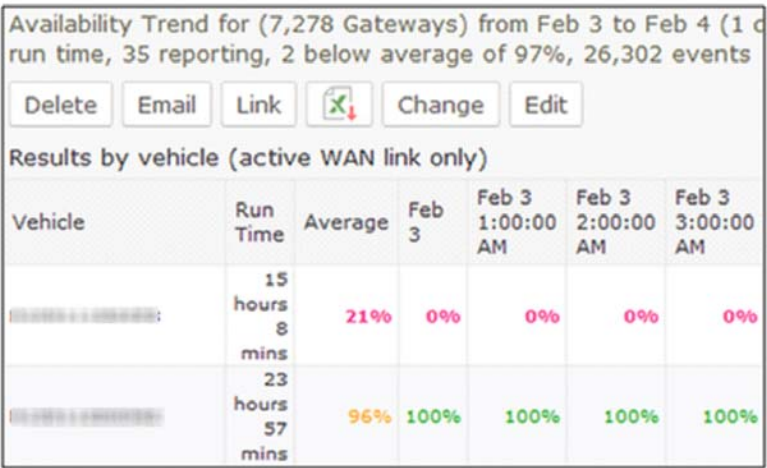
Figure 5-6: Available Options on a Generated Report

Delete: deletes the current generated report

Email: provides a popup through which the report can be emailed to one or more recipients. The popup provides fields to specify recipient email addresses, the sender, a subject, and a custom message. The custom message is prepended to the report content in the email.

Note: the AMM will automatically append a link to the report at the bottom of the email. The base URL of this link is configured by the AMM administrator and if it is changed, the backend processes of the AMM must be restarted in order for the new base URL to be used in the report emails. For hosted AMM's, contact Support to restart these processes.

Link: displays a popup containing the URL to the report which can be copied and pasted for later use (e.g. to send in an email).

Excel: exports the report to Excel.

Change: provides a list of all report types, allowing the report to be changed to a different report type.

Edit: displays the report edit screen where report parameters can be changed.

6: Common Procedures

This chapter describes common procedures that can be performed on the AMM.

Note: if the menus listed in the following sub sections are not available on your AMM, please contact Support for assistance in adding them.

6.1 Copying Configurations Between Gateways

The Copy and Deploy panels are used to copy a configuration from a source device to one or more target devices.

The *Copy* panel is used to specify a configuration as a *template* from one source gateway, and to allow selection of one or more target gateways. The AMM then prepares the configuration file(s) to be copied.

The *Deploy* panel is used to apply the configuration files to the selected gateways. The panel also provides information about each target device's configuration state, and provides additional functions for dealing with out-of-sync configurations.

The following steps describe this process:

Note: this procedure applies to both oMG and ALEOS devices. However, the target and destination devices must be of the same type.

1. Navigate to the Gateway tree in the AMM.
2. Select the device from which the configuration files are to be copied.
3. Navigate to **Config->Deploy->Copy** as shown in Figure 6-1 or right click on the device and select **Copy Configuration**.

Figure 6-1: Config->Deploy->Copy Menu

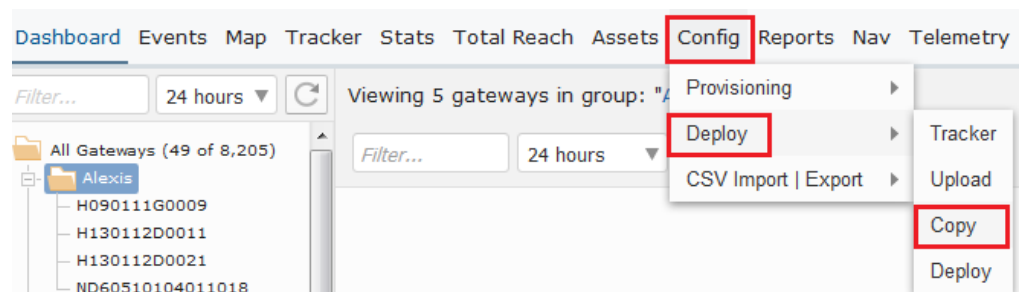One of the following popups will be displayed:

- **Configuration Confirmed**:

Please be advised that the source gateway's configuration was last confirmed on Thu Apr 14 15:33:57 P
2016. To get a more up-to-date confirmed configuration, please use the Revert action for this gateway on
Config/Deploy/Deploy page.

> This message is displayed for ALEOS gateways because the AMM does not have a reliable way to confirm that it has the latest configuration from the gateway, and so the onus is on the user to confirm this. This may not be displayed for oMGs because they usually notify the AMM regarding out-of-band configuration changes. However, if an oMG is not *remote enabled*, then the message will be displayed. Reverting will instruct the AMM to throw away its copy of the configuration and retrieve the version from the gateway, under the assumption that the user has used a master gateway to build up the config to be pushed out to the rest of the fleet.

