ALEOS 4.9.0 Release Notes

ALEOS 4.9.0 is for AirLink MP70, MP70E, RV50, RV50X, GX450 and ES450 gateways. For upgrade instructions, refer to the ALEOS 4.9.0 Software Configuration User Guide.

Note: Gateways running ALEOS 4.9.0 or higher cannot be downgraded to ALEOS 4.8.x.

IMPORTANT NOTICE

As part of Sierra Wireless's continued commitment to ensuring the highest level of security on all AirLink devices, the upgrade process for this release will detect the following potentially insecure device configurations and make corresponding configuration changes to mitigate the potential security impact:

- If **User** has a ***default password***: Access to Telnet/SSH and server-initiated MSCI over the cellular interface will be disabled. Users of these services are advised to set a strong, unique User password prior to upgrading.
- If **Sconsole** has a ***default password***: The account will be disabled until a password is set. Users of reverse telnet are advised to set a strong, unique Sconsole password before upgrading.
- If DMZ is set to automatic and the device is not using Public IP (**DMZ Enabled** is set to ***Automatic*** and **Host Connection Mode** is not set to ***Ethernet Uses Public IP***): DMZ will be disabled. Users of DMZ but not Public IP are advised to set **DMZ Enabled** to ***Manual*** before upgrading.

If a device has already been upgraded, these services can be re-enabled using ACEmanager or AirLink Management Service (ALMS).

In addition to the above changes, the viewer account has been removed and will no longer be accessible in this release.

Advance Notice

The issues described in this section do not apply to ALEOS 4.9.0, but may affect your deployment and use of ALEOS in a future release.

Browser Support

Please note that releases after ALEOS 4.9.0 will support the following browsers:

- Chrome (latest version)
- Firefox (latest version)
- Internet Explorer 11 (latest patch version)
- Edge (latest patch version)

Internet Explorer 9 and 10 will no longer be supported in post-4.9.0 releases.

© 2018 Sierra Wireless. All rights reserved.

Automatic DMZ

To increase the security of ALEOS-based devices, the DMZ option of Automatic will be removed in releases after ALEOS 4.9.0. In ACEmanager, this setting is under Security > Port Forwarding > DMZ Host Enabled.

DMZ is disabled by default. After the Automatic option is removed, you will have to specifically set the mode to Manual and manually enter an IP address.

If DMZ Host Enabled has been set to Automatic, it will be set to Disabled after the upgrade. If you attempt to upload a template with DMZ set to Automatic, the uploaded value will be ignored.

New Features

Radio Modules

Updated firmware for the following radio modules:

MC7455

- Generic: SWI9X30C_02.24.03.00
- AT&T: SWI9X30C_02.24.03.00
- Sprint: SWI9X30C_02.24.03.00
- Verizon Wireless: SWI9X30C_02.24.05.06

MC7430

- Generic: SWI9X30C_02.24.05.06
- DoCoMo: SWI9X30C_02.24.05.06
- Telstra: SWI9X30C_02.24.05.06
- KDDI: SWI9X30C_02.24.05.06

MP70E (MC7354) now supports AT&T Plasma ID

RV50X and MP70: Added image switching support for KDDI with MC7430.

Added dual SIM automatic fail-over to automatically switch the radio module firmware.

ACEmanager

The “viewer” user account has been removed.

The “sconsole” user account is now disabled by default.

- If the “sconsole” user was previously using the default password, the “sconsole” account will be disabled after upgrading.
- To enable the “sconsole” account, ALEOS requires the customer to set a password.

Added a new setting for Telnet/SSH Access Policy. Telnet/SSH can now be set to LAN+WAN, LAN (default) or Disabled. When upgrading a gateway to 4.9.0, if the user password is default, Telnet/SSH is set to LAN.

© 2018 Sierra Wireless. All rights reserved.

Added a new setting for Server-Initiated MSCI. This setting is labeled “HTTP Server And ACEview Services” in ACEmanager. Server-Initiated MSCI can now be set to LAN+WAN, LAN only (default) or Disabled. When upgrading a gateway to 4.9.0, if the user password is default, this setting is set to LAN only.

Status

MP70/MP70E: The state of sensor calibration for Dead Reckoning is now reported in the Status > Location page.

MP70/MP70E: If Vehicle (CANBus) Data Collection is enabled, the Status > Service page will display status of CANBus - J1979 Protocol and CANBus - J1939 Protocol.

MP70/MP70E and RV50X: LTE-Advanced and associated Carrier Aggregation info is now displayed on the Status > Home and Status > WAN/Cellular pages when it is available, even if there is no active traffic.

WAN / Cellular

Eliminated connection retries from ALEOS when a BELL SIM card receives error 3GPP-33 (3G only).

LAN

Host Port Routing will only show Gateway options when the Route mode is set to Gateway

The Link WAN Coverage to Interface setting, which appeared on the LAN > Ethernet and LAN > USB pages in ACEmanager, now has its own page: LAN > Link WAN Coverage.

