



Operation and Configuration Guide

oMM



SIERRA
WIRELESS®

oMG-ED-121006
4.8
September 4, 2015

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 cellular modems are not advised without proper device certifications. These areas include environments where cellular radio can interfere such as explosive atmospheres, medical equipment, or any other equipment which may be susceptible to any form of radio interference. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

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.

Limitations of Liability

This manual is provided "as is". Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

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.

Customer understands that Sierra Wireless is not providing cellular or GPS (including A-GPS) services. These services are provided by a third party and should be purchased directly by the Customer.

SPECIFIC DISCLAIMERS OF LIABILITY: CUSTOMER RECOGNIZES AND ACKNOWLEDGES SIERRA WIRELESS IS NOT RESPONSIBLE FOR AND SHALL NOT BE HELD LIABLE FOR ANY DEFECT OR DEFICIENCY OF ANY KIND OF CELLULAR OR GPS (INCLUDING A-GPS) SERVICES.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product may include 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

© 2015 Sierra Wireless Inc. All rights reserved.

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage®, WISMO® and the Sierra Wireless and Open AT logos are registered trademarks of Sierra Wireless, Inc. or one of its subsidiaries.

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 Desk:	Phone:	1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	Contact:	http://www.sierrawireless.com/sales
Post:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Technical Support:	Hours:	6:30 AM to 4:30 PM Pacific Time
	Email:	imt-support@sierrawireless.com
	Phone:	1-866-468-2968
	KBase:	http://imt-kbase.sierrawireless.com/
Web:	http://www.sierrawireless.com/	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases: www.sierrawireless.com

Document History

Version	Date	Updates
4.8	September 4, 2015	Updates for oMM 2.14

Version	Date	Updates
4.7	June 30, 2015	Updated images to new skin
4.6	October 6, 2014	Updated for oMM 2.13
4.5	August 5 2014	Converted to SWI Template



Contents

1. INTRODUCTION	11
1.1. Who Should Read This Guide.....	11
1.2. What is the oMM.....	11
1.3. Supported oMGs	11
1.4. Supported Browsers.....	11
1.5. Determining the Version Number	11
1.6. Related Publications.....	12
2. OVERVIEW	13
2.1. Logging In.....	13
2.2. General Layout.....	13
2.3. Tabs.....	14
2.4. Option Tabs.....	14
2.5. Gateway Tree.....	16
2.5.1. Filter Box	17
2.5.1.1. Gateway Tree Filter Options	17
2.5.2. Groups and Sub-Groups	18
2.5.3. Changing Gateway Details.....	18
2.6. Main Display: Filtering and Options.....	19
2.6.1. Filter Text Field	20
2.6.2. Time Period.....	20
2.6.3. Nominal Events	20
3. MAIN TABS.....	21
3.1. Dashboard.....	21
3.1.1. Dashboard: List View	22
3.1.1.1. Parameters	23
3.1.2. List View: Color Coding.....	23
3.1.3. List View: Sorting	24
3.1.4. Dashboard: Graph View.....	24
3.1.5. Dashboard: Threshold View.....	25
3.2. Events Tab	26
3.3. Map Tab	26
3.3.1. Navigating Within the Map	28
3.3.2. Filtering Gateways	29
3.4. Stats Tab	30
3.4.1. Views.....	31
3.5. Total Reach Tab.....	32
3.6. Config Tab	33
3.6.1. Provisioning.....	33
3.6.1.1. Setting the Template Configuration.....	33
3.6.1.2. Provisioning VPNs	33
3.6.1.3. Provisioning Management Tunnels.....	38

3.6.1.4.	Controlling Configurations when Moving Gateways between Groups.....	39
3.6.2.	Deploy	39
3.6.2.1.	Tracker.....	39
3.6.2.2.	Upload.....	41
3.6.2.3.	Copy.....	42
3.6.2.4.	Deploy.....	43
3.6.3.	CSV Import Export	44
3.6.3.1.	WAN WiFi and WLAN WiFi Security	44
3.7.	Admin Tab	46
3.7.1.	Gateways	46
3.7.2.	Users	47
3.7.3.	Stats	48
3.7.4.	Groups.....	49
3.7.5.	Thresholds.....	50
3.7.6.	Zones	52
3.7.7.	Sessions.....	57
3.7.8.	Remote Sessions	57
3.7.9.	User Activity	58
3.7.10.	DNS Servers	58
3.7.11.	Debug.....	59
4.	OPTIONAL PACKAGES	60
4.1.	Tracker	60
4.2.	Nav	61
4.2.1.	Nav Panel Overview.....	61
4.2.2.	Dispatching.....	62
4.2.3.	Send Message	63
4.2.4.	Message List	64
4.3.	Telemetry.....	65
4.4.	Asset Manager	66
5.	REPORTS	68
5.1.	Saved Templates	68
5.2.	Generated Reports	69
A.1.	WAN CSV	71
A.2.	WLAN CSV	72
A.3.	VPN CSV	73



List of Figures

Figure 1- oMM Login Screen.....	13
Figure 2 - General layout of the oMM	14
Figure 3 - oMM Tabs	14
Figure 4 - Option Tabs	14
Figure 5 - Menu items under Options Tab	14
Figure 6 - Gateway Tree	16
Figure 7 - Filter Box in Gateway Tree	17
Figure 8 - Filter Options	17
Figure 9 - Group Context Menu	18
Figure 10 - Gateway Context Menus.	19
Figure 11 - Location of Filter and Option Fields.....	20
Figure 12 - View of Main Tabs	21
Figure 13 - Dashboard Buttons	21
Figure 14 - List View	21
Figure 15 - Graph View	22
Figure 16 - Threshold View	22
Figure 17 - List View Showing Various Parameters	23
Figure 18 - Color Coded Icons.....	23
Figure 19 - Column Headings with Arrow Indicating Sort Order.....	24
Figure 20 - Graph View	24
Figure 21 - Clicking Reset to return to multi graph view	24
Figure 22 - Stats Tab	25
Figure 23 - Values Exceeding Thresholds	25
Figure 24 - Additional Threshold Details.....	25
Figure 25 - Events tab.....	26
Figure 26 - Map Tab.....	27
Figure 27 - Gateway Marker Popup.....	27
Figure 28 - Google Map Controls.....	28
Figure 29 - Map Level Detail with Terrain Enabled.....	29
Figure 30 - Satellite Level Detail with Sub Options Enabled	29
Figure 31 - Map filter fields.....	29
Figure 32 - Stats Tab	30
Figure 33 - Stats Tab View Buttons	31
Figure 34 - Data Sorted by Temperature	31
Figure 35 - Selecting a Time Period for Data Display.....	31
Figure 36 - Total Reach Tab	32
Figure 37 - VPN Provisioning Listing Screen - Listing for a Selected Group.....	34

Figure 38 - VPN Provisioning Listing Screen - Listing for a Selected Gateway	34
Figure 39 - VPN Info Bubbles	37
Figure 40 - Example of Inheritance Indicators on Configuration fields	37
Figure 41 - Management Tunnel Info Bubble	39
Figure 42 - Tracker Panel	40
Figure 43 - Filtering by Gateway	41
Figure 44 - Upload Tab	41
Figure 45 - Copy Panel	42
Figure 46 - Selecting configuration files to copy	42
Figure 47 - Deploy Panel	43
Figure 48 - The Seven Deployment Function Buttons	44
Figure 49 - Gateways Tab	46
Figure 50 - Users Panel	47
Figure 51 - New User Screen	48
Figure 52 - Adding a Stat	49
Figure 53 - Groups in the Gateway Tree	49
Figure 54 - Group Administration Screen	50
Figure 55 - Thresholds Panel	51
Figure 56 - Zones Panel	53
Figure 57 - Zone Configuration Screen	54
Figure 58 - Map Area Controls	54
Figure 59 - Map Bounding Box	54
Figure 60 - Dragging a point on the bounding box	55
Figure 61 - Adding more points to the bounding box	56
Figure 62 - Raw Latitude/Longitude Pairs Used to Define a Zone	56
Figure 63 - Sessions Panel	57
Figure 64 - Remote Sessions Panel	57
Figure 65 - User Activity Panel	58
Figure 66 - Panel Listing DNS Servers	58
Figure 67 - Add or Edit DNS Server Panel	58
Figure 68 - Tracker Tab Plotting Locations	60
Figure 69 - Tracker Tab Options	60
Figure 70 - Navigator Panel	61
Figure 71 - Gateway Selection List	62
Figure 72 - Adding a New Destination	62
Figure 73 - Deleting a Destination	63
Figure 74 - Send Message Panel	63
Figure 75 - Displaying the Send Message Panel	63
Figure 76 - Message List	64

Figure 77 - Displaying the Message List Panel.....	64
Figure 78 - Text Message Screen.....	65
Figure 79 - Telemetry Tab.....	65
Figure 80 - Assets Tab.....	66
Figure 81 - Screen for Adding/Editing an Asset.....	66
Figure 82 - Toggling the Show Advanced Config Button.....	68
Figure 83 - Menu to Show or Hide the Show Advanced Config Button.....	68
Figure 84 - Additional Report Functions	68
Figure 85 - List of Saved Templates	69
Figure 86 - List of Generated Reports	69
Figure 87 - Available Options on a Generated Report.....	69



List of Tables

Table 1 - Sample Excel Data	31
-----------------------------------	----



1. Introduction

This document provides instructions for using the oMM user interface, reports and optional applications. The oMM can be hosted by Sierra Wireless or purchased as a standalone server appliance. Note that the hosted version offers fewer administrative functions.

1.1. Who Should Read This Guide

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

1.2. What is the oMM

The oMM is a powerful browser-based software application that enables users to configure, monitor, and analyze oMGs and associated applications/accessories (such as Asset Manager Wi Fi tags).

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 oMM server. The oMM uses these data logs to present current and historical activity.

The oMM 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 oMM is available both as a "hosted" version which is hosted by Sierra Wireless servers, and as a standalone appliance which can be purchased and administered by a customer.

In this document an oMG 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: since a gateway is often installed in a vehicle, the term is often also used in place of the word "vehicle".

1.3. Supported oMGs

oMM 2.14 has been tested with:

- oMG 3.12.1
- oMG 3.14

1.4. Supported Browsers

oMM 2.14 has been tested on Internet Explorer 11.0. Other supported browsers include Chrome and Firefox. The oMM application requires the use of browser "cookies". Ensure that this option is enabled on your browser before logging into the oMM.

1.5. 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.

Version	Details
oMM 2.14	August 21, 2015
oMM 2.13	October 8, 2014

1.6. Related Publications

APP-ED-101101 - Tracker User Guide	Provides information for the Tracker application.
oMM-ED-081002 - Total Reach User Guide	Provides information for the Total Reach 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.
oMG-ED-121006 oMG Operation and Configuration Guide for R3 3.9	Provides information about operating the oMG.
oMM-ED-130604 - oMM User Guide 2.12.pdf	Provides information about operating the oMM.

All related documentation is available from the Knowledge Base:
<http://kbase.inmotiontechnology.com>.



2. Overview

The oMM 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 oMM is shown below the login fields.



Figure 1- oMM 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 oMM consists of the following key features:

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

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 oMM.