- **Configuration not Confirmed**:

The system has detected that the gateway selected as 'Source' for the Copy Config operation is not in Syr
which indicates that oMM does not have the latest configuration from the gateway. It is advised to wait for t
synchronization to take place prior to attempting the copy operation again.

> This message may be displayed for ALEOS and oMG devices, and indicates that the configuration on the source gateway is not in sync with the AMM. Either wait for a syncronization to occur, or use the **Sync** button on the Deploy screen to force a sync.

Note: the following functions are available on the Deploy screen for these states: Revert, Force, Apply, Hold, and Copy.

Note: this panel is also available by locating the source gateway in the Gateway Tree, right-clicking on it, and selecting Copy Configuration.

Note: by default, the selected gateway will also be selected as a destination device to copy to, and a respective warning will be displayed indicating this.

---

4. Verify that the device in the *Source* field matches that which was selected in Step 2.

5. Click on a device from the Gateway tree to select it as a target, or hold down Ctrl and then click on multiple gateways to add multiple targets. This will add the gateway(s) to the **Copy Config to** field. Alternatively, enter the ESNs or names of one or more devices, separating each device ESN/name with a comma. Be sure that the ESN/number of the source device, which was added by default as a destination device, has been removed from this field.

6. Select **All Files** to copy all configuration files, or uncheck this field and select the individual files to copy. Note that some devices only have a single configuration file. Figure 6-2 shows the selection of specific files for an oMG.
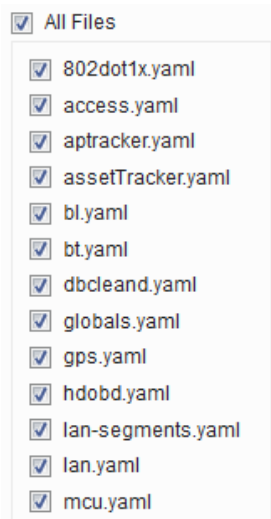
Figure 6-2: Selecting configuration files to copy on an oMG.

7. (Optional) Click **Skip Version Check** to ignore inconsistencies between the source and target device versions. Only enable this option if you are certain that the source and target gateways are compatible, despite any version discrepancies.

8. (Optional) Click **Skip Platform Check** (available for ALEOS only) to ignore inconsistencies between the source and target device types. Only enable this option if you are certain that the source and target gateways are compatible, despite any platform discrepancies.

9. (Optional) Click **Reboot automatically after changes are applied** (available for ALEOS only). The destination devices will reboot once the selected files have been successfully copied to them. It's recommended that this option be left as enabled, to match the behavior of ACE Manager.

10. Click **Copy**. The selected files will be scheduled for copy to the specified destination devices and the AMM will redirect to the *Deploy* screen. If there is a syncronization issue between the configurations, an error message will be displayed and the AMM will remain on the *Copy* panel in which case the issues will needed to be resolved manually. For more information about configuration states and available functions see: Deploy).

11. Review the *State* column on the *Deploy* panel for each target gateway and manually correct or deselect any that are not in the *Modified* state.

12. Click the **Apply** button. The changes will be pushed to the devices when they check in and their state will change to *Out of sync-local* until the configuration update is complete. Once complete, the state will change to *In-Sync* for oMGs and *Config Confirmed* for ALEOS devices. Note that for an ALEOS device, this process will start when the device checks in. For an oMG device, this process will start immediately if the device is online and communicating.

6.2 Adding Multiple Gateways to an AMM

AMM 2.15.1.1 and above includes a feature to import multiple gateways using device ID information stored in a CSV file.

An additional benefit of this feature is that it can also be used to reorganize the folder structure for existing gateways and move those gateways into new groupings.

Use the following steps to import multiple gateways from a CSV file:

1. Click on the **Upload** button:
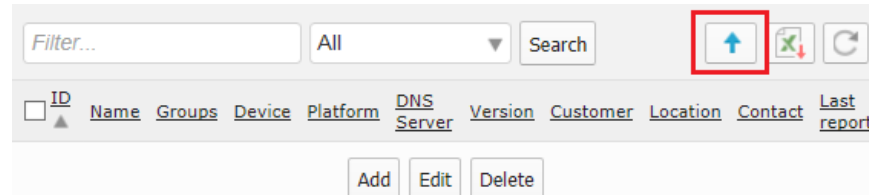
Figure 6-3: The upload button which provides the ability to add multiple gateways

2. Click **Template** to generate and open a new CSV file.
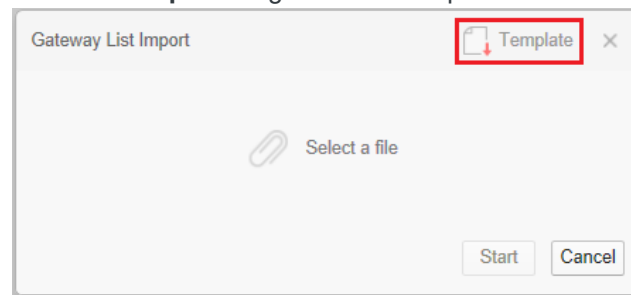
Figure 6-4: Creating a new CSV from the template.

