SIERRA WIRELESS IS NOW SEMTECH®

ALEOS 4.18.0

RELEASE NOTES

About ALEOS 4.18.0

This release of ALEOS 4.18.0 is for the AirLink® MP70, RV50X, RV55, LX40 and LX60. These release notes describe known issues, new features, security enhancements and bug fixes that apply to this release.

Customer Recommendations for ALEOS 4.18.0

- For customers using SNMP, Semtech recommends using the alternative OIDs, as the deprecated OIDs could be removed on the next update of the MIB (Management Information Base) file for remote SNMP clients. The MIB file is available on the Semtech Source.
- For customers using OpenVPN, Semtech may deprecate OpenVPN support for the 64-bit Blowfish encryption algorithm in a future ALEOS release, or if security updates are required on the OpenVPN package. Semtech recommends that you migrate any existing Legacy VPN implementations (including OpenVPN) to the Standard implementation for increased features and support.
- To enhance router security, ALEOS 4.18.0 introduces changes relating to the user password. Although most customers will not be affected by the changes, Semtech recommends you consult the application note ALEOS 4.18.0 Password Changes for a full description of password configuration and behavior in ALEOS 4.18.0.
- If you are using ALMS and have not enabled the LWM2M protocol on your routers yet, it is time to switch your routers to LWM2M before upgrading to ALEOS 4.18.0. For more information about the differences between LWM2M and MSCI, please refer to the application note ALEOS 4.18.0 Password Changes.
- AAF Developer Studio is not supported from ALEOS 4.16 or later ALEOS versions. For information on continuing to use AAF Developer Studio, contact sierrawireless.com/support.

Known Issues

ACEmanager	
	When entering the password to re-authenticate before a downgrade can begin, an issue exists in Firefox where a typed character may be missed, resulting in a "Failed to confirm password" error. In this case, you can click the "show text" icon () to confirm that the password is complete before clicking "Confirm Password". This issue has not been observed when using the Google Chrome™ or Microsoft® Edge browsers.
ALMS	
	An issue exists where, for routers using MSCI and running ALEOS 4.18.0, templates generated in ALMS containing the admin password cannot be applied. When generating a template in ALMS, ensure that templates do not contain the password.

New Features

Radio Modules	
	Updated EM7511 Verizon radio firmware to SWI9X50C_01.14.24.00 002.064_000.
Networking	
	Enhanced LAN IP/MAC Table page (Status > LAN IP/MAC Table) in ACEmanager to provide the Host Interface Watchdog statuses.
	Populated the IP LAN/MAC Table with the hostname of a connected device, when available.
	Added support for wired 802.1X authentication. Only devices with correct authentication credentials will connect to the Ethernet LAN when 802.1X wired authentication is enabled.
Wi-Fi	
	Added a new setting, "Enable Hidden SSID Reconnect Support", to give the router the ability to recover a Wi-Fi connection to a hidden SSID.
VPN	
	Improved throughput for non-FIPS IPsec tunnels.
Location	
	Added an option to show altitude within ACEmanager and at*gnssstatus? and Event Reports.
	Added AT*DISPALT to enable/disable the ability to show the altitude in GPS and SMS commands.
Telemetry	
	Added support for J1979 Standardized odometer. If you do not want to use this PID (0xA6), you can disable it under Services > Vehicle Telemetry > Use Standardized Odometer.
Software Update	
	Added additional checks to radio module firmware upgrade that verify the checksum of a new radio image.
Cellular	
	Moved IMSI to Status > Cellular > General.

	Added a UI item to configure the COPS timeout.
SMS	
	Added the SMS Message Format setting when SMS Mode is Outbound Only.
Radio Tools	
	Modified the QXDM capture menu so that a provided sqf filter does not go through validation.
	Added a “Max Attempts to Read SIM” setting to retry talking to the SIM in QC and the cellular radio based on a counter that can be configured in ACEmanager.
ALEOS	
	Added the ability to display signal-strength bars on Status > Cellular and the Device Status (Log in) Screen.
	Added description to the MIB so the OID can be understood without referring to the user documentation. By adding these descriptions, it was identified that lot of OIDs were obsolete and lot of elements were accessed using OID that do not reflect the layout of the UI. These have been marked as “deprecated or obsolete” in the documentation.
	ACEview Service no longer shares a password with ACEmanager by default. In ALEOS 4.18.0, ACEview Service can be enabled under Admin > Advanced.
	Added a prompt in ACEmanager asking to enter the ACEmanager password before proceeding with a software downgrade. See also Known Issues on page 2.
	Added the ability to disable the default user account.
	Added a UI element that indicates if the device is capable of using LWM2M.
	Added the ability in the ACEmanager UI to delete all user data, including ALEOS logs.
Services	
	Changed the behavior of Telnet/SSH Access Policy to be Disabled by default after a reset to factory default.
	Added an AT command to set the Telnet/SSH Access Policy.
Applications	
	Added five Custom AAF Parameters intended to be read/write from an AAF application. These items are not used by ALEOS.
Security	
	Removed accessibility to the plain-text admin password in AT commands, ACEmanager, ALMS and AMM.
	Added additional self-protection fragments to the kernel configuration and security compilation flags to binaries.
Logging	
	Added interface index information to IP Logging output files.
	Added the ability to start packet capture at boot.

