ALEOS 4.4.8 Release Notes

ALEOS 4.4.8 is for AirLink GX440/400, ES440, and LS300 gateways.

Note: Please note that this release addresses the GPS 2019 Rollover event for the specified devices. Sierra Wireless recommends upgrading the following gateways to version 4.4.8 before November 3, 2019:

- *LS300, GX400—AT&T, Canada and International*
- *GX440—Verizon Wireless (Note: CDMA fallback must also be disabled)*
- *GX440—AT&T and Canada*

For more information, see the Sierra Wireless Product Bulletin: 2019 GPS Week Number Rollover.

Note: This release does not address GPS rollover for CDMA devices LS300, GX400—Verizon Wireless and Sprint. For these devices, GPS must be disabled or devices must be upgraded.

Upgrade Considerations

If your gateways are currently running the early ALEOS versions listed below, please read these guidelines before upgrading ALEOS.

ALEOS 4.3.5 or earlier

If you are updating a gateway from ALEOS 4.3.5 or earlier:

1. See Upgrading from Older Versions of ALEOS Firmware to identify the upgrade path and any intermediate steps needed to upgrade to the latest firmware.
2. Install the interim build(s) required.
3. If you require ACEmanager Remote Access, install ALEOS 4.4.4.004.
4. Install ALEOS 4.4.8.

ALEOS between 4.3.5 and 4.4.4.004

If you require ACEmanager Remote Access, ensure that you install ALEOS 4.4.4.004 before upgrading to the latest firmware.

New Features

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. The setting is located under WAN/Cellular > WAN/Cellular > Advanced. Default is “Enable”.
LAN	
	Added an option in ACEmanager to enable or disable Reset Host Interface. The setting is located under LAN > DHCP/Addressing > General. Default is “Enable”.

Security Enhancements

Security and CVE Vulnerabilities	
	Addressed potential vulnerabilities related to CVE-2017-11176 (see https://nvd.nist.gov/vuln/detail/CVE-2017-11176)
	Addressed potential vulnerabilities related to CVE-2016-7117 (see https://nvd.nist.gov/vuln/detail/CVE-2016-7117)
	Addressed potential vulnerabilities related to CVE-2016-1583 (see https://nvd.nist.gov/vuln/detail/CVE-2016-1583)
	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)

Bug Fixes

GPS	
	Addressed the GPS 2019 Rollover issue by ensuring that GPS time used for NMEA and system time remains accurate after a GPS system offset reset occurs
WAN/Cellular	
	The configured WAN Keep Alive period is now preserved after the initial 1 hour back-off period when recovering from a WAN Keep Alive-initiated reboot.

Wi-Fi	
	GX440/400: Resolved an issue where the Marvel Micro AP SSID is momentarily broadcast when the Wi-Fi mode is set to disabled
VPN	
	Resolved an issue where user-uploaded SSL VPN certificates and key files were not preserved across reboots
Security	
	GX440: Resolved an issue where port forwarding was impaired when the gateway had a dual-Ethernet X-Card installed
Services	
	Setting “Remote Login Server Telnet/SSH Port” to 0 now functions as specified in the user guide.
	Resolved an issue that was preventing system uptime from being reported in SNMP trap messages
Serial	
	Resolved an issue where LAN-connected devices were unable to reach the WAN when USB Serial was configured
ALEOS AT Commands	
	The AT+COPS command is now allowed a longer period of time to complete successfully, so that Carrier Operator Selection would work correctly under all circumstances
Error Handling	
	Resolved an issue where excessive timeout error messages when communicating with the radio prevented gateways from rebooting and reconnecting
Applications	
	Resolved an issue where the M3DA server hostname was badly provisioned when the MSCI URL contained a port definition
Account	
	Resolved an issue where an account reactivation command was not being sent because the command contained restricted characters
	LS300: Resolved an issue where sconsole and uasuser accounts were not disabled after resetting the gateway to factory defaults