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

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

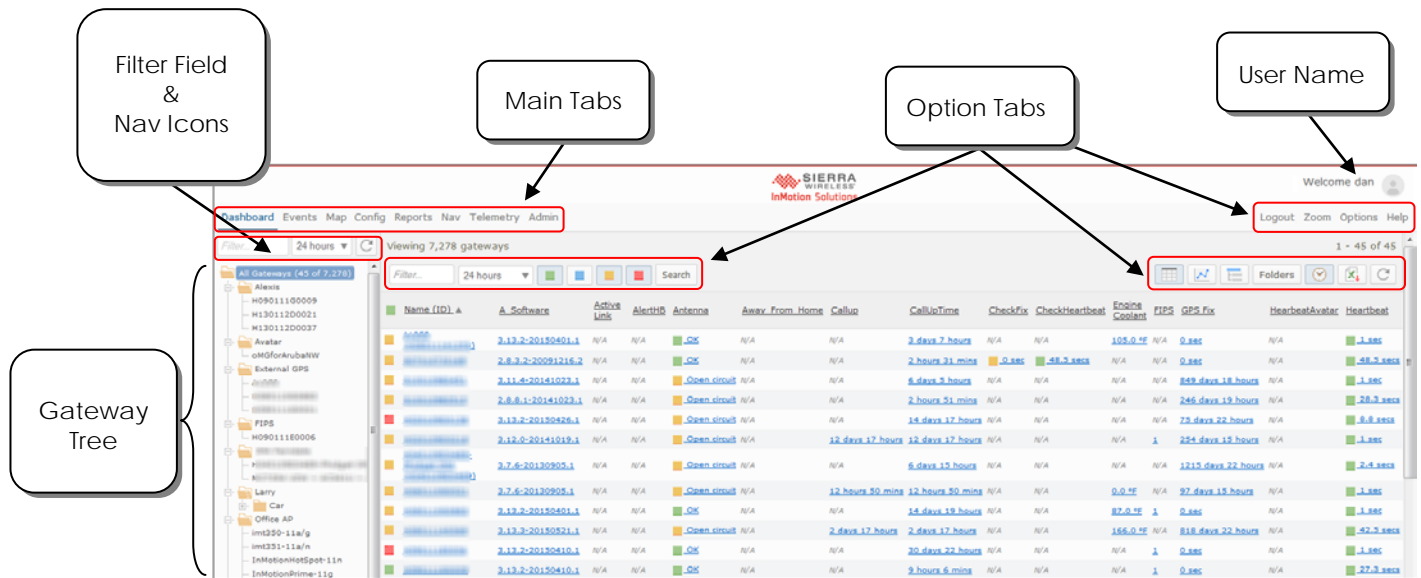


Figure 2 - General layout of the oMM

2.3. Tabs

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

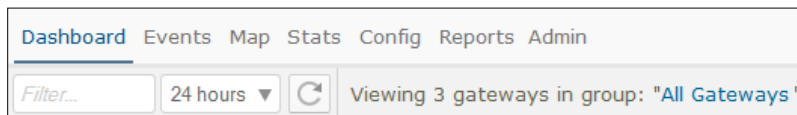


Figure 3 - oMM Tabs

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

2.4. Option Tabs

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

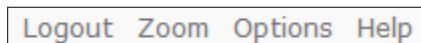


Figure 4 - Option Tabs

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

Zoom: hides/shows the navigation tree and heading information (oMM 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.

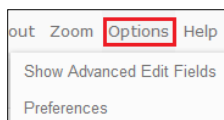


Figure 5 - Menu items under Options Tab

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 oMM performs authentication.
 - **Remote Authentication:** will be available for selection when a Customer Group is selected which has been configured with LDAP authentication (see *LDAP* in Section 3.7.4 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:*
 - **oMM:** 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.
- **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 Section 3.1.1.1 - 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: opens the online help feature for the oMM.

2.5. 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.

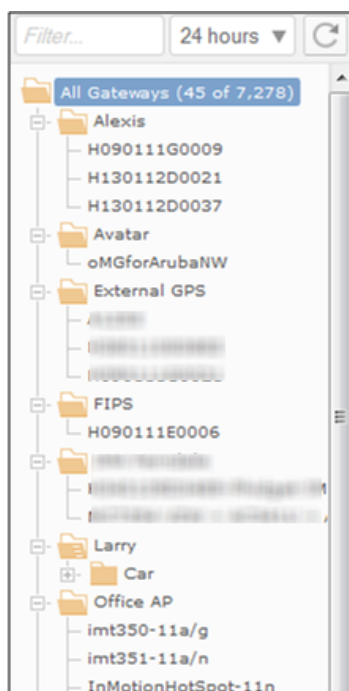


Figure 6 - Gateway Tree

2.5.1. Filter Box

The *Filter* field for the gateway tree allows users to enter the full or partial name of a gateway, or any other data label the gateway may have including all *Dashboard* items displayed (e.g. IP address, Callup Link, Battery, etc.).

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". The *Filter* field is not case sensitive. 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.

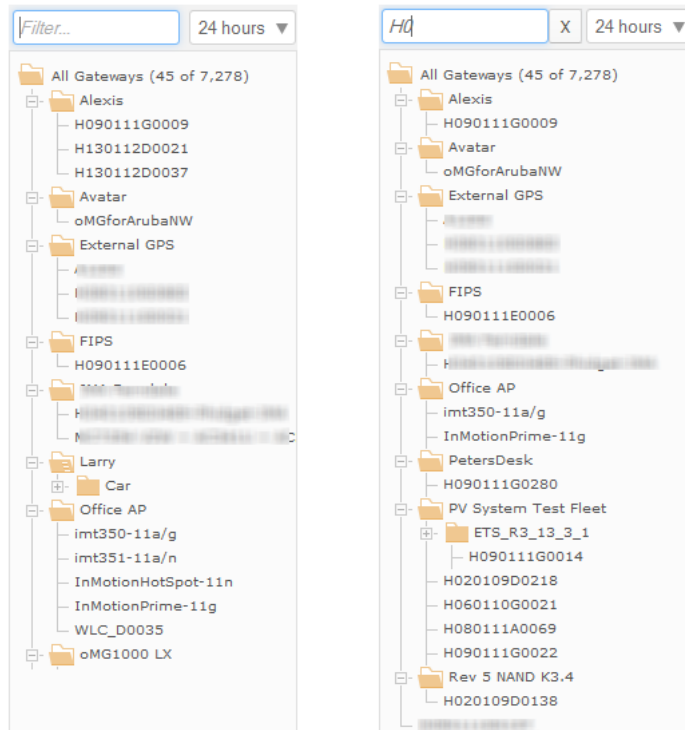


Figure 7 - Filter Box in Gateway Tree

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

2.5.1.1. Gateway Tree Filter Options

The following fields are also used for filtering:

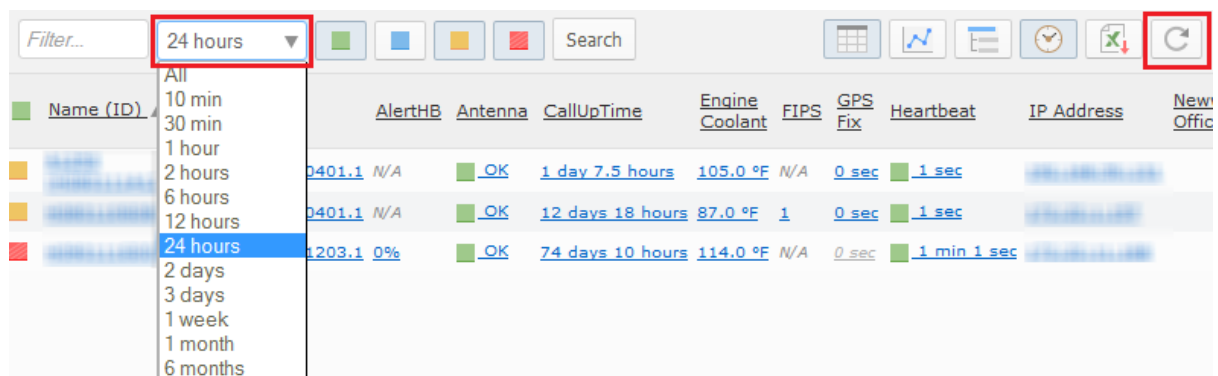


Figure 8 - Filter Options

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 oMG has been deployed.

2.5.2. 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 sub categorization.

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

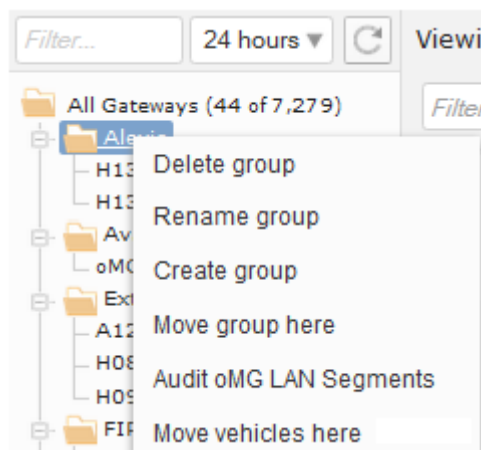


Figure 9 - Group Context Menu

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 oMM 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 a 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 vehicle here: click on a vehicle to select it. Right-click on a group and select this option to move the vehicle to the group.

2.5.3. 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:

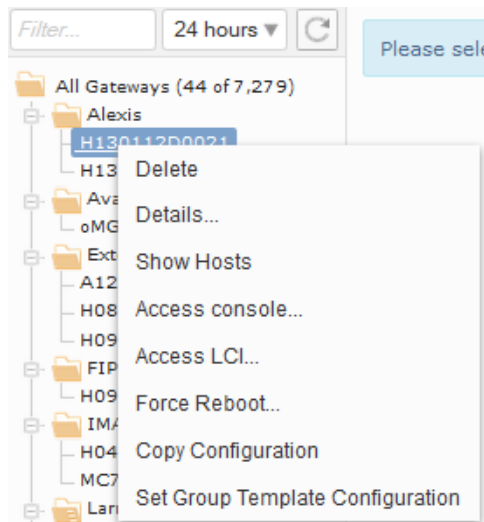


Figure 10 - Gateway Context Menus.

Delete: select to delete a particular gateway.

Details: opens the *Add or Edit Gateway* panel in a new browser. Users can update oMG details. For more information about the options available in this panel, see Section 3.7.1.

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 gateway. The URL and port are provided which can be copied and pasted for use when connecting using a 3rd party SSH application. A button is also provided in the popup window which allows for shell access in the browser using a Java applet.

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

Force Reboot: forces the gateway to be rebooted.

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 be 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: Section 3.6.1 - Provisioning.

2.6. Main Display: Filtering and Options

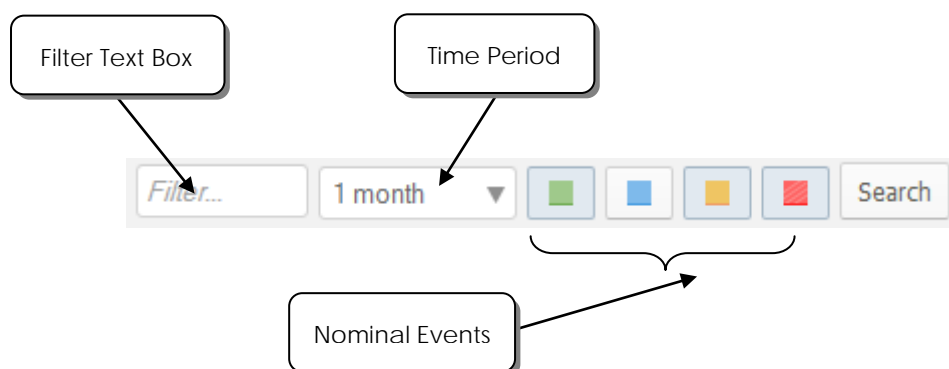


Figure 11 - Location of Filter and Option Fields

2.6.1. 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.

2.6.2. Time Period

Select a time period from the drop down list. Only gateways which have reported data to the oMM (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.

2.6.3. Nominal Events

Nominal events include any event where a threshold is exceeded. See Section 3.7.5 - *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 oMM. 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 oMM administrators for each user.

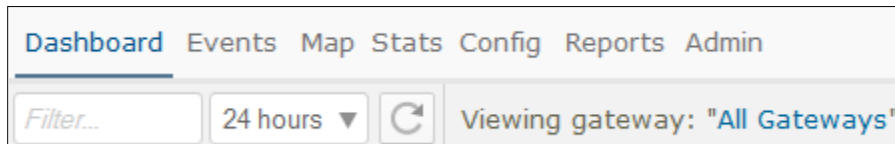


Figure 12 - View of Main Tabs

3.1. Dashboard

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

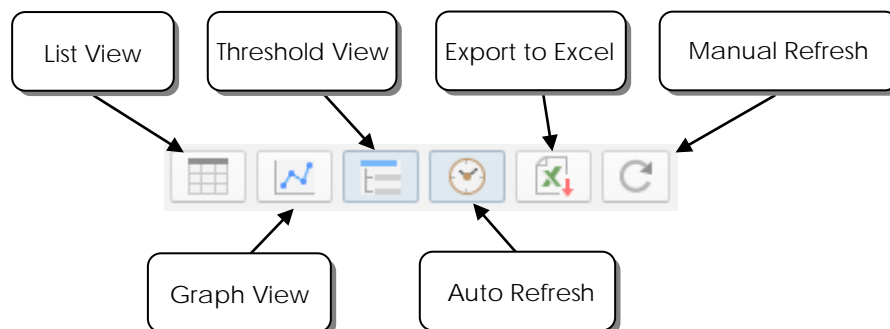


Figure 13 - Dashboard Buttons

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.

