ALEOS 4.10.0 Release Notes

ALEOS 4.10.0 is for AirLink LX60. It is not compatible with AirLink MP70 Series, RV50 Series, GX450 and ES450 gateways.

New Features

Radio Modules

Supports WP7601 and WP7603 radio modules.

Ethernet

Supports 2 GigE LAN Ports.

Ethernet port MAC addresses are now shown on the Status > Ethernet page.

Default Password

Each gateway has a unique default ACEmanager password (found on the device label).

When using the Reset to Factory Default command in ACEmanager, you can configure the Reset Mode to preserve custom passwords and other settings. Three Reset Modes are available:

- Preserve Core Settings (default)—Preserves passwords and network settings. See the ALEOS 4.10.0 Software Configuration User Guide for a list of preserved settings.
- Preserve Only User Password—All settings except the ACEmanager (user) password are returned to the factory default values.
- Reset All—All settings and passwords are reset to default. A confirmation prompt will appear.

Note: A long press of the device Reset button behaves the same as "Reset All".

The minimum password length has increased to 8 characters, and the default for Maximum Login Attempts has been set at 3.

WAN / Cellular

Added an option to support MSS (Maximum TCP segment size) clamping on TCP connections inbound/outbound from/to the Cellular WAN interface.

Located under WAN > Cellular > Advanced > MSS Clamping

Location

Added Self-Training Assisted GPS. Enabling this feature provides faster time to first fix following a restart.

Serial

The Aux port on the LX60 is configurable as an RS-485 interface.

Wi-Fi

Supports 802.11b/g/n/ac (Wave 2 Client Mode):

- Configurable as Access Point or Client
- Access Point (LAN) mode supports up to 10 clients.

Security and CVE Vulnerabilities

Telnet and SSH access can be disabled or limited to LAN or LAN and WAN.

Addressed potential vulnerabilities related to CVE-2016-1583 (see https://nvd.nist.gov/vuln/detail/CVE-2016-1583)

Addressed potential vulnerabilities related to CVE-2016-7117 (see https://nvd.nist.gov/vuln/detail/CVE-2016-7117)

Addressed potential vulnerabilities related to CVE-2016-9806 (see https://nvd.nist.gov/vuln/detail/CVE-2016-9806)

Addressed potential vulnerabilities related to CVE-2017-16939 (see https://nvd.nist.gov/vuln/detail/CVE-2017-16939)

Addressed potential vulnerabilities related to CVE-2016-2070 (see https://nvd.nist.gov/vuln/detail/CVE-2016-2070)

Addressed potential vulnerabilities related to CVE-2017-16544 (see https://nvd.nist.gov/vuln/detail/CVE-2017-16544)

Addressed potential vulnerabilities related to CVE-2016-2148 (see https://nvd.nist.gov/vuln/detail/CVE-2016-2148)

Updated TCPDUMP package to version 4.9.2 to resolve several CVEs.

Addressed potential vulnerabilities related to CVE-2017-14106 (see https://nvd.nist.gov/vuln/detail/CVE-2017-14106)

Updated openssl to version 1.0.2l. This addresses potential vulnerabilities related to CVE-2016-2182, CVE-2016-6303, CVE-2016-2179, CVE-2016-2181, CVE-2016-6302

Addressed dnsmasq vulnerability via CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Addressed potential vulnerabilities related to CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088 (WPA handshake traffic) (see https://www.kb.cert.org/vuls/id/228519)

Addressed potential vulnerabilities related to CVE-2016-2070 (see https://nvd.nist.gov/vuln/detail/CVE-2016-2070)

Addressed potential vulnerabilities related to CVE-2017-8890 (see https://nvd.nist.gov/vuln/detail/CVE-2017-8890), CVE-2017-9077 (see https://nvd.nist.gov/vuln/detail/CVE-2017-9077), CVE-2017-9076 (see https://nvd.nist.gov/vuln/detail/CVE-2017-9076)

Addressed potential vulnerabilities related to CVE-2017-7472 (see https://nvd.nist.gov/vuln/detail/CVE-2017-7472)

Addressed potential vulnerabilities related to CVE-2016-5195 (see https://nvd.nist.gov/vuln/detail/CVE-2016-5195)

Bug Fixes

WAN / Cellular

Removed unnecessary static route in DHCP offer

Wi-Fi

Added an option to disable 802.11w support, allowing older Apple devices to connect to the access point. The default setting for 802.11w support continues to be Optional.

ALEOS AT Commands

AT*NETSTATE now reports WAN status accurately.

Events Reporting

Pulse Accumulator 1 can now be selected in the Events Reporting events list.

ALMS

Resolved an issue where the ALMS Server URL field was present when connected to ALMS using MSCI. This field is only valid for the LWM2M connection.

Known Issues

Wi-Fi

The LX60 in Access Point (LAN) mode may, under certain conditions, intermittently discontinue broadcasting its SSID if there are no clients connected. To resolve this issue, reboot the LX60.