SIERRA WIRELESS IS NOW SEMTECH®

AirLink OS 5.1

RELEASE NOTES

About AirLink OS 5.1

This release of AirLink OS 5.1 is for the AirLink XR90, XR80, XR60 and RX55. These release notes describe new features, bug fixes and known issues that apply to this release.

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

Note: *AirLink OS 5.1 removes the Wi-Fi Indoor/Outdoor switch for Global (EU/AUS) SKUs. After upgrade to AirLink OS 5.1, only bands that are allowed for both indoors and outdoors are now enabled (and only DFS channels are available) for EU and AUS customers.*

For customers using Global (EU/AUS) routers, please be advised that:

- *If your router Access Point was configured to use an indoor channel with DFS disabled, after upgrade a message will appear advising that the configuration is invalid. You will need to reconfigure the Access Point.*
- *If your router Access Point was configured to use an indoor-only channel with DFS enabled (channels 36–48, 52–64), after upgrade the router will use a new channel instead of the previously configured channel. A message will appear advising that the router is using a new channel.*

Change of Behavior Notices

For other change of behavior items see, Location and Telemetry on page 5.

Type	Description	Target AirLink OS Version	Action
Deprecation	WEP support for AP configuration has been removed from the RX55 to align security best practices with the other AirLink OS-powered devices. Semtech does not expect this to impact users as the RX55 currently fails to connect to APs using WEP security.	5.1	If WEP is being used for AP security authentication, Semtech recommends modifying this to a more secure security protocol.
Behavior change	AirLink OS 5.1 removes the indoor/outdoor switch that enabled the 5150–5350 GHz Wi-Fi frequencies for Australia, EU, and UK routers. AirLink OS 5.2 will reintroduce the ability to enable the 5150–5250 GHz Wi-Fi frequencies for indoor use.	5.1	Enable DFS to use 5 GHz DFS Wi-Fi frequencies. Upgrade to AirLink OS 5.2, when available, to continue to use the 5150–5250 GHz Wi-Fi frequencies.
Deprecation	The RX55 and RX55 Wi-Fi devices will have the ability to enable Container Applications removed in a future release. This does not affect the RX55 Wi-Fi Plus model. Semtech does not expect this to affect users as the memory available for applications is extremely limited on these devices.	TBD	Contact your Semtech representative to discuss edge compute-capable devices.
Behavior change	The default value for Wi-Fi AP “Client Isolation” will be changed to “Enabled”.	7.0	No action required; existing project configurations will not be modified.

Upgrade Notes

Semtech has tested and validated upgrading to AirLink OS 5.1 from the following releases:

- 5.0
- 4.1.33
- 4.1.26
- 4.0.23

Your routers must have AirLink OS 4.0.23 or later installed before they can be upgraded to AirLink OS 5.1. Direct upgrade to AirLink OS 5.1 from AirLink OS 3.1 and earlier is not supported.

Upgrade Path Matrix

If the router is running AirLink OS version...	Upgrade to...	Notes
2.0.49 2.0.52	3.0.35	Upgrading directly from 2.0.49/2.0.52 to 3.1.26 or 4.0 will fail, resulting in radio module failure and WAN disconnection.
2.1.30	3.1.26	Downgrading from 3.0 to 2.1 is not supported.
3.0.35 3.1.24 3.1.26	4.0.23	
4.0.23	5.0.86	
4.1.x	5.1.78	Downgrading from AirLink OS 4.1 to an earlier build is not supported.
5.0.x	5.1.78	

