



FUSION™ LTE ROUTER

Cal/Amp®

CUMULATIVE SOFTWARE RELEASE NOTES
Covers PN 039-9300-003 up to revision V1.2
Revised July 2019

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 Fusion are used in a normal manner. Fusion 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 Fusion, or for the failure of Fusion to transmit or receive such data.

LEGAL NOTICES

© Copyright 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019 - 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 Fusion LTE modems are designed and intended for use in fixed and mobile applications. ^{RF Exposure} "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 Fusion user manual (PN 001-0000-602) before commissioning.

1 Scope

This document contains the cumulative Fusion release notes associated with the Fusion firmware (CalAmp PN 039-9300-003) up to revision V1.2 (build PROD V1.2.14_R201907020800).

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

2 Changes in V1.2 (PROD V1.2.14_R201907020800 from PROD V1.2.13_R201801111600)

2.1 FIXES

FUS-486	CLONE - Deprecating COLT weak ciphers affects Fusion
N/A	Corrected some build issues with the IPSec module.

2.2 ENHANCEMENTS

3 Changes in V1.2 (PROD V1.2.13_R201801111600 from PROD V1.2.12_R201706151500)

3.1 FIXES

FUS-479	CLONE - KRACK WPA2 Vulnerability.
N/A	Removed a useless WIFI log.

3.2 ENHANCEMENTS

4 Changes in V1.2 (PROD V1.2.12_R201706151500 from PROD V1.2.11_R201611090800)

4.1 FIXES

FUS-309	Time page issues.
FUS-372	Memory leak in cesGateway.
FUS-469	Remove GPS UDP port above 1024 restriction.
FUS-471	Gateway time-out message during local upgrade of cell card (MC7750).
FUS-474	IPSec sometimes does not start after power cycle.
N/A	Adjusted AAVL help text to reflect line endings.

4.2 ENHANCEMENTS

5 Changes in V1.2 (PROD V1.2.11_R201611090800 from PROD V1.2.10_R201608010800)

5.1 FIXES

FUS-213	SNMPv3 SHA Authentication does not work.
FUS-427	Root login requires only first 8 characters of the password to authenticate.
FUS-435	Remove telnet from remote administration.
FUS-441	EVDO mode reported as CMDA 1xRTT.
FUS-450	AAVL Settings>Remote Delivery>UDP Hosts, 4th Octet is truncated to 2 digits.
FUS-451	SNMPv3 noauth & md5 doesn't work.
FUS-453	Customer is experiencing their Fusion shutting down before the define ignition time setting "After ignition line off, Shutdown in 180 minutes".
FUS-457	StationMonitor table too small (warning).
FUS-459	Loss of Verizon Data Session.
FUS-460	Local UDP GPS Reports to broadcast.
N/A	SNMP MIBS missing some SSH and HTTPS parameters.

5.2 ENHANCEMENTS

N/A	Active monitoring of cell interface state.
-----	--

6 Changes in V1.2 (PROD V1.2.10_R201608010800 from PROD V1.2.9_R201604110830)

6.1 FIXES

FUS-443	Build issues (When building from a clean LUCEE2.1.1 environment).
FUS-444	Disable the 90 second L2UP to L3UP connection watchdog.

6.2 ENHANCEMENTS

7 Changes in V1.2 (PROD V1.2.9_R201604110830 from PROD V1.2.8_R201512161600)

7.1 FIXES

N/A	Larger web pages (this prevents some fields to wrap around more than one line).
N/A	Missing USB log files (added a sequential prefix to the filename).
FUS-424	Fixed a DeviceOutlook buffer overflow.
N/A	Adjusted some software module names (hostapd, smcroute, dropbear).

7.2 ENHANCEMENTS

N/A	SSH support.
N/A	GRE support (up to 2 tunnels).
N/A	Multicast static routing support.
N/A	Telnet can now be enabled and disabled through the GUI.
N/A	TCP MSS clamping when passing traffic inside the IPsec tunnel.
N/A	HTTP and HTTPS are now available at the same time.
N/A	Cellular "Band selection" for cell cards with catalog identifier "G".
FUS-403	Changed security default settings (only HTTPS is now enabled by default in remote admin section).

