ALEOS 4.16.0

RELEASE NOTES

About ALEOS 4.16.0

This release of ALEOS 4.16.0 is for the AirLink® MP70, RV50, RV50X, RV55, LX40 and LX60. These release notes describe new features and bug fixes that apply to this release.

Important: *ALEOS 4.16.0 is the last release for the AirLink RV50. This product will not be tested or supported after December, 31, 2022.*

Note: ALEOS 4.16.0 supports TLS 1.3, TLS 1.2 (default setting after update and reset to factory default), and removes support for TLS 1.0. and 1.1.

Note: ALEOS 4.16.0 adds the WPA3 Wi-Fi authentication type. Please be aware that downgrading ALEOS from 4.16.0 to 4.15.4 will cause any configured Wi-Fi Client WPA3 settings to revert to the previously supported authentication type, and the Wi-Fi Client will not be able to connect. See also Wi-Fi on page 4.

Note: The WEP Authentication Security Type will be deprecated in ALEOS 4.17.0. ALEOS 4.16.0 provides the option only for backward compatibility with older devices. Using WEP is strongly discouraged as it is not secure.

Note: Please note that ALEOS-powered AirLink routers will be offline during a firmware upgrade. With a combined ALEOS firmware and radio module firmware update, the offline period may be 15 minutes or more.

Important: *The Sierra Wireless IP Manager Dynamic DNS service is intended for limited use in testing or evaluation scenarios. This service is unmonitored and is provided without any service level commitments or uptime expectations. This service may go offline periodically and without notice. This service should not be used in any mission-critical customer application, and Sierra Wireless recommends that customers configure an alternate commercial dynamic DNS service. Note that Sierra Wireless will discontinue our free IP Manager Dynamic DNS Service (hosted at eairlink.com) effective July 1, 2023.*

Sierra Wireless encourages all customers to maintain their AirLink routers with the current ALEOS release and security patches via our AirLink Management Service (ALMS). Sierra Wireless tests and validates upgrades from the previous two major software releases. If you have routers running an ALEOS release older than the previous two major releases it is recommended that you follow the tested and supported upgrade path.

In addition, other than basic questions that can typically be answered in our existing product documentation, Sierra will only provide technical support for the current and the previous two major software releases via our technical support organization. For example, the current version of ALEOS is 4.16 and we continue to support ALEOS 4.15 and ALEOS 4.14.

If you have a support issue with a version prior to ALEOS 4.14, you will be asked to upgrade to a supported version before engaging our technical support organization.

If you need to downgrade a router, you must first perform a factory reset, then install the downgraded version and then perform a second factory reset. We do not provide technical support on routers that have not been factory reset before and after a downgrade has been performed.

Refer to the table below for the supported ALEOS versions and upgrade paths.

ALEOS Release	Support Level	Upgrade Path
ALEOS 4.16	Supported	n/a—This is the currently released version
ALEOS 4.15	Supported	Upgrade to 4.16
ALEOS 4.14	Supported	Upgrade to 4.15 or 4.16
Previous ALEOS Releases	Limited support. Upgrade to a supported release for technical support	Upgrade to supported release

Note that downgrading ALEOS 4.15.2, ALEOS 4.15.3, and ALEOS 4.15.4 on specific routers is prevented because specific newer routers contain hardware components (substitutions) that are not supported on older versions of ALEOS. Refer to the following table for the details.

ALEOS Version	Availability	LX40/60	RV50	RV50X	RV55	MP70	Notes
4.15.0	Dec. 2021	✔	✔	✔	✔	✔	Feature release
4.15.1	Dec. 2021	✔					AT&T 3G sunset check
4.15.2	Jan. 2022		✔	✔	✔		• Radio module bootloader upgrade • Prevents installation lower than this version on newer incompatible hardware
4.15.3	Apr. 2022	✔	✔	✔	✔	✔	• Radio module bootloader upgrade • Prevents installation lower than this version on newer incompatible hardware
4.15.4	July 2022	✔	✔		✔		• Support for additional eSIM suppliers • Prevents installation lower than this version on newer incompatible hardware
4.16.0	Nov. 2022	✔	✔	✔	✔	✔	• Feature release • Critical Maintenance for RV50 ends Dec 31, 2022. This is the final release for the RV50. • Factory release H1 2023 TBC

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. For more information, please see the application note Testing AirLink Devices Before Deployment.