Viewing 5 gateways in group: "All Gateways" 1 - 2 of 2

1 month

Search

<div></div>	Name (ID) ▲	Software	Antenna	CallUpTime	Engine Coolant	FIPS	GPS Fix	HeartbeatAvat
<div></div>	<div></div>	3.13.3-20150521.1	<div></div> OK	4 days 18 hours	102.0 °F	1	0 sec	22 days 11 ho
<div></div>	<div></div>	3.11.1-20140728.1	<div></div> Open circuit	2 days 21 hours	60.0 °F	N/A	65 days 23 hours	2 mins 57 sec

Figure 14 - 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.

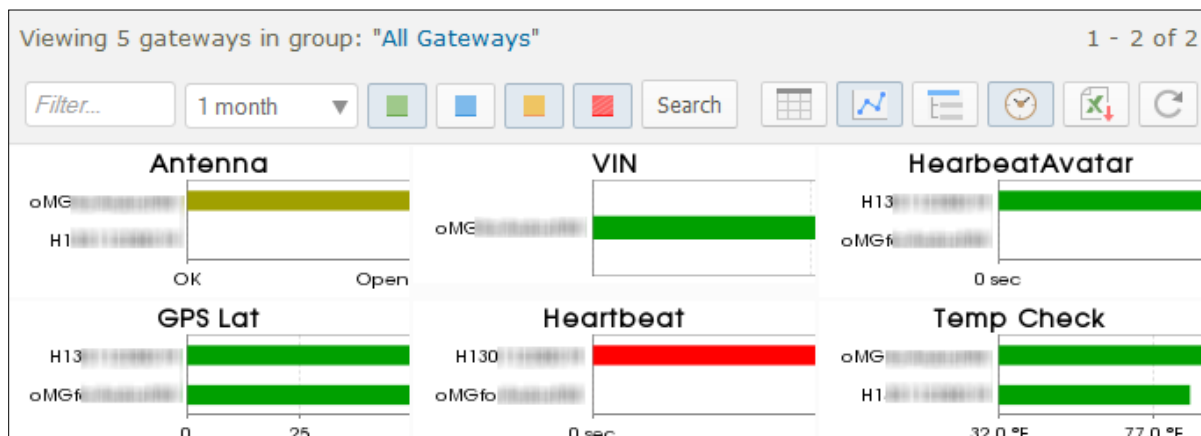


Figure 15 - Graph View

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.

Viewing 5 gateways in group: "All Gateways"						1 - 2 of 2	
Filter...	1 month				Search		
Threshold					Minimum	Maximum	
Heartbeat (All Gateways) ...	1		1		1 min 21 secs	22 days 11 hours	
GPS Satellites (All Gateways) ...		1		1	0	10	
ConfigState (All Gateways) ...		1		1	In sync	Configuration reset initiated	
Antenna (All Gateways) ...		1		1	OK	Open circuit	
Temp Check (All Gateways) ...			2		87.8 °F	96.8 °F	
VIN (All Gateways) ...			1		OZEN MUL-PRO v1.1	OZEN MUL-PRO v1.1	

Figure 16 - 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 oMM 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.

Viewing 5 gateways in group: "All Gateways" 1 - 2 of 2

Filter... 1 month [Green] [Blue] [Yellow] [Red] Search [Grid] [Line] [List] [Clock] [Download] [Refresh]

	Name (ID) ▲	Software	Antenna	CallUpTime	Engine Coolant	FIPS	GPS Fix	HearbeatAvat
[Red]	[Redacted]	3.13.3-20150521.1	[Green] OK	4 days 18 hours	102.0 °F	1	0 sec	22 days 11 ho
[Yellow]	[Redacted]	3.11.1-20140728.1	[Yellow] Open circuit	2 days 21 hours	60.0 °F	N/A	65 days 23 hours	2 mins 57 sec

Figure 17 - List View Showing Various Parameters

3.1.1.1. Parameters

The *Dashboard* items are made available by creating thresholds (see Section 3.7.5 - *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 oMG last reported its latitude/longitude coordinates.

Satellites: the gateway is equipped with a 12-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 (°C). The gateway has a built-in temperature sensor.

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.

[Green]	H0 [Redacted]	3.13.2-20150410.1	N/A	N/A	[Green] OK
[Yellow]	InMotionPrime-11g (H0 [Redacted])	3.11.4-20141023.1	N/A	N/A	[Yellow] Open circuit

Figure 18 - 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) column.

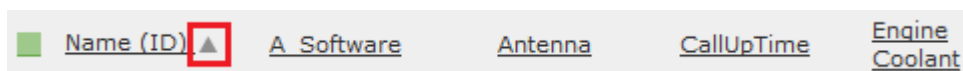


Figure 19 - Column Headings with Arrow Indicating Sort Order

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).

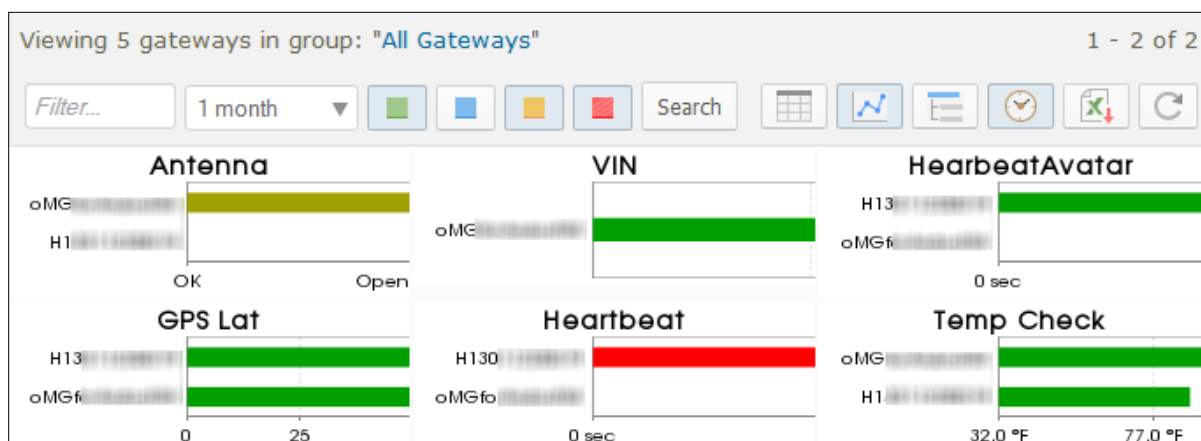


Figure 20 - Graph View

To enlarge a graph, click on the bars within the graph. To return to the multi-graph view, click on **Reset** as shown here:

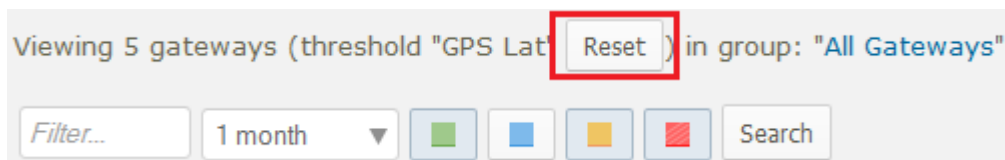


Figure 21 - Clicking Reset to return to multi graph view

Some graphs can provide even greater detail. For further details for a single gateway, click on a bar or data point within the graph. A new browser window/tab will open, displaying the Stats for the gateway. The image below shows greater detail for *ReportIdleTime* for a single gateway. For more information, see Section 3.4 - *Stats Tab* for more information.

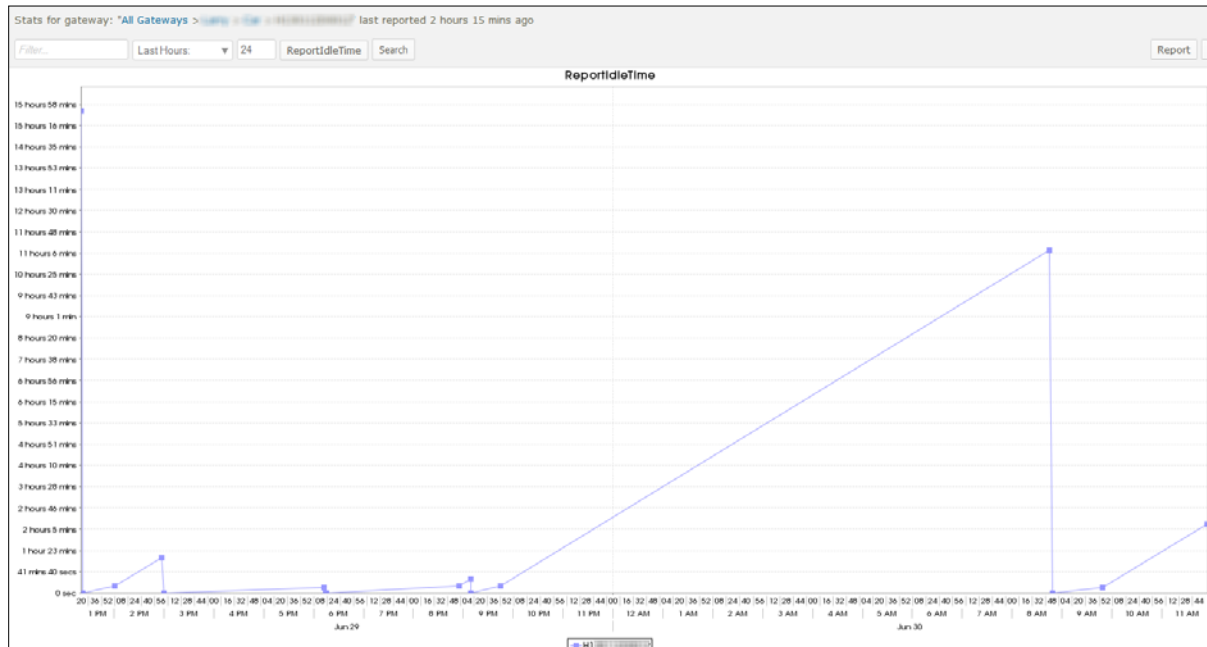


Figure 22 - Stats Tab

Note: Readonly distinguishes items that can be modified from those that cannot and is present when a user has read-only privileges (i.e. no write or edit privileges).

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.

Viewing 7,278 gateways				1 - 45 of 45	
Filter...	24 hours	■	■	■	■
Search					
Threshold	■	■	■	■	
ConfigState (All Gateways) ...	6	13	24	In sync	Configuration reset initiated
Heartbeat (All Gateways) ...	5	6	34	1 sec	19 hours 29 mins
TSES (All Gateways) ...	1	2	9	22 secs	54 days 17 hours

Figure 23 - Values Exceeding Thresholds

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

Threshold	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Minimum	Maximum
<div><div></div> ConfigState (All Gateways) ...</div>	6	13	24		In sync	Configuration reset initiated
<div><div></div> H1 ... Conflict</div>	<div><div></div> H13 ... Conflict</div>	<div><div></div> H09 ... Conflict</div>	<div><div></div> H13 ... Conflict</div>			
<div><div></div> H1 ... Conflict</div>			<div><div></div> H02 ... Conflict</div>			
<div><div></div> H0 ... Out of sync - remote</div>	<div><div></div> MC7354 VZW + AC341U + AC340UOFW</div>		<div><div></div> H14 ... Configuration reset</div>			
	<div><div></div> Configuration reset initiated</div>		<div><div></div> initiated</div>			
<div><div></div> H13 ... Configuration reset</div>	<div><div></div> H13 ... Configuration reset</div>	<div><div></div> H13 ... Configuration reset</div>	<div><div></div> H13 ... Configuration reset</div>			
<div><div></div> initiated</div>	<div><div></div> initiated</div>	<div><div></div> initiated</div>	<div><div></div> initiated</div>			

Figure 24 - 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 Section 3.7.5 - *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 oMM for a specific time period. For advanced users, this feature is useful for testing or troubleshooting gateways.