3. Open the file in a spreadsheet application.
4. Edit the CSV file to include information about each gateway to add to the AMM. See Device CSV for more information about how to populate this CSV file.
5. Save the CSV file.
6. Click **Select a file** and select the CSV that was saved to disc.
7. Click **Start** to import the devices.

After the import is complete, a summary page is presented to provide information about the result of the import process.

6.3 Transitioning AirLink Gateways from ALMS to the AMM

This section describes how to transition AirLink gateways which are currently managed through the Air Link Management System (ALMS), to report to an AMM instead.

Figure 6-5 shows an example AirLink device in ALMS called *Warren's GX450*, that is to be transitioned to an AMM:
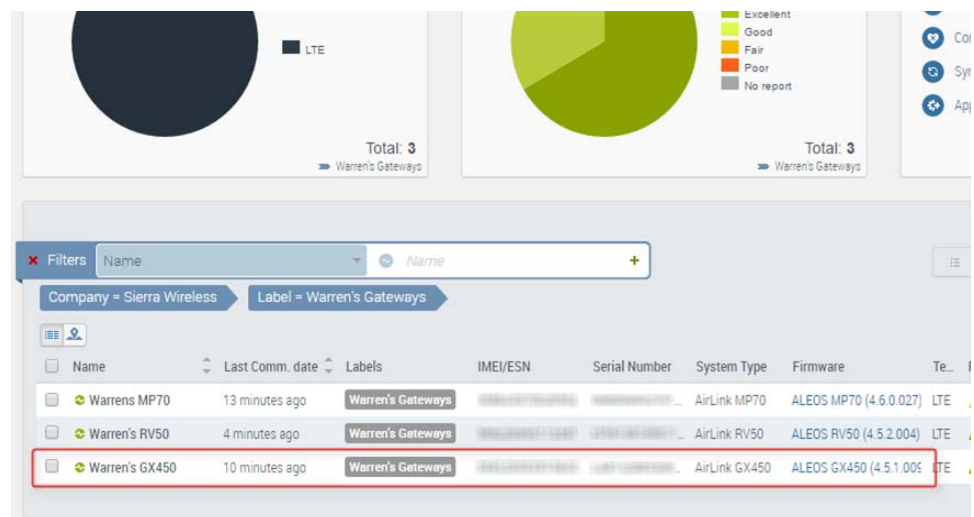
Figure 6-5: An AirLink Device Managed on ALMS that is to be transitioned to an AMM.

The gateway is currently configured to report to ALMS as shown in Figure 6-6:

Figure 6-6: Current Server URL of the Device to Transition from ALMS.

To transition the AirLink device, log in to ALMS and update the **Server URL** field to point to the IP address or URL of the AMM.

To perform this process for a fleet of gateways, use a template as described in the following steps:

1. Log in to ALMS.

2. Navigate to **Configure->Templates**.

3. Click the green "+" dropdown and select **Brand-new**:
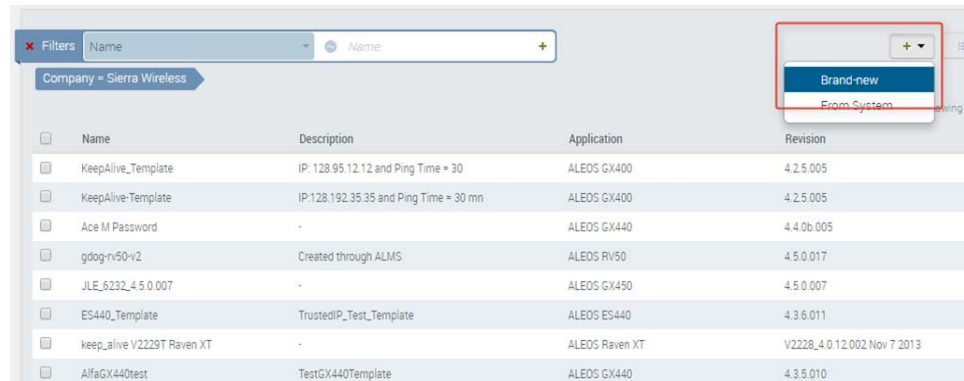
4. Select the appropriate firmware for the type of gateway being transitioned. In the example above, a GX450 (ALEOS GX450 (4.5.1.009)) is being transitioned. For multiple gateways of different types, a separate template will need to be created for each gateway type.

