ALEOS 4.15.0

RELEASE NOTES

About ALEOS 4.15.0

This release of ALEOS 4.15.0 is for the AirLink LX60, LX40, RV50, RV50X, RV55 and MP70. These release notes describe new features and bug fixes that apply to this release.

Note: ALEOS 4.15.0 supports TLS 1.3 and default downgrade support to 1.2, but allows 1.0 and 1.1. Starting with release 4.16.x, ALEOS will no longer support TLS 1.0. and 1.1.

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 4.15 and we continue to support ALEOS 4.14 and ALEOS 4.13. If you have a support issue with a version prior to ALEOS 4.13, you will be asked to upgrade to a supported version before engaging our technical support organization. Our testing of downgrades involves first performing a factory reset, then installing the downgraded version. We do not provide technical support on routers that have not been factory reset before a downgrade was performed. See the table below.

ALEOS Release	Support Level	Upgrade Path
ALEOS 4.15	Supported	n/a
ALEOS 4.14	Supported	Upgrade to 4.15
ALEOS 4.13	Supported	Upgrade to 4.14 or 4.15
Previous ALEOS Releases	Limited support. Upgrade to supported release for technical support	Upgrade to supported release

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 with the planned operation workflow 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.

New Features

Radio Modules	
	Updated firmware for the following radio module: MC7430: • Generic: 02.36.00.00 • Docomo: 02.36.00.00 • KDDI: 02.36.00.00
ALEOS	
	MP70 and RV55: Added a check that devices are set to data-only mode to ensure they are not affected by AT&T 3G sunset.
Cellular	
	Added support for displaying “Suspended” and “Terminated” eSIM states.
	Disabled eDRX for all WP76xx radios.
	Added a retry mechanism to IP manager so that hostname lookup will be retried if the initial lookup fails.
WAN	
	Added DHCP relay support for all WAN interfaces.
Wi-Fi	
	Added a Simple Captive Portal feature for all Wi-Fi enabled ALEOS devices, with customizable user session length and disclaimer text.
	Added an Advertise WAN Access option to the Wi-Fi configuration for the chosen SSID where the clients can communicate with one another but will not have default access to WAN.
	Added AT commands for configuring all Wi-Fi settings.
	Added UI and AT commands for configuring Wi-Fi Client static IPs.
	Added support for WAN static IP configuration for remote APs.
	Added tooltip and implemented querying for all SSIDs and Wi-Fi cards for AP Isolation AT command.
ACEmanager	
	Added the ability to customize a legal banner that will be visible from the login screen.
	Reworked configuration of Exclude/Restrict bands to clarify the template generation in ALMS under Admin > Band Diagnostic Settings,
	Added VPN status to the Device Status items that can be shown on the Login screen.
Logging	
	Added “Unique ID” field to remote logging.
	IP Logging now resumes session after switching tabs in ACEmanager.

Radio Module Firmware Update
Added options for managing Radio Module Firmware Updates and firmware images.
Added the ability for ALMS to add and remove radio module firmware.
Added the ability to display a list of available network operator firmware under Admin > Radio Module Firmware > Radio Module Firmware Management from ACEmanager and ALMS.
Provided ALMS the ability to display a list of currently installed radio module firmware under Admin > Radio Module Firmware > Radio Module Firmware Management.
Services
Added a WAN option to Telnet/SSH Access Policy under Services > Telnet/SSH.
Added support for additional SNMP actions, including: • List of AP Wi-Fi SSID(s) • List of MAC addresses per AP Wi-Fi SSID(s) • Device Uptime
Smart GPS Bias Control
Disabled Dynamic Power Optimization for GNSS on MC73xx radio.
The gateway powers off the GPS antenna when GPS is disabled.
Added the ability to intelligently control the GPS antenna bias to avoid issues with some multi-element antenna systems. This feature is enabled by default on upgrading to ALEOS 4.15.0.

Security Enhancements

General
Enhanced ALEOS password storage to higher encryption algorithm.
Added stack canaries (also known as stack protection, StackGuard, and /gs) to various ALEOS binaries.
Added PIE to various ALEOS binaries.
Rate-limited connection rate for SSH and Telnet.
Rate-limited TLS renegotiation requests to prevent potential DoS attack.
Security and CVE Vulnerabilities
Addressed potential vulnerabilities related to CVE-2020-8037.
Addressed potential vulnerabilities related to CVE-2021-27803.
Addressed potential vulnerabilities related to CVE-2019-20838.
Addressed potential vulnerabilities related to CVE-2020-36254.
Addressed potential vulnerabilities related to CVE-2018-1000500.
Addressed potential vulnerabilities related to CVE-2021-27218.