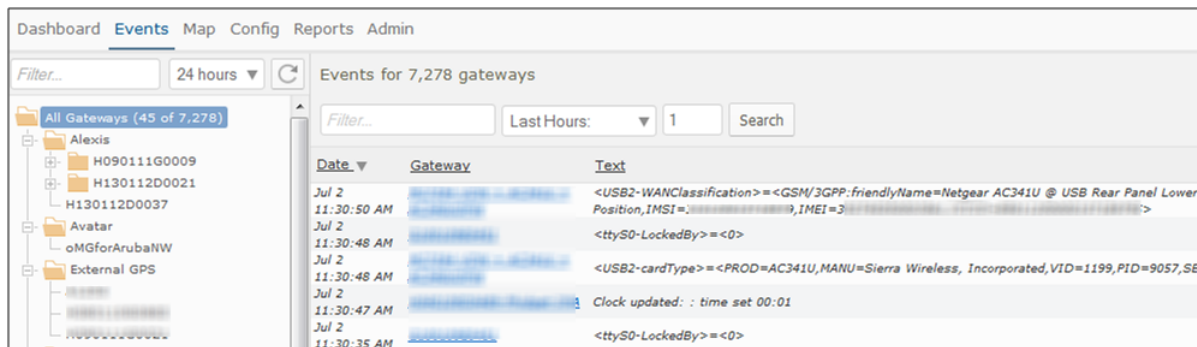


Figure 25 - Events tab

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.
- 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 Excel.

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.

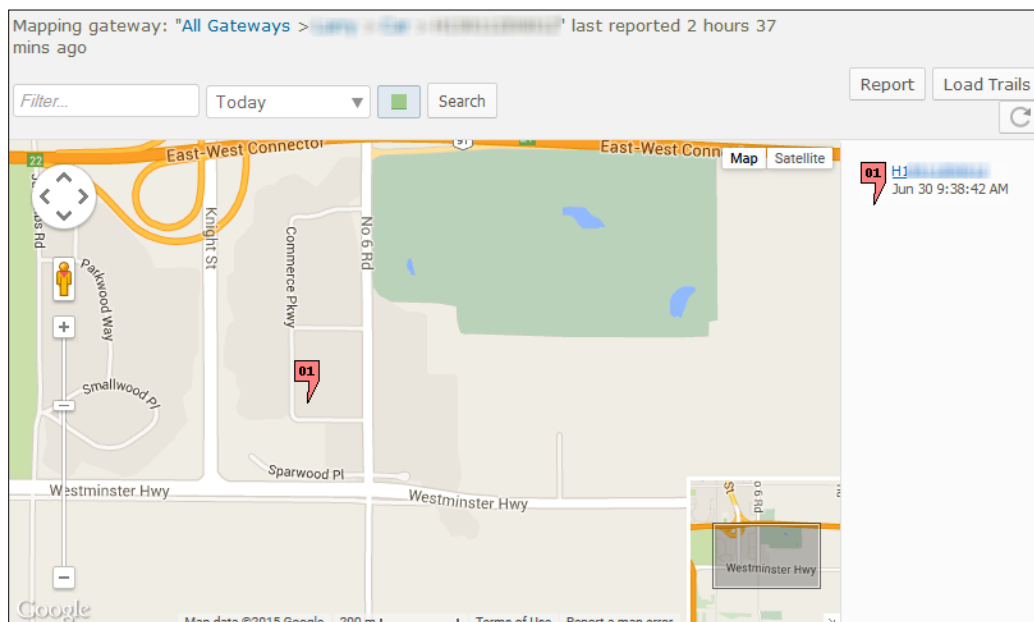


Figure 26 - Map Tab

Gateways are identified using numerical markers, with a list of details by gateway shown to the right of the map. The colour of the marker corresponds to the threshold colour 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:

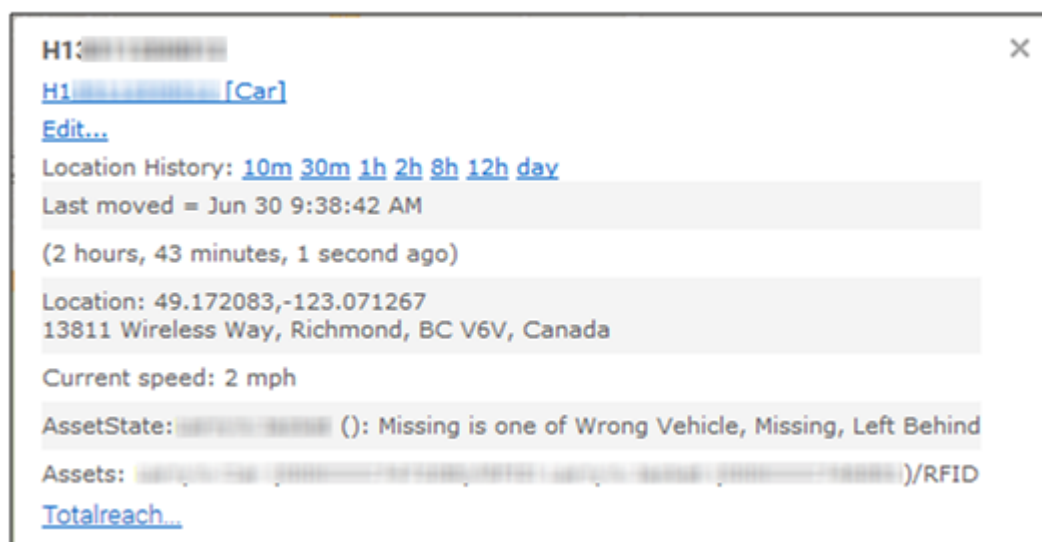


Figure 27 - Gateway Marker Pop-up

The popup displays the following primary information:

Gateway ESN: the serial number assigned to the oMG.

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.

Current Speed: the current speed of the vehicle.

EngineRPM: the current engine speed (RPM).

Threshold information: displays the specific threshold name and values which are responsible for the color of the marker (e.g. in the screenshot above, the marker is red due to an idle time of greater than 10 minutes). Therefore the popup displays *ReportIdleTime* along with the value which has exceeded that threshold's error condition.

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.

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

3.3.1. Navigating Within the Map

The oMM 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 28) to zoom in and out.
- To pan using the map controls, press one of the four arrows in the white circle:



Figure 28 - 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 29 - 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 two options:

- **45°**: when enabled, displays buildings and other features from a 45° degree, perspective view, at lower (i.e. closer) zoom levels.
- **Labels**: when enabled, displays map labels such as street names.



Figure 30 - 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:

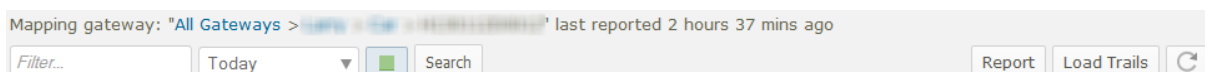


Figure 31 - Map filter fields

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 oMM 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.

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

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

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

3.4. 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.

Label	Gateway	Date	Value
AbsoluteLoadValue		2012/09/20 17:37:01	0
AbsoluteThrottlePosition		2012/09/20 17:37:05	18.431
AbsoluteThrottlePosition		2011/12/14 14:12:10	0
AbsoluteThrottlePosition		2011/12/07 10:43:19	0
AbsoluteThrottlePosition		2010/06/21 18:45:03	0
AbsoluteThrottlePosition		2010/05/26 10:24:17	0

Figure 32 - 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.

3.4.1. Views

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

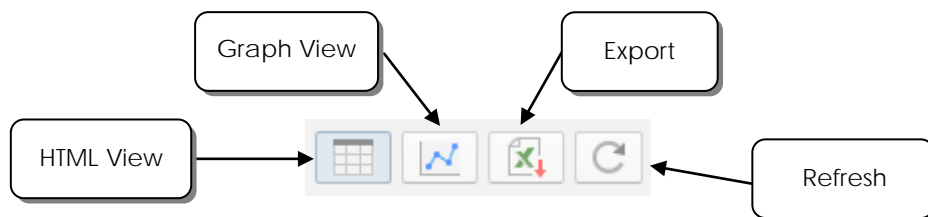


Figure 33 - Stats Tab View Buttons

HTML: list of data in columns. Data may be sorted by clicking the column header.

Graph: provides a graphical view of the data.

Export: export the data to Excel.

Refresh: manually refresh the information.

For the default view (HTML), the results are sorted by date, with the most recent at the top of the list. However, data may be sorted by clicking on column headers. In the example below, data is sorted by temperature values, in descending order. This is denoted by the downward pointing triangle. Clicking on the column header a second time will sort the data in ascending order, and the triangle will point upwards.

Temperature imt350-11a/q	Jun 30 12:48:23 PM	95.0 °F
Temperature H05	Jun 30 12:48:14 PM	82.4 °F
Temperature H1	Jun 30 12:47:49 PM	91.4 °F
Temperature H0	Jun 30 12:47:32 PM	84.2 °F
Temperature H14	Jun 30 12:47:14 PM	86.0 °F

Figure 34 - Data Sorted by Temperature

Use the drop-down box to select the time period for which to display the data. The options are *Latest*, *Last Hours*, *Previous Days*, *Previous Months* and *Range*. Enter the numerical information in the corresponding box. The image below shows the time period for the previous 2 hours. Click on **Search** to call up the data.

Figure 35 - Selecting a Time Period for Data Display

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

Table 1 - Sample Excel Data

Date	Stat	Gateway	Value
3/21/2009 5:05	Link1-TotalrxBytes	H078	740,069

Date	Stat	Gateway	Value
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

3.5. Total Reach Tab

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

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 Figure 36 below).
4. Click the button corresponding to the type of connection to use (e.g. VNC):

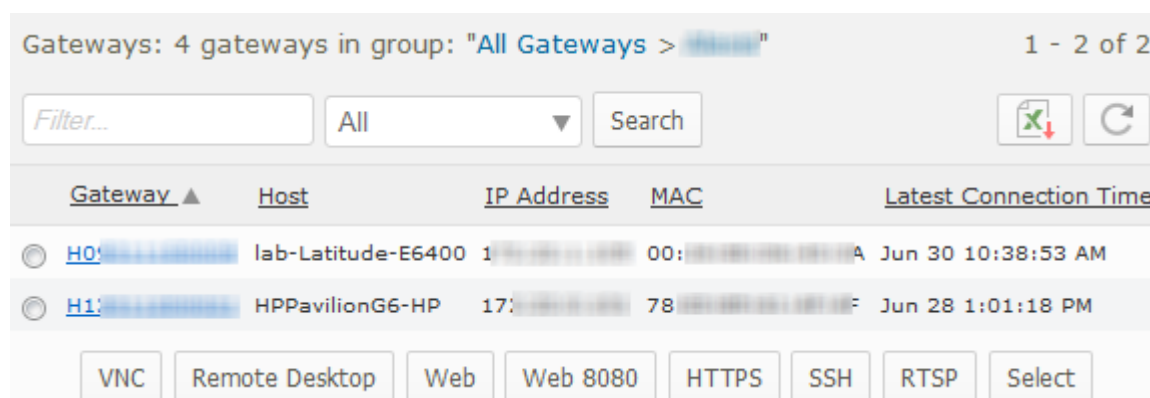


Figure 36 - Total Reach Tab

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 oMM users must be granted Total Reach privileges by the oMM 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*.

3.6. Config Tab

The *Config* tab provides access to the *Tracker*, *Copy*, *Upload*, *Deploy*, *WiFi Security Import/Export*, and *VPN 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.

3.6.1. Provisioning

oMM 2.14 and above provide the *Provisioning* menu which allows for the configuration of VPNs and management tunnels on either a single oMG or groups of oMGs running version 3.8 through 3.14. This mechanism is also used by fleet operators to implement PSK rotation for VPNs.

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.

Note: provisioning on oMM 2.14 works with oMG's running 3.8 through 3.14. 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.

3.6.1.1. 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.