Semtech 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

Cellular	
	Added a “Check Manual Radio Firmware” cellular adapter state. If “Radio Firmware Switching” is set to “Manual”, the radio module firmware will be updated (if required), before the “Initializing SIM” state appears. After the “Initializing SIM” state, the existing “Check Radio Carrier” state appears. During this time, the router validates the required radio module firmware (as defined by the SIM card and the Radio Firmware Switching settings), ensuring that it is present and active.
	Began transition from built-in R2C eSIMs to plastic SmartSIM for LPWA HL7800 on Global SKUs. An AirLink OS alert is raised if an LPWA SIM is not detected.
	Updated the displayed network information when the system is notified that the SIM IMSI value changes (for Sierra SmartSIMs, for example).
Networking	
	Added minimum and maximum values for Simple Captive Portal and Extended Captive Portal Session Timeout and Extended Captive Portal Idle Timeout.
	Simple Captive Portal: AirLink OS 5.1 features increased web server security. Inline scripts are no longer allowed in html pages. This means that if you want to include script tags in your html file, you must create a javascript file and call the file in the login.htm file.
	Added support for Dynamic DNS.
	Added support for DHCP Relay.
	Multi-WAN routing rules now support a list of IP addresses for destination and source IP fields.
	Added configurable settings to the Network Watchdog: timeout and payload size for ICMP ping, and timeout for DNS lookup.
VPN	
	To avoid an issue where high-bandwidth sustained UDP traffic passing through a FIPS tunnel could initiate a kernel panic, QoS traffic classifiers and bandwidth profiles starting with “IPsec FIPS DL Cap” are not allowed. This prefix is reserved for system-generated QoS entries. (These system-generated QoS entries are non-templatable.) When upgrading to AirLink OS 5.1, it is recommended to not have QoS traffic classifiers and bandwidth profiles starting with the prefix “IPsec FIPS DL cap”. Such QoS traffic classifiers and bandwidth profiles will be overwritten after enabling IPsec FIPS mode if they have same name as system-generated QoS entries.
	Added OpenVPN support. AirLink OS supports connecting to OpenVPN 2.5 and OpenVPN 2.6 servers.
Wi-Fi	
	Added the ability to configure a redundant RADIUS authentication server for Wi-Fi authentication.
	Added support for New Zealand Wi-Fi geolocation.
	Added support for Japan Wi-Fi geolocation.
	Removed Indoor/Outdoor switch for Global (EU/AUS) SKUs. Only bands that are allowed for both indoors and outdoors are now enabled.
	RX55: Removed the option for channels 36–48 when geolocated to Canada or non-geolocated NA SKU.
	Enhanced the Connected Clients table by showing connected clients’ RSSI.

Location and Telemetry	
	Enhanced GNSS Local Reports with the ability to specify a fixed source port. The setting is blank by default. If blank, a random source port will be chosen.
	Deprecated the telemetry data point atp.wanrdy (WAN Ready) that was no longer being reported correctly in AirLink OS 5.0.
	Added a new Telemetry data point that is incremented and included in every report that is sent to ALMS and MQTT. This allows for detection of report losses.
	Added support for the new J1979 standard odometer PID on newer vehicles (manufactured after 2019).
	You can now choose from several options how location fixes are filtered/reported when ignition is OFF (that is, when the vehicle is parked). This remedies Location Fixes drifting when vehicles are parked and are in Dead Reckoning mode.
	Added support for AMR Coverage Map and Coverage Trail reports for connected HPUE modems.
	XR80/XR90: Replaced GNSS Firmware Selection with an option to enable or disable Dead Reckoning.
	Added a new feature that allows the router to report HPUE-related data over MQTT and/or via AirVantage.
	Added IPv6-related data points to telemetry reporting and the AirLink Telemetry Protocol specification.
	Added a feature in which users can enable and download NMEA logs from the router.
AirLink OS	
	Hybrid Cloud moved out of beta.
	Container Applications has moved from Beta to Early Adopter.
	Added an error message to the UI "switch" component ( ) that will appear if validation fails.
	Added certificate management features under Security > Certificates. The certificate management solution enables the router to interact with the customer's EST certificate infrastructure to support certificate enrollment and automated renewal.
	Replaced the Logout button with an "Account" button that allows you to view Account Details and Logout from AirLink OS.
Logging	
	Log messages containing WAN interface IP addresses have been moved from INFO level to NOTICE level.
	Added metadata to IP Capture, which is included in a new tar.gz file to download.
	Changed the extension of the Radio Module Log file from .raw to .qmdl.
	Implemented audit log rotation. Audit logs now automatically rotate when full.

