SIERRA WIRELESS
A SEMTECH COMPANY

AirLink OS 5.0

RELEASE NOTES

About AirLink OS 5.0

AirLink OS 5.0 is a production release for the AirLink XR90, XR80 and RX55. These release notes describe new features, bug fixes and known issues that apply to this release.

- New Features and Enhancements
- Bug Fixes
- Known Issues

Sierra Wireless encourages all customers to maintain their AirLink routers with the current AirLink OS release and security patches via our AirLink Management Service (ALMS). Sierra Wireless tests and validates upgrades from the previous major software releases.

Note: WEP security mode will be deprecated in a future AirLink OS release. Although WEP appears as a selectable security mode for AirLink RX55 Wi-Fi configuration, WEP cannot be applied. Please select another authentication type.

Upgrade Notes

Sierra Wireless has tested and validated upgrading to AirLink OS 5.0 from the following releases:

- 4.1.26
- 4.0.23

Warning: *Downgrade from AirLink OS 4.1 to an earlier build is not supported. The Software Image Management features (Admin > Software Image Management), including "Switch to backup image", are disabled (and will be re-enabled in future releases). Please contact Sierra Wireless for further guidance if you need to downgrade.*

Warning: *Your routers must have AirLink OS 4.0.23 or 4.1.26 installed before they can be upgraded to AirLink OS 5.0. Direct upgrade to AirLink OS 5.0 from AirLink OS 3.1 and earlier is not supported.*

Upgrade Path Matrix

If the router is running AirLink OS version...	Upgrade to...	Notes
2.0.43	**3.0.35**	Upgrading directly to 3.1.26 or 4.0 from 2.0.43 will fail, resulting in radio module failure and WAN disconnection.
2.0.45 **2.1.30** **3.0.35**	**3.1.24**	Downgrading from 3.0 to 2.1 is not supported.
3.1.24 **3.1.26**	**4.0.23**	
4.0.23	**4.1.30, 5.0.49**	Downgrading from AirLink OS 4.1.x to an earlier build is not supported.
4.1.x	**5.0.49**	

Sierra Wireless recognizes that our customers deploy devices in a wide range of network environments with varying configurations. It is always good practice to install a new AirLink OS release with the planned operation workflow on a few trial devices to ensure that standard operation is maintained within your environment before deploying the new release across your fleet of AirLink devices.

New Features and Enhancements

EM9190 and EM7690 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 03.10.11.00
- AT&T: 03.10.07.00
- FirstNet: 03.10.07.00
- T-Mobile: 03.10.07.00
- Generic: 03.10.07.00
- Bell: 03.09.11.00
- Telus: 03.09.11.00
- Rogers: 03.10.07.00
- Telstra: 03.04.03.00
- Softbank: 03.10.07.00
- KDDI: 03.10.07.00
- DOCOMO: 03.10.07.00

EM7411 and EM7421 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 01.14.23.00
- AT&T: 01.14.22.00
- FirstNet: 01.14.22.00
- T-Mobile: 01.14.03.00
- Bell: 01.14.13.00
- Generic: 01.14.22.00 (EM7411)
- Generic: 01.14.13.00 (EM7421)
- Sierra: 01.14.03.00
- Bell: 01.14.13.00
- Telus: 01.14.03.00
- Rogers: 01.14.03.00

