Vanguard™
Broadband Cellular Router

CUMULATIVE SOFTWARE RELEASE NOTES
Covers PN 039-7230-001, revision V5.1.4A
Revised May 2015

IMPORTANT NOTICE

Because of the nature of wireless communication, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the Vanguard 3000 are used in a normal manner. Vanguard 3000 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. CalAmp accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using Vanguard 3000, or for the failure of Vanguard 3000 to transmit or receive such data.

LEGAL NOTICES

© Copyright 2012- CalAmp.

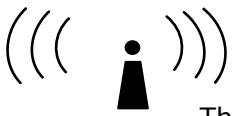
All information contained herein and disclosed by this document is confidential and the proprietary property of CalAmp, and all rights therein are expressly reserved. Acceptance of this material signifies agreement by the recipient that the information contained in this document is confidential and that it will be used solely for the purposes set forth herein. Acceptance of this material signifies agreement by the recipient that it will not be used, reproduced in whole or in part, disclosed, distributed, or conveyed to others in any manner or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the express written permission of CalAmp.

All CalAmp logos and trademarks are the property of CalAmp. Unauthorized usage is strictly prohibited without the express written permission of CalAmp.

All other company and product names may be trademarks or registered trademarks of their respective owners. Products and services of CalAmp, and those of its licensees may be protected by one or more pending or issued U.S. or foreign patents.

Because of continuing developments and improvements in design, manufacturing, and deployment, material in this document is subject to change without notification and does not represent any commitment or obligation on the part of CalAmp. CalAmp shall have no liability for any error or damages resulting from the use of this document.

RF EXPOSURE COMPLIANCE REQUIREMENTS



The Vanguard 3000 modems are designed and intended for use in fixed and mobile applications. "Fixed" assumes the device is physically secured at one location and not easily moved to another location. Maintain a distance of at least 20 cm (8 inches) between the transmitter's antenna and any person while in use. This modem is designed for use in applications that observe the 20 cm separation distance.

Please read and understand the important regulatory and safety information contained in the Vanguard 3000 user manual (PN 001-9300-001) before commissioning.

1 Scope

This document contains the Release Notes associated with the Vanguard 3000 firmware (CalAmp PN 039-7230-001).

A description of fixes and enhancements from the previous releases is presented. A description of known issues that may affect each released version is also presented, along with workarounds (when applicable).

2 Changes in V5.1.4A (from V5.1.3A)

2.1 FEATURES

No new features in this release.

2.2 FIXES

VAN-118	Kernel security has been improved against attackers with physical access.
VAN-119	*LAN Settings* > *Remote Administration* > *Telnet* = 0 now correctly forwards telnet packets to the DMZ host when *Router* > *DMZ Support* > *DMZ* is enabled.
VAN-120	Improved detection and recovery in cases of loss of WiFi connectivity.
	Update web page Copyright notices to *2015*.

3 Changes in V5.1.3A (from V5.1.3)

3.1 FEATURES

	Rename "GPS" web pages to "GPS/GNSS" (Global Navigation Satellite System). Add support for GLONASS when the internal receiver supports it.
VAN-23	SNMP can now report a trap when RSSI, averaged over a period of time, falls below or above specified thresholds. See the new *Diagnostics* > *SNMP Traps* web page.
VAN-24	(Easter Egg: clicking on the *GPS* > *Status* > *Position* data launches Google Maps.)

3.2 FIXES

	More improvements in the reporting of EC/IO.
	Fix a race condition that could prevent the I/O events from being transmitted by SMS.
	Resolve issues with transmitting log via *Diagnostics* > *Log File Actions* > *TFTP to Server*.
	Fix *Unit Status* > *Basic Settings* > *Unit ID* displaying blank after after a config from an older version of firmware is uploaded via *Firmware Update* > *Configuration File*.
	Correct the processing of configuration upgrades coming from DeviceOutlook. For any of the table parameters (*WLAN Settings*> *Client* > *Access Points*, *Router* > *Port Forwarding* > *IP Mapping Table*, *Security* > *IPsec* > *Tunnel Table*, etc.) if the Vanguard and the new configuration both have either a single table entry or both have multiple table entries then the upgrade is processed correctly. If one has a single entry and the other has multiple entries, then the tables are *combined*. (Workaround: add a "dummy" entry if necessary to make sure that both tables have multiple entries before scheduling a configuration upgrade.)
	(In consultation with Technical Support, special *Unit ID* values cause extra debugging information to be written. "DEBUG_UNIT_STATUS" writes to the syslog and "SIERRA_DMLOG" and "SIERRA_DMLOG_UP" write both to the syslog and create a file that can be downloaded via the URL *http://192.168.1.50/sierra_dmlog.gz*)