Security Enhancements

Security and CVE Vulnerabilities
Addressed potential vulnerabilities related to CVE-2024-47745.
Addressed potential vulnerabilities related to CVE-2024-47685.
Addressed potential vulnerabilities related to CVE-2016-6129.
Addressed potential vulnerabilities related to CVE-2022-0934 CVE-2023-28450 CVE-2023-50387 CVE-2021-3448
Addressed potential vulnerabilities related to CVE-2020-15862 CVE-2019-20892 CVE-2022-44792 CVE-2022-44793 CVE-2015-8100
Addressed potential vulnerabilities related to CVE-2023-52425 CVE-2023-52426 CVE-2022-43680 CVE-2024-45490 CVE-2024-45491
Addressed potential vulnerabilities related to CVE-2024-42154.
Addressed potential vulnerabilities related to CVE-2024-1086.
Addressed potential vulnerabilities related to CVE-2023-48795.
Addressed potential vulnerabilities related to CVE-2023-38403.
Addressed potential vulnerabilities related to CVE-2023-38039 CVE-2023-46218 CVE-2023-46219 CVE-2024-0853

Bug Fixes

Cellular
Resolved an issue where an APN lookup failure resulted in a blank APN entered in the radio. The behavior of the radio with a blank APN is carrier dependent and may result in the router being unable to pass traffic.
Resolved connectivity issues with the EM7511 radio module firmware for Bell by forcing CEMODE to 2 using the SDK API.
Resolved an issue with global connectivity on Sierra ready-to-connect plastic SIM cards by updating the default APN.
Resolved an issue where the Network State on the Status > Home page reported an incorrect status after a failed ping test and network recovery.

	Resolved an issue where an 18-digit ICCID caused connectivity problems.
	Resolved an issue where some Bell SIM IMSIs were not parsed properly and the APN was not auto entered.
	Resolved an issue with Automatic SIM Switching. The Service Loss Timeout will now start for SIM switching on the Non-Primary Network when Radio Module Firmware Switching is enabled.
Wi-Fi	
	Resolved an issue with reduced Wi-Fi throughput when using small TCP window sizes.
	Resolved an issue where Wi-Fi clients were having issues reconnecting to access points with a hidden SSID.
	Resolved connectivity issues when using the Wi-Fi B Client with a static IP assignment.
Networking	
	Due to reconnection issues, linking USB to the WAN is no longer supported. If a router is using USB link to WAN, it will be disabled when upgrading to 4.18.0.
	Resolved an issue where the DMNR "N-MHAE-KEY" field was missing in the ACEmanager UI.
	Resolved an issue where Hairpin NAT was blocking outbound traffic on port-forwarded ports.
VPN	
	Resolved an issue where sending location reports through a Host-to-LAN VPN stopped working after upgrade to ALEOS 4.17.1.
Location	
	Resolved an issue where latitude and longitude values between 0 and -1 degrees resulted in negative values being turned into positive values.
Events Reporting	
	Resolved an issue where the year was reported incorrectly in an Event Report that used the "Type, Length, Value" Action Type.
Logging	
	Resolved an issue where an incorrect log message was displayed when the OpenVPN tunnel was down.
	Resolved an issue where an error message was printed on the serial console when adding a RMFW image to the radio store using at command, even though the operation was successful.
SMS	
	Resolved an issue where SMS commands containing trailing white-spaces were not sent when the SMS Mode was set to "Control and Gateway" or "Gateway Only".
	Resolved an issue where the SMS command "&&&status" received no reply when no GPS was available on device.
ALEOS	
	Resolved an issue where the ACEmanager "Locations" tab could be seen for non-GNSS devices.
	Resolved an issue where access to ACEmanager would be delayed while it fetched some icons remotely (via Cloudflare).
	Fixed an issue where a failure in the ping monitor would sometimes not set the link of the interface to the correct state.

Applications	
	Resolved an issue where AVTA (AirLink Vehicle Telemetry Application) would not work on non-Wi-Fi AirLink routers.
ALMS	
	Resolved an issue where the router was not able to communicate with ALMS using MSCI with a IPv6 address assigned along with “Verify Peer Certificate” enabled.
	Resolved an issue where LWM2M sync failed when IP Address Preference was set to IPv4 and IPv6 Gateway.
	Resolved issues with some static WAN IP devices communicating with ALMS via LWM2M.

Upgrade Notes

Warning: ***Upgrading from ALEOS 4.15.x and earlier releases to 4.18.0 is not directly supported.*** *All ALEOS-powered routers must be upgraded to ALEOS 4.16.0 before upgrading to a release later than 4.16.0. ALEOS 4.16.0 includes enhancements that must be applied before upgrading to a later release.*

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 several minutes or more.

Semtech encourages all customers to maintain their AirLink routers with the current ALEOS release and security patches via our AirLink Management Service (ALMS/AMM). Semtech 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 4.18.0 and we continue to support ALEOS 4.17.x and ALEOS 4.16.

If you have a support issue with a version prior to ALEOS 4.16, 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 4.18.0	Supported	n/a—This is the currently released version
ALEOS 4.17.x	Supported	Upgrade to 4.18.0
ALEOS 4.16	Supported	Upgrade to 4.18.0
Previous ALEOS Releases	Limited support. Upgrade to a supported release for technical support	Upgrade to supported release

Note that downgrading to older ALEOS versions from 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.

Note: Semtech recognizes that our customers deploy routers 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 routers to ensure that standard operation is maintained within your environment before deploying the new release across your fleet of AirLink routers. For more information, please see the application note Testing AirLink Devices Before Deployment.