8 Changes in V1.2 (PROD V1.2.8_R201512161600 from V1.2 (V1.2.7_R201506150800))

8.1 FIXES

FUS-375	Fusion with adjacent IP addresses can't communicate with each other.
FUS-378	Wi-Fi client web page display issue.
FUS-390	Logs shows "I3ready" internal indication sent two times instead of once.
N/A	Rogue packet filter
N/A	Corrected package name conflict between two internal modules.
N/A	Wi-Fi access point channel 157 not properly mapped.
N/A	Create directories needed by the "Modem manager" at the start of a connect cycle (if they go missing). Write the event in the flight recorder.
N/A	Adjusted a modem manager internal buffer size (was too small). Could cause a useless operation during the connect step and was causing a warning in the logs.

8.2 ENHANCEMENTS

FUS-370	Netmotion "Locality application" support.
FUS-374	Changed the root password.
N/A	Added mdmcfgd to the Linux daemon monitoring list, if it dies reboot the device.
N/A	Updated hostapd from 0.7.3 to 2.4.
N/A	Updated openssl from 1.0.0d to 1.0.2d.
N/A	iptables now contains the LOG target.

9 Changes in V1.2 (PROD V1.2.7_R201506150800) from V1.2 (V1.2.6_R201503091900)

9.1 FIXES

FUS-321	IPsec tunnel fails because firewall holes are not opened.
FUS-328	iptables duplicate rules and chains.
FUS-329	IPsec label issue (when the field is not configured, the ipsec.conf is not populated with the tunnel information).

FUS-331	IPSec goes down then up on LAN interface cable connect/disconnect.
FUS-332	ETH0-as-a-WAN does not ACK the DHCP offer.
FUS-338	Invalid "client id" field in DHCP client messages.
FUS-350	IPSec local IP address sometime set to 127.0.0.1

9.2 ENHANCEMENTS

N/A	New version of IPSec (Strongswan 5.3.0 instead of 5.2.2).
N/A	IPSec drop filters (when a tunnel is down, discard its regular traffic).
N/A	Default route switching improvements.
FUS-319	Use "0.us.pool.ntp.org" as the default NTP server.
FUS-325	Fusion connection status mismatch leads to "connection down" until Fusion is power cycled.
FUS-344	Special address filtering.
FUS-348	Enable DO by default (Harris).

10 Changes in V1.2 (PROD V1.2.6_R201503091900) from V1.2 (V1.2.5_R201412081200)

10.1 FIXES

FUS-312	Support changes to Wi-Fi test script used in Production (no effect to deployed units)
---------	---

10.2 ENHANCEMENTS

N/A	Correct several entries in the General Settings > Time > Time Zone drop-down list
-----	---

11 Changes in V1.2 (PROD V1.2.5_R201502251700) from V1.2 (V1.2.4_R201412081200)

11.1 FIXES

FUS-182	Frequent disconnect/reconnects on CDMA eventually Fusion reboots.
FUS-217	Station monitor causing occasional reboots.
FUS-242	WWAN Authentication field (None, Any, PAP, CHAP) not working.
FUS-261	IPSec goes down but not back up original interface on default route switching.
FUS-262	Fusion generated IPSec configuration file gets corrupted. Returns to normal if IPSec is disabled/re-enabled.
FUS-267	GPSD parameter initialization must not delay IPC request from being served.
FUS-270	IOMNGRD parameter initialization must not delay IPC request from being served.
FUS-271	IOMNGRD must not call parmreg function on parmreg callback.
FUS-305	File system full.
N/A	The IPSec "Local Id" and "Remote Id" fields can be configured by an IP address or host name in the same field (instead of 2 separate fields).
N/A	Fixed iptables filter priority issue between the "IPSec" filters and the "Mac Allow" filters".

11.2 ENHANCEMENTS

FUS-244	NTP client support.
FUS-266	IP traffic policy of WAN interface must be "deny all" instead of "accept all".
FUS-289	WWAN mode selection (Automatic, LTE Only, 3G2G Only). This is only for MC7700 and MC7750 cell cards.
N/A	Adjusted the copyright note in the bottom of the web pages.
N/A	IPSec <ul style="list-style-type: none">- Updated version (Passed to Strongswan 5.2.2)- Removed the "Nat Traversal" parameter from the GUI.- Removed the "Perfect Forward Secrecy" from the GUI.- Added the "Phase 2 DH group" parameter in the GUI.- Adjusted help text in the GUI.- Active monitoring of tunnel states.
Fus-263	IPSec local/remote id improvement. <ul style="list-style-type: none">- Add "Local Id" parameter in the GUI- Add name in "Remote Id" field.
N/A	Added a "Restore Factory Defaults" button in the web pages.
N/A	Added RSSI and RSRQ to the SNMP MIBs.
N/A	Slowed down the polling rate of the "FusionLTE linux daemons" by the station monitor module.
N/A	Disabled log generation by the Apache daemon (HTTP server) causing to take too much space.