4 Changes in V5.1.3 (from V5.1.2B)

4.1 FEATURES

VAN-5	To support carriers that report the country code prefix in the SMS Sender address of incoming messages but expect an International or Domestic dialing prefix on outgoing messages, add *Diagnostics* > *SMS* > *Replace Country Code* & > *With ... in Responses* fields.
	To simplify the management of configuration files for a fleet of Vanguard 3000s, *Firmware Update* > *Configuration File* > *Upload* now accepts any filename that begins with "config" and ends with ".xml", for example: *config_1ADAM12.xml* or *config_SN_123456.xml*.

4.2 FIXES

VAN-6	In certain cases, the Cell Connection > GSM Settings page would report "SIM REJECTED / PIN ACCEPTED" when a PIN-locked SIM was installed. A locked SIM without a remembered PIN now displays as "SIM LOCKED / PIN REQUIRED".
	Improve the collection of cell module data that, on certain carrier networks, could cause the Unit Status web page to report the incorrect Service Type (CDMA instead of HSPA), RSSI and/or EC/IO.
	When upgrading from much older firmware (circa 5.0.2), detect DeviceOutlook/COLT parameters used for testing and replace them with the current default values.
	Update web page Copyright notices to *2014*.

5 Changes in V5.1.2B (from V5.1.2A)

5.1 FEATURES

No new features in this release.

5.2 FIXES

	Rename *Unit Status* "*PPP Subnet Mask*" & "*PPP P-t-P*" to "*Cell Subnet Mask*" & "*Cell Gateway*" to clarify that the cell module does not report the IP address of the carrier's side of the radio link.
	Improve handling of DeviceOutlook's Send SMS feature when used with the carriers' email-to-SMS gateways. Report ICCID back to DeviceOutlook.

6 Changes in V5.1.2A (from V5.1.2)

6.1 FEATURES

No new features in this release.

6.2 FIXES

903.8	The RSSI LED is now updated correctly (broken by the RSSI fix in 5.1.2).

6.3 KNOWN ISSUES

N/A.

7 Changes in V5.1.2 (from V5.1.1)

7.1 FEATURES

	The restriction preventing *Cell Connection > Primary Carrier* and *Secondary Carrier* from both being CDMA carriers (eg. Verizon and Sprint) has been removed.
	Diagnostics > SMS: The SMS CLI (Command Line Interface) allows a small set of commands to be sent to the Vanguard 3000 over SMS. Commands exist to: obtain the status of the unit (including the state of the analog & digital inputs), to start & stop the VPN connection, to open or close either the relay outputs, and to reset the unit. Commands can be restricted to be accepted only if they arrive from one of up to three "friendly" SMS Sender addresses and only if they contain a specified password. *I/O Settings > Settings > SMS Notification*: Changes to the analog & digital inputs can be reported to up to three destination SMS addresses.
	GPS > Store and Forward: The Vanguard can be configured to store the reports generated by the *GPS > Remote Delivery* configuration when out of coverage (*Unit Status > PPP Status* is DOWN). Those reports will be forwarded to the host(s) defined when the router re-establishes its cellular connection
	COLT has been renamed to *DeviceOutlook*. Update web page & Help. Improve firmware & config update mechanisms to match the server-side DeviceOutlook 1.6.1 release.
	ODP: Allow *I/O Settings > Settings* to set 127.0.0.1 as the I/O Manager address when ODP is enabled so that co-resident ODP applications can use the NMEA I/O protocol to control the I/O ports.

7.2 FIXES

	In the online Help for *Cell Connection > Primary/Secondary > Authentication Protocols*, clarify that not all carriers support Auto negotiation. For these carriers, either PAP or CHAP, or both, must be explicitly selected. Add missing Help for *Cell Connection > Automatic Carrier Switching* and clarify upgrade filenames in *Firmware Update* Help.
	Update the collection of RSSI & ECIO information as per cell modem manufacturer recommendations (fixes incorrect reporting of CDMA 1xRTT RSSI).
	ODP: Make sure read/write permissions for /odp are set in all subdirectories.

