ALEOS 4.17.0

RELEASE NOTES

About ALEOS 4.17.0

This release of ALEOS 4.17.0 is for the AirLink® MP70, RV50X, RV55, LX40 and LX60. These release notes describe new features and bug fixes that apply to this release.

This release includes security updates to address vulnerabilities not currently under active exploitation.

Warning: ***Upgrading from ALEOS 4.15.x and earlier releases to 4.17.0 is not directly supported.*** *All ALEOS-powered routers must be upgraded to ALEOS 4.16.x before upgrading to 4.17.0 or later. ALEOS 4.16.x includes enhancements that must be applied before upgrading to a later release.*

Warning: *You cannot update your router to 4.17.0 using the AT command AT*FWRMUPDATE.*

Note:

- *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.*
- *AVMS/AMM package generation has been discontinued for the AirLink RV50.*
- *The WEP Authentication Security Type is removed 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.*
- *Sierra Wireless plans to deprecate OpenVPN support for the 64-bit Blowfish encryption algorithm in ALEOS 4.18.0.*

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.

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 has discontinued our free IP Manager Dynamic DNS Service (hosted at eairlink.com) effective July 1, 2023. For more information, read this bulletin or contact Sierra Wireless support.*

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 4.17 and we continue to support ALEOS 4.16 and ALEOS 4.15.

If you have a support issue with a version prior to ALEOS 4.15, 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 4.17	Supported	n/a—This is the currently released version
ALEOS 4.16	Supported	Upgrade to 4.17
ALEOS 4.15	Supported	Upgrade to 4.16[a]
Previous ALEOS Releases	Limited support. Upgrade to a supported release for technical support	Upgrade to supported release

a. **Upgrading from 4.15 to 4.17 is not directly supported.** Please see the Warning on page 1.

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

ALEOS Version	Availability	LX40/60	RV50	RV50X	RV55	MP70	Notes
4.15.4	July 2022	?	?		?		• Support for additional eSIM suppliers • Prevents installation lower than this version on newer incompatible hardware • Factory installed only
4.16.0	Nov. 2022	?	?	?	?	?	• Feature release • Critical Maintenance for RV50 ends Dec 31, 2022. This is the final release for the RV50.
4.16.1	Apr. 2023				?	?	• AirLink Router Connection Issue update requiring an additional factory reset • For routers affected by the Connection Issue, upgrade to ALEOS 4.16.2 below • Security update
4.16.2	May 2023				?	?	• AirLink Router Connection Issue update • Security Update
4.17.0	Sept. 2023	?		?	?	?	• Security update • Feature release

Note: Sierra Wireless 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.

Supported AAF Applications

The following applications have been tested and verified to work with ALEOS 4.17.0:

- AVTA 1.4.1.01
- AMMER 1.0.7
- AVTC 1.0.1.001
- ACEview 4.0.2.3

New Features

Radio Module Firmware

Updated firmware for the following radio modules:

EM7565:

- ATT: 01.14.22.00
- Generic: 01.14.22.00

MC7430:

- DOCOMO: 02.38.00.00
- Generic: 02.38.00.00

WP7607:

- Generic: 02.37.06.05
- Sierra: 02.37.06.05

WP7702

- AT&T: 02.36.06.00
- Generic: 02.36.08.09
- Sierra: 02.36.08.09
- Verizon: 02.22.12.00

Wi-Fi

Added new requirement for all Wi-Fi related AT commands to turn off Wi-Fi before setting any new Wi-Fi configurations through AT commands. See also AT Commands on page 4.

Removed support for WEP in both Wi-Fi Access Point and Client modes. If the router has WEP configured before the upgrade to 4.17, during the migration process, the Wi-Fi will be disabled on the router.

Cellular

Changes made to Reliable Static Route (RSR) where now, the only Ethernet interface that can be used is the one corresponding to the WAN configurable port (Port 4 on MP70, port 2 on LX60).

Customers with RSR setups from previous releases may have to check their setup before updating.

Networking

Added improvements to the LAN watchdog so it behaves the same as all WAN watchdogs with the same configuration settings.

AMM/ALMS

Added support for custom certificates for the AMM management tunnel.

Improved the ALMS display of “Cellular End-to-End Connection” status to display as text (matching ACEmanager) instead of numbers.