ALMS	
	Introduced beta version of Hybrid Cloud, an enhancement for ALMS accounts that provides an extra layer of security and on-premises controls for your management system. To engage with this beta program, please contact Sierra Wireless.
	Smart Reporting rules have been updated to include an action with the trigger and filter parameters. The Smart Reporting UI now has a new action definition section that enables the configuration of “Send to ALMS” actions. System Smart Report objects (rule, dataset, trigger, filter and action) are no longer editable.
Wi-Fi	
	Added reporting of remote access point attributes (including SSID name, security protocol, RF band, RF channel and signal bars) to the logs of the Wi-Fi client device.
	Added a feature to the Wi-Fi status page to display the Wi-Fi standard running on a remote access point.
Location Reporting	
	Added the ability to configure multiple local reporting configurations with multiple Report Types and Destinations.
Telemetry	
	Enhanced the user interface in Services > Telemetry > Custom Reports. All Custom Reports are now configured using “edit page” screens instead of in-table editing.
	AirLink OS reports telemetry data to AV using ATP, the AirLink Telemetry Protocol. AirLink OS 5.0 has implemented ATP 3.1. Earlier revisions of the protocol are not supported.
GPIO	
	Added support for GPIO digital output.
Apps	
	Added the ability to use the entrypoint/cmd from the image rather than requiring the user to enter one when deploying the container.
	Added a container on-failure restart policy.
AirLink OS	
	Improved how items in the progress bar are displayed when modifying settings or creating a template. The list of items no longer includes values related to UI application processes.
	Added the ability to add a button and its parameters to a template file.
Networking	
	Added a “Rule Name” column in the Network Watchdog > Monitoring Rule table to display the name configured when creating the rule. When upgrading from AirLink OS 4.x, the names for existing rules are converted to “Monitoring Rule 1”, “Monitoring Rule 2” in sequential order (as there was no name field in 4.x).
VPN	
	To facilitate successful VPN reconnection across large fleets of routers using ACM, a random retry delay between 0 to 30 seconds was added.

Templates
When performing a software upgrade, the templates that are stored in the router (default template and backup image) will be deleted if they were not created using the current firmware version (5.0 and above).
Added a means to prevent templates created from different software versions and hardware from being applied to a router. “Version mismatch” and “Device mismatch” errors will appear.
Simple Captive Portal
Added a “Last Updated At” timestamp to display the last remote splash page package update.

Bug Fixes

Templates
Resolved an issue where Public IP addresses could not be configured as port forwarding addresses under Networking > Firewall > Port Forwarding rule > Create Port Forward Rule > Forward to Device. Multicast, Broadcast, LinkLocal, Wildcard and Loopback addresses remain read-only.
Resolved an issue where user-defined smart reporting rules in a template did not apply because of a “not a valid reference” error.
Resolved an issue where a template created from the current configuration could include the “system-defined” LAN segment created when IP Passthrough was configured; this template could cause errors when applied to other routers.
Resolved issues where a device template created on a router containing the settings listed below failed when attempting to apply the template to a fleet of routers, if the routers had those settings previously configured: • Fully Qualified Domain Names • Smart Reporting • LAN Segments • Network Watchdog > Monitoring Rules • Multi-WAN
Resolved an issue where, while in Template mode, actions such as changing the Local User password, reboot, software update, reset to factory default, or ping/traceroute commands could be applied to the router.
Networking and Connectivity
Resolved an issue where a global Multi-WAN rule (from all to all for all traffic) via a Wi-Fi or Ethernet interface resulted in all WAN traffic being blocked upon reboot.
Resolved an issue where XR80 and XR90 North American SKUs could not connect to ALMS using the LPWA interface.
Resolved an issue where square brackets in user-defined Multi-WAN policy names were converted to escape characters when the names appeared in the “Applies to Policy” lists when configuring Multi-WAN rules.
Resolved an issue where, when a full traffic isolation (srcip=0.0.0.0/0, dstip=0.0.0.0/0) Multi-WAN rule is applied against the Default LAN segment, DNS queries may be rejected from LAN-connected hosts.
Resolved an issue where a device connected to the router via Ethernet did not get a new LAN segment IP address after the LAN segment on the Ethernet port has changed.

