ALEOS 4.14.0 Release Notes

ALEOS 4.14.0 is for AirLink MP70, LX60, LX40, and RV55 routers, and RV50/50X gateways.

Note: Sierra Wireless recognizes that our customers deploy devices in a wide range of network environments with varying configurations. It is always good practice to install a new ALEOS release on a few trial devices to ensure that standard operation is maintained within your environment before deploying the new release across your fleet of AirLink devices.

Note: Devices manufactured on ALEOS 4.14.0 or later or devices that are reset to factory default on ALEOS 4.14.0 or later have the ACEmanager local access restricted to HTTPS only. ACEmanager should then be accessed using the default 9443 port: https://192.168.13.31:9443/

Note: Multiple reboots will occur when upgrading from ALEOS 4.13.0 to 4.14.0. If the upgrade requires a radio module firmware update, the device may be offline for approximately 15 minutes.

Note: A change to DHCP Mode (see LAN on page 7) restricts the "Auto" setting to the device's WAN port only. If a device has a non-WAN Ethernet port configured in "Auto" mode, that port will no longer have WAN functionality after upgrading to ALEOS 4.14.0.

Note: WEP security algorithm is not supported when Wi-Fi AP is configured for 5GHz.

New Features

Radio Module Firmware
Updated firmware for the following radio modules: EM7511: • Bell: 01.07.02.00 • Generic: 01.14.02.00 • AT&T: 01.14.02.00 • Sierra: 01.14.02.00 EM7565: • Generic: 01.14.02.00 • AT&T: 01.14.02.00 • Sierra: 01.14.02.00 MC7455: • Generic: 02.33.03.00 • Verizon: 02.33.03.00 • AT&T: 02.32.11.00 • Sprint: 02.32.11.00 • Sierra: 02.33.03.00 MC7430: • Docomo: 02.33.03.00 • KDDI: 02.33.03.00 • Telstra: 02.33.03.00 WP7601: • Verizon: 02.37.06.00 WP7603: • AT&T: 02.37.00.00 • Generic: 02.37.03.00 WP7607: • Generic: 02.37.03.00 WP7609: • Generic: 02.28.03.05 WP7610: • Verizon: 02.37.06.00 • AT&T: 02.37.00.00 • Generic: 02.37.03.00 WP7702: • Sierra: 02.35.02.00
Added a mechanism to validate radio module firmware ISO files before they can be installed on the device. ALEOS will reject ISO files if they have been partially downloaded or are otherwise corrupt.
Cellular
Added support for EM7511 AT&T radio module firmware version 01.14.02.00 to support AT&T FirstNet Band 14 Carrier Aggregation.
Added support for Bell Jasper SIM.
Added the ability for a Bell SIM to switch to Bell-compatible radio module firmware instead of Generic on EM7511 radios.
Added an option to allow blocking outbound radio traffic for debugging and testing purposes.
Restored Backup APN functionality, and added the ability to configure a timeout before switching to the Backup APN.
eSIM-compatible LX40 or LX60: If no physical SIM is present, the router switches to the eSIM at startup.
eSIM, if available, is enabled by default. Existing configurations are not changed after upgrading to 4.14.0. However, after resetting a device running 4.14.0 to factory default, eSIM will be enabled.
Added eSIM activation status to ACEmanager under Home > General > Network State and Cellular > General > R2C eSIM Activation Status.

	Added a field in ACEmanager displaying the eSIM ICCID to Status > Cellular > Advanced.
	Added a field in ACEmanager displaying the Serving PLMN to Status > Cellular > Advanced. This information can also be queried using the AT command AT*SRVPLMN?
	For WP7702 (CatM/NB1) radio modules, added an option to control the Extended Discontinuous Reception setting in Cellular > Advanced. The setting can also be controlled with an AT command.
	For WP7702 (CatM/NB1) radio modules, added settings to control Cellular IoT Preferences under the Cellular > Advanced tab. These settings can also be controlled with AT commands.
	Added a setting to select Service Domain Preference to the Cellular > Advanced settings.
	Resolved a timing issue in the radio driver that would cause radio to fail the enumeration process at boot.
	Automatic SIM switching no longer requires the cellular watchdog to be disabled.
	When Active SIM Based Firmware Switching is disabled, the Automatic SIM Switching Service Loss Timeout can now be set to 5 minutes.
LAN	
	Added support for DHCP Option 12 Hostname for both DHCP Client and Server, and added DHCP Client Options in ACEmanager.
	Added support for DHCP Option 6 (Domain Name Server) in the DHCP Options list.
Wi-Fi	
	MP70: Added the ability to configure Wi-FI Captive Portal when set in dual mode.
VPN	
	Fixed the Standard VPN implementation to properly connect to Cisco ASAs with multiple remote subnets.
Services	
	Added AMM Management Tunnel Status to Status > Services.
	Added support for multiple NTP servers.
	Added support for the device to act as an NTP server.
AT Commands	
	Revised the ATS23 command to accept data, parity and stop bits with or without comma separation, and to set the baud rate only.
	Added a new AT command, AT*CREATERESETCFG, to trigger a restore point on next boot.
	Added a new AT command for connecting to ALMS. Running AT*AVMS_CONNECT=1 has the same functionality as clicking the “Connect” button in Services > ALMS > AirLink Management Service
	Added AT+COPS=? to provide a list of available operators.