Supported AAF Applications

The following applications have been tested and verified to work with ALEOS 4.16.0:

- AVTA 1.4.1.01
- AMMER 1.0.7
- AVTC 1.0.1.001 (deprecated for GNX-6)
- ACEview 4.0.2.3

New Features

Radio Module Firmware	
	Updated firmware for the following radio modules: EM75xx: • ATT: 01.14.13.00 • Bell: 01.14.13.00 • Generic: 01.14.13.00 • Sierra: 01.14.13.00 • Rogers: 01.14.13.00 • Verizon: 01.14.20.00 WP76xx: • Sierra: 02.37.03.00 • AT&T: 02.37.03.05 • Generic: 02.37.03.05 WP77xx • AT&T: 02.36.06.00 • Generic: 02.36.06.00 • Sierra: 02.36.06.00 *Note: There is a known issue in WP76xx modules with the LWM2M stack for AT&T. The module firmware cannot be certified prior to release. Because of this, LWM2M usage on WP7603 and WP7610 is disabled for AT&T only. This is also in accordance to AT&T requirements.*
	Reduced transmit power on B48 to comply with regulatory certifications.
	Added the ability for a Rogers SIM card to switch to Rogers radio module firmware if available in radio store.
	Removed the automatic exclusion of B29 put in place in earlier versions of ALEOS.
VPN	
	Enhanced GRE Tunnel configuration to include: • Support for configurable GRE tunnel IP as a CIDR • Support for multiple subnets • Configurable routes for the custom tunnel IP address and subnet • Firewall support for custom tunnel IP address and subnet
	Updated MSCI certificate bundle to support Digicert.

ACEmanager	
	Added a “Reset Radio” button under Admin > Radio Tools to force reboot of the radio module.
	Added the capability to upload or delete a QXDM filter on the Admin > Radio Tools page.
	Added a “Force Reboot” button under Admin > Reset.
	Added Power Input Voltage, Board Temperature, and Radio Module Internal Temperature as options to display as Device Status items on the ACEmanager login screen.
	Added a “Reboot after template upload” option to the Template Upload/Download screen.
	A user password in ACEmanager or an AT command now requires at least one lower case letter, one upper case letter and one number.
SMS	
	Added the ability to provide multiple phone numbers to an Event Reporting Action.
	Added the following settings to the Preserve Core Settings (Reset to Factory Default mode) list: • SMS Mode • SMS Prefix • SMS Password • Enabled Trusted Phone • Trusted Phone List The SMS Password is now reset after resetting the router to factory defaults in “Reset All” mode.
	Added an SMS command to change the Reset to Factory Default “Reset Mode” of the router.
	Added an SMS command to perform a Reset to Factory Default.
Wi-Fi	
	MP70: • Moved the 802.11w support setting to the General tab under Wi-Fi for an AP. • The Transition Mode is no longer a configurable setting for an AP, and depends on the 802.11w support value directly. • Added two status fields to show Transition Mode and WPA3 Configuration State values for an AP, updated on the next boot.
	Added support for WPA3 Personal/Enterprise (allowed on SSID 1 for the MP70 only).
	Support for WPA3 Personal/Enterprise added for RV55/LX: • WPA3 Personal only • WPA3 Personal Transition Mode • WPA3 Enterprise only • WPA3 Enterprise Transition Mode
	When enabling Wi-Fi, the default configuration will be WPA3.
	Imposed a restriction on the AT command to modify the Security Authentication Type so that IEEE802.11w support cannot be disabled with a WPA3 SSID / Remote AP.
	Added MSS Clamping configuration to the Wi-Fi interface(s).
	Added a “Download Wi-Fi Client Logs” feature, to download a list of up to 128 connected clients from ACEmanager.