EM9190 and EM7690 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 03.14.10.00
- AT&T: 03.14.10.04
- FirstNet: 03.14.10.04
- T-Mobile: 03.14.10.01
- Generic: 03.14.10.04
- Bell: 03.14.10.01
- Telus: 03.14.10.00
- Rogers: 03.14.10.01
- Telstra: 03.10.07.00
- Softbank: 03.10.07.00 (EM9190 only)
- KDDI: 03.10.07.00 (EM9190 only)
- DOCOMO: 03.10.07.00 (EM9190 only)

EM9293 Radio Module Firmware

Carrier Firmware Matrix:

- Generic: 02.15.01.00
- Verizon: 02.16.05.00
- AT&T: 02.15.01.00
- FirstNet: 02.15.01.00
- T-Mobile: 02.15.01.00

Although it appears that EM9293/ROGERS (XR80 or XR90) firmware can be added in the Radio Module Image Management store, the firmware will not be populated. Radio Module Firmware for ROGERS will be included in a later release.

Added smart transmit to EM9293 for XR80 and XR90.

EM9291 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 02.16.05.00
- Generic: 02.15.01.00AT&T: 02.15.01.00
- FirstNet: 02.15.01.00
- T-Mobile: 02.15.01.00
- Bell: 02.15.01.00
- Telus: 02.15.01.00

Although it appears that EM9291/ROGERS (XR60) firmware can be added in the Radio Module Image Management store, the firmware will not be populated. Radio Module Firmware for ROGERS will be included in a later release.

Reduced TX power in the 3550–3700 MHz frequency range to meet FCC/IC requirements when paired with the system antenna.

EM7411 and EM7421 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 01.14.24.00
- 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
- Sierra: 01.14.03.00
- Bell: 01.14.13.00
- Telus: 01.14.03.00
- Rogers: 01.14.03.00

HL7800 Radio Module Firmware

Carrier Firmware Matrix:

- AT&T: 4.7.1.0
- FirstNet: 4.7.1.0
- Sierra: 4.7.1.0

Added support for HL7800 4.7.1.0 firmware. Existing routers on 4.6.9.4 or 4.4.14.0 will remain on their respective versions.

Note: *Downgrades for routers with HL7800 4.7.1.0 are not supported. The new routers with 4.7.1.0 are incompatible with AirLink OS 5.0. Note that this firmware will come pre-installed from the factory on new devices as of March 2025.*

Bug Fixes

Networking and Connectivity

Resolved an issue where a network interface may be disabled if the router experiences a power interruption while the network watchdog is restarting that interface.

Resolved an issue where secondary LAN inputs on a Multi-WAN Policy had incorrect DNS configuration.

Upgrade issue: Resolved an issue where a custom network monitoring rule migrated from 4.1 to 5.0 resulted in the zone being invalid.

XR60: Resolved an issue where a log message that incorrectly indicated an invalid Wi-Fi interface would appear on non-Wi-Fi XR60 routers upon reset to factory defaults. Note that connectivity was unaffected.

Resolved a Network Watchdog issue causing cellular connectivity instability on a router configured in IP Passthrough mode. The issue caused restarts of the device when a Ping timeout attempted to restore connectivity.

Resolved an issue with network disconnects in IP Passthrough mode by improving IP Passthrough logic to handle cellular network provider-initiated disconnects.

Addressed client DNS resolution failures when a Multi-WAN policy rule fully segregated all traffic (0.0.0.0/0 or ::/0) from a LAN segment to a constrained set of WAN interfaces. In some circumstances, DNS queries by hosts connected to the router would fail.

Resolved a Network Watchdog issue causing cellular connectivity instability on a cellular device configured in IP Passthrough mode. The issue could cause repeated restarts of the device when a Ping timeout attempted to restore connectivity.

Resolved an issue where routers updated from AirLink OS 3.0 to 5.0 had an issue with Multi-WAN Policies targeting secondary WAN interfaces.

Resolved an issue where the router sometimes did not detect (for about 15 minutes) that an external HPUE modem had been unplugged from the router.