	As part of the new Custom Reset feature, added AT commands to query: • a reset template's presence and name • the versions of AAF apps present on device
	Enhanced the AT command parser so that if a concatenated AT command contains invalid characters or a failed command then the AT command will be aborted.
ACEmanager	
	Devices manufactured on ALEOS 4.14.0 or later or devices that are reset to factory default on ALEOS 4.14.0 or later have the ACEmanager local access forced to HTTPS only. By default, ACEmanager should then be accessed using the default 9443 port: https://192.168.13.31:9443/
	Added a banner linking to information about AirLink Complete device management. You can dismiss the banner at any time.
	Added the ability to preserve ACEmanager Local Access Setting when resetting with "Preserve Core Settings".
	Added the Template status to the Device Status Screen configuration.
	Added the Reset Mode to the confirmation message after clicking Reset to Factory Default.
	Added the ability to perform a Reset to Factory Default to a custom configuration. This feature is also available in ALMS and AMM. The Custom Reset feature in ALEOS 4.14.0 adds: • the ability to create a reset template out of the current device settings, save it on the device and set it as the reset template • a setting to configure the hardware reset button behavior: Reset All (default) and Reset to Custom Configuration • an AT Command, AT*RESETBTNCONFIG, to query and set the Reset Button Configuration • a setting to preserve AAF apps on reset if the Reset to Custom Configuration option is chosen for Reset Configuration or Reset Button Configuration.
	Relocated all reset/reboot-related settings to a new Reset menu on the ACEmanager Admin tab.
	Renamed the Admin > Radio Passthru screen to Admin > Radio Tools and moved Radio Module Debug Information and Radio Module Actions from Admin > Advanced to Radio Tools.
	Added the option to set the Minimum TLS Version to 1.3 on the Admin > Advanced screen.
	Under the WAN/Cellular tab, DMNR Configuration and PNTM Configuration now only appear if the carrier (SIM) is Verizon (these are Verizon specific features). Under the Status tab, PNTM now only appears if the carrier (SIM) is Verizon.
General	
	Added infrastructure to connect to Sierra's server and allow remote debugging.
	Added local and remote troubleshooting support for GNX-6 Companion devices connected to MP70 or LX60WT routers.

Security Enhancements

General
Fixed a potential strcpy buffer overflow.
Added protection against possible buffer overflow.
Added level 2 security to prevent being able to read/write the SMS password through AT commands when not identified as a user.
Applied a patch to pppd to address CVE-2020-8597
Added openSSL 1.1.1d to ALEOS, and updated the following applications to support openSSL 1.1.1d: • openVPN • ipsec-tools • CoovaChili • syslog ng
Security and CVE Vulnerabilities
Addresed potential vulnerabilities related to CVE-2017-6004.
Address potential vulnerabilities related to CVE-2019-20636.
Fixed vulnerability against glibc 2.26 to address the following: • CVE-2017-16997 • CVE-2019-9169 • CVE-2017-15670 • CVE-2017-15804 • CVE-2018-1000001 • CVE-2018-6485
Addressed potential vulnerabilities related to CVE-2014-5461.
Updated net-snmp package to address potential vulnerabilities related to: • CVE-2018-18066 • CVE-2018-18065
Updated PPP to version 2.4.8 to address potential vulnerabilities related to: • CVE-2020-8597 • CVE-2018-11574
Updated Hostapd to address potential vulnerabilities related to: • CVE-2019-11555 • CVE-2019-13377 • CVE-2019-16275
Updated coreutils to version 8.32 to address potential vulnerabilities related to CVE-2015-4042.
Fixed command injection in UpdateRebootMgr to address potential vulnerabilities related to CVE-2020-8781.