12 Changes in V1.2 (PROD V1.2.4_R201412081200) from V1.2 (V1.2.3a_R201406301400)

12.1 FIXES

FUS-238	IP Filters Source = Any option is broken
FUS-240	MC7719 (Catalog Model K) always reports "Inactive".
FUS-241	LTE monitor broken in 1.2.3a (Change in a parameter name caused the monitoring to fail).
FUS-243	Improvements to the USB logs: <ul style="list-style-type: none">a) Header of each logs now contains the temperature and the GPS position.b) WAN "active probe disconnect" reason sent to UDP logs.c) The GPS USB logs now contain the exact same thing as the web page.d) Display external names instead of internal names
FUS-249	Active Probe minimum for Verizon is too long.
FUS-250	Active Probe takes twice as long to trigger as expected.
FUS-251	LTE Monitor triggers are now sent to syslog.
FUS-252	Network connection up but no data connection
FUS-258	Support recent board revisions
FUS-259	WWAN interface shows inactive and layer 2 started anyway.

12.2 ENHANCEMENTS

None.

13 Changes in V1.2 (PROD V1.2.3a_R201406301400) from V1.2 (PROD V1.2.1_R201312190900)

13.1 FIXES

N/A	Fix for Sierra 7750 rapid LTE->disconnect->LTE (preserves dynamic IP address)
N/A	Fix to preserve full USB RX MTU when TX MTU set to < 1500 bytes (Sierra 7750)
N/A	Changed modem manager's poll frequency for AT-interface modems from 2 to 5 seconds due to text-based I/O, intended for Altair-based modems
FUS-226	Correction of Band20 catalog number in Web GUI

13.2 ENHANCEMENTS

HTTPS Function to support secure communications between Fusion and DeviceOutlook, added DeviceOutlook Secure Communications with HTTPs enable/disable buttons in DeviceOutlook page in Fusion's Web GUI.
Improved modem/WWAN information written by USB logger
u-boot support for Board Revision A

14 Changes in V1.2 (PROD V1.2.1_R201312190900) from V1.2 (PROD V1.2.0_R201311011000)

14.1 FIXES

5770	Serial PAD Error with UDP and friendly IP address
N/A	Fixed 3G Connection Fallback on Verizon
N/A	Fixed USB Logger GPS Format
DMDP-694	Fixed issue where Configuration may not be applied if sent by Device Outlook

14.2 ENHANCEMENTS

Wifi 5 GHz support
Wifi support of 40 MHz channels

15 Changes in V1.2 (PROD V1.2.0_R201311011000) from V1.1 (PROD V1.1.8_R201308201400)

15.1 FIXES

N/A	Fixed small IPSec issues
N/A	Fixed GPS TAIP-format reports have invalid checksum
N/A	Fixed 3G Connection
N/A	Fixed WWAN Interface disable not properly stopping WWAN

15.2 ENHANCEMENTS

IPSec Multiple subnets traffic sent in same tunnel
IPSec Packet Compression
IPSec ability to edit a tunnel entry
Bluetooth Alpha (manual configuration)
Device Outlook server Initiated Communication using SMS Messages
WiFi Access Point able to Hide SSID

16 Changes in V1.1 (PROD V1.1.8_R201308201400) from V1.1 (PROD V1.1.7_R201307121300)

16.1 FIXES

N/A	Fixed Carrier ID reported in DeviceOutlook Modem page
-----	---

17 Changes in V1.1 (PROD V1.1.7_R201307121300) from V1.1 (PROD V1.1.6_R201302221200)

17.1 FIXES

5795	IPsec cannot support multiple remote subnets
5490	NMEA IP Setting correction
5942	Fixed dual sierra modem startup failure
	Fixed import and upgrade feature with IE when Security setting (Include local directory path when uploading files to a server) is enabled.
5895-5894	Fixed OTA upgrade and configuration via DeviceOutlook
5951	Fixed Serial PAD and USB Flash Drive Interaction
	Fixed carrier initiated disconnect using mc7750
	Fixed Reboot time indication to report accurate value.
5887	IPsec private to private problems when access port 80