AT Commands

The following AT commands are now password protected and must be unlocked using AT*ENTERCND=<User Password>:

- AT*FWRMUPDATE
- AT*FWUPDATE
- AT*FWSTORE
- AT*TPLUPDATE
- AT*OPENVPN_CLIENT_CERT
- AT*OPENVPN_CLIENT_KEY
- AT*OPENVPN_CA_CERT

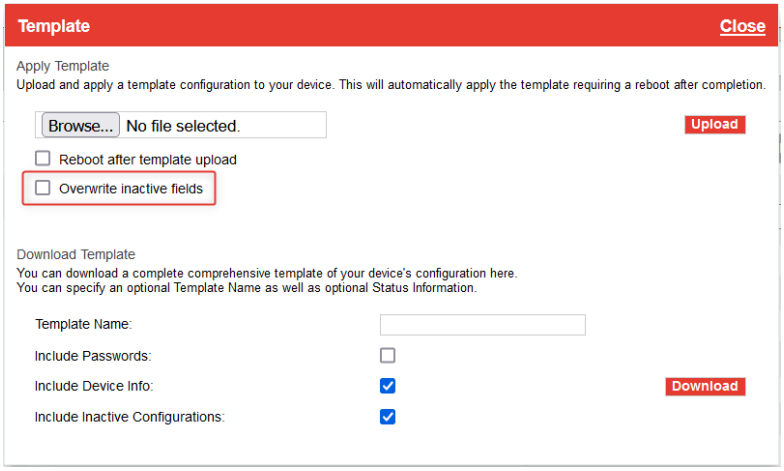
	Added new AT commands WIFI_PASSPHRASE and WIFIAP_PASSPHRASE to set the passphrase for Client and AP.
	Added a new AT command (AT*WIFI_STARTSTOP) that allows you to start/stop the Wi-Fi. This command is required if you make any Wi-Fi configuration changes.
	Updated WIFI_STARTSTOP command to block user from starting Wi-Fi when Wi-Fi Mode is set to disabled.
	Added the following AT commands for OpenVPN configuration: • AT*OPENVPN_USER • AT*OPENVPN_PASS • AT*OPENVPN_CA_CERT • AT*OPENVPN_CLIENT_CERT • AT*OPENVPN_CLIENT_KEY
	Added new AT command AT*ETHPORTCHANGE= for specifying a (port number, port mode) to set up or down.
Logging	
	Added a warning when the logs are not set at default level.
	Added the ability for the log file name to be unique so that each log update does not use the same name for the file name.
	Reworked UI usability in IP logging and enhanced the capability to enable long-time capture from RAM or Flash.
Events Reporting	
	Added “When none is ready” (when there is no WAN available) Event Operator for the Network State event.
ALEOS	
	Added a Radio Module RAM Dump feature.
	Added the ability to capture QXDM modem logs directly from the router.
	Added a ping monitor for VPN.
	Added enhanced signing capability for software releases.

Improved templates to prevent duplicate fields and to provide the option to exclude inactive configurations when generating templates.

As a best practice, you should apply a template to a device by:

1. Generating the template on the same ALEOS release as the target routers.
2. Resetting the target routers to factory default settings before applying the template.

To preserve template behavior from the previous release, select **Overwrite inactive fields** when applying (uploading) a template to the router.



Dynamic DNS

Added warning messages to ACEmanager to reflect deprecation of IP Manager.

Security Enhancements

General

Addressed OpenNDS null pointer dereference bugs.
Updated Simple Captive Portal to use a random FAS key for authentication.
Updated XML parsing libraries for security upgrades.
Modified some upload scripts for templates and golden templates so that only .xml and .txt files can be uploaded to the device.
The following AT commands now password protected and must be unlocked using AT*ENTERCND=<User Password>: • AT*FWRMUPDATE • AT*FWUPDATE • AT*FWSTORE • AT*TPLUPDATE • AT*OPENVPN_CLIENT_CERT • AT*OPENVPN_CLIENT_KEY • AT*OPENVPN_CA_CERT

Fixed an issue where certificates could be loaded with unsafe names.
Fixed an issue where commands could be executed from the Ping menu in ACEmanager.
Fixed some configuration parameters on the ACEmanager TLS server to prevent Secure Client-Initiated Renegotiation.
Prevented passwords (Wi-Fi, for example) that appear hidden from being shared through the UI. Created an eye icon to allow the user to see passwords when they are entered.
Added rate limiting to SSH port over USB interface to protect against brute-force log-in attempts.
Fixed some configuration parameters in the ACEmanager server to prevent Secure Client-Initiated Renegotiation.
Updated jquery from 1.11.0 to 3.6.2 to fix possible vulnerability in ACEmanager.
Security and CVE Vulnerabilities
Addressed potential vulnerabilities related to CVE-2023-36328.
Addressed potential vulnerabilities related to CVE-2021-36369.
Updated curl to address potential vulnerabilities related to CVE-2023-28322.
Addressed potential vulnerabilities related to CVE-2020-36694 and CVE-2023-31436 and CVE-2018-17182.
Updated expat to 2.5.0 to address potential vulnerabilities related to CVE-2022-40674.
Addressed potential vulnerabilities related to CVE-2021-3999 and CVE-2020-10029 and CVE-2019-25013.
Addressed potential vulnerabilities related to CVE-2023-27371.
Addressed potential vulnerabilities related to CVE-2022-38725.
Addressed potential vulnerabilities related to CVE-2016-6129 and CVE-2018-12437.
Addressed potential vulnerabilities related to CVE-2022-3715.
Addressed potential vulnerabilities related to CVE-2022-40617.
Addressed potential vulnerabilities related to CVE-2022-4603.
Addressed potential vulnerabilities related to CVE-2019-17362.
Addressed potential vulnerabilities related to: • CVE-2022-42915 • CVE-2022-32221 • CVE-2023-23914 • CVE-2022-42916 • CVE-2022-43551 • CVE-2022-43552 • CVE-2022-35260 • CVE-2022-35252 • CVE-2023-23916 • CVE-2023-23915
Updated BusyBox to address potential vulnerabilities related to CVE-2022-30065.
Addressed potential vulnerabilities related to CVE-2022-0547.