To address potential vulnerabilities related to CVE-2020-8782, added a warning banner to ACEmanager when AAF Development Mode is enabled.
Updated dbus to version 1.10.28 to address potential vulnerabilities related to CVE-2019-12749.
Updated curl to address potential vulnerabilities related to: • CVE-2019-5481 • CVE-2019-5482
Applied a patch to Bash to address potential vulnerabilities related to CVE-2019-18276.
Updated tcpdump to version 4.9.3 to address the following: • CVE-2018-10103 • CVE-2018-10105 • CVE-2018-14461 • CVE-2018-14462 • CVE-2018-14463 • CVE-2018-14464 • CVE-2018-14465 • CVE-2018-14466 • CVE-2018-14467 • CVE-2018-14468 • CVE-2018-14469 • CVE-2018-14470 • CVE-2018-14879 • CVE-2018-14880 • CVE-2018-14881 • CVE-2018-14882 • CVE-2018-16227 • CVE-2018-16228 • CVE-2018-16229 • CVE-2018-16230 • CVE-2018-16301 • CVE-2018-16451 • CVE-2019-15166 • CVE-2018-16300 • CVE-2018-16452 • CVE-2017-16808 • CVE-2018-19519 • CVE-2018-16300 • CVE-2019-1010220
Updated libpcap to version 1.9.1 to address the following: • CVE-2019-15161 • CVE-2019-15162 • CVE-2019-15163 • CVE-2019-15164 • CVE-2019-15165

Bug Fixes

WAN/Cellular
Expanded the MSS Clamping settings to allow for automatic clamping.
Changed the default values for the MTU and MSS DMNR tunnel settings to ensure that default settings would allow unfragmented traffic to go through the tunnel.
Removed the ability to configure IP Passthrough on USB by MAC address.
Resolved an issue where local destination reports were not working correctly with IP passthrough. When upgrading to 4.14 with IP passthrough enabled and a local destination report interval set, the local destination report will be set to “IP passthrough” mode.

	LX40/LX60: Resolved an issue where user-entered APN was not restored properly upon reset to core settings.
	Resolved an issue where IMSI was reported only when the radio would connect to a network. IMSI is now also reported when radio is scanning and not connected to any network (R2C behavior).
LAN	
	MP70: Resolved an issue where the Ethernet port speed could not be configured.
	Modified “Auto” DHCP mode to apply exclusively to the device’s WAN port(s).
Wi-Fi	
	Updated default values for the following Wi-Fi settings: • Security Authentication for AP Mode: WPA2 AES • Bandwidth Mode: 5 GHz Frequency, 80 MHz Width.
VPN	
	Resolved an issue where the tunnel source cannot be defined as the WAN IP address.
Serial	
	Resolved an issue where TCP PAD communication could become disabled during an outbound TCP PAD connection attempt. Inbound TCP PAD connection attempts during an outbound TCP PAD connection attempt are now terminated cleanly. As well, an invalid Destination Address of 0.0.0.0 will not result in an outbound TCP PAD connection attempt.
Location	
	Updated SMS GPS and Status commands so that they will provide a correct location for latitudes and longitude values that are between 0 and -1 degrees.
	Resolved an issue where the GPS fix was momentarily lost.
	Added configuration options for Local Report Destination IP to resolve issues when using IP Passthrough mode.
Statistics	
	Resolved an issue with inconsistent reporting of bytes sent on cellular uplink.
ALMS	
	Resolved an issue where bytes sent and received over the WAN could wrap around 32-bit value and show a drop in the counts.
	Resolved an issue where ALEOS did not respond to error codes provided by AVC1.
ACEmanager	
	Resolved an issue where ACEmanager would warn about an incorrect radio module firmware when upgrading RV50 from 4.9.3.002 to 4.13.0.017
AT Commands	
	LISTIP AT command now requires syntax “AT*LISTIP?”

SMS	
	LX40/LX60: Resolved an issue where data usage was not reported correctly via SMS.
	Resolved an issue where ALEOS devices were not able to send SMS messages containing Unicode characters.

Known Issues

Serial	
	When Remote Login Server Mode is set to Telnet, and Telnet/SSH Access Policy is set to Disabled, SSH still accepts connections on the LAN. In order to block both Telnet and SSH connections in this case, go to Services > AT (Telnet/SSH) and change Remote Login Server Mode from Telnet to SSH.
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.
VPN	
	Customers should note that if Gateway Virtual IP Type is set to Automatic, any content in the Gateway Virtual IP field is ignored.
AT Commands	
	Due to changes made to the ATS0 command, this command cannot be used as part of a concatenated AT command string.

For more information contact us:

USAT | Connect What's Critical
605 Eastowne Drive, Chapel Hill, NC 27514

Phone: (888) 550-8728
Email: info@usatcorp.com
Web: https://usatcorp.com