Tip: *the amount of work required to transition gateways can be significantly reduced by first updating all of gateways to a consistent (and ideally latest) version of the firmware for each gateway type. Use the Update status widget on the main dashboard to see the current state of the fleet, and upgrade those gateways that are not current.*

---

5. Ensure the following fields have been configured in the **Services/ALMS/ General** section:
   - **AirLink Management Service**: set to enabled.
   - **Server URL**: set to either of the following:

        http://ip_address:8082/msci

        https://ip_address:8083/msci

Note: the IP address can be replaced with a fully qualified domain name.

   - **Device Initiated Interval**: set to the preferred communication frequency. For an on-premise AMM, the frequency can be set to a low as one minute.

6. Click **Save**:

7. Name the template and provide a description:

8. Navigate to the **Monitor -> System** page in ALMS.

9. Select the appropriate device in ALMS and click **Apply template:**
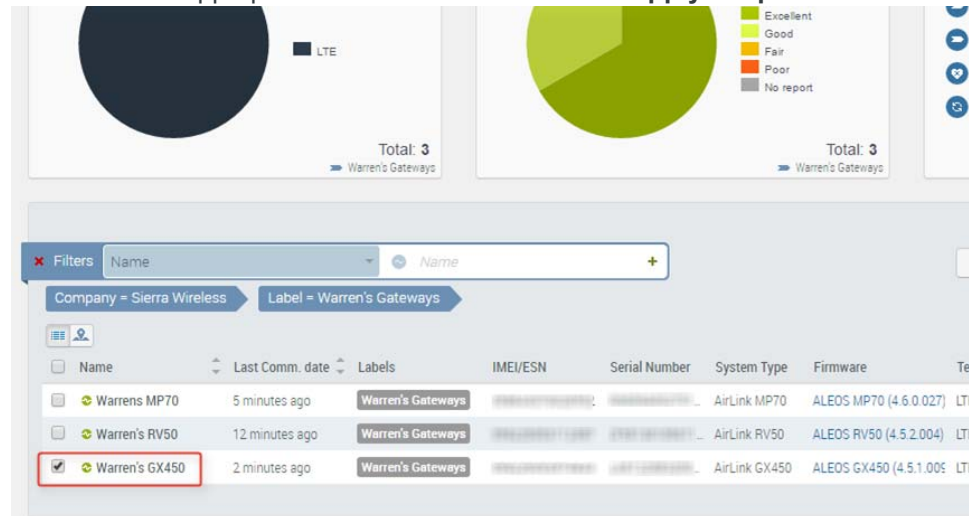
10. Select the newly created template and click **Apply template**. Choose to reboot the device and optionally schedule the reboot in *Advanced Settings*. An *Apply Settings* operation is launched. The next time the gateway checks in, it will apply the template, reboot the gateway, and have it redirected to the AMM.

11. Log out of ALMS,

12. Log in to the AMM.

13. Navigate to **Admin->Gateways**.
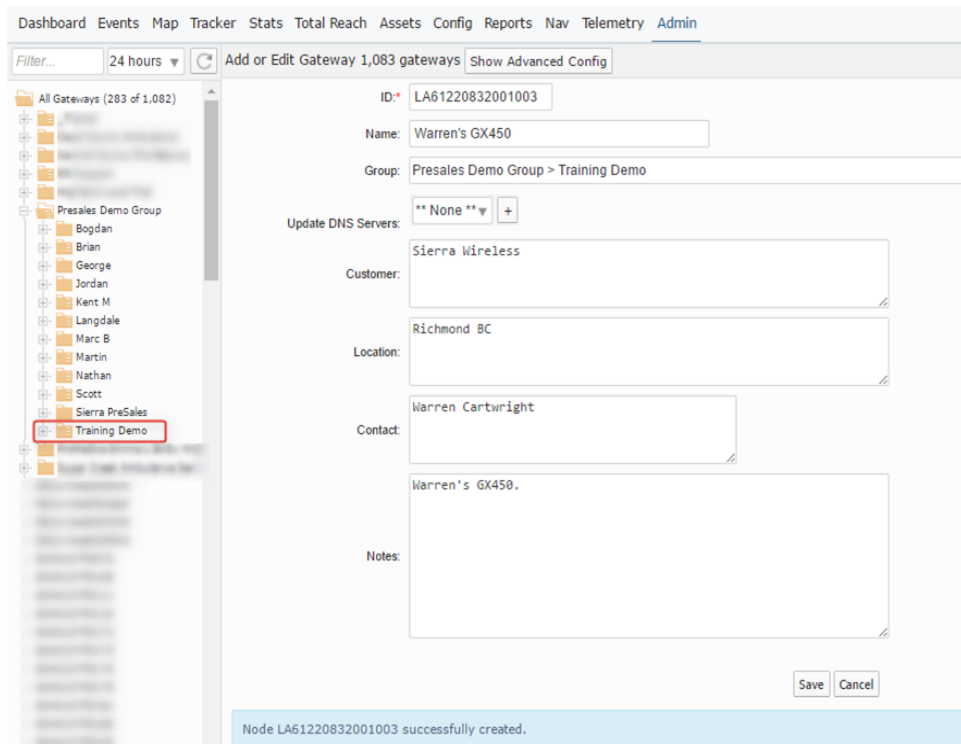
14. Click **Add** at the bottom of the screen.

