ALEOS 4.13.0 Release Notes

ALEOS 4.13.0 is for AirLink MP70, LX60, LX40, and RV55 routers, and RV50/50X gateways.

New Features

Radio Module Firmware

Updated firmware for the following radio modules:

EM7511:
- Generic: 01.08.04.00
- Sprint: 01.08.04.00

EM7565:
- Telstra: 01.11.00.00

MC7304:
- Generic: 05.05.78.00

MC7455:
- Generic: 02.32.11.00
- AT&T: 02.32.11.00

MC7430:
- Generic: 02.33.03.00

WP7601:
- Verizon: 02.18.05.00

WP7603:
- AT&T: 02.28.03.01
- Generic: 02.28.03.01
- Sierra: 02.28.03.03

WP7607:
- Generic: 02.25.02.01
- Sierra: 02.28.03.03

WP7609:
- Generic: 02.25.02.01
- Sierra: 02.28.03.03
- Telstra: 02.28.03.05

WP7610:
- Verizon: 02.28.03.04
- AT&T: 02.28.03.01
- Generic: 02.28.03.01
- Sierra: 02.28.03.03

WP7702:
- Verizon: 02.22.12.00
- Sierra: 02.22.12.00

Cellular

Added Sierra Wireless “Ready to Connect” embedded SIM (eSIM) functionality for AirLink ALEOS devices with WP7607, WP7609 and WP7610 modules. For single SIM devices, the eSIM functions as a second SIM. For dual SIM devices, the eSIM is available as a tertiary SIM. eSIM can be enabled/disabled and configured using ACEmanager.

Added support for Blank APN to allow the AirLink device to connect to certain networks with a blank APN.

Added support for displaying LTE carrier aggregation, if the radio module supports it.

Added a setting to allow or disallow IPv6 ping responses.

Deprecated Backup APN settings.

Added Diagnostic Settings for further band control.

Vehicle Telemetry

Added telemetry support for LX60 telemetry SKU.

	The default value of the GenX Companion Remote Configuration Server IP has been updated to 192.119.178.51.
VPN	
	The “Standard” VPN implementation introduced in ALEOS 4.12.0 is now the default implementation for new devices shipping with ALEOS 4.13.0.
	Revised the Split Tunnel settings in ACEmanager. A new section, Out of Band Policies, allows you to control incoming or outgoing traffic through the public Internet when VPN tunnels are configured.

Security Enhancements

General	
	Prevented reading files via the tcpdump -V command in iplogging.
	Fixed potential buffer overflow issues.
	Reworked parser bounds-checking to mitigate potential data exposure.
	Prevented Reverse SSH from being used to proxy network traffic.
	Updated certificate due to renaming of Comodo CA to Sectigo.
Security and CVE Vulnerabilities	
	Addressed potential vulnerabilities in net-snmp package related to: CVE-2018-18066 and CVE-2018-18065
	Updated ncurses to version 6.1 to address potential vulnerabilities related to: CVE-2018-10754.
	Addressed potential vulnerabilities related to hostapd and wpa_supplicant: • CVE-2019-9498 • CVE-2019-9497 • CVE-2019-9496 • CVE-2019-9499 • CVE-2019-11555 • CVE-2019-9495 • CVE-2019-9494 • CVE-2018-14526 • CVE-2017-13088 • CVE-2017-13087 • CVE-2017-13081 • CVE-2017-13086 • CVE-2017-13084 • CVE-2017-13080 • CVE-2017-13078 • CVE-2017-13079 • CVE-2017-13077
	Updated openLDAP to 2.4.48 to address CVE-2019-13565 and CVE-2019-13057.

Updated openLDAP to 2.4.47 to address:
- CVE-2019-13565
- CVE-2017-17740
- CVE-2017-9287
- CVE-2017-14159
- CVE-2015-6908
- CVE-2015-1545
- CVE-2015-3276

Updated curl to 7.65.3 to address CVE-2019-5443.

Updated expat to 2.2.7 to address CVE-2018-20843 and CVE-2012-6702

Removed libical package, addressing potential vulnerabilities related to:
- CVE-2016-5826
- CVE-2016-5827
- CVE-2016-5823
- CVE-2016-5824
- CVE-2016-5825

Updated bash to version 5.0 to address potential vulnerabilities related to:
- CVE-2016-7543
- CVE-2016-9401
- CVE-2019-9924

Updated libtomcrypt to address potential vulnerabilities related to CVE-2016-6129.

Updated BusyBox to address potential vulnerabilities related to:
- CVE-2018-20679
- CVE-2018-1000500
- CVE-2017-16544
- CVE-2019-5747
- CVE-2017-15873
- CVE-2017-15874

Bug Fixes

WAN/Cellular

Corrected behavior where IP Manager would stop sending periodic updates after some uptime. IP Manager now sends periodic updates correctly.

Resolved an issue where Automatic SIM switching would not reliably switch to the other SIM when device boots without a cellular connection.