	Resolved an issue where it was possible to select the same IP Passthrough Destination MAC Address on different cellular interfaces even though this is an invalid configuration. IP Passthrough Destination MAC Addresses must now be unique, and is now enforced via the UI and Datastore. Upon upgrading from a previous version, this uniqueness will also be checked. If in the (unsupported) case where a duplicate Destination MAC Address existed on an active configuration, the first active configuration will remain and the remaining will be deactivated. A notification alert will appear. Any inactive configurations that duplicate the Destination MAC Address of an active configuration will have their Destination MAC Address logged and cleared. If a user is experimenting with configuring the same Destination MAC device for multiple cellular interfaces' passthrough, they will have to first clear the Destination MAC field before adding it to a new cellular interface.
	Resolved an issue where a Multi-WAN policy did not route traffic as intended when the policy was defined using a Service (i.e., based on port numbers).
	Resolved an issue where overlapping IP rules from configured Multi-WAN policies stopped WAN traffic from passing.
Cellular	
	Updated the T-Mobile PLMN list to resolve issues with APN and radio module firmware assignment.
	XR80 and XR90: Resolved an issue where Sierra LPWA SIMs were unable to connect.
	Resolved an issue where KDDI, DOCOMO, and SOFTBANK carrier PRIs could be added to an unsupported device.
	Resolved issues with the Preferred Technology setting for Multi APN virtual interfaces. In AirLink OS 4.0 it was possible to specify a different preferred technology for each virtual interface even though each virtual interface will, in practice, have the same preferred technology. In AirLink OS 4.1 the preferred technology can now only be set for the parent interface, and each virtual interface will use the same value. Upgrading to AirLink OS 4.1 will set the preferred technology to Auto unless every virtual interface specified the same preferred technology, in which case that will be used instead. If a preferred technology is required for your deployment, Semtech recommends setting it to the same value on each AirLink OS 4.0 virtual interface before upgrading to 4.1. See also Known Issues on page 12.
	Resolved an issue where the log message “Invalid 5G SNR value” was incorrectly reported as an Error.
	RX55 and XR60: Resolved an issue where SLOT 2 could not be selected for SIM templates with the Association Type “slot ID”.
	Resolved an issue where XR80/90 5G North American routers may experience permanent and irreversible connectivity issues on 5G band n41 used by T-Mobile and Rogers due to an issue in the Qualcomm cellular firmware.
Wi-Fi	
	XR60: Resolved an issue where a WPA2/WPA3 SSID was scanned as WPA3.
	XR80 and XR90: Resolved an issue with inconsistent SSID scan results.
	XR60: Resolved an issue where a notification about an unavailable channel appeared after enabling an additional SSID for the 5GHz AP interface.
	RX55 and XR60: Resolved an issue where the router was unable to connect to SSIDs containing backslash or quote characters.
	XR60: Resolved an issue with Wi-Fi configuration. Removed unsupported 1x1 MIMO option. The XR60 always operates in 2x2 MIMO mode now.

	RX55: Resolved an issue where throughput decreased when the TCP window size was small.
	XR80 and XR90: Resolved an issue where the router did not connect to hidden access points in virtual dual band mode.
	XR80 and XR90: Resolved an issue with long connection times to hidden access points.
	XR80 and XR90: Fixed Wi-Fi connection priorities when connecting to hidden access points..
	Resolved an issue where the remote AP SSID record could not be removed from the Client SSID Database after switching from manual to automatic SSID selection.
	Resolved an issue in the UI where the default channel for 5 GHz with Auto Channel disabled was an unavailable channel.
	Resolved an issue where the Wi-Fi Standard was not displayed on the status page for Wi-Fi Access Points.
	Resolved an issue where the UI showed the incorrect connected access point SSID after switching between different remote access points.
	XR60: Resolved an issue where configuring invalid channel/bandwidth combinations (such as 116 + 40 and 116 + 80) did not prompt a notification and a reversion to a valid setting.
	Resolved an issue where the router Access Point in auto-channel 40 MHz or 80 MHz mode did not follow the Wi-Fi Client when the remote access point moved to channel 165.
	Resolved an issue where Wi-Fi geolocation status was not clear about country support. Added the statuses “Unknown (restricted)” (when the region cannot be determined) and “India (restricted)” (when the geolocated region is not supported).
	RX55: Resolved an issue where the router entered an “Invalid configuration” state when using APs with automatic channel selection.
	Resolved an issue where some connected Wi-Fi clients were not disconnecting properly when the router’s access point was turned off.
	Resolved an issue where the list of Wi-Fi channels was not refreshed according to the Outdoor parameter value when the router’s Wi-Fi region was set to Europe.
	XR80: Resolved an issue where the router was performing a DFS Channel Available Check (CAC) for a Client interface instead of an Access Point interface.
	XR80: Resolved an issue where the Scan Now button did not work when both Client and AP were enabled.
	XR60: Resolved an issue where some manually selected channels and bandwidths produced unexpected broadcast channels and bandwidths.
	XR60: Resolved an issue where the status “Invalid Configuration” appeared after enabling Wi-Fi 5GHz Access Point when Region was set to Global. When the router’s Wi-Fi region is set to “Global”, Wi-Fi AP with 5GHz is not configurable. Status will show “Unknown(Restricted)” with an alert.
	Resolved an issue where a Wi-Fi SSID containing a **[** or **]** character would fail to be preserved following an upgrade to AirLink OS 5.0, causing loss of Wi-Fi connectivity to any SSID with the affected characters.
	Resolved an issue where an upgrade from AirLink OS 4.0 to 5.0 reset any manually configured Wi-Fi SSID priorities to their default values.
Serial	
	Resolved an issue that resulted in incorrect ACL rules when using both Port1 and Port2 in PAD mode.
AirLink OS	
	Fixed a typo in the Status/Monitoring Dashboard Last Logins window.