The DHCP Reservation list has been increased from 5 to 20.

Wi-Fi

MP70/MP70E: Added the ability to specify operating Channels for Wi-Fi

Security and CVE Vulnerabilities

Management frame protection (IEEE 802.11) is now supported.

MP70 and GX450: Addressed potential data packet replay vulnerability on Wi-Fi.

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

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

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

Addressed potential vulnerabilities related to CVE-2017-9078 and CVE-2017-9079 (Dropbear) (see https://nvd.nist.gov/vuln/detail/CVE-2017-9078 and https://nvd.nist.gov/vuln/detail/CVE-2017-9079)

© 2018 Sierra Wireless. All rights reserved.

Addressed potential vulnerabilities related to CVE-2016-2180, CVE-2016-2182, CVE-2016-6303, CVE-2016-2179, CVE-2016-2181, CVE-2016-6302 (openSSL)
(see https://www.openssl.org/news/secadv/20160922.txt)

Addressed potential vulnerabilities related to CVE-2015-8983, CVE-2015-8982 (gnu-glibc)
(see https://nvd.nist.gov/vuln/detail/CVE-2015-8983)
(see https://nvd.nist.gov/vuln/detail/CVE-2015-8982)

Addressed potential vulnerabilities related to CVE-2016-9919
(see https://nvd.nist.gov/vuln/detail/CVE-2016-9919)

Addressed potential vulnerabilities related to CVE-2016-10229
(see https://nvd.nist.gov/vuln/detail/CVE-2016-10229)

Addressed potential vulnerabilities related to CVE-2016-7937 (tcpdump)
(see https://nvd.nist.gov/vuln/detail/CVE-2016-7937)

Addressed potential vulnerabilities related to CVE-2017-7520 and CVE-2017-7479 (OpenVPN)
(see https://nvd.nist.gov/vuln/detail/CVE-2017-7520
and https://nvd.nist.gov/vuln/detail/CVE-2017-7479)

Addressed potential vulnerabilities related to CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496 (dnsmasq) (see https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00006.html)

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)

Services

New MP70/MP70E Vehicle Telemetry capabilities:

- Configure direct interface to vehicle's diagnostic port (OBD-II or J1939).
- Configure threshold and duration for vehicle/driver behavior events such as harsh acceleration, deceleration and cornering.
- Added a Vehicle Telemetry logging subsystem (available under Admin > Log > Configure Logging) to control logging related to the Vehicle Telemetry feature.

MP70: A limitation exists where ACEmanager displays CAN Bus-related fields only if the MP70 is CAN Bus capable. Dead Reckoning and Driver Behavior features are available on all MP70s. However, connecting the router to the vehicle bus to enable telemetry-assisted Dead Reckoning reporting will have no effect if the MP70 is not CAN Bus capable.

Location

MP70/MP70E now supports Dead Reckoning. It can be enabled or disabled under Location > Global Settings.

The dead reckoning requires re-calibration if:

- MP70/MP70E was rebooted through the ATZ command
- Watchdog timeout was initiated
- the SIM card is removed

© 2018 Sierra Wireless. All rights reserved.

Location Reports can now be sent over a valid WAN connection even if no SIM is installed.

Users are now able to select from a menu which NMEA sentences the gateway will report.

MP70/MP70E supports automatic upgrade of the GNSS firmware.

Once the MP70/MP70E is calibrated, it shall return to calibration within 3 minutes after the MP70 is rebooted and driving is resumed.

If the orientation of the MP70/MP70E changes after GNSS sensors have been calibrated, click Clear GNSS Calibration to calibrate in the new mounting. A reboot is necessary.

Applications

Applications now have access to IP Passthrough settings via the Airlink Application Framework.

Bug Fixes

Recovery Mode

Improved eMMC write stability.

Status

Global ID is now named Serial Number on the Status > About page.

Resolved an issue where the PNTM status page was displaying "DSCP" instead of the number of bytes in one or more fields.

Resolved an issue where network status was not updated correctly because of delays related to the cellular debounce timer.

Resolved an issue where deviceID was incorrectly reported after applying a template, rebooting and connecting the router to a PC with a USB cable.

Resolved an issue where the Status > Cellular page was showing the incorrect Radio Technology.

WAN / Cellular

Fixed issue where brief (~1second) cellular outages resulted in Network Link state being reported as Down for ~30 seconds.

MP70/MP70E: Resolved an issue where the WAN port was bridged to the other Ethernet ports after bootup.

Resolved an issue where policy routing did not work with the following settings:

- Wi-Fi first priority (connected)
- Cell second priority (connected)
- Ethernet third priority (not connected)

© 2018 Sierra Wireless. All rights reserved.

MP70: Resolved an issue where the device was not acquiring IPv6 address on Telstra network when it was configured as dual IPv4/v6.

MP70: Resolved an issue where the device requested both IPv4 and IPv6 addresses on Telstra network when configured as IPv4 only.

When using the monitor feature to test the health of WAN connections users can now enter an FQDN as well as an IP address.

MP70/MP70E, RV50/RV50X: Resolved an issue where the downlink bandwidth throttle was not working.

Service Timeout now correctly uses Service Status rather than Carrier Service Availability. If this setting is enabled and the cellular interface loses service, the device will wait a user-configured amount of time (minimum 10 minutes) before switching to the secondary SIM. During this wait time a ping will be sent out of the interface every 30 seconds.

LAN

Resolved an issue in the Link WAN Coverage to Interface feature where the Radio Link Delay setting was being ignored.

Corrected issue preventing IP Passthrough from working on the USB and Ethernet interfaces.

ALEOS no longer replies to link-local ARP requests.

Removed unnecessary static route in DHCP offer.

Wi-Fi

GX450: Resolved an issue where the Wi-Fi access point failed to use the configured TKIP encryption protocol.

GX450: Resolved an issue where the Wi-Fi channel selection was not working

MP70/MP70E: Changed the configuration of AP client ageout timer to disallow the use of 0 to 59 seconds. Using the value of 0 for this timer could cause undesirable disconnects of Wi-Fi LAN clients. Starting from this release, the minimal value is 60 (seconds).

MP70/MP70E: Fixed a missing beacon problem when the device AP uses the same channel as 15+ other APs.

VPN

Key Usage/Extended Key Usage is allowed to be used for verifying server certificate.

When setting up an OpenVPN tunnel, the dialog box where users could enter the certificate or the key prompted for the certificate only. Now the user is prompted to enter either a certificate or key, as appropriate for the selected operation.

OpenVPN will now optionally retry on username/password authentication error.

MP70/MP70E: Resolved an issue where the VPN tunnel prevented clients from receiving DHCP offers from the MP70/MP70E.

Resolved an issue with Split Tunnel when working with a WAN interface

© 2018 Sierra Wireless. All rights reserved.

Resolved an issue with IPSec VPN where network traffic could be occasionally blocked.

Security

Resolved an issue where inbound port filtering rules were blocking forwarded ports to the host device.

Resolved an issue with Port Forwarding where the device forwarded inbound traffic from a public port that was not on the “Allowed” list.

Ensured that Trusted IP rules and Port Filtering rules are applied before Port Forwarding rules. Please note that Port Filtering rules now apply to traffic from trusted IPs.

Services

Resolved an issue where the device did not retry failed DNS lookups.

Resolved an issue where the device did not perform DNS lookups on FQDN addresses after DNS TTL expired.

Resolved an issue where remote users were unable to log into a device behind the gateway using SSH.

Location

MP70/MP70E: Resolved an issue where switching GNSS constellations required power-cycling the unit.

Resolved an issue where GPS reporting stopped when an FQDN was used as the reporting server.

Resolved an issue where MP70/MP70E Vehicle Telemetry Sensors Calibration Status indicated Calibration Not Started after the unit calibrated and the vehicle was parked for more than 5 minutes.

MP70/MP70E: The location fix may display Dead Reckoning even in clear sky. This is due to any difference between the satellite fix and the Dead Reckoning fix. The DR fix has higher priority.

Serial

RV50/RV50X: Resolved an issue where serial data in PAD mode was being corrupted when the Ethernet port was disabled.

Applications

Resolved an issue where the AAF framework was unable to establish connection with the remote server.

Resolved an issue to prevent deadlock inside the LWM2M library and facilitate LWM2M client restart when WAN IP address changes.

AAF application can now correctly use the system.reboot API.

Admin

Resolved an issue where the PLMN was occasionally being logged with unprintable characters.

Resolved an issue where sometimes the device's up time was not logged after rebooting.

© 2018 Sierra Wireless. All rights reserved.

IP Logging log file contents have been renamed to avoid problems with sending captured log files via email.

ALEOS AT Commands

Resolved an issue where the AT commands *IPPING? and *IPPINGADDR were not working. These commands, along with the new *MONITORTYPE command, now support all WAN interfaces, including Ethernet WAN and Wi-Fi WAN.

Resolved an issue where remote users could not change the user password using a Telnet session.

AT*NETSTATE now reports WAN status accurately.

Call Manager

MP70E: ALEOS will now make no additional connection attempts if Verizon throttles RTT.

ACEmanager

Resolved an issue where ACEmanager incorrectly displayed a “Development Firmware - Not suitable for production use” banner.

Known Issues

Dead Reckoning

MP70: The maximum horizontal error is 100 meters. For an uncalibrated unit, the Estimated Position Uncertainty (meters) will appear as 99.0.

MP70: Dead Reckoning cannot be enabled/disabled using ALMS.

Wi-Fi

MP70: Due to a high priority security update, the MP70 will temporarily only support a maximum of 65 clients. This issue will be corrected in an upcoming release.

© 2018 Sierra Wireless. All rights reserved.