7.3 KNOWN ISSUES

N/A.

8 Changes in V5.1.1 (from V5.1.0B)

8.1 FEATURES

860	Added support for failsafe web page & COLT OTA firmware upgrades on appropriate hardware. (The upgrade process can take up to 15 minutes depending on the size of the upgrade. If the unit is powered-off or reset during the upgrade, it will remain at its original firmware version and may reattempt the upgrade at next boot.)
870	*Cell Connection > Modem-to-Modem*: In applications that require modems to communicate directly with each other, as compared to communicating only to Hosts or having a Host relaying communications between modems, carriers might assign "nearby" IP addresses to the other modems which overlap with the network defined by *Unit Status > PPP > PPP IP Address* and *PPP Subnet Mask*. Enabling this option will

	force *PPP Subnet Mask* to 255.255.255.255 to work-around this. **Warning: This setting may not resolve the issue in all cases. It may be necessary to request that the carrier reassign IP addresses of some modems.**
	The Vanguard 3000's cellular ICCID is now displayed on the *Unit Status* web page.

8.2 FIXES

5743	Improved monitoring and restart of dropped PPTP connections.
	Fixed *Unit Status > Basic Settings > Power Management > When Voltage Drops Below* so that a setting of 0.0 Volts still monitors the *After Ignition Line Off* time setting.
	Fixed issue with invalid firewall rules being created on Vanguards without WiFi.

8.3 KNOWN ISSUES

Issue	Web Browser times-out during failsafe upgrade
Symptom	Large upgrades may take longer than the browser is programmed to wait for the "Upgrade Successful!" web page, displaying a "Gateway Timeout!" or similar message.
Workaround	Wait enough time for the upgrade to complete and the unit to reboot then click on the browser's Refresh button to start a new connection to the Vanguard 3000.

9 Changes in V5.1.0B (from V5.1.0)

9.1 FEATURES

	New COLT server addresses & ports: COLT Enterprise Services (CES) servers & maintenance servers are now hosted at *ota.calamp-ts.com*, port *20511*. New units and units that have been factory-defaulted (press and hold the RESET button) will show these new values. Units upgraded from 5.1.0 will retain their existing settings so users are encouraged to go to the *Diagnostics > CES Config* web page and enter the new values

9.2 FIXES

	Problems with *Cell Connection > GSM Settings > Change PIN Status* not saving the PIN across resets has been corrected.
	Issues with services, such as Web or SNMP, on devices on the local LAN being unreachable through an IPsec tunnel because the Vanguard's instance of those services was "capturing" the requests, have been fixed.
	With *Serial > External PAD > PAD Mode* = Server, *Pad Protocol* = TCP and Quiet mode enabled, the serial port still displayed "RING" on an incoming call. This has been fixed. (To enable Quiet mode, enter the commands ATQ1 and AT&W on the serial port.)
	I/O Settings > Digital Input Status > Digital Input 2 always reported Normal in 5.1.0, now fixed.
	Fields in *Cell Connection > GSM Settings* and *CDMA Settings* are inaccessible (grayed-out) when Cell *Connection > Active Carrier* is set to Automatic to prevent the possibility of interference with Automatic Carrier Switching activity. To be able to update these settings, first change the *Active Carrier* to Primary or Secondary.
	An issue that could cause the SMS Manager service on port 6290 to stop accepting client connections has been fixed.
	Access by the *admin* user to internal commands, such as *ping*, has been restored.
	An issue with the GPS coordinates sent in COLT periodic reports has been fixed.

	To make sure that COLT scheduled actions are performed at the expected time, if *Unit Status* > *Basic Settings* > *Network Time* is not enabled then the internal time of day clock is set when the GPS receiver first receives a valid time report.
	A race condition between DNS and NTP that could prevent the *Network Time* from being fetched soon after the WAN connection was established has been resolved.

9.3 KNOWN ISSUES

N/A.