3.6.1.2. Provisioning VPNs

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

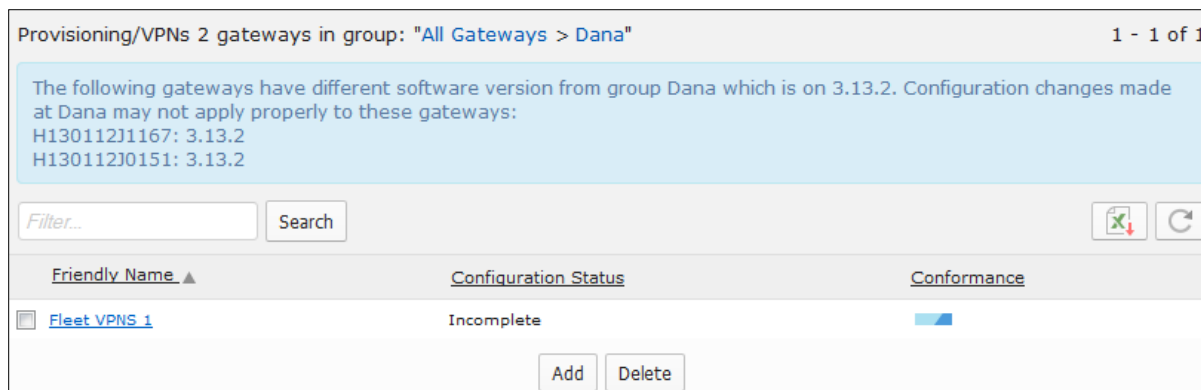


Figure 37 - VPN Provisioning Listing Screen - Listing for a Selected Group

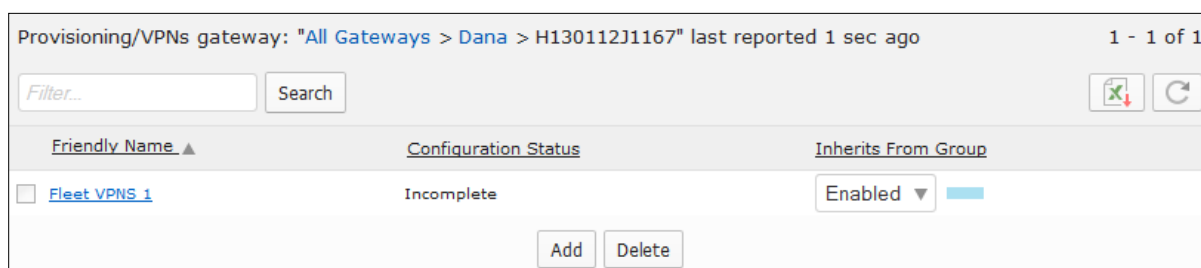


Figure 38 - VPN Provisioning Listing Screen - Listing for a Selected Gateway

Note: A software version check is performed at the group level and any differences are highlighted as shown in Figure 37. A group inherits the software version from the source gateway in the 'set template config' operation (see Section 3.6.1.1), 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:

	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 exist at the gateway:

- **Conformance Bar:** visually indicates if the configuration assigned to the selected oMG conforms to the group from which it inherits:

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

3.6.1.2.1. 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 Section 3.6.1.1.
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.

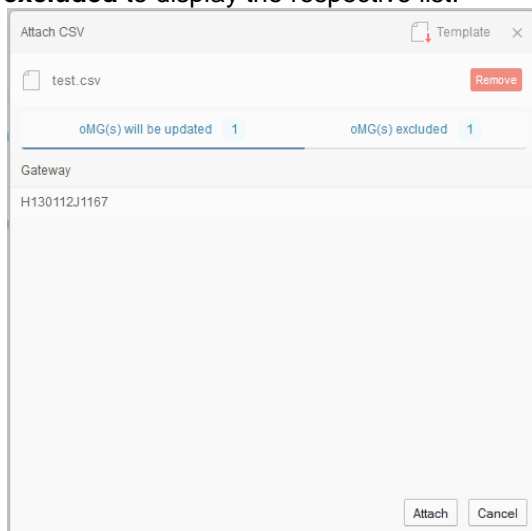
Note: At the group level, only links and monitors that are common in all gateways within the group will be displayed as options.

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:

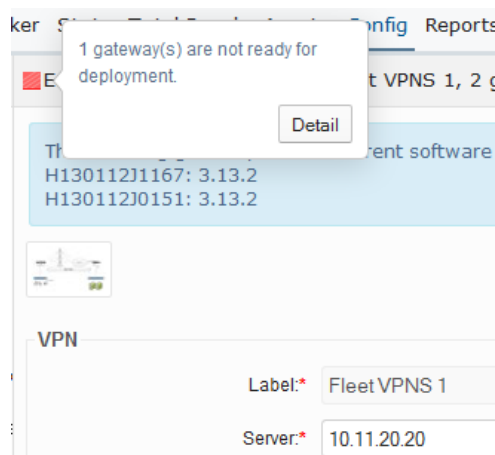
- a. **Template** (top right corner): generates a blank CSV file which can be populated with VPN PSK information (see A.3 - VPN CSV).
- b. **Select a CSV file:** allows for a populated CSV file to be selected and attached to the configuration. The values in this .csv file will override those on the configuration 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 Section 3.6.2.4 - 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:

The image shows a 'VPN' configuration form. It has two input fields: 'Label:*' with the value 'Fleet VPNS 1' and 'Server:*' with the value '10.11.20.20'. To the right of the 'Label' field is a red-bordered box containing an information icon and the text: 'Free form text to uniquely identify this VPN profile.'

Figure 39 - 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:

The image is a screenshot of the 'Editing Provisioning/VPNs on Fleet VPNS 1, gateway: "All Gateways > Dana > H13011"' screen. It shows three sections: 'VPN', 'Enterprise Network', and 'Vehicle Network'. Each section has an 'Inherit' button highlighted with a red box. The 'VPN' section has 'Label:*' (Fleet VPNS 1) and 'Server:*' (10.11.20.20). The 'Enterprise Network' section has 'Enterprise Network Subnets:*' (10.10.20.20/24). The 'Vehicle Network' section has 'Vehicle Network Subnets:*'.

Figure 40 - Example of Inheritance Indicators on Configuration fields

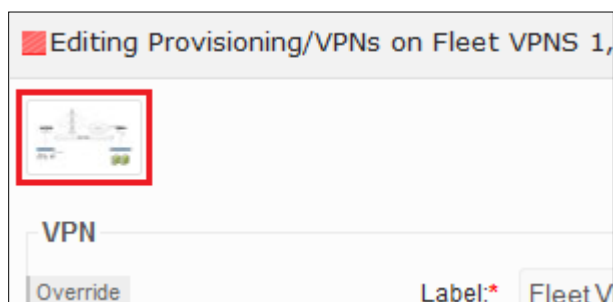
To change whether a setting inherits or overrides from the parent group, click on the indicator and select the respective option:

The image shows a dropdown menu for the 'Enterprise Network' section. It has two options: 'Inherit value from parent group.' (selected) and 'Assign a custom value and override parent group.'

- **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 oMM 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 oMM 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.

3.6.1.3. 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.

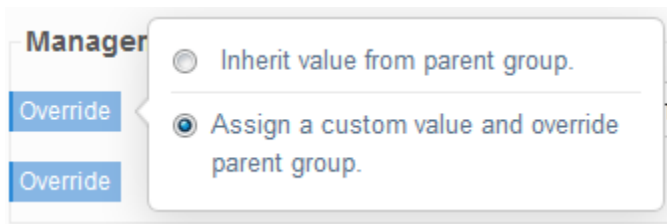
To edit a VPN configuration to a group or gateway:

1. Ensure the template configuration has been assigned to the group as described above in Section 3.6.1.1.
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 *oMM 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 Section 3.6.2.4 - Deploy).

Note: syntax checking is performed by the oMM 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:

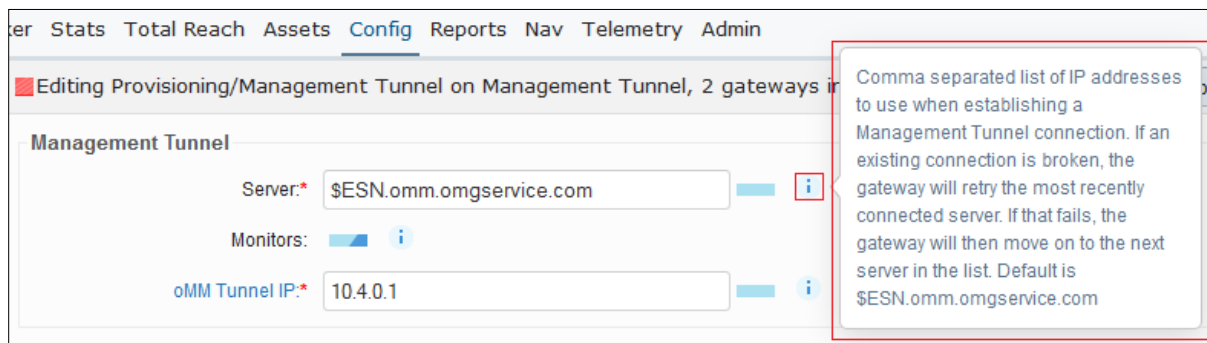


Figure 41 - Management Tunnel Info Bubble

3.6.1.4. 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.

3.6.2. Deploy

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

3.6.2.1. 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 Section 4.1 - **Tracker**). Using GPS TAIP, gateways can send GPS information at a much higher frequency than via the normal event stream.

Tracker Config

Existing Group: /0 (2) (will reload once selected)

IP Address:* (number format only)

Listener Port:* 0 (firewall needs to be opened)

Gateway	TAIP Vehicle ID	Message Format	Send Interval
H0: [redacted]	666 out of sync	<input checked="" type="checkbox"/> LN <input checked="" type="checkbox"/> PV out of sync	120 out of sync
O1: [redacted]	SS out of sync	<input type="checkbox"/> LN <input type="checkbox"/> PV	0 out of sync
Add: oMGforAru Filter (gateway: "oMGf [redacted] ")	out of sync	<input type="checkbox"/> LN <input type="checkbox"/> PV	out of sync

Apply Delete

Figure 42 - 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 oMM 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 oMM.

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:

Add: **TRK** Filter (7,278 gateways)

Su TRK-Fiona-01 (TAIP-6000-0001)

TRK-Frank-04 (G010106D0302)

TRK-Gonzo-02 (TAIP-6000-0002)

TRK-Holly-03 (TAIP-6000-0003)

TRK-Jess-05 (TAIP-6000-0005)

Notes:

Reporting within: (days)

Matching Vehicles (click to limit):

1-EMS
 05-02
 07-02
 07-03
 08-02
 09-02
 10-F0373

Apply Delete

Figure 43 - 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.

3.6.2.2. Upload

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

Upload Configuration File

Apply to: H1 Filter (gateway: "H1")

Configuration file: Browse_ No file selected.

Browse_ No file selected.

Browse_ No file selected.

Browse_ No file selected.

Upload

Figure 44 - Upload Tab

Uploading the configuration file:

- **Apply to*:** the oMG to which the file(s) will be copied to. Enter the oMG'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.

3.6.2.3. Copy

The *Copy* panel is used to copy the configuration file from an oMG to be used as a *template* for other oMGs.

Figure 45 - Copy Panel

Copying the oMG configuration file:

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

Note: users can enter more than one oMG 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 oMG.
 - To copy specific files from the source oMG, uncheck **All Files** to deselect all files and place a checkmark beside each file to copy:

Figure 46 - Selecting configuration files to copy

- **Skip version check**: by default, configuration files can only be copied to oMGs 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.
- **Copy**: click to copy the file(s); this opens the *Deploy* panel.

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

* denotes a required field

3.6.2.4. Deploy

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

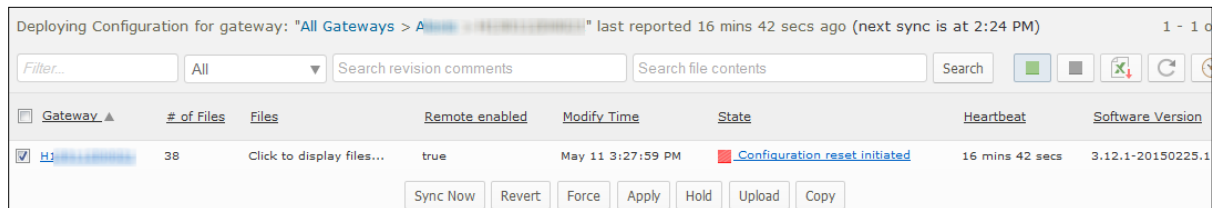


Figure 47 - Deploy Panel

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

- **Filter edit box:** filters the list on part or all of an oMG name.
- **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 3.6.3.1.2 - *Deploying PSK Rotation through the oMM 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 oMGs.

Information is provided in five columns:

- **Gateway:** lists the oMGs connected to the oMM. The list is based on those oMGs 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 oMG 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 oMG's configuration was last modified.
- **State:** using green, yellow and red circle icons, this information allows administrators to see the state of each oMG's configuration:
 - **In sync:** the configuration is synchronized with the oMM.
 - **Awaiting rollback:** the configuration is waiting to be rolled back from that on the oMM.
 - **Awaiting rollforward:** the configuration is waiting to be rolled forward to that on the oMM.
 - **Conflict:** the config on the oMM and on the oMG have both been modified. To manually resolve this, choose the desired configuration to use, and overwrite the other configuration with it.
 - **Incomplete:** an oMG 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.
 - **Modified:** changes have been made on the oMM but are waiting for a user to review and apply them before they will be pushed out to the gateway.
- **Software Version:** the current software version of the gateway listed.

There are seven functions for deployment:

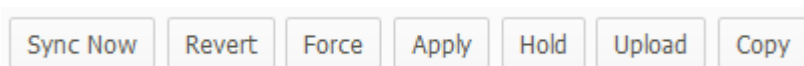


Figure 48 - The Seven Deployment Function Buttons

- **Sync Now:** use this function to initiate synchronization between the oMG and the oMM. Always ensure that the configuration is in sync before making any changes to configuration files or pushing a new configuration to the oMG. Note: this button is only available when a single oMG is selected. To select a single oMG click on an oMG's gateway link in the Deploy list, or select the oMG in the Gateway Tree.
- **Revert:** pulls the oMG copy of the configuration into the oMM regardless of the Sync State.
- **Force:** pushes the oMM copy of the configuration out to the oMG regardless of the Sync State.
- **Apply:** applies changes made on the oMM 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 oMG to another or to a group of oMGs.
- **Upload:** applies configuration files that have been previously backed up to a PC.

3.6.3. CSV Import | Export

3.6.3.1. WAN WiFi and WLAN 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 Section 3.6.1.2 - Provisioning VPNs for more information).

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

Note: WEP encryption is not supported for credential rotation.

3.6.3.1.1. 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.

3.6.3.1.2. Deploying PSK Rotation through the oMM

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 oMM and deploying the settings to the fleet of oMG's. Information about the CSV file is available in Appendix A - 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 Appendix A - CSV File Information for information about the CSN 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 oMM 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 Section 3.6.2.4).
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. 776677667766776677667766776677) 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.

3.7. Admin Tab

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

3.7.1. Gateways

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

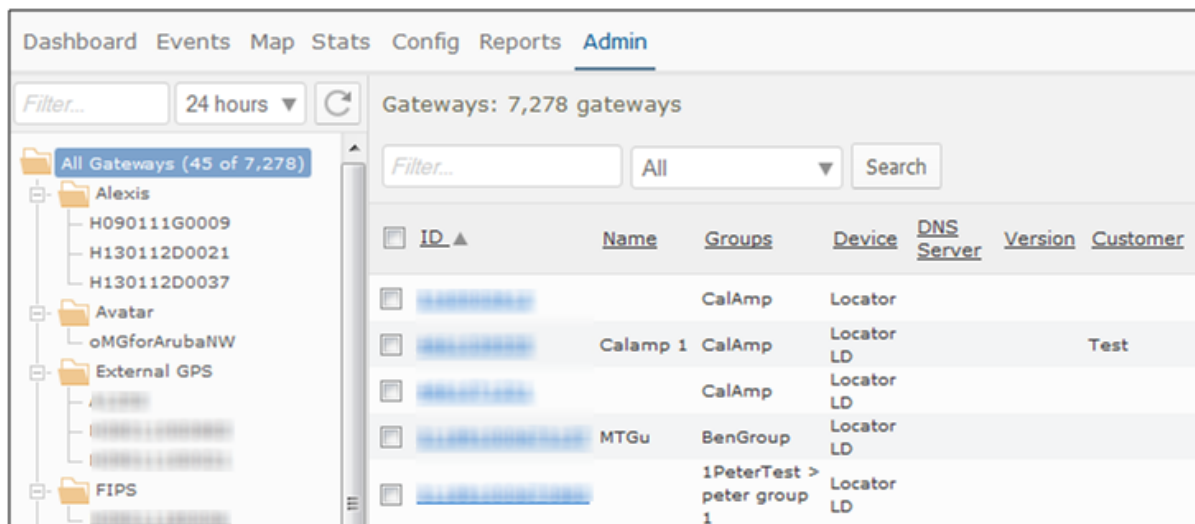


Figure 49 - Gateways Tab

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**: 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 Section 3.7.10. 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.

Deleting a Gateway

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

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 oMM matches it based on the ESN. Thus, administrators can pre-assign gateways to a fleet and configure additional properties.

3.7.2. Users

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

Name	Email	Owner Group	Account Expiry	Last Login Location	Last Login Time	Bytes Transferred
6277		All Gateways	2013/02/20	1	2013/02/06 21:00:37	0 MB
admin		All Gateways	N/A	2	Jul 2 10:58:58 AM	10,552.656 MB
alex		All Gateways	N/A		N/A	0 MB
AndrewTest		John	N/A	1	2013/06/10 13:48:26	0 MB
AndrewTest2		1PeterTest	N/A	1	2013/05/29 10:59:04	0 MB

Figure 50 - Users Panel

Adding new user
Show Advanced Config

Identification

Name:*
Email:
(default email used for notifications)
Customer group:
** All **
Password:
Confirm:
Expiry:

Privileges

OMM:
None
Read
Read/Write
Tabs:
All
Reports:
All
Available Items (60)
Filter...
Selected Items (0)
Network
Network/Availability Trend
Network/Availability Details
Network/Coverage Map
Network/Coverage Trails
Stats:
All

Preferences

Measurement units:*
Imperial
Metric (for number and unit formatting)
Position Format:*
Decimal Degrees
Degrees:Minutes,DecimalMinutes
Format CSV output values same as HTML
Dashboard timespan:
24 hours
Tracker refresh:*
30 (s)
Dashboard refresh:*
30 (s)
Oldest report:*
90 (days)
Max concurrent logins:
(blank for no restriction)
Restricted IP:
(a.b.c.d)
Max threshold emails/day:
Nav Stop List:
Creation Time Ascending
Time Zone:
Server TimeZone
Dashboard Items:
Use applicable thresholds in default order
Telemetry Dashboard:
Use applicable telemetry stats in default order

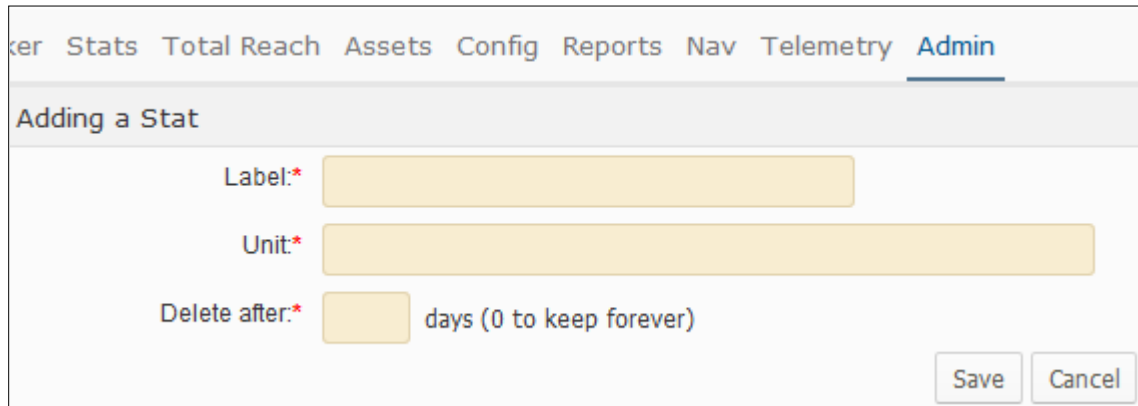
Figure 51 - New User Screen

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* in Section 2.4.
- Click **Save** to save the new user.

3.7.3. Stats

A *stat* defines a parameter value collected by the oMM. The *Stats* panel is used to add, delete, and modify the many parameters that are monitored and tracked by the oMM.



ker Stats Total Reach Assets Config Reports Nav Telemetry Admin

Adding a Stat

Label:*

Unit:*

Delete after:* days (0 to keep forever)

Save Cancel

Figure 52 - Adding a Stat

Do not modify these parameters unless under direct consultation with Sierra Wireless personnel.

3.7.4. Groups

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

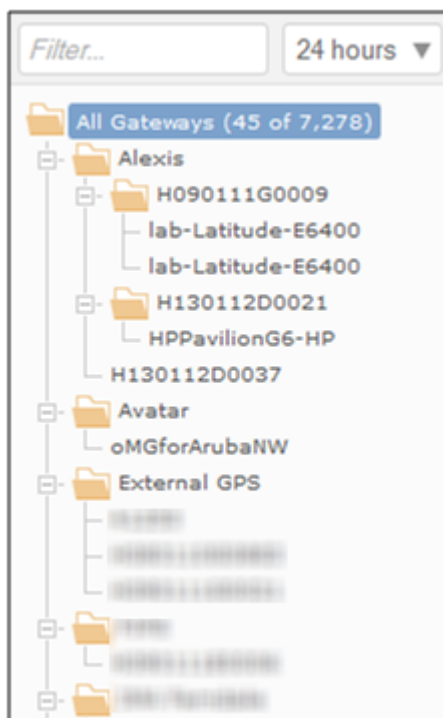


Figure 53 - Groups in the Gateway Tree

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

Adding a new Group:

The screenshot shows the 'Admin' tab in a web interface. Below the navigation bar, there are several input fields and a section for group authentication. The 'Name' field is a text input with a yellow background. The 'Parent group' field is a dropdown menu showing '** All **'. The 'Group software version' field is a dropdown menu showing 'None'. The 'Group authentication' section has a label 'Authentication type:' followed by two radio buttons: 'Local' (selected) and 'LDAP'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 54 - 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 oMM.
 - **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* in section *Section 2.4*);

3.7.5. 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*.

Label	Node or Group	Stat	Warning Criteria	Error Criteria
A-Software	All Gateways	SoftwareVersion		
AbsoluteThrottlePosition	All Gateways	VIN		
Active Link	H130112D0037	ActiveLink		
Air Temp	All Gateways	AssetBattery	equals 3,000%	
Air Temp	Group: Highland Local Trial	AmbientAirTemperature		

Figure 55 - 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.
- **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 position***: 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.

- **SNMP Trap:** when enabled, an SNMP Trap is sent by the oMM 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 oMM.

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.
 - SNMP Trap: when enabled, an SNMP Trap is sent by the oMM 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 oMM.

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

3.7.6. 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.

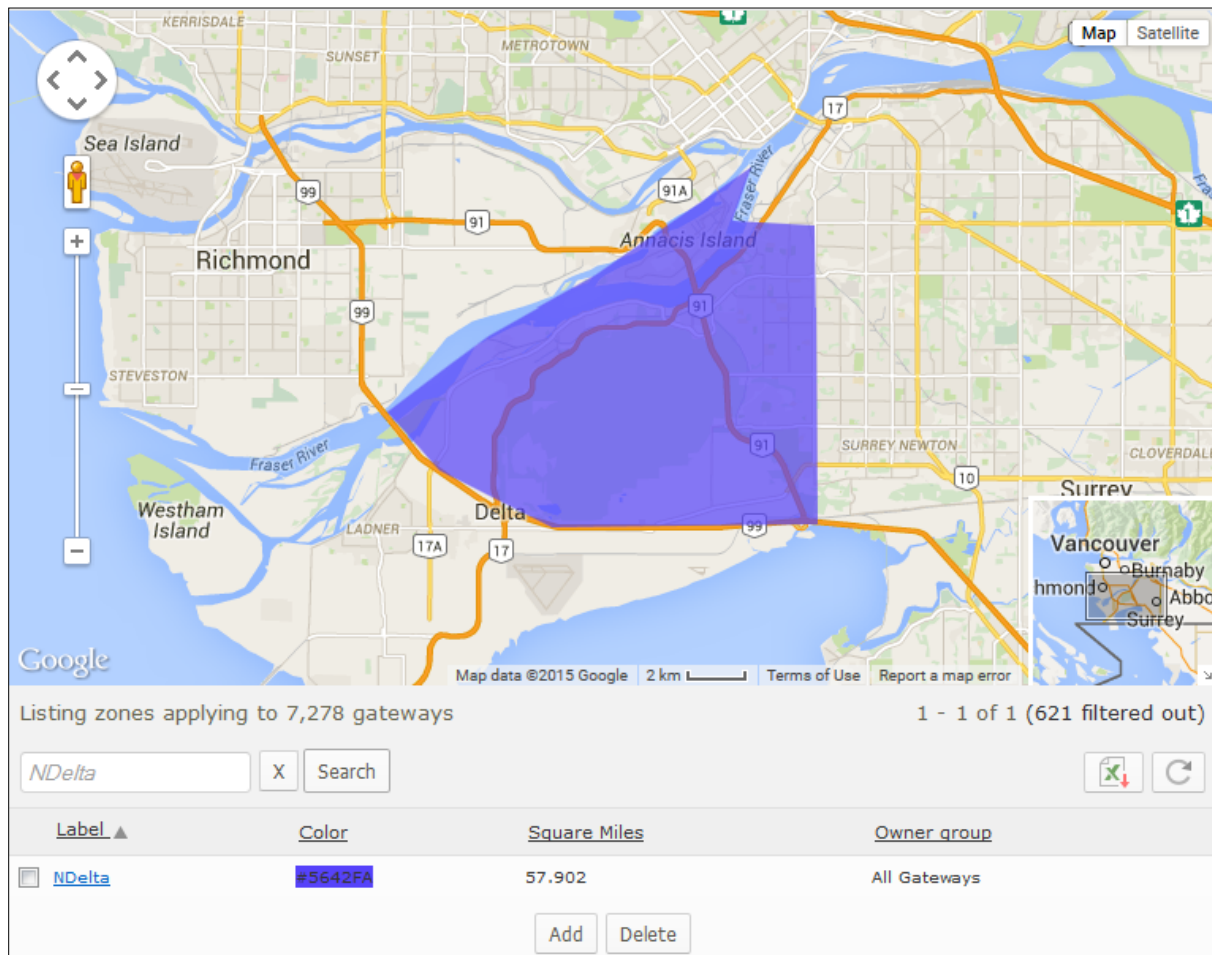


Figure 56 - Zones Panel

Adding a new zone

- 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 57 - Zone Configuration Screen

10. 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 58 - Map Area Controls



Figure 59 - 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 60 - 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.

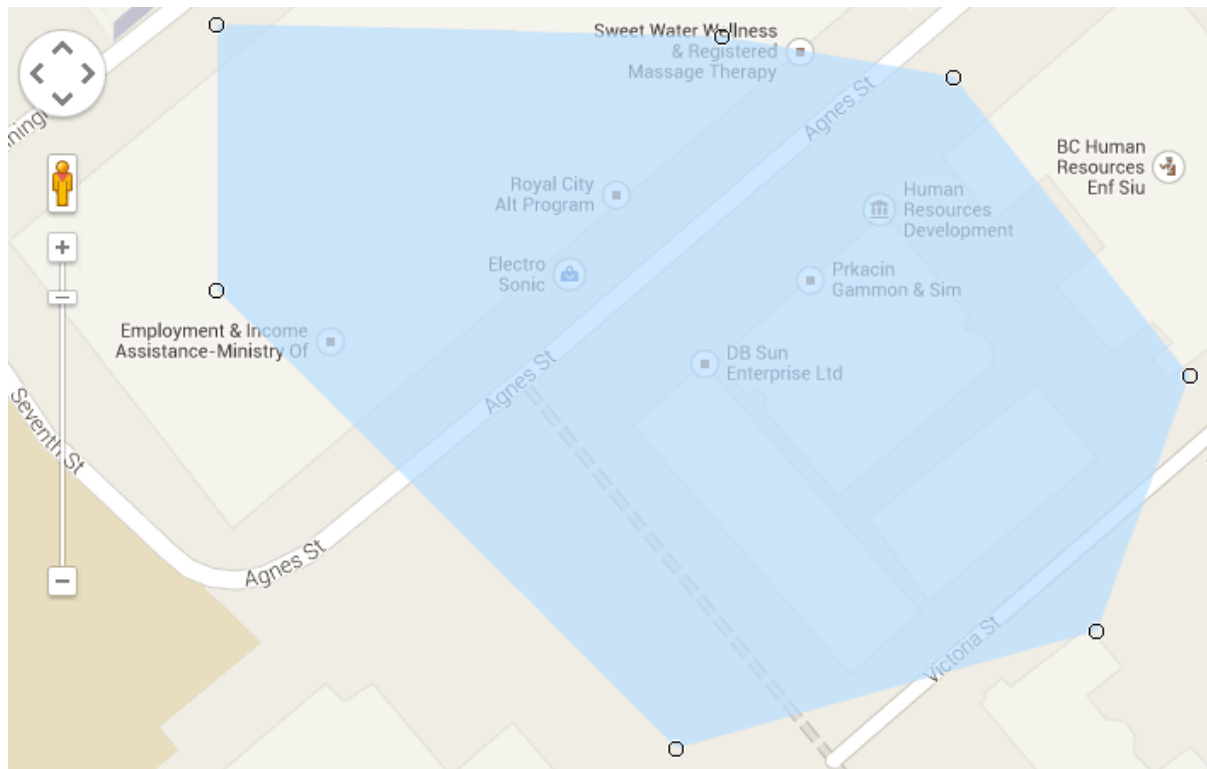


Figure 61 - Adding more points to the bounding box

- 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 62 - Raw Latitude/Longitude Pairs Used to Define a Zone

11. 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.

3.7.7. Sessions

The *Sessions* panel provides the list of the users logged into the oMM. 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*.



Users currently logged in								1 - 8 of 8
Filter...		All	Search					 
<input type="checkbox"/> Username ▲	Login Host	Login Time	Last Page	Last Page Time	Page Time	# of pages	Last Message	
<input type="checkbox"/> admin	7 [IP address]	Jun 24 5:31:06 PM	dashboard.vm	Jun 30 3:11:32 PM	2 secs	13,142	N/A	
<input type="checkbox"/> admin	2 [IP address]	Jun 25 3:04:17 PM	dashboard.vm	Jun 30 3:11:43 PM	0 sec	13,806	N/A	
<input type="checkbox"/> admin	1 [IP address]	Jun 30 2:55:00 PM	reports.vm	Jun 30 2:55:00 PM	0.5 secs	2	N/A	
<input type="checkbox"/> admin	2 [IP address]	Jun 25 10:51:27 AM	dashboard.vm	Jun 30 3:11:46 PM	0 sec	14,437	N/A	
<input type="checkbox"/> admin	5 [IP address]	Jun 24 5:59:53 PM	dashboard.vm	Jun 30 3:11:28 PM	0.1 secs	16,386	N/A	

Figure 63 - Sessions Panel

3.7.8. Remote Sessions

For appliance oMMs only (i.e. oMMs 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 Section 3.5 - 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.

Active Reachthrough Sessions on Gateways: gateway: "All Gateways > H090111G00" last reported 14.6 secs ago

Filter...

All

Search

<input type="checkbox"/>	Port ▲	Gateway	LAN Host	Host Port	Started At	Connected Users
<input type="checkbox"/>	5,900	H090111G00	172.22.0.100	5,900	Aug 27 9:55:53 AM	[admin@10.1.66.140, logaccess@10.1.66.140]

Stop

Figure 64 - 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 Section 3.5 - Total Reach Tab for more information).

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

3.7.9. User Activity

On appliance oMMs only (i.e. not hosted oMMs), 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*.



Audit history 7,278 gateways					1 - 134 of 134
Filter...		Last Hours: ▼	24	Search	 
Time ▲	User	Host	Node or Group	Action	
Jun 29 5:19:39 PM	admin	208.80.155.8	H10	Execute report connectivity_graph (run) for Jun 28 5:19:38 PM to Jun 29 5:19:38 PM (1 day)	
Jun 29 5:19:52 PM	admin	208.80.155.8	H13	Execute report connectivity_graph (run) for Jun 28 5:19:51 PM to Jun 29 5:19:51 PM (1 day)	
Jun 29 5:20:00 PM	admin	208.80.155.8	H14	Execute report connectivity_graph (run) for Jun 28 5:19:59 PM to Jun 29 5:19:59 PM (1 day)	
Jun 29 5:20:07 PM	admin	208.80.155.8	H14	Execute report connectivity_graph (run) for Jun 28 5:20:06 PM to Jun 29 5:20:06 PM (1 day)	
Jun 29 5:20:17 PM	admin	208.80.155.8	H14	Execute report connectivity_graph (run) for Jun 28 5:20:16 PM to Jun 29 5:20:16 PM (1 day)	
Jun 29 5:20:24 PM	admin	208.80.155.8	H14	Execute report connectivity_graph (run) for Jun 28 5:20:24 PM to Jun 29 5:20:24 PM (1 day)	

Figure 65 - User Activity Panel

3.7.10. DNS Servers

The oMM 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 oMM, 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.



Add or Edit DNS Server			1 - 1 of 1
Filter...		Search	 
Server name ▲	IP Address	Domain	
<input type="checkbox"/> VehicleDNS	dns1.AmbulancesRUs.com	AmbulancesRUs.com	
		Add Delete	

Figure 66 - Panel Listing DNS Servers

Adding a new DNS server:

Add or Edit DNS Server	
Server name:*	<input type="text" value="VehicleDNS"/>
Lifetime:*	<input type="text" value="300"/> (seconds)
IP Address:*	<input type="text" value="dns1.AmbulancesRUs.com"/> (eg: dyndns.org or ipaddress)
Domain:*	<input type="text" value="AmbulancesRUs.com"/>
Save Cancel	

Figure 67 - 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: DNS servers cannot be deleted if there are oMGs associated with it.**

* denotes a required field

3.7.11. 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

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

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

4.1. Tracker

The *Tracker* package plots the geographical locations of all units/vehicles in a fleet or selected vehicles within a fleet. If the package is installed, a *Tracker* tab will be available in the oMM.



Figure 68 - Tracker Tab Plotting Locations

The following options are available/relevant to Tracker:

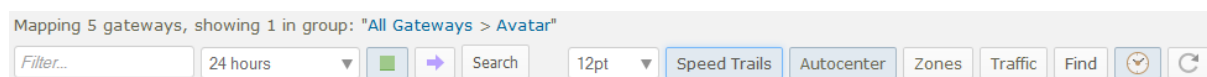


Figure 69 - Tracker Tab Options

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.

4.2. 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 oMM 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 oMM.

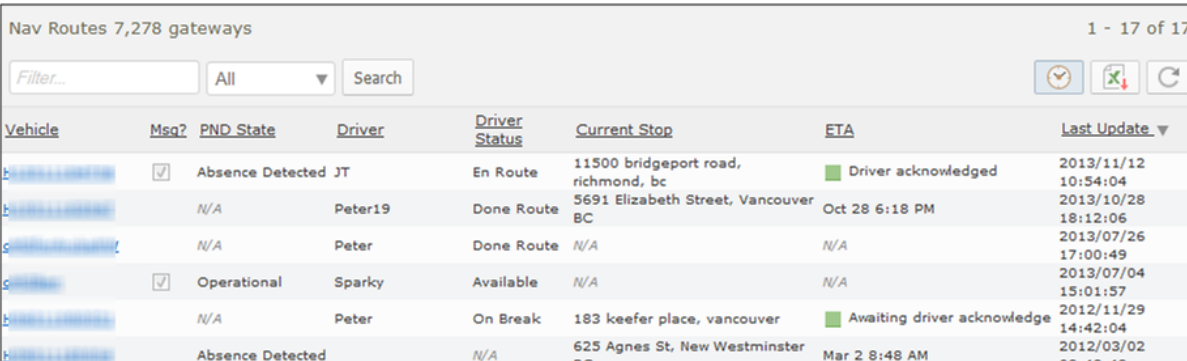
The Garmin PND and the oMG are physically connected via a serial cable and are installed in a vehicle. The PND automatically reports its location via the oMG to the oMM using the oMG's onboard application and wireless WAN connection.

At the control center, administrators can view real-time vehicle locations on a map displayed on the oMM 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 oMM.

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.

4.2.1. Nav Panel Overview

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



Vehicle	Msg?	PND State	Driver	Driver Status	Current Stop	ETA	Last Update
11500 bridgeport road, richmond, bc	<input checked="" type="checkbox"/>	Absence Detected	JT	En Route	11500 bridgeport road, richmond, bc	Driver acknowledged	2013/11/12 10:54:04
5691 Elizabeth Street, Vancouver BC	<input type="checkbox"/>	N/A	Peter19	Done Route	5691 Elizabeth Street, Vancouver BC	Oct 28 6:18 PM	2013/10/28 18:12:06
N/A	<input type="checkbox"/>	N/A	Peter	Done Route	N/A	N/A	2013/07/26 17:00:49
N/A	<input checked="" type="checkbox"/>	Operational	Sparky	Available	N/A	N/A	2013/07/04 15:01:57
183 keefer place, vancouver	<input type="checkbox"/>	N/A	Peter	On Break	183 keefer place, vancouver	Awaiting driver acknowledge	2012/11/29 14:42:04
625 Agnes St, New Westminster BC	<input type="checkbox"/>	Absence Detected	N/A	N/A	625 Agnes St, New Westminster BC	Mar 2 8:48 AM	2012/03/02 08:48:48

Figure 70 - 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 oMM received information about Nav.

4.2.2. 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 71 - 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:

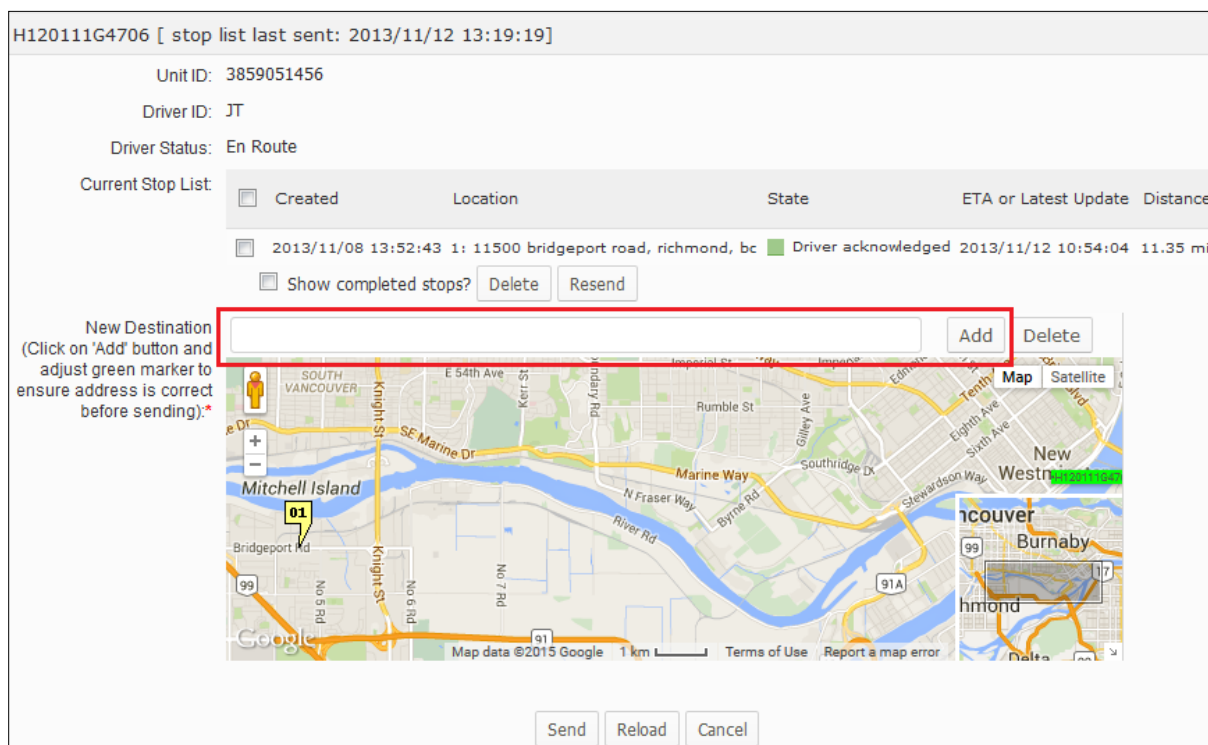


Figure 72 - Adding a New Destination

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

Figure 73 - Deleting a Destination

4.2.3. Send Message

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

Figure 74 - Send Message Panel

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

Figure 75 - 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

4.2.4. 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.

Query Responses 7,278 gateways

1 - 27 of 27 (1,411 filtered out)

Filter...

Previous Months: 24

Search

Time ▼	From	To	Message	Responses	Latest Status	Last update
2014/06/20 11:26:05	H1	Operator	Hi Server	N/A	Received	
2014/06/20 10:58:44	Operator	H10	Good Morning	N/A	<div></div> Viewed	2014/06/20 10:59:06
2014/01/13 15:31:28	Operator	roy-desk	ss	N/A	<div></div> Gateway not reachable	2014/01/13 15:32:25
2013/11/15 15:36:47	Operator	H12	test 2	1 of 1	<div></div> User Responded	2013/11/15 15:37:33
2013/11/15 15:26:23	H1	Operator	Hiya	N/A	Received	
2013/11/15 13:19:36	H1	Operator	It Is Raining	N/A	Received	

Figure 76 - Message List

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

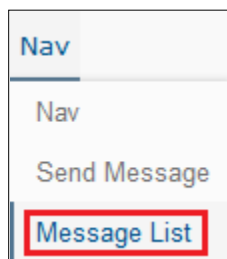


Figure 77 - Displaying the Message List Panel

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

Send Text Message

Vehicle(s):* Available Items (1) Filter... Selected Items (0)

H130112D0045

Email a copy to: (addresses)

Message text:*

Response choices: response 1
response 2
response 3

One response choice per line. Optional.

Current Question:

- response 1:
- response 2:
- response 3: H120111G4706@2013/11/12 10:59:12,

Send Cancel

Figure 78 - 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.

4.3. Telemetry

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

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*.

Viewing 7,278 gateways

Filter... 24 hours Search

Name (ID) ▲	Engine Coolant	IdleTime	OBIdleTime	OBDII Scanner	OBDSscannerConnected	speed
	105.0 °F	N/A	789 days 20 hours	N/A	Connected	N/A
	N/A	N/A	7 days 2 hours	N/A	N/A	N/A
	N/A	N/A	698 days 6 hours	N/A	N/A	N/A
	0.0 °F	N/A	926 days 14 hours	N/A	N/A	N/A
	87.0 °F	N/A	848 days 20 hours	N/A	N/A	N/A

Figure 79 - Telemetry Tab

4.4. Asset Manager

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

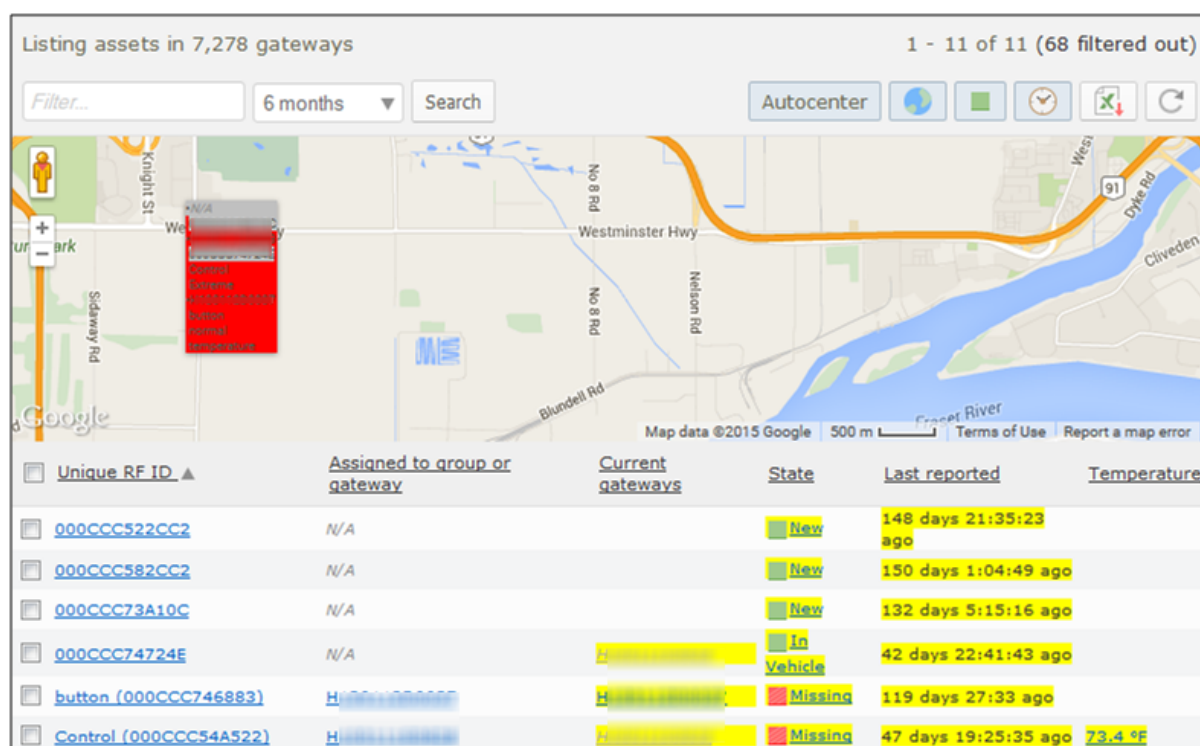


Figure 80 - Assets Tab

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**.

The screenshot shows the 'Editing Asset' form for asset ID 000CCC522CC2. The form includes the following fields:

- Unique RF ID: 000CCC522CC2
- Label: (empty)
- Type of asset: RFID
- Assigned to group or gateway: Group: All Gateways (7,278 gateways)
- Notes: (empty text area)

At the bottom of the form are three buttons: Save, Delete, and Cancel.

Figure 81 - 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 oMM. 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 oMM. In addition to reports for the core oMM 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.

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.

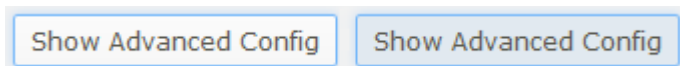


Figure 82 - Toggling the Show Advanced Config Button

The option to show or hide the **Show Advanced Config** button is found in *Options > Show Advanced Edit Fields*:

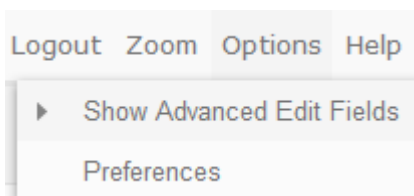


Figure 83 - Menu to Show or Hide the Show Advanced Config Button

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 84 - Additional Report Functions

Save Results: Allows the report to be saved on the oMM. 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 oMM 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 *Availability Trend* was scheduled for one gateway on two different days, while the Event Viewer Reports were scheduled for 3 different gateways.



Saved reports for 7,278 gateways				1 - 131 of 131
<input type="text" value="Filter..."/>	All ▼	<input type="button" value="Search"/>	<input type="button" value="Readonly"/>	 
Report Name ▲	Type of report	Gateway(s)	Next Run Time	
<input type="checkbox"/> 4832 test report	Coverage Trails	XXXXXXXXXX	N/A	
<input type="checkbox"/> a1-excl	Statistics Graph	Group: Larry	N/A	
<input type="checkbox"/> a1-html	Statistics Graph	Group: Larry	N/A	

Figure 85 - 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.

Generated reports for gateway: "All Gateways > HomeL33333333" last reported 1305 days 1 hour ago 1 - 1 of 1 (1,177 filtered out)

All ▼

Search





<input type="checkbox"/> <u>Report Name</u> ▲	<u>Type</u>	<u>Size</u>	<u>Run Time</u>	<u>Gateway(s)</u>	<u>User login name</u>
<input type="checkbox"/> Yesterday for all	Availability Trend, availability as uptime over gateway run time, 35 reporting, 2 below average of 97%, 26,302 events	0.403 MB	Feb 4 12:40:42 PM	All Gateways	admin

Delete

Figure 86 - 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:



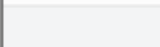
Availability Trend for (7,278 Gateways) from Feb 3 to Feb 4 (1 d run time, 35 reporting, 2 below average of 97%, 26,302 events)						
<input type="button" value="Delete"/>	<input type="button" value="Email"/>	<input type="button" value="Link"/>		<input type="button" value="Change"/>	<input type="button" value="Edit"/>	
Results by vehicle (active WAN link only)						
Vehicle	Run Time	Average	Feb 3	Feb 3 1:00:00 AM	Feb 3 2:00:00 AM	Feb 3 3:00:00 AM
	15 hours 8 mins	21%	0%	0%	0%	0%
	23 hours 57 mins	96%	100%	100%	100%	100%

Figure 87 - 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 oMM will automatically append a link to the report at the bottom of the email. The base URL of this link is configured by the oMM administrator and if it is changed, the backend processes of the oMM must be restarted in order for the new base URL to be used in the report emails. For hosted oMM'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.

Appendix A. CSV File Information

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.

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:

# 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
H111111 G0021	Test-WPA2-PSK-AES(N)	Test-WPA2-PSK-AES(N)	mypassphrase	zzbbffddeeff112233445566ff
H111111 G0765	Test-WPA2-PSK-AES(N)	Test-WPA2-PSK-AES(N)	mypassphrase	aabbffddeeff112233445566ff

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 oMM.
- 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 oMM.
- 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:** G100108B0111
- **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 oMM.

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 oMM will only import those rows whose VPN Name matches that of the selected VPN currently open on the provisioning screen. If left blank, the oMM 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:

# 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 oMM.
- 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.