Resolved an issue where the CPU Load (average) dashboard widget displayed the incorrect labels for load values.
Resolved an issue where undoing a configuration setting (Setting "A") did not undo other changes that depended on Setting "A".
Resolved an issue where the saved settings progress bar showed an incorrect count of modified fields when adding a scanned SSID.
Resolved an issue where edit pages that have no editable fields displayed "Create" or "Edit" in their titles and "Cancel" and "Create" or "Update" buttons (a "Close" button appears now).
Resolved an issue where a dataset could not be edited due to changed or missing datapoint paths after a software upgrade. If datapoint paths have changed after a software upgrade, you can now delete those paths and save the dataset.
VPN
Resolved an issue where, when editing an IPsec Tunnel configuration, a WAN interface that had been disabled appeared in the WAN INTERFACES list as "Value not available".
Resolved an issue where it appeared that VPN data usage could be reported in the dashboard Data Usage chart (a **VPN** label appeared in the chart's legend when a tunnel had been established). This data cannot be displayed, and VPN data usage has been removed from the Dashboard data usage chart.
Resolved an issue where a memory leak occurred when the VPN status was refreshed.
Software Upgrade and Downgrade
Resolved an issue where a device name with a / character (or other special character in the cjson library) did not migrate correctly after a software upgrade, causing existing configurations (port forwarding rules, for example) using that device name to fail.
Resolved an issue where a precisely timed device reboot would prevent the reset to factory defaults after a firmware downgrade from ALMS.
Resolved an issue where all radio module firmware could be deleted upon downgrade and subsequent factory reset. Now, only the firmware that is installed on present radios will persist the downgrade. Note that because this fix is in AirLink OS 5.1, a downgrade to 5.1 (from a later 5.1 version or from 6.0) is required to see the affected changes.
Captive Portal
Resolved an issue where some default values in Extended Captive Portal returned an invalid HTTP response. These default values have been removed.
Location and Telemetry
Resolved an issue where trip odometer and odometer readings for J1939 vehicles were accidentally swapped.
Resolved an issue with location fix error handling by adding a Maximum Vehicle Speed setting under Services > Location. Speeds detected by the router that are above this value will be considered erroneous. Customers should not adjust the setting unless it is absolutely necessary.
Upgrade issue: Resolved an issue where system filters applied to user-created Smart Reporting rules were removed after upgrade. From AirLink OS 5.0 onwards, system filters cannot be attached to user-defined datasets or rules.
Resolved an issue where Remote Location Reports stopped being sent to TCP servers after the router's WAN connection changed.
XR60: Resolved an issue where there was a long delay to update the Wi-Fi region after GNSS was enabled.

Resolved an issue where the router could report Location Fixes that used fewer than three satellites.
Resolved an issue where Telemetry GPIO-related ATP items were not sent to AