ALEOS 4.12.0 Release Notes

ALEOS 4.12.0 is for AirLink MP70 Series routers, LX60 routers, LX40 routers, RV50 Series gateways and the RV55 router.

Important: ***If you are using RV50 Series 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 4.12.0. For more information, please refer to Sierra Wireless Product Bulletin: 2019 GPS Week Number Rollover.*

New Features

New AirLink product: RV55

ALEOS 4.12.0 supports the first release of the AirLink RV55 LTE-A Pro router.

The RV55 has two Wi-Fi radios that can be configured as Access Points or Clients.

The RV55 serial port can be configured as a standard 9-wire or dual 4-wire serial port. In dual port mode, the RV55 can connect to devices with a Y cable (available from Sierra Wireless).

WAN

Changed WAN Ping Monitor minimum values, increased frequency of pings, and allowed configuration of number of pings.

Wi-Fi

Added a new feature for network interface switching based on Wi-Fi signal strength (under Wi-Fi > Monitor). When the RSSI is low enough, the network interface will switch from Wi-Fi to Cellular. When RSSI is high enough, the network interface will switch back from Cellular to Wi-Fi.

802.1x Authentication: Added an option to select using PEAP Authentication with or without a Client CA Certificate. By default, using the certificate is required.

LX60, LX40 and RV55: A new setting of “Not Preferred” is available for selecting Wi-Fi Access Point channels/frequencies (2.4 GHz or 5 GHz). Selecting this setting causes the device to attempt to connect to the other frequency first and then fall back to the not-preferred frequency.

Vehicle Telemetry

The title and revision of the installed vehicle telemetry configuration file is now displayed in ACEmanager.

Added a CAN passthrough feature for non-vehicle CAN bus applications.

Serial	
	Added TCP Persistent Connection settings to introduce an auto-connect mechanism for TCP PAD mode.
VPN	
	Added a new “Standard” VPN implementation that provides support for IKEv1, IKEv2 and MOBIKE.
	Added support for Host-to-LAN VPN.
	MP70, RV50 and RV55: Added IPsec FIPS Mode and FIPS 140-2 encryption standards. Only IKEv2 is supported in FIPS mode.
	Added IPv6 “4-in-6” IPsec Tunnel Support.
	Standard IPsec Implementation users can specify a list of networks to be excluded from a full tunnel.
	Added support for aes256gcm16 encryption in Standard IPsec Implementation *Note: ACEmanager prevents you from selecting aes25gcm16 as the IKE encryption when using an IKEv1 tunnel. However, when using ALMS there will be nothing to prevent you from making this selection.*
	Added an option to allow ALMS and AMM servers to be exempted from full tunnel.
	The Key Group column in the ESP Algorithms table is now hidden when Perfect Forward Secrecy is disabled.
	A Reset VPN Tunnels button replaces the Set VPN Policy buttons. This button resets all VPN tunnels across all tunnel types without needing to reboot the router or gateway.
AT Commands	
	RV55: Added AT commands to support dual serial mode.
	RV55: Updated various AT commands to work with dual Wi-Fi features; for example, *MACWIFI, *WIFIMODE .
	Removed the *HANGUPTORESET command.
AirLink Application Framework	
	RV55: When RS232 Dual Port Mode is enabled, the second port can be reserved for AAF.
ALMS	
	ALEOS logs can be now retrieved from ALMS.

Security Enhancements

General

- Upgraded to kernel 4.9.88 in an effort to enhance general security and provide future support.
- MP70: Addressed potential data packet replay vulnerability on Wi-Fi.
- Implemented a refactored firewall to increase security and reduce the time required to apply a firewall configuration.
- Prevented Reverse SSH from being used to proxy network traffic.
- Prevented reading files via the tcpdump -V command in iplogging.

Security and CVE Vulnerabilities

- 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-2017-5715 (see https://nvd.nist.gov/vuln/detail/CVE-2017-5715)
- Addressed potential vulnerabilities related to CVE-2018-1000517 (see https://nvd.nist.gov/vuln/detail/CVE-2018-1000517)
- Addressed potential vulnerabilities related to CVE-2018-16840 and CVE-2018-16842 (see https://nvd.nist.gov/vuln/detail/CVE-2018-16840 and https://nvd.nist.gov/vuln/detail/CVE-2018-16842)
- Addressed potential vulnerabilities related to CVE-2016-6354 (see https://nvd.nist.gov/vuln/detail/CVE-2016-6354)
- Addressed potential vulnerabilities related to CVE-2019-8912 (see https://nvd.nist.gov/vuln/detail/CVE-2019-8912)
- Addressed potential vulnerabilities related to CVE-2018-11574 (see https://nvd.nist.gov/vuln/detail/CVE-2018-11574)
- Addressed potential vulnerabilities related to CVE-2015-9059 (see https://nvd.nist.gov/vuln/detail/CVE-2015-9059)