17.2 ENHANCEMENTS

OTA LTE module software upgrade
IP Persistence
Support LTE Band 20
Store and forward GPS
Telnet user now sync with web page user

18 Changes in V1.1 (PROD V1.1.6_R201302221200) from V1.1 (PROD V1.1.5_R201210151700)

18.1 FIXES

N/A	improved of 3G to 4G roaming
N/A	Improved the Enable/Disable mechanism of the WWAN interface
N/A	Corrected the automatic shutdown mechanism
N/A	The unit password and WIFI passphrases can now support space characters
5487	SNMP issues fixed
N/A	WWAN0 and WWAN1 do not allow setting static IP address for known public cellular carriers
N/A	IPsec tunnels must have unique labels constraint removed
	The board hardware revision has been corrected and reports the exact information
5352	Dynamic MTU is now supported
5504	SNMP get and set are now working with SNMPv3
5526	AT&T carrier is properly shown in WWAN status page
5631	Fusion GPS 4pps option has been removed
5640	WiFi client is now able to connect if SSID contains a space character
5656	IPsec tunnels connection issue
5694	Fixed issue with WiFi AP in 802.11 n mode and WPA
5700	Several Web pages were improved
5711	WPA/WPA2 passphrase now performs accurate field validation
5712	Local delivery UDP host 1 to remote addresses fixed
5716	APN field now supports 128 chars

18.2 ENHANCEMENTS

USB Serial Interface support
COLT support
Https support
Radius support
Simultaneous support of two WAN cellular modems
Improvements of IPSEC, Nat Support and detection of duplicate tunnels
Added the ability to export and import the unit configuration
The WWAN Web page now displays the APN in use
Disconnection probe integrated to every WAN interfaces

19 Changes in V1.1 (PROD V1.1.5_R201210151700) from V1.1 (PROD V1.1.4_R201208031330)

19.1 FIXES

N/A	The unit ID can now support to have space characters
5465	The ignition signal can no longer leak to the Alarm input
5527	The WWAN display was showing unsupported modes
5552	Power cycling multiple times may reset unit to factory settings
5567	The configuration file has been made more robust to corruption during saves

5641	DDNS was not functioning properly
5643	Interface up may not be detected for WiFi client using static IP addresses
5670	Stability improvement for support to new band 13 cellular modules
5727	Avoid possible crash when NMEA Manager IP address is set to Auto

19.2 ENHANCEMENTS

Cellular connection robustness is improved
Disconnection detection of all cellular supported modems improved
Software package embeds a Flash image for allowing supplier to pre-program Flash devices
WiFi Access Point interface enabled by default (implies WiFi client disabled by default)
Remote administration mode enabled by default
WWAN interfaces enabled by default
Firmware using SDK v1.8.0, allowing use of newer Cell module firmware from Sierra Wireless
Improved LTE status reporting in Web pages
Full support of Novatel E362 (FW 1.41) and E371 (FW 3.32) modems
SIM status added to the WWAN Web pages
New module for storing log data on a USB Flash drive
Provision for DDNS visible IP address added

20 Changes in V1.1 (PROD V1.1.4_R201208031330) from V1.1 (PROD V1.1.4_R201206070830)

20.1 FIXES

5500	Improved compatibility with Firefox browser
5511	Improved TCP handler for multiple clients
5520	Some parameters changes through Web pages would not be saved without a reboot
5523	The Unit ID would not accept some characters such as ""
5541	Information was missing from the Altair band 14 cellular module
5558	Web password rule (8 to 15 characters) was not enforced
5566	Enabling NAT on a WAN interface would not take effect immediately
5619	Occasional invalid sentence from GPS module could freeze unit
5621	Reset to factory defaults with setup button would sometimes not function properly
5622	WWAN disconnection was not properly reported
5624	SIM wrongly reported as missing in some cases
5626	IPsec settings on Web pages would not be saved

20.2 ENHANCEMENTS

5550	Support of Ubiquiti SR71A WiFi module, providing support to 802.11n (in addition to b and g)
5578	Support of two non-simultaneous cellular modules from same vendor

21 Release V1.1 (PROD V1.1.4_R201206070830)

21.1 FIXES

Initial release.