15. Pre-populate the details of the gateway, as they should appear in the AMM:
    - **ID**: use the serial number of the gateway.
    - **Name**: enter a friendly name.
    - **Group**: preselect the group to place the gateway into. Use the **Admin -> Groups** feature to create groups, if they do not exist.

Note: the other fields are optional.

Note: as an alternative to adding individual gateways to the AMM one by one as described in steps 13 to 15 above, oMM 2.15.1.1 and above supports adding multiple gateways using a template. This can also be used to organize gateways into desired groups. See Adding Multiple Gateways to an AMM for more information.

Figure 6-7: Pre-Populating Gateway Details

Once the gateway receives its updated device management reporting location and calls in to the AMM, the device will show up either in the main directory listing, or in the folder that was pre-populated when the gateway was registered:

Figure 6-8: The Gateway in the AMM after calling in to the AMM

A: CSV File Information

A

The content of the CSV files includes a number of comments at the start of the file each of which is preceded by a "#" character to denote that it's a comment. The comments provide hints and information about how the files should be modified/edited. This is followed by one "header row" containing the column names, and then one or more rows of data as specified below.

Note: these files are not supported for ALEOS devices. For more information on supported features see: Features Supported for ALEOS Devices.

A.1 WAN CSV

The WAN WiFi CSV file contains the following information:

ESN: the ESN of the oMG for which the settings apply to/should be applied to.

WiFiNetworkName: the name of the WiFi access point profile that the settings are for.

SSID: the SSID of the access point.

PSKKey: the PSK passphrase for the access point.

PSK: the pre-shared key for the access point.

The following is a sample of a .CSV file for WIFI configuration:

Table 1-1: Sample WIFI Configuration

This CSV file contains a header line followed by the data lines representing the selected ESNs and their WIFI configuration.
The header line identifies the fields that are needed to configure the WIFI networks for an ESN.
For Import to work: the header must be complete and match the data lines that follow.
Each line must have the ESN followed by one or more WIFI networks.
Each WIFI network is defined by a set of fields: WiFiNetworkName SSID PSKKey PSK
You should only update the PSK field. If any other field is modified: Import will not work.
The fields in a WIFI network must be positioned in the exact order without any additional field in the set.
#

ESN	WiFiNetworkName	SSID	PSKKey	PSK

Table 1-1: Sample WIFI Configuration

H111111G00 21	Test-WPA2-PSK-AES(N)	Test-WPA2-PSK-AES(N)	mypassphrase	zzbbffddeeff11 2233445566ff
H111111G07 65	Test-WPA2-PSK-AES(N)	Test-WPA2-PSK-AES(N)	mypassphrase	aabbffddeeff11 2233445566ff

The following rules must be adhered to when modifying and deploying WAN WiFi CSV files:

- There must be one "header row" containing a contiguous set of columns with the following names: ESN, WIFINetworkName, SSID, PSKKey, PSK.
- A valid value for each column must be specified for each data row.
- Each ESN specified must be for a valid oMG connected to the AMM.
- Each selected oMG must have a corresponding row in the CSV.
- The configuration of each selected oMG must be in sync with the configuration on the AMM.
- Each WIFINetworkName value in the CSV must be unique (i.e. different configurations for the same WIFINetworkName are forbidden).
- Duplicate rows (i.e. rows with same values for each column) are forbidden. However, if duplicate rows are found, the last instance will be used.
- The PSKKey value must contain a hex or passphrase and must match that configured on the specified oMG. Note that this value is automatically derived based on the PSK entered on the oMG.
- The PSK must be either a hexadecimal value 64 bytes in length, or between 8 and 63 ASCII characters in length depending on the value of PSKKey.
- The PSKKey, and SSID must match those configured for the specified WiFi access point profiles on the specified oMG(s).
- Each oMG must be remotely configurable.
- Each WIFINetworkName listed in the CSV must be configured as an access point profile for the specified oMG. Likewise, each access point profile configured on each oMG must be listed in the CSV.