Bug Fixes

WAN/Cellular

- Resolved an issue where IP passthrough over USB was not working.
- Resolved an issue where setting the radio band through ALEOS caused an invalid mask to be set.
- Resolved an issue with a signal strength error when the WAN connection was connected to the Verizon/Sprint 3G network

Wi-Fi	
	Resolved an issue where the Network State was not reporting the true status of Wi-Fi connectivity.
	LX60/LX40: Removed the Client Ageout Timer setting because it was not supported by the hardware.
	Resolved an issue with connecting end devices. As a result, for WPA2 Enterprise security authentication, only CCMP is supported as the encryption cipher suite.
LAN	
	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.
VPN	
	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.
	Updated the certificate used by the OpenVPN Management Tunnel for AMM connections.
	Resolved an issue where the gateway accepted unsolicited inbound traffic not in the Friend List when full tunnel was configured.
GPS	
	External TCP Polling for location reports can now occur at a rate that is faster than the default interval of 30 seconds.
	Addressed the GPS 2019 Rollover issue for MC73xx radio modules by ensuring that GPS time used for location reporting and system time remains accurate after a GPS system offset reset occurs.
Serial	
	Resolved an issue where an initial attempt to establish a PAD connection to an FQDN would fail when serial was in TCP or UDP mode.
	Resolved an issue where FQDN input fields rejected entries longer than 39 characters. FQDN fields now accept up to 255 characters.
	Modbus ID 43 will no longer result in an extra “0x2b” inserted in the Modbus stream.
	AT Telnet will now work when the gateway is configured for Reverse Telnet operation.
Events Reporting	
	Messages in the Type, Length, Value (TLV) format now contain “seconds” in the time field.

AirLink Application Framework

Resolved an issue where AAF displayed stale data at startup. If you are using AVTA or AMMER, please upgrade your applications:

From	To
AVTA 1.1.2.010	AVTA 1.1.2.011
AMMER 1.0.4.004	AMMER 1.0.4.005

Resolved an issue where AAF-based configuration was generating excessive error messages.

Admin

Resolved an issue where negative temperatures of the radio module (-10 °C, for example) were being reported incorrectly.

AT Commands

A new AT command AT*IPPINGSEC has replaced AT*IPPING to get and set the values of the test interval of the Ping Test and Traffic Monitor. The command accepts seconds instead of minutes.

Resolved an issue with the AT command AT*NETIPPREF to allow inputs of 0 and 1 to match ACEmanager.

Resolved an issue where ERROR was returned when the text of an SMS sent by AT command included commas.

Services

Resolved an issue where the Telnet/SSH Access Policy field would not be correctly migrated when transitioning between ALEOS versions.

ACEmanager

Resolved an issue where the M3DA password was not stored as part of the template.

Resolved an issue where the Shutdown Delay after Ignition Off setting rejected values over 43200 seconds.

ALMS

Resolved an issue where the outbound port filtering setting in ALMS was not matching the setting as it was configured in ACEmanager.

Hardware

LX60: Resolved an issue where the device could become stuck in a reboot loop if it was reset to factory defaults immediately preceding a recovery firmware update.

Known Issues

VPN

OOB settings on the ACEmanager VPN > Split Tunnel page are not supported in FIPS mode for full tunnels. To allow OOB traffic from a network/IP, add the IP to the exemption list in the tunnel configuration.

Applying configuration templates with existing IPsec VPN settings from a previous version of ALEOS is not supported, and may cause IPsec tunnel traffic to stop. As standard practice, Sierra Wireless recommends that templates be created and applied to AirLink gateways running the same version of ALEOS.

With an IPsec tunnel configured with Standard Implementation, FIPS, MOBIKE, Full Tunnel and Host-to-LAN, VPN traffic continues over the previous WAN interface after a WAN switch.

AMM

Loading a template causes AMM Management Tunnel port to reset to empty, as the downloaded template has no port set.

To work around this issue, add a line to the template file to enable the AMM Management Tunnel. For example:

```
<page name="Services">
<section name="MSCI">
 <item msciid="5027" title="Server URL" value="https://na.m2mop.net/device/
msci/com" />
 <item msciid="10258" title="Auto Synchronize Configuration" value="1" />
 <item msciid="10241" title="TLS Verify Peer Certificate" value="0" />
 <item msciid="15500" title="HTTP Server And ACEview Services" value="1" />
 <item msciid="10034" title="Enable AMM Management Tunnel" value="1190" />
</section>
```

Wi-Fi

RV55: When Wi-Fi A and Wi-Fi B are both set to Access Point/5 GHz mode, some selected Wi-Fi A and B Channel combinations may cause the SSID to disappear. If this occurs, please try configuring a different channel combination.

AT Commands

LX40: ATZ (reboot command) over USB serial does not reset the device.