RX55: Resolved an issue where the throughput for the UDP traffic over the Cellular interface could be low, especially for small packet sizes.
Resolved an issue with low throughput on bridge interfaces.
Resolved an issue where traffic between LAN devices and the router's Ethernet or Wi-Fi WAN interfaces was misrouted when the incoming LAN-side packets were from the same subnet as the WAN interface.
Cellular
Resolved an issue where SIM Database settings may be reset upon upgrade to 4.1 from a router that had been originally deployed on AirLink OS 2.1.
Resolved an issue where radio module image switching away from a carrier PRI with a network-pushed APN to a carrier PRI unavailable in the Radio Module Image Management store resulted in loss of connectivity. The device will now fall back to the GENERIC carrier PRI in this situation.
Resolved an issue with missing information in the logs by adding a new log for the cellular Active SIM information.
XR80: Resolved an issue where a cellular interface could report unusually low SNR values.
Resolved an issue where, after entering the SIM PIN, the SIM PIN field indicated an incorrect entry with the text "SIM PIN should be 4 to 8 digits long" when the device was online with the correct PIN and the PIN had been saved to the router.
Resolved an issue where the option "5G-SA Only" appeared in the Preferred Technology menu when the router has a non-5G radio module.
Resolved an issue where an installed radio module firmware image may not be updated to the correct version after a switch to backup image and re-initiating the software upgrade.
RX55: Resolved an issue where during throughput testing for low packet sizes, the router occasionally entered an Out of Memory state and rebooted.
Resolved an issue where, when an XR Series router was connected to a 5G network, LTE primary band info was not shown under System > Radio Module.
RX55: Resolved an issue where, when adding EM7411 radio module firmware to Radio Module Image Management, a validation error indicated the addition will exceed the maximum number of entries in the table even when there were available entries in the table.
XR90: Resolved an issue where, after disconnecting an XP cartridge and performing a software upgrade, the radio module firmware for the disconnected cartridge appeared under System > Admin > Software Versions.
Wi-Fi
Resolved an issue when the list of Wi-Fi channels was not refreshed according to the Outdoor parameter value when the device was geolocated in Europe.
Resolved an where an "invalid path" error appeared in the Regular Logs when the remote AP SSID name contained square bracket characters.
Resolved an issue where it was not possible to delete a RADIUS configuration that is not in use when AP security mode is not set to "WPA-Enterprise".
Resolved an issue with not displaying DFS channel information by adding a notification for when the router changes DFS Wi-Fi channel.
Resolved an issue with scanning and connecting to a Wi-Fi network with a 1-character SSID like "1" or "A" (Sierra Wireless recommends against using such network names).

	XR80/90: Resolved an issue where Auto Channel selection could select a channel that was not on the available channels list when the Access Point was set for the EU Region with DFS channels enabled.
	Removed a redundant “MSS Disabled” option when configuring MSS Clamping.
	XR80: Resolved an issue where the router could not connect to an access point with a hidden SSID.
	XR80/XR90: Resolved an issue where the router could not connect to WPA-PSK-TKIP networks.
AirLink OS	
	XR90: Resolved an issue where the XP1 cartridge showed an incorrect state on the dashboard after being removed.
	Resolved an issue where, under Diagnostics > Radio Module Log, non-cellular radio WAN interfaces were listed in the Radio menu.
	Resolved an issue with the width of the “System” column in the System > Logs > Log Level table.
	Resolved an issue where it was possible to create a configuration name for a Virtual APN using special characters such as [ ] ( ) and have the virtual APN configuration rejected (unable to be saved) without the UI indicating an error.
VPN	
	Resolved an issue where escape characters in the VPN tunnel name were improperly displayed.
	Resolved an issue with VPN ACLs when using 0.0.0.0/0 as remote/local subnets.
	Resolved an issue where any Multi-WAN rules that apply to IPsec Policies for Client Tunnels were removed after the router reboots.
	Resolved an issue where, when VPN tunnels were disabled or in a “Connecting” state, clicking the REFRESH button on the Networking > IPSec Status page produced a Command execution alert in the UI.
	XR90: Resolved an issue where, when the router is used as the VPN server, the tunnel could be established, but bi-directional ping traffic did not work.
	Resolved an issue where, when editing an IPsec Tunnel configuration, a WAN interface that was disabled appeared in the WAN INTERFACES list as “Value not available”.
Software Upgrade and Downgrade	
	Resolved an issue where, after a software upgrade, a user-configured SIM configuration name for Multi-APN virtual interfaces did not display correctly on the dashboard (under WAN > Radio Module).
Serial	
	Resolved an issue where it was possible to configure “privileged” ports 1 to 1023 for TCP PAD operation and other services. Such services will not work on these ports.
Captive Portal	
	Resolved an issue where, in certain configurations, data packets with invalid source IP addresses were sent out the cellular WAN interface when the Wi-Fi Simple Captive Portal was enabled. Packets with invalid source IP addresses could previously cause the cellular link to drop with certain carriers, preventing captive portal traffic from passing.
	Resolved an issue where the Simple Captive Portal remote splash page did not download due to WAN unavailability after a router reboot.