Bug Fixes

Radio Module	
	Resolved an issue with WP7610 radio modules where SMS message were not received properly for some carriers.
	Increased the reliability of radio firmware carrier switching.
	Fixed log messages regarding missing radio module firmware file in rmstore, and fixed behavior of the AT*RMFWSWITCH command.
Networking	
	Fixed an issue where VRRP was tracking only the Cellular WAN interface.
	Fixed an issue with VRRP protocol that was causing VRRP to reboot continuously.
	Fixed issue with VRRP where the backup connection was only being switched to after the LAN connection went down.
	Fixed an issue where Ethernet WAN status was not being correctly displayed.
	Fixed an issue where Ethernet port status was not set to “powered off” when the port was turned off.
	Fixed an issue where the Ethernet port in auto DHCP mode displayed its status as WAN port when it was a LAN connection.
	Fixed an issue where the Local Report Destination IP Address was incorrect when IP Passthru was Enabled.
	Resolved an issue with Ethernet WAN Auto Mode where the Ethernet interface was always selected regardless of its priority.
Cellular	
	Resolved an issue where the APN was mishandled on select regional carriers.
	Resolved an issue with the “Network Password” field for PAP and CHAP authentication mode in the UI.
Wi-Fi	
	Fixed an issue where it was possible to set invalid values for Wi-Fi Client security type.
	Fixed an issue where WPA3 clients were not showing up in the Connected/Rejected Clients table properly.
	Fixed an issue where log messages were not warning the user when attempting to set a Wi-Fi password for Open security.
	Addressed an issue where the user could manually set Wi-Fi Authentication to WEP over the CLI interface.
	Fixed an issue where Wi-Fi status still showed “Active” after shutting down Wi-Fi with AT*WIFI_STARTSTOP.
	Fixed an issue where Wi-Fi status showed as “Not Set” when Access Point was configured with Open security.

Resolved an issue where bridged Wi-Fi subnets were not displayed in the LAN address table properly.
Resolved an issue where the Wi-Fi LED was not displaying proper behavior on LX routers.
VPN
Updated OpenVPN client for improved security while maintaining cipher compatibility with ALEOS 4.16.2.
Resolved an issue where the OpenVPN tunnel was not restored after WAN connectivity was lost.
Resolved an issue where traffic from a non-bridged mode Wi-Fi AP was routed through the VPN tunnel.
Resolved an issue where source IP violations occurred when recovering from a cellular disconnect.
Resolved an issue where port forwarding did not work with Host to LAN VPN configurations.
AT Commands
Fixed an issue where AT*WIFI_SECTYPE was not returning proper values for WPA3 security.
Updated AT command lock level to automatically be set to level 2 when using Telnet.
Fixed an issue with the command ETHPORTCHANGE command on MP70.
Resolved an issue where the SENDTORM command could not be sent to the radio module.
Fixed an issue where AT*netop? would return an error.
Resolved an issue where updating the router to ALEOS 4.17.0 using AT*FWRMUPDATE would fail due to insufficient space. *Note: You will not be able to update your router to 4.17 using an AT command.*
Added a new result code to INSTATE_RAW? query: 126 — Radio retry backoff delay is set to more than 60 seconds.
ALMS
Resolved an issue where some AirLink routers stopped reporting to ALMS after a software upgrade.
Resolved an issue where MAC addresses were not displayed in the LAN IP/MAC table in ALMS.
Resolved issues with displaying the LAN IP/MAC table in ALMS.
Fixed an issue with LWM2M protocol where [DTLS] Abbreviated handshake must turn into full handshake when session does not exist anymore.
Logging
Fixed an issue where error messages would appear in ALEOS logs regarding invalid port forwarding configuration.
Resolved an issue where logs failed to upload after an initial successful log upload to ALMS.
Fixed an issue where error messages would appear in ALEOS logs regarding invalid port forwarding configuration.

ACEmanager	
	Removed the option to upgrade radio module firmware from the Software and Firmware upgrade screen. You can select only ALEOS software for upgrade now.
AAF	
	Added an option to set TLS 1.3 when setting up an AAF app with ssl.https Lua module.
Admin	
	Fixed ToD (time-of-day) reboot interval to reboot at the configured interval.
Software Update	
	Resolved an issue where software updates from recovery mode could fail.
Events Reporting	
	Resolved an issue where the event report in TLV format for MSCIID 643 (ECIO) was incorrect.
SMS	
	Resolved an issue where the SMS command “&&&status” did not return a reply when no GPS was available on the router.