# ALEOS 4.9.4 Release Notes

ALEOS 4.9.4 is for AirLink GX450 and ES450 gateways.

**Important:** ***If you are using gateways with GPS enabled, it is critical to upgrade to this release before November 3, 2019 0:00 UTC.*** *This release addresses the GPS 2019 Rollover issue by ensuring that GPS time used for location reporting and system time remains accurate after a GPS system offset reset occurs. Failing to upgrade to this release can lead to issues with location reporting, such as the inability to acquire a GPS fix and inaccurate timestamps. Systemic issues such as loss of communications with management systems and invalidation of certificates can also arise if you do not upgrade your gateways to ALEOS 4.9.4.*

## Upgrade Path

If you are updating a gateway from an older version of ALEOS (prior to 4.5.1), first update the gateway to ALEOS 4.5.1 before updating to 4.9.4.

## New Features

### Radio Modules

Updated firmware for the following radio module:

MC7354

- Verizon: SWI9X15C_05.05.58.05

### Default Password

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 4.9.4 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: Previously, a long press of the Reset button behaved according to the configured Reset Mode. As of 4.9.4, a long press of the device Reset button behaves the same as "Reset All".*

### ACEmanager

A notification prompts you to change the password if you are using the non-unique default password to log in to ACEmanager.

| | |
|---|---|
| **WAN/Cellular** | |
| | Added an option in ACEmanager to support MSS (Maximum TCP segment size) clamping TCP connections inbound/outbound from/to the Cellular WAN interface.<br>The setting is located under WAN/Cellular > WAN/Cellular > Advanced. Default is “Enable”. |
| **LAN** | |
| | Added a fully configurable subnet mask for setting the IP Passthrough Default Gateway. |
| **Serial** | |
| | Added a setting to disable or enable sending an “OK” message from the serial port after the gateway boots. |
| | Added TCP Persistent Connection settings to introduce an auto-connect mechanism for TCP PAD mode. |

# Security Enhancements

| | |
|---|---|
| **Security and CVE Vulnerabilities** | |
| | Addressed potential vulnerabilities related to CVE-2018-4061 (see https://nvd.nist.gov/vuln/detail/CVE-2018-4061) |
| | Removed default SNMP user credentials to address potential vulnerabilities related to CVE-2018-4062 (see https://nvd.nist.gov/vuln/detail/CVE-2018-4062) |
| | Addressed potential vulnerabilities related to CVE-2018-4063 (see https://nvd.nist.gov/vuln/detail/CVE-2018-4063) |
| | Addressed potential vulnerabilities related to CVE-2018-4065 (see https://nvd.nist.gov/vuln/detail/CVE-2018-4065) |
| | Addressed potential vulnerabilities related to CVE-2018-4067 (see https://nvd.nist.gov/vuln/detail/CVE-2018-4067) |
| | Addressed potential vulnerabilities related to CVE-2016-2148 (see https://nvd.nist.gov/vuln/detail/CVE-2016-2148) |
| | Addressed potential vulnerabilities related to CVE-2016-1583 (see https://nvd.nist.gov/vuln/detail/CVE-2016-1583) |
| | Updated TCPDUMP package to version 4.9.2 to resolve several CVEs. |
| | 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-2017-8816 (see https://nvd.nist.gov/vuln/detail/CVE-2017-8816), CVE-2017-8817 (see https://nvd.nist.gov/vuln/detail/CVE-2017-8817), CVE-2018-1000007 (see https://nvd.nist.gov/vuln/detail/CVE-2018-1000007) |

| | |
|---|---|
| | Updated curl from 7.55.1 to 7.59.0, addressing potential vulnerabilities related to CVE-2017-8816 (see https://nvd.nist.gov/vuln/detail/CVE-2017-8816), CVE-2017-8817 (see https://nvd.nist.gov/vuln/detail/CVE-2017-8817), CVE-2018-1000007 (see https://nvd.nist.gov/vuln/detail/CVE-2018-1000007) |
| | Addressed potential vulnerabilities related to CVE-2016-7117 (see https://nvd.nist.gov/vuln/detail/CVE-2016-7117) |
| **General** | |
| | Newly manufactured gateways have a unique default ACEmanager password (found on the device label). |
| | Implemented additional security improvements to protect against remote attacks. |
| | Addressed potential data packet replay vulnerability on Wi-Fi. |
| | An option to set the minimum TLS version is now available under Admin > Advanced. |