A.2 WLAN CSV

The WLAN WiFi CSV contains the following information. Note that the information (excluding the ESN) is stored both for the physical WLAN and the three virtual BSSID's.

ESN: the ESN of the oMG for which the settings apply to/should be applied to. Note: this field cannot be changed via the .csv file.

WLANDeviceName: the friendly name of the WLAN profile. Note: this field cannot be changed via the .csv file.

Channel: the WiFi channel (i.e. centre frequency) within the spectrum to be used.

NetworkType: the version of the 802.11 protocol to be used by this access point (either 802.11b/g or 802.11n).

Mimo: if set to "y", multiple WAN antennas are enabled for Multiple Input Multiple Output (MIMO) operation. If set to "n", MIMO is disabled.

SecondaryChannel: the channel which is combined with the primary channel to provide a 40 MHz channel instead of a 20 MHz channel.

LanSegment_x: the name of the LAN segment assigned to the access point.

IsAutoSSID_x: if set to "y", the SSID (Service Set Identifier) field for the WLAN has been auto generated by the oMG. If set to "n", the SSID was manually entered.

SSID_x: the SSID. Can be auto generated or manually entered as indicated by *IsAutoSSID* above. Note: this field cannot be changed via the .csv file.

IsBroadcastSSID_x: if set to "y", the WiFi device broadcasts its SSID. If set to "n", the SSID is not broadcasted.

EnableWMM_x: if set to "y", support for WMM (Wireless MultiMedia extensions) has been enabled for the device. If set to "n", WMM has not be enabled.

Encryption_x: specifies the type of encryption used by the access point.

Note: depending on the encryption selected, additional fields will be included specific to that encryption type.

For more information on WLAN settings see the *oMG Operations and Configuration Guide*.

The following are example fields of a .CSV file for WLAN configuration. Note that the large number of encryption specific parameters which normally follow the *Encryption* column have been left out due to space constraints:

- **ESN**: H111614G1832
- **WLANDeviceName**: Atheros WLM54AG @ mini-PCI Slot
- **Channel**: 11
- **NetworkType**: 802.11b/g
- **Mimo**: n
- **SecondaryChannel**: none
- **LanSegment_1**: y
- **IsAutoSSID_1**: y
- **SSID_1**: $ESN
- **IsBroadcastSSID_1**: y
- **EnableWMM_1**: n
- **Encryption_1**: WPA/CCMP

The following rules must be adhered to when modifying and deploying VPN CSV files:

- There must be one "header row" containing a contiguous set of column names.
- Each oMG must be remotely configurable.
- Each selected oMG must have a corresponding row in the CSV.
- Each configuration field must be configured on the selected oMGs.

- Values in the CSV must be present and must match those on the selected oMGs.
- Each selected oMG must be in sync with the AMM.

Duplicate rows (i.e. rows with same values for each column) are forbidden. However, if duplicate rows are found, the last instance will be used.

A.3 VPN CSV

The VPN CSV contains the following information:

ESN: the ESN of the oMG for which the settings apply to/should be applied to.

Pre-shared_key: the PSK to use for accessing the VPN.

VPN Name (optional): specifies the VPN for which the pre-shared key applies. If specified, the AMM will only import those rows whose VPN Name matches that of the selected VPN currently open on the provisioning screen. If left blank, the AMM will assume the settings for a row are relevant to the selected VPN currently open on the provisioning screen.

The following is a sample of a .CSV file for VPN configuration:

Table 1-2: CSV for VPN

# This CSV file contains a header line followed by the data lines representing the selected ESNs and their configurations.			
# VPN Name column is for users who have multiple VPNs and want to consolidate upload data of all VPNs in one master CSV. Leave column empty if you do not use this feature.			
ESN	**Preshared_key**	**VPN Name**	
H111111G3111	ABC1234	testvpn	

The following rules must be adhered to when modifying and deploying VPN CSV files:

- There must be one "header row" containing a contiguous set of columns with the following names: *ESN*, *Preshared_key*, and *VPN Name*.
- Each oMG must be remotely configurable.
- Each selected oMG must have a corresponding row in the CSV.
- Each tunnel name must be configured on each selected oMG.
- Each configuration field must be configured on the selected oMGs.
- Values in the CSV must be present and must match those on the selected oMGs.
- Tunnel names must be unique.
- Each selected oMG must be in sync with the AMM.
- Each VPN profile must exist on the selected oMGs, and each VPN profile from each selected oMG must be in the CSV.
- Duplicate rows (i.e. rows with same values for each column) are forbidden. However, if duplicate rows are found, the last instance will be used.