To resolve configuration inconsistencies between Extended Captive Portal and Simple Captive Portal, Extended Captive Portal now targets LAN segment instead of Wi-Fi APs.
Resolved an issue where user firewall rules did not take effect for Captive Portal LAN clients.
Resolved an issue where Extended Captive Portal and Simple Captive Portal could be enabled on the same LAN segment.
Location and Telemetry
Resolved an issue where MQTT reports stopped sending after a certain period.
Resolved an issue where, when a router booted up with no WAN connectivity, but had a Location Fix, it did not switch to GPS-NMEA as time source. Please note that the NTP polling interval affects how quickly the router can switch between NTP and GPS-NMEA protocols. By default, the polling interval is set to one hour, and the router uses NTP until the interval expires.
Resolved an issue where the router did not report IPv6 WAN status items.
Resolved an issue where engine fault datapoints (diagnostic trouble codes) were not reported to ALMS.
Resolved an issue where ignition status was not be reported to ALMS. This affected AMR Trips Reports, where different trips are merged because of missing ignition start and end markers.
Resolved an issue where the router could report an incorrect location fix during startup.
Resolved an issue where calculated odometer readings lagged behind dash odometer readings. Please note that calculated odometer readings may be temporarily off from the dash odometer by +/- 1 due to the KM unit boundary between dash odometer and calculated odometer not being aligned.
Resolved an issue where link status was reported to AirVantage for changes on the Primary WAN link only. AirVantage Advanced Mobility Reporting reports now include link status changes for all configured WAN interfaces.
Resolved an issue where an incorrect number of satellites could be displayed under Status/ Monitoring > Dashboard and Status/Monitoring > Services > Location. Now, when GNSS is enabled and service is lost, the satellite count is reset to 0.
ALMS
Resolved an issue where excessively large data payloads sent from the router caused synchronize operations to fail.
Resolved an issue where Cellular interfaces and virtual interfaces were unsorted in the Hardware Interfaces and Status Monitoring pages in ALMS.

Known Issues

Cellular
An issue exists where CLAT must be disabled when using a SIM with IPv6 only in order for the router to connect to ALMS. ALMS does not support communication over IPv6.
XR80: An issue exists where an XP Cellular cartridge interface can appear as a selectable WAN interface in various configuration menus when the cartridge is not connected.

AirLink OS does not support multiple IPv6 addresses assigned via SLAAC/DHCPv6. Only the last IPv6 address will be used
XR80-LTE/RX55: An issue exists where, under System > Radio Module, only DL carrier aggregation information is shown. UL carrier aggregation information is not displayed.
An issue was observed where a radio that disconnected from the 5G network erroneously reported that the Service Type was NR5G (NSA) with a 5G band while it was connected to LTE.
XR90: It was observed that XP Cellular-1 APN failed to pass traffic after the router was powered down, XP2 cartridge connected, and then rebooted. However, the issue could not be reproduced.
Wi-Fi
RX55/XR80: An issue exists where some Pixel 6 phones keep connecting to and disconnecting from the 5 GHz Wi-Fi (WPA2) access point.
Removed the 2×2 MIMO option from the UI. This option is not supported.
XR80/XR90: An issue exists where the Wi-Fi LED color may occasionally stay blinking green irrespective of the signal strength when the router Wi-Fi Client is connected to a remote Wi-Fi access point.
An issue exists where the Wi-Fi LED may occasionally flash blue and red when AP mode is enabled but no clients are connected. The LED should flash purple once per second with the router in this state.
An issue exists where an XR80/90 client displays a scanned Fortinet access point configured with WPA3 Enterprise mode as WPA2 Personal, and the router cannot connect.
XR90: After configuring Dual-Band Wi-Fi Client Connection settings, a “Cannot display the component” error may appear. However, the router operates in dual-band configuration with no issues.
An issue exists where an XR80 client displays a scanned Cisco Meraki access point configured with WPA2 Enterprise mode as WPA Personal, and the router cannot connect. This occurs when 802.11w support is required on the Cisco Meraki AP. If 802.11w support is disabled or optional, the XR80 shows the correct security mode, and the XR80 can connect.
RX55: Does not support connecting to a Cisco 9117AX access point when configured to broadcast a WLAN on 2GHz and 5GHz bands with WPA2.
RX55: An issue exists where Ethernet LAN to Wi-Fi LAN UDP throughput is lower than expected.
An issue exists where the XR Series router cannot connect to a Fortinet access point set for “WPA2 PMF- Required” when the router is also set to “PMF - REQUIRED”. The XR Series client successfully connects when set to “PMF - OPTIONAL”.
The XR Series router in 2.4GHz (802.11 b/g/n/ax) Client mode cannot connect to a Cisco 9117AX remote access point.
An issue exists where throughput from Wi-Fi LAN to Wi-Fi WAN (using two Wi-Fi interfaces for TX/RX) may be lower than expected. Sierra Wireless recommends configuring channel separation as wide as possible on Access Points. Configuring adjacent channels is not recommended.
Networking and Connectivity
RX55: An occasional issue exists where the Ethernet is disabled, but the physical interface is still up. A host connected to the port may report the link is up though no traffic from the device goes to the host. The link light is also lit when the Ethernet is disabled and a cable is connected to a host.