The Non-Primary Network Timeout setting (formerly Secondary Network Timeout) under Cellular > General > Automatic SIM Switching now has a range of 0 (disabled) to 255 hours when Active SIM Based Firmware Switching is enabled.

Resolved an issue where values for Automatic SIM Switching could not be returned to default.

Wi-Fi	
	RV55/LX60: Resolved an issue where Apple devices connected but did not pass traffic under the conditions described below: • Access Point Mode: n/ac 5 GHz • Channel Frequency: Any, Width: 20 or 20/40 MHz • Security Authentication: WPA/WPA2 Personal/Enterprise • Encryption: AES
	Resolved an issue where devices, with Bridge Wi-Fi to Ethernet enabled, stopped connecting to Wi-Fi access points after upgrading from 4.9.3 to 4.12.0.
VPN	
	Resolved an issue where sometimes GRE tunnel status displayed as “Connected” when it was not connected.
	Resolved an issue where, when configured with VPN Standard Implementation, FIPS, MOBIKE, Full Tunnel and Host-to-LAN, the IPsec tunnel was maintained on the previous WAN interface after a WAN switch.
	Resolved an issue where traffic originating from the gateway itself destined for remote VPN subnet would go out over the tunnel with the IP address of the gateway as the source address, rather than the LAN IP address.
	Resolved an issue where port forwarding was not applicable to traffic coming from an openVPN tunnel.
	Resolved potential issues with VPN configuration by adding Gateway Virtual IP validation in ACEmanager.
Serial	
	Resolved an issue where FQDN input fields rejected entries longer than 39 characters. FQDN fields now accept up to 255 characters.
	Resolved an issue where the firewall did not always allow USB PPP traffic on boot.
Location	
	RV55 LTE-A Pro devices no longer reject GNSS messages in the NMEA stream that have an extra field value.
	Resolved an issue where location streaming reports were not available on the USB Serial interface.
	RV50X: Resolved a no SNR problem with GNSS radio.
	Resolved an issue where GPS stream stopped and did not resume after an Active SIM switch.
Vehicle Telemetry	
	Resolved an issue where the correct fuel level was not reported at startup.
SMS	
	Added an SMS Message Format setting for selecting 3GPP or CDMA/3GPP2 message formats to suit certain carriers. The default message format from previous versions of ALEOS remains the default.

Dynamic DNS
Removed obsolete providers from the list of dynamic DNS providers.
AT Commands
AT*DATZ can now be used to set or query datz on any serial interface.
LX40: Resolved an issue where ATZ (reboot command) over USB serial did not reset the device.
AT*AAFINSTALL now returns a single OK at the end of execution.
Restored AT commands used for radio bypass mode operation.
Event Reporting
MP70: Resolved an issue where SNMP trap events were not sent for Digital Input 5.
Resolved an issue where SNMP trap events were not sent when I/O pin state changes occurred in intervals smaller than 2 seconds.
Resolved an issue where the reported Bytes Sent value (Status > Cellular > Statistics) could reach maximum and reset to zero.
ALMS
Resolved issues with applying ALEOS 4.12.0 templates in ALMS using LWM2M.
Resolved an issue where device LWM2M connections did not recover from a stalled connection.
Resolved an issue where, after a failed ALEOS firmware upgrade via LWM2M, subsequent update attempts resulted in immediate fail indications.
Resolved an issue where ALMS would reject an FQDN address for GPS Report Server 1 IP in the ALMS template.
ACEmanager
Resolved an issue where AAF applications could not be installed using ACEmanager over HTTPS.
Improved speed of the ACEmanager user interface.
Miscellaneous
Resolved an issue with the ALEOS 4.12.0 firmware installer that prevented devices running ALEOS 4.9.3 from being upgraded while in recovery mode.
RV55: Resolved an issue with LED Power Saving Mode feature.
MP70: Improved reliability of Ethernet switch
Resolved an issue where the GNSS Reboot Watchdog and Enable Wi-Fi RSSI Link Monitoring settings were not correctly saved and restored when using ALEOS templates.

Known Issues

ALMS	
	The default IPsec Implementation is Standard implementation. Applying a template with Legacy implementation (prior to ALEOS 4.12.0) from the management system may result in a non-functional VPN configuration on the gateway or router. For this reason, as for all versions, Sierra Wireless recommends using a template from 4.13.0 on a 4.13.0 device.
Wi-Fi	
	LX60 and RV55: An issue exists with iPhone 6 connecting but not passing traffic when the router is set to: • Access Point Mode: n/ac 5 GHz • Channel Frequency: Any, Width: 20 MHz • Security Authentication: WPA/WPA2 Personal/Enterprise • Encryption: AES
	LX60 and RV55: An issue exists where devices cannot connect when the router is set to: • 802.11w support: Optional • Encryption: TKIP • Security Authentication: WPA2 Personal/Enterprise *Note: TKIP is a deprecated Wi-Fi security protocol and is not supported with 802.11w Protected Management Frames.*