10 Changes in V5.1.0 (from V5.0.2)

10.1 FEATURES

	Automatic Carrier Switching
	• *Cell Connection* > *Carrier* > *Active Carrier* now has an *Automatic* option. Automatic instructs the modem to choose the carrier based on conditions defined in the *Automatic Carrier Switching* section.
	• *Automatic Carrier Switching*
	  ○ *Stay on Primary until no connection for*: If the modem fails to connect to the Primary Carrier, or loses the connection with the Primary Carrier for one of the specified number of minutes, or the RSSI or ECIO levels fall below the specified thresholds, it will attempt to connect using the Secondary Carrier. **Note: Depending on the carrier, the WAN IP address may change which may require sockets to be re-established.**
	  ○ *Stay on Secondary until no connection for*: If the modem fails to connect to the Secondary Carrier, or loses the connection with the Secondary Carrier for one of the specified number of minutes, or the RSSI or ECIO levels fall below the specified thresholds, it will attempt to connect using the Primary Carrier. **Note: Depending on the carrier, the WAN IP address may change which may require sockets to be re-established.**
	  ○ *Return to Primary after*: In case the Secondary Carrier is more expensive, the modem will only remain on the Secondary Carrier for the specified amount of time and then attempt to return to the Primary Carrier. If zero, the modem will remain on the Secondary Carrier as long as its connection is good.
	• To prepare a unit for Automatic Carrier Switching, choose *Primary* as the *Active Carrier*, set up and test the *Primary Carrier* credentials. Similarly, choose *Secondary* as the *Active Carrier*, set up and test the *Secondary Carrier* credentials. Finally, configure the conditions on which carrier switching should occur, and set the *Active Carrier* to *Automatic*.
	• At boot time, the unit always attempts to first connect with the Primary carrier.
	• If a *Secondary Carrier* is not defined, selecting *Automatic* will have no effect and the unit will behave as if the *Active Carrier* were set to *Primary*.
	• RSSI & ECIO values are averaged over about a 30 second period to avoid spurious carrier switching. Also, RSSI and ECIO settings are only tested while the unit has an active connection to a carrier.
	• ECIO (a measure of interference -- values in dBm closer to 0 indicate weaker interference) is now displayed on the *Unit Status* home page.
	• When Automatic Carrier Switching is enabled, the *Unit Status* > *PPP* > *PPP Status* field also indicates the current carrier switching state.

	The Vanguard 3000 now contains a *CalAmp On-Line Telemetric* (COLT) Client that

	communicates with a *CalAmp Enterprise Services* (CES) Server to provide customers with various status, measurement and upgrade services. The Client can be configured from the *Diagnostics > CES Config* web page.
	IPsec Remote ID: In cases where the remote endpoint identifies itself with a different address, perhaps because it is passing through a firewall, a connection may fail and the View log contains the message "We require peer to have ID x.x.x.x but peer declares y.y.y.y" where x.x.x.x is the *Remote IP Address* of the tunnel. In these cases, enter y.y.y.y as the *Remote ID* and it will be used during establishment of the tunnel.

10.2 FIXES

	Issues in 5.0.2 firmware with CDMA Provisioning and SIM PIN operation have been resolved
	The Google nameservers 8.8.8.8 and 8.8.4.4 are no longer provided as a fallback. The carrier must provide nameserver addresses to be used by Vanguard 3000 internal services and when *LAN Settings > DNS Resolving > DNS Auto* is enabled.
	The actions of *LAN Settings > IP Filtering* now take place after *MAC Filtering* before all other internal firewall rules, such as those from *LAN Settings > Remote Administration*, so that explicit IP Filters can override the Vanguard 3000's default behavior.
	Issues with entering a *LAN Settings > Remote Administration > Admin Password* containing special characters such as dollar sign "$" or asterisk "*" have been resolved. Now, all printable ASCII characters except apostrophe "'" are valid.
	Issues where the *Unit Status* or *Cell Connection* web pages attempt to get information from the cell module before it is ready, usually right after boot or after a carrier switch, have been addressed.
	The *Cell Connection > Carrier* web page will refuse to Save if the Primary and Secondary carriers use the same cellular protocol (GSM/CDMA).
	The IPsec engine is always loaded into memory, even if *Security > IPsec > IPsec* is disabled. This has no performance effect if no IPsec tunnels are defined although the memory consumed may affect ODP applications.
	Security > IPsec > Tunnel Monitor > Delay, previously limited to 255 seconds, has been extended to 65535 seconds. Similarly, *Phase 1 Key Lifetime* and *Phase 2 Key Lifetime*, previously limited to 255 minutes, has been extended to 65535 minutes.
	Duplicate "WLAN to WAN" entries in the *LAN Settings > IP Filtering > Direction* drop-down list have been corrected.
	Issues with *Diagnostics > Logging > Auto-Logging*, used in consultation with CalAmp's Technical Services personnel, have been fixed.