	Add user-configurable sorting for Connected Clients information.
	Added tables for displaying connected Wi-Fi clients and rejected Wi-Fi clients in ACEmanager. *Note: RV55, LX40, LX60 do not display Data Sent and Data Received in the Wi-Fi connected client table.*
	Added a table to show available access points in range when the router Wi-Fi is in Client mode.
	Added Access Point Status to Wi-Fi > General. Statuses are Active and Inactive (Misconfigured).
Networking	
	Added Hairpin NAT feature for Ethernet, Wi-Fi and USB, accessible on the Security > Port Forwarding page.
	Added improvements to WAN Monitors, including the ability to restart a WAN Link that has a monitor failure before triggering a Network Watchdog reboot.
	Added “Blocked IPs - Inbound” and “Blocked IPs - Outbound” security options.
	Increased the number of Alternate DNS entries under LAN > Global DNS.
Cellular	
	Improved the logic to set the MTU on cellular link. If the MTU is not returned by the SDK or the MTU is too large, then clients on AT&T will get an MTU of 1430 and clients on FirstNet will get an MTU of 1342.
Ethernet	
	Added MSS Clamping configuration to the Ethernet interface(s).
AAF	
	Exposed the MSCIIDs for Override APN, Network User ID and Network Password for both SIM1 and SIM2 in AAF.

Security Enhancements

General	
	Updated expat to version 2.4.7.
	• Removed ncurses from ALEOS. • Updated procps to procps-ng version 3.3.17.
	• Updated openssl 1.0 to version 1.0.2u. • Updated openssl 1.1 to version 1.1.1m.
	Updated openssl-1.1.1o to 1.1.1q.
	Updated hostapd and wpa_supplicant to version 2.10.
	Updated zlib to version 1.2.11.

Removed https support to weak ciphersuites.
SSH server: Updated dropbear to version 2020.81 and disabled weak ciphers.
Updated strace to version 5.13.
Updated openNDS to version 9.1.1.
Security and CVE Vulnerabilities
Addressed potential vulnerabilities related to CVE-2021-33643, CVE-2021-33644, CVE-2021-33645.
Addressed potential vulnerabilities related to CVE-2022-1012.
Addressed potential vulnerabilities related to CVE-2021-20322.
Addressed potential vulnerabilities related to CVE-2018-25032, CVE-2016-9841, CVE-2016-9843, and CVE-2016-9840.
Updated openvpn to version 2.5.5 to address potential vulnerabilities related to CVE-2022-0547.
Addressed potential vulnerabilities related to CVE-2022-23219.
Addressed potential vulnerabilities related to CVE-2021-45079.
Addressed potential vulnerabilities related to CVE-2022-23218.
Addressed potential vulnerabilities related to CVE-2021-40490.
Addressed potential vulnerabilities related to CVE-2020-8648.
Updated GMP to address potential vulnerabilities related to CVE-2021-43618.
Updated ncurses to version 6.3 to address potential vulnerabilities related to: CVE-2021-39537, CVE-2018-19211, CVE-2018-19217, CVE-2019-17594, and CVE-2019-17595.
Updated StrongSwan to version 5.9.4 to address potential vulnerabilities related to CVE-2021-41990 and CVE-2021-41991.
Updated OpenLDAP to address potential vulnerabilities related to CVE-2022-29155.
Updated OpenLDAP to version 2.5.7 to address potential vulnerabilities related to CVE-2021-27212.
Updated BusyBox to address potential vulnerabilities related to CVE-2022-28391.
Updated BusyBox to version 1.33.1 to address potential vulnerabilities related to CVE-2021-28831.
Updated BusyBox to version 1.35.0 to address potential vulnerabilities related to: • CVE-2021-42374 • CVE-2021-42386 • CVE-2021-42385 • CVE-2021-42384 • CVE-2021-42382 • CVE-2021-42381 • CVE-2021-42380 • CVE-2021-42379 • CVE-2021-42378 • CVE-2021-42376
Addressed potential vulnerabilities related to CVE-2021-38604.