Addressed potential vulnerabilities related to CVE-2020-35457.
Addressed potential vulnerabilities related to CVE-2020-6096.
Addressed potential vulnerabilities related to CVE-2020-1751.
Addressed potential vulnerabilities related to CVE-2020-1752.
Addressed potential vulnerabilities related to CVE-2021-3326.
Addressed potential vulnerabilities related to CVE-2019-16746.
Addressed potential vulnerabilities related to CVE-2019-14895.
Addressed potential vulnerabilities related to CVE-2019-17133.
Addressed potential vulnerabilities related to CVE-2019-18805.
Addressed potential vulnerabilities related to CVE-2015-4047 and CVE-2016-10396.
Addressed potential vulnerabilities related to CVE-2020-8177, CVE-2020-8169 and CVE-2020-8284.
Addressed potential vulnerabilities related to CVE-2019-17362.
Addressed potential vulnerabilities related to CVE-2020-27743 and CVE-2020-13881.
Addressed potential vulnerabilities related to: • CVE-2020-25682 • CVE-2020-25683 • CVE-2020-25687 • CVE-2020-25681 • CVE-2020-25685 • CVE-2020-25684 • CVE-2020-25686 • CVE-2019-14834
Addressed potential vulnerabilities in openLDAP related to; • CVE-2020-36222 • CVE-2020-36225 • CVE-2020-36228 • CVE-2020-36226 • CVE-2020-36223 • CVE-2020-36221 • CVE-2020-36229 • CVE-2020-36230 • CVE-2020-36224 • CVE-2020-12243 • CVE-2020-25692 • CVE-2020-36227 • CVE-2021-27212 • CVE-2020-25709 • CVE-2020-25710
Addressed potential vulnerabilities related to CVE-2018-20843.
Addressed potential vulnerabilities related to CVE-2020-1967.
Addressed potential vulnerabilities related to CVE-2020-27780.
Addressed CVE-2019-20838 by updating PCRE.
Addressed potential vulnerabilities related to CVE-2018-19115.

Addressed potential vulnerabilities in glib related to CVE-2019-12450 and CVE-2019-13012.
Updated blueZ to address potential vulnerabilities related to CVE-2020-27153 and CVE-2017-1000250.
Updated pam_tacplus to address CVE-2020-27743.
Addressed CVE-2021-36727, CVE-2021-36728[a], CVE-2021-36729, CVE-2021-36730[a], CVE-2021-36731, CVE-2021-36732[a]

a. Fixed in previous release, and listed here to match security bulletin.

Bug Fixes

Networking and Connectivity
Resolved an issue with device connectivity by allowing ALEOS to boot with default values when critical Ethernet MSCIIDs are set to NOTSET.
Fixed an issue where sometimes at startup, the DNS override fails.
Wi-Fi
Resolved a timing issue related to the 4-way WPA2 handshake.
RV55: Resolved an issue where all Wi-Fi B Client settings did not appear.
Resolved an issue where a device in Wi-Fi Client mode for WPA2 Enterprise in EAP-TLS authentication type did not show a CA certificate option.
LAN
Resolved an issue where USBnet DHCP Mode was always shown as Server.
MP70: Resolved an issue where Ethernet LAN status did not report the correct state of disabled Ethernet ports.
Resolved an issue where DHCP Option 66 was not working.
VPN
Resolved an issue where no VPN connection could be established from the peer if the Out of Band policy for Incoming Traffic was set to Allow.
Changed the default value for UDP Encapsulation from disabled to enabled.
Resolved an issue where exempted VPN subnets were not accessible when VPN tunnel was down.
Resolved an issue where exempted traffic could go out the wrong WAN interface.
Events Reporting
Resolved an issue where Turn Off Services was not working for high data limits.
ACEmanager/ALEOS
ALEOS will now allow access to ACEmanager for log extraction in case of radio failure. The AirLink router reboots for extended radio recovery attempts will now rely on the less aggressive Network Watchdog.

Resolved an issue where access to ACEmanager could fail after loading a template from AMM containing an apostrophe in the name.
LX60: Removed settings for Dead Reckoning and Driver Behavior. LX60 hardware does not support these features.
LX40/LX60: Resolved an issue where upgrading from ALEOS 4.12 or prior to 4.14 could cause APN settings to be lost.
AT Commands
Updated AT*NETSTATE and AT*NETSTATE_RAW to support eSIM specific network states.
Resolved an issue where the ATS0 command could not be used as part of a concatenated AT command string.
Applications
Resolved an issue where AAF applications requiring HTTPS failed to start after OpenSSL was upgraded.
Location
Resolved an issue where the EM75xx radio would reset in some scenarios when a Private APN was in use where DNS server addresses were not provided.

Known Issues

Networking and Connectivity
RV series: To achieve optimal uplink performance with a Windows PC directly connected via Ethernet to an AirLink RV series router, the Windows PC needs an up-to-date Ethernet driver. See the RV55 Hardware User Guide for details on the required Ethernet driver version.
LAN
VLAN does not function with VRRP or VPN. Do not configure VLAN with VRRP or VPN.