10.3 KNOWN ISSUES

N/A.

11 Changes in V5.0.2 (from V5.0.1)

11.1 FEATURES

	Serial web page now supports word length, parity & stop bits for both External and Internal serial ports.
	The *Unit Status* web page now displays the Main Voltage.
	For greater security when copying config files offline, passwords & keys are now encrypted as they are written to the config file.

	Support 12-bit A-to-D converter, when installed.
	For ODP users, more Vanguard & cell module identity information is available, and commands are now available to control carrier selection & data session status.
	For ODP users, "raw" GPS reports are available on port TCP 6259.

11.2 FIXES

	The latest version of cell modules can now be correctly set to Verizon or Sprint.
	Traffic with local IP addresses can no longer "leak" onto the WAN as IPsec tunnels are being negotiated.
	Problems with the *Security > IPsec > Tunnel Monitor* feature have been resolved.
	Cell Connection PAP and CHAP requests are now correctly sent to the carrier.
	Cell Connection > GSM Settings > Band Selection now refreshes the web page after Saving.
	Diagnostics > Logging > Display no longer displays in one long line.
	Certain *Serial* web page changes require a reboot – the unit now displays this fact before rebooting.
	Serial > External PAD > Incoming Port now maintains its value after disable/enable.
	The *LAN Settings > DNS Auto* radio button no longer gets stuck on Enable.
	DHCP now hands out the correct maximum number of leases.
	The GPS driver could crash if multiple clients connected to the Local or Remote TCP servers, now fixed.
	A memory leak when determining carrier type (GSM/CDMA) could eventually lead to an unexpected reboot, now fixed.
	For ODP users, the appmgr.log file is now rotated when it exceeds 100K.
	For ODP users, the report of a huge "CPU usage" value in the log has been fixed.

11.3 KNOWN ISSUES

N/A.

12 Changes in V5.0.1 (from V5.0.0)

12.1 FEATURES

No new features in this release.

12.2 FIXES

	SNMP traps can now be directed to addresses over an IPsec tunnel. To do so: • *LAN Settings > Bind Services to Eth IP* must be enabled; • *Security > IPsec*. The tunnel must have Local Subnet set to LAN.
	Cell Connection > System Monitor > Periodic Ping now works correctly. Note that this feature is only active when the cell connection is UP.
	The Unit ID is now correctly reported in NMEA $IIALR messages.
	WLAN Settings > Access Point > DNS Auto now correctly services DNS queries soon after the unit boots.
	Router > Static Routes no longer pops-up a JavaScript error when WAN or VPN Client routes are adding on Vanguard 3000 units that do not have WiFi.
	A memory leak that could lead to the cell connection being restarted after 3+ days of operation has been fixed

12.3 KNOWN ISSUES

Issue	Only one GRE tunnel allowed for each set of unique endpoints.
Symptom	
Workaround	

Issue	Web page refreshes during carrier switch may result in inaccurate data display.
Symptom	
Workaround	Refreshing data after carrier switch is complete will display updated data.

13 Release of V5.0.0

13.1 FEATURES

	Initial Product Release.
	Cell Connection web page allows the credentials for a Primary and Secondary Carrier to be defined. The Active Carrier can be selected from the web page.

13.2 FIXES

N/A.

13.3 KNOWN ISSUES

Issue	SNMP traps will not go through an IPSec tunnel.
Symptom	
Workaround	

Issue	Only one GRE tunnel allowed for each set of unique endpoints.
Symptom	
Workaround	

Issue	IPSec and/or PPTP tunnels get misdirected when WiFi client mode is default route.
Symptom	
Workaround	

Issue	Web page refreshes during carrier switch may result in inaccurate data display.
Symptom	
Workaround	Refreshing data after carrier switch is complete will display updated data.

About CalAmp

CalAmp is a leading provider of wireless communications products that enable anytime/anywhere access to critical information, data and entertainment content. With comprehensive capabilities ranging from product design and development through volume production, CalAmp delivers cost-effective high quality solutions to a broad array of customers and end markets. CalAmp is the leading supplier of Direct Broadcast Satellite (DBS) outdoor customer premise equipment to the U.S. satellite television market. The Company also provides wireless data communication solutions for the telemetry and asset tracking markets, private wireless networks, public safety communications and critical infrastructure and process control applications. For additional information, please visit the Company's website at www.CalAmp.com.