A.4 Multiple Device Import CSV

The device CSV is used for importing multiple devices into the AMM and contains the following information:

ID: the serial number of the device to import into the AMM.

Name (optional): the friendly name of the device as it is to appear in the AMM.

Groups: the names of one or more groups within the AMM to add the device(s) to.

Note: multiple device import is supported in oMM 2.15.1 and above, and is only available to users who have administrative access to the Admin->Gateways screen.

The following is a sample of a CSV file for VPN configuration. The first row of data shows a gateway being added to two folders, the second row of data shows a gateway being added to a single folder, and the third row shows a gateway being added to a subfolder.

Table 1-3: CSV for Device Import

```
# This CSV file contains a header line followed by the data lines representing the
 gateways to be imported to the oMM.
#
# -A comma (,) is required as a field delimiter.
# -Double quotation marks (") are required for any fields containing commas.
# -A greater-than sign (>) is required as a delimiter for groups.
# Example: CA10882023210,Unit 102,JT > AirLink
#
# -Groups that do not exist in the oMM will be created as defined by the structure in the
 CSV file.
# -Duplicate IDs in the CSV file will be ignored except for the first instance.
# -Options will be provided for user to decide how to deal with a gateway entry in the CSV
 file if its ID already exists in the oMM system.
# -Users can choose to ignore the entry or instruct the oMM to modify the gateway name
 and group in the system according to the CSV file if these fields are not empty.
# -Entries without group information which do not already exist in the oMM system will
 be populated with the group the user was assigned to in Admin->Users.
# -All gateways being added/modified via CSV import will be logged in User Activity.
```

ID	Name	Groups	
H111111G3111	Bob's Gateway	"Fleet1,Fleet2"	
H241511G2191	Jon's Gateway	"Fleet 1"	
H351511H3122	Mary's Gateway	"Fleet 1>Users>Super Users"	

The following rules must be adhered to when modifying and deploying CSV files which importing devices:

• There must be one "header row" containing a contiguous set of columns with the following names: *ID*, *Name*, and *Groups*.

• The value for the Groups column must be surrounded by double quotes when more than one group name is provided.

- Device ID's must be unique.

Note: if a gateway listed in the CSV already exists on the AMM, it will be moved to the group(s) specified in the CSV, if they differ from those to which the gateways are assigned to on the AMM.

B: Features Supported for ALEOS Devices

This section lists the features of the AMM that are available for ALEOS devices.

B.1 Tabs

Main tabs:
- Dashboard
- Events
- Map
- Stats
- Config - only the following two sub menus are supported:
  · Copy
  · Deploy

  See Config Tab for more information.
- Reports (see AMM Reports Guide)
- Admin - all sub menus are supported except for *DNS Servers*. See Admin Tab for more information. Note that some features may be platform specific.

For more information see Main Tabs.

Additional tabs:
  · Logout
  · Zoom
  · Options - all options are supported
  · Help

For more information about tabs see Option Tabs

B.2 Gateway Tree Menu Context Menus

When right-clicking on ALEOS devices, the following menus/functionality are supported:
- Delete
- Details
- Request Reboot
- Copy Configuration

For more information about these features see: Changing Gateway Details.

When right-clicking on a fleet of ALEOS devices, the following menus/functionality are supported.
- Delete group
- Rename group

- Create group
- Move group here
- Move vehicles here

Note: when a fleet of mixed ALEOS and oMG devices is selected, additional menus applicable only to oMG devices may also be shown. For customer fleets consisting of only ALEOS devices, these additional menus will be disabled. If oMG devices are added and selected, these menus will become enabled.

For more information on these features see: Groups and Sub-Groups.

B.3 Stats Reported by ALEOS Devices

This section lists the stats that can be reported by ALEOS devices. Note that ALEOS devices may not report stats with every communication, and stats related to hardware not supported by a device will not be reported (e.g. if a device does not support GPS, then it will not report GPS stats).

Note: oMG devices report more stats than ALEOS devices, some of which are not reported by ALEOS devices.

B.3.1 Implicitly generated as Misc Events

- **Gateway Type:** the type of gateway (oMG or ALEOS).
- **Cell Technology**: the radio technology being used.
- **Current Operator**: the network operator.
- **MDN**: the phone number:
- **Platform**: the type of platform (e.g. oMG, GX400, RV50, etc.).
- **SoftwareVersion**: the version of the device's software.
- **RSSI**: the received signal strength indication.
- **RadioFirmwareVersion**: the version of the device's radio firmware.
- **BuildString**: the build number of the ALEOS software.