# Bug Fixes

| | |
|---|---|
| **ACEmanager** | |
| | The setting for remote access to ACEmanager now applies to both IPv4 and IPv6. |
| **LAN** | |
| | Restored the use of DHCP Option 33 for adding static routes. |
| | Resolved an issue where ICMP redirect messages for INVALID state traffic were not sent over LAN interfaces. |
| | PPPoE connection will no longer drop when cellular connection is lost. |
| | Resolved an issue where DNS proxy resolution did not work for statically assigned hosts. |
| | Resolved an issue where the Ethernet interface was not disabled until the WAN connection was established. |
| **WAN/Cellular** | |
| | Response to Incoming Ping is now working correctly when used with IP Passthrough. |
| | Resolved an issue where Response to Incoming Ping was not working correctly when set to Pass to Host. |
| | Resolved an issue where an incorrect APN appeared for a specific MCC/MNC combination. |
| | Resolved an issue where Carrier Operator Selection did not work correctly. |
| **Wi-Fi** | |
| | Marvel Micro AP SSID is no longer broadcast when the Wi-Fi mode is set to disabled. |
| | Resolved an issue where the Network State was not reporting the true status of Wi-Fi connectivity. |

| | |
|---|---|
| **Serial** | |
| | Resolved an issue where FQDN input fields rejected entries longer than 39 characters. FQDN fields now accept up to 255 characters. |
| | Resolved an issue where initial FQDN outbound PAD sessions (TCP and UDP) did not use the correct IP address. |
| **GPS** | |
| | Addressed the GPS 2019 Rollover issue by ensuring that GPS time used for location reporting and system time remains accurate after a GPS system offset reset occurs. |
| | External TCP Polling for location reports can now occur at a rate that is faster than the default interval of 30 seconds. |
| **VLAN** | |
| | Resolved an issue where an Ethernet host could not access the gateway via the gateway's VLAN address and access the WAN. |
| **ALEOS AT Commands** | |
| | Resolved an issue where the ATLISTIP command did not return the correct information for all ALEOS devices. |
| **Events Reporting** | |
| | Pulse Accumulator 1 can now be selected in the Events Reporting events list. |
| | Messages in the Type, Length, Value (TLV) format now contain "seconds" in the time field. |
| | Resolved an issue where ACEmanager did not save negative values entered for RSSI threshold reporting. |
| **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. |
| | Resolved an issue with configuring port filtering in ALMS. |
| | Resolved an issue with displaying Persisted Bytes Sent and Received. |
| **Logging** | |
| | Removed certain statistics from logs. |
| **VPN** | |
| | Resolved an issue where user-uploaded SSL VPN certificates and key files were not preserved across reboots. |
| | Resolved issues that led to improper operation of VPN failover. |
| | Resolved an issue where the primary or secondary VPN did not reconnect after a cellular connection outage, when VPN Failover was used. |
| **Services** | |
| | Resolved an issue where setting "Remote Login Server Telnet/SSH Port" to 0 did not disable Telnet. Setting "Remote Login Server Telnet/SSH Port" to 0 now functions as specified in the user guide. |

| | |
|---|---|
| | Improved reliability of Low Power mode. |
| | Fixed Low Power Mode. The gateway now responds to a logic LOW level on the Ignition Sense line. |
| | GX450 with Wi-Fi: Resolved an issue where the gateway remained in Low Power Mode after Ignition Sense went HIGH. |
| | Fixed an issue with SSH key generation. |
| **Applications** | |
| | Resolved an issue where the ALMS Device Initiated Interval could be reset to default with ALMS Protocol set to “Try LWM2M, Fallback MSCI” after connecting to ALMS on LWM2M. |
| **General** | |
| | Improved the longevity of the device flash memory. |