After starting the iPerf client (Networking > Diagnostics) in ALMS, if the client does not respond, a “Stop” button does not become available to terminate the process, and no error is returned. To recover, exit the ALMS Configuration for the router and then enter the Configuration again.
QOS: DSCP packet marking does not work. Please contact Sierra Wireless for assistance with this feature.
RX55: Unlike XR Series routers, the RX55 does not support Multi-WAN Policies for AirVantage Software Servers and AirVantage Management Servers.
Port forwarding to the router’s localhost for remote access is not configurable. Devices that upgrade to this release will retain the configuration; however if the device is factory reset or updates are made to the port forwarding configuration, this rule cannot be reconfigured. It is possible to restore the rule via a template update as a workaround.
An issue exists where a Multi-WAN policy does not route traffic as intended when the policy is defined using a Service (i.e., based on port numbers). To resolve the issue, disable DPAA.
When creating a bandwidth profile under Quality of Service (QoS) > Bandwidth Policies, the UI converts Download and Upload settings from kilobytes and kilobytes/sec to megabytes and megabytes/sec. These conversions are inexact: 40,000 KB is converted to 39.06 MB, for example.
IPv6 DNS Propagate fails for the Ethernet WAN interface. Manually configured DNSv6 servers are not propagated from WAN to HOST-PC on the LAN.
XR90: QoS (traffic shaping and policing) cannot be applied for traffic to/from the gateway itself, and may not be applied to some flows through the gateway.
XR90: An issue exists where IPv6 routes on multi-APN interfaces were not created after multiple reboots.
VPN
An issue exists where high-bandwidth sustained UDP traffic passing through a FIPS tunnel can initiate a kernel panic. To avoid the issue, limit the source bandwidth or, for the download path (for ingress UDP FIPS traffic over non-Ethernet WANs only), use router QoS settings to limit traffic.
An issue exists where the Status/Monitoring Dashboard displays an incomplete list of VPN tunnels or stale VPN tunnel associated with each WAN interface. For complete VPN status information, see Status/Monitoring > Networking > IPsec Status.
An issue exists with two different VPN connections operating on a LAN-side host PC and traffic passing through a single XR80, TCP throughput was degraded, while UDP throughput was good.
After creating a HOST-TO-LAN IKEv1 tunnel with ACM server with multiple subnets, the tunnel state may report “Partially Connected. Some Child SA's failed” although the tunnel is connected with all Child SA’s.
An issue found during testing exists where router-originated ICMP pings on Non-FIPS, non-MOBIKE, full tunnels stop during a WAN switch from Wi-Fi to Cellular. After manually reconfiguring ICMP pings for the new WAN interface, successful pings will resume. Note that this issue does not exist when regular network traffic is flowing in the tunnels.
An issue exists where, if the Intermediate certificate is loaded before the CA certificate is loaded, the Intermediate certificate is the first one and then the CA certificate is appended. This certificate order causes connection issues with the ACM. To remedy the issue, load the Intermediate certificate in the place where the CA certificate is loaded, and load the CA certificate in the place where Intermediate certificate is loaded.
The minimum VPN failover time is approximately 48 seconds, regardless of DPD timeout.
IPv4 IPsec VPN (connected over cellular) does not work after IPv6 Clat is enabled.