B.3.2 Generated through specific DELS events

- **ConfigurationState**: the configuration sync status of the gateway.
- **GPS Location-latitude / GPS Location-longitude**: the device's GPS coordinates.
- **GPS Location-miles**: the miles traveled on a given day.
- **GPS Location-speedmph**: the speed, in miles per hour.
- **GPS Location-zone**: the zone in which the gateway traveled. See Zones for more information.
- **GPS Satellites**: the number of satellites that are in view.
- **GPSFix**: the time since the last GPS fix.

- The following stats provide WAN information for the active link:
  - **LinkX-ActiveLink**
  - **LinkX-IPAddress**
- The following stats provide WAN information for AirLink.
  - **Reserved0-CallUpTime**
  - **Reserved0-IPAddress**

Note: the AMM converts the metric GPS data obtained from ALEOS devices into miles. The AMM will then display the data in the units set by the user in the AMM's preferences.

B.3.3 Other

- **ReportIdleTime**: represents the device's heartbeat.
- **RemoteSocketAddress**: the remote socket address reported by Airlink.

C: Firewall Considerations

The AMM requires the following TCP/IP and UDP/IP access.

Note: that oMG to AMM communications can all be embedded into the SSL VPN.

Note: in the following table, To in the Direction column refers to traffic going to the AMM, and From refers to outbound traffic from the AMM.

Table 3-1: TCP/UDP Port Summary

Purpose	Service	Protocol	Port	Direction	Description
oMG	Ping	ICMP	N/A	To/From	Used to verify communication between an oMG and AMM.
	Messages	TCP/UDP	1501	To/From	TCP: optimized bulk oMG to AMM messages. UDP: optimized individual oMG to AMM messages. Note: optional - only open if the Management Tunnel (Port 1194) is not in use.
	SSH	TCP	9987	To	Secure copy for log files from oMG to AMM. Note: optional - only open if the Management Tunnel (Port 1194) is not in use.
	SSH	TCP	2222	From	Used for deployment services.

Table 3-1: TCP/UDP Port Summary

Purpose	Service	Protocol	Port	Direction	Description
System	Email	TCP	25	From	AMM to user email. Note: only open if the AMM is not using an internal relay server to send emails.
	DNS	UDP	53	From	Name resolution for email. Note: only open if the AMM is using an external DNS server.
	NTP	UDP	123	From	System time synchronization. Note: only open if the AMM is using an external time server.
	Software Upgrades	TCP	80	To/From	Used for AMM software upgrades being done on a private APN or full IPSec tunnel. Destinations: • repo1.inmotiontech-nology.com • repo2.inmotiontech-nology.com
	SSL VPN	UDP	1194	To/From	oMG/tech support Management tunnel, and AMM upgrades. Destinations: • cproxy1.inmotiontech-nology.com • cproxy2.inmotiontech-nology.com
	Mapping Services (Maps and Tracker)	TCP	443	To	Google Maps service ports. Destinations: • maps.googleapis.com • maps.google.com • www.google.com

Table 3-1: TCP/UDP Port Summary

Purpose	Service	Protocol	Port	Direction	Description
User (only open if the AMM is to be accessed directly from an external source - not recommended due to security issues)	HTTP	TCP	8080	To	User Interface.
	HTTPS	TCP	8443	To	User Interface.
	VNC	TCP	5900-6000	To	Remote User interface from AMM to operator workstation.

D: Supported Time Zones

D

oMM versions 2.15 and below support North American time zones.

oMM 2.15.1.1 and above support the following time zones:

- Abu Dhabi
- Adelaide Darwin
- Alaska
- Atlantic Time (Canada)
- Amsterdam Copenhagen Madrid Paris Vilnius
- Arizona
- Astana Dhaka
- Auckland Wellington
- Azores
- Bangkok Hanoi Jakarta
- Beijing Chongqing Hong Kong Urumqi
- Brussels Berlin Bern Rome Stockholm Vienna
- Buenos Aires Georgetown
- Brasilia
- International Date Line West
- Canberra Melbourne Sydney
- Central America
- Central Time (US & Canada)
- Chennai Kolkata Mumbai New Delhi
- Chokurdakh
- Coordinated Universal Time-02
- Coordinated Universal Time-11
- Eastern Time (US & Canada)
- E.Europe
- Greenland
- Greenwich Mean Time: Dublin Edinburgh Lisbon London
- Hawaii
- Indiana (East)
- Islamabad Karachi
- Istanbul
- Jerusalem
- Kabul
- Kuala Lumpur Singapore Taipei
- Kathmandu
- Kiritimati Island
- Kuwait Riyadh

- Moscow St.Petersberg Volgograd
- Mountain Time (US & Canada)
- Mexico City
- Newfoundland
- Pacific (US & Canada)
- Saskatchewan
- Samoa
- Santiago
- Seoul
- Tehran
- Yangon