21.2 ENHANCEMENTS

Initial release.

22 Known Issues with Latest Release

Latest Release	V1.2 (PROD V1.2.13_R201801111600)
Issue	(FUS-183) Active disconnection probe not properly operating on multiples WAN simultaneously.
Symptom	When operating on multiples WAN simultaneously the disconnection probe will not force the disconnection of the second WAN if the first WAN is already disconnected.
Workaround	None.
Issue	(FUS-185) USB log may not react properly to checked/unchecked log items.
Symptom	When disabling the interface log checkbox the application will continue to log those events.
Workaround	None.
Issue	(FUS-205) In some cases the upgrade process did not complete (Fails) but remains in the upgrading state forever.
Symptom	When performing an upgrade while using Firefox 18 the upgrade will finish as if it were successful but the would not actually be complete.
Workaround	After upgrading using Firefox 18, carefully verify the firmware version to ensure that the upgrade was indeed successful. If the upgrade had failed restart the upgrade procedure.
Issue	(FUS-208) Firefox 18 does not prevent the user to navigate outside the upgrade page during an upgrade.
Symptom	When performing an upgrade while using Firefox 18, there is no warning that the upgrade will abort if the user navigate outside the upgrade page.
Workaround	Avoid refreshing the page or navigating to another page during upgrades with Firefox 18.
Issue	(FUS-209) Upgrade progress bar seem to never end
Symptom	When performing an upgrade in some conditions the upgrade progress bar will remain indefinitely.
Workaround	An upgrade takes a maximum of 10 minutes if it has been more than 10 minutes, navigate back to Maintenance Status to verify the current Firmware version. Repeat the upgrade procedure if the Firmware have not been upgraded.
Issue	(FUS-210) Firmware upgrade must be verifying compatibility with environment before being committed
Symptom	There is very little verifications done before accepting a firmware upgrade to FUSION. As of this writing, only verifications of HW compatibility are being done. The following verifications must also be done: 1- Verify that u-boot is compatible 2- Verify that all env variables obtained from u-boot are also compatible

	If any of these is not met, fail the upgrade and keep the current system intact.
Workaround	The customer is expected to manage upgrade package files.
Issue	(FUS-212) Some web pages are incompatible with Chrome web browser.
Symptom	When using Google Chrome some web pages will not be properly displayed.
Workaround	Use Internet explorer or Firefox to configure the unit.
Issue	(FUS-214) eth2 interface may lose connectivity when under heavy traffic at 100 Mbps
Symptom	When running heavy traffic on eth2 interface the interface may lose connectivity.
Workaround	For high traffic application use eth0 or eth1 or limit eth2 speed to 10 Mbps.
Issue	(FUS-293) WWAN Gobi SDK reports write urb error repeatedly
Symptom	After upgrading the device, we seem to get "...write urb..." error. Seems related to a WWAN cell card that is not fully activated and/or provisioned.
Workaround	Keep disabled any WWAN interface that is not in use or mentioned in the hardware profile.
Issue	(FUS-300) Web page upgrade through WWAN interface completes but "success" message missing.
Symptom	When upgrading the firmware using the web page and the user is passing by a WWAN interface, the upgrade completes and the device is rebooted. The client's web page does not get properly notified and stays with an "upgrading" message.
Workaround	Under investigation.
Issue	(FUS-301) VTEL connectivity issue with latest cell card firmware (V1.2.4)
Symptom	WWAN connection takes 9 minutes before connecting.
Workaround	Under investigation.
Issue	(FUS-303) FusionLTE SIM Status shows junk.
Symptom	Junk is seen in the SIM field.
Workaround	Under investigation.
Issue	(FUS-392) Serial PAD remote access breaks when DMZ is enabled.
Symptom	Serial PAD access through WAN interface does not work if DMZ enabled.
Workaround	Disable DMZ to access serial PAD from a remote location.
Issue	(FUS-393) AAVL Remote Delivery not accessible from WWAN connections.
Symptom	Access to AAVL not accessible through WWAN connection.
Workaround	Under investigation.