Software Upgrade/Downgrade
An issue exists where an AirLink OS software upgrade may fail when an unexpected reboot occurs during the upgrade, possibly triggered by cellular service loss and an auto-SIM switch.
An issue has been observed after an upgrade from AirLink OS 4.0.23 to 4.1 or higher where the State reported under Admin > Software Image Management may remain in “synchronizing” for an extended period and no image is indicated under Backup.
An issue exists during a software update where a “tar file is truncated” error sometimes occurs and the software update fails. This is due to a timeout when fetching the upgrade package, and is most often seen when the upgrade is on a network drive. If this occurs, run the software update again.
An issue exists where, after a software upgrade, the Radio Module Image Management table is full, the HL7800 (LPWA) FW image is not present and the LPWA Adapter Status is “Stopped”. To resolve, delete any unused radio module image(s) from the list, leaving no more than nine images, and then reboot the router.
Templates
An issue exists where a template created on a router with an enabled, operating Extended Captive Portal configuration fails when applied to a router that is in factory defaults. To remedy the issue, ensure that Extended Captive Portal is Disabled before creating the template and enable the feature after applying the template.
An issue exists where a template created from the current configuration failed to apply to the same router after factory reset. The issue occurs when the conditions below are met: 1. Create and replace the default “WAN” zone in the Default Policies with a zone created including no multi-APN virtual interfaces. 2. Configure multi-APN on the cellular interface. 3. Revert the APN configuration to manual or auto. -or- 1. Configure multi-APN on the cellular interface. 2. Create and replace the default “WAN” zone in the Default Policies with a zone created including the multi-APN virtual interfaces. 3. Revert the APN configuration to manual or auto. To resolve the issue: • Use the “Modify template from local file” option to delete the Virtual APN from the default policies and save (export) the new file. • In general, do not template multi-APN zones if setup is not multi-APN.
A device template created on a router containing the following settings will fail when attempting to apply the template to a fleet of routers, if the routers have those settings previously configured: • DHCP Reservation > Fixed IP Assignment • DMZ
AirLink OS
An issue exists where a router configured with Multi APN and two or more IPsec tunnels that runs continuously can see its memory usage increase until an automatic reboot is triggered. Network traffic is unaffected, and the automatic reboot recovers the system.
An issue exists where the AirLink OS local access URL https://airlink./ (as shown in the Quick Start Guide) does not work on computers running Ubuntu. Use https://192.168.1.1 instead.

The Create PEM Certificate feature does not make the valid configuration combinations clear. The ROOT CERTIFICATE field is not optional in some configurations. The valid combinations are one of the following: • NAME + CERTIFICATE + PRIVATE KEY • NAME + ROOT CERTIFICATE • NAME + CERTIFICATE + PRIVATE KEY + ROOT CERTIFICATE
After using the SWITCH TO BACKUP IMAGE option, the Radio Module Image Management table and the cellular radios still have the Radio Module Firmware images from the previous active build. To update both the table and the radios, use ALMS to upgrade to the backup image (now the active software) or use the local UI and run a software update to the same software build.
ALMS
An issue exists where, under Networking > Diagnostics > IP Capture, the in-progress button continues to spin after an IP capture is completed.
When registering a router, the Basic Workflow in Pre-Configuration is not compatible with AirLink OS-based routers.
Location and Telemetry
An issue exists where the GNSS location map appears in the local UI but may not appear in the ALMS UI due to a lag in satellite count data being provided to ALMS. To resolve immediately, manually synchronize the router with ALMS. Please note the issue may reoccur and another manual sync may be required.
An issue exists where GNSS Smart Reporting store-and-forward data points collected during a cellular network outage are not saved after the router is power cycled.
Forwarding GPS info from local ports to the serial port does not work if the destination is set to 127.0.0.1. Use the Default LAN IP address instead.
Serial
XR80/XR90: Serial port 1 supports 8N1 Serial port data bits setting only.
Simple Captive Portal
An issue exists where the log-in splash page does not reappear on a client device after the session timeout expires. The splash page will reappear when the Wi-Fi connection is disconnected/ reconnected, or the browser is closed/reopened.
Apps
An issue exists where the LAN Segment on which the container was running is not retained after a template is applied to the router. The container runs on the Default LAN segment after a template is applied no matter which LAN Segment is specified in the template.