Updated curl to 7.84.0 to address potential vulnerabilities related to:

- CVE-2022-22576
- CVE-2022-27782
- CVE-2022-27781
- CVE-2022-27775
- CVE-2022-27780
- CVE-2022-30115
- CVE-2022-27779
- CVE-2022-27776
- CVE-2022-27774
- CVE-2022-32207

Updated curl to 7.80.0 to address potential vulnerabilities related to:

- CVE-2022-22623
- CVE-2021-22946
- CVE-2022-27778
- CVE-2021-22897
- CVE-2021-22923
- CVE-2021-22925
- CVE-2021-22947
- CVE-2021-22898

Updated curl to 7.78.0 to address CVE-2021-22898.

Addressed potential vulnerabilities related to CVE-2021-35942.

Updated openVPN to address CVE-2020-15078.

Addressed potential vulnerabilities related to CVE-2021-33574.

Addressed potential vulnerabilities related to CVE-2021-0129, CVE-2021-3588, CVE-2022-0204, and CVE-2021-3658.

Bug Fixes

Radio Module	
	Added a recovery mechanism to try to resolve an issue where the radio is in “Boot and Hold” mode.
Networking	
	LX40: Resolved an issue where firewall failures occurred when IPP was enabled.
	Resolved an issue where VRRP did not work after the router was reset to factory defaults.
Cellular	
	Resolved an issue where the ping monitor did not restart after a radio disconnect.
Wi-Fi	
	Resolved an issue where the router could not connect to the APN using PAP/CHAP authentication.
	Resolved an issue where non-bridged Wi-Fi connected hosts could not pass traffic when a full VPN tunnel was enabled.
	MP70: Addressed an issue where Wi-Fi access points may not be started if Wi-Fi client does not connect right away at boot with Wi-Fi mode configured to “Both”.
Location	
	Resolved an issue where Device ID was not reported correctly in user-defined NMEA sentences.
VPN	
	Resolved an issue where the VPN status appeared as “Up” when the WAN was disconnected.
	Resolved a potential issue with OpenVPN certificates being rejected by changing the default value for certificate validation to “Key Usage/Extended Key Usage”.
SMS	
	Fixed an issue where the AT+CGSMS setting in ACEmanager did not properly set and read the values saved on the radio.
AT Commands	
	Resolved an issue with the ATF command.
	Resolved an issue with the command at*aafinstall.
	Resolved an issue with validating the SET function of AT*IPPINGADDR.
	Removed the AT*DELFW command.
SSH	
	Fixed “Make SSH Keys” button and updated text displayed when the button is pressed.

Template	
	Resolved an issue where ALEOS was unable to generate SSH keys. *Note: ALEOS no longer generates DSS keys as part of SSH keys. After updating to ALEOS 4.16.0, previous keys will be removed and must be regenerated.*
ALMS	
	Resolved an issue where M3DA connections were refused, resulting in an inability to install AAF applications.
USB	
	Resolved issues with showing and hiding settings depending on the USB Device Mode on the LAN > USB page.
SNMP	
	Fixed write access from SNMP for GPIO configuration, adding an enhancement that modifying GPIO configuration requires authentication.
IP Logging	
	Fixed an issue with filter strings where options “z” and “r” were stripped from commands. Commands containing these options now return an error.
ACEmanager	
	Implemented a validation function to ensure the device status screen does not contain unwanted information.

Known Issues

ALMS	
	The Status > LAN IP/MAC table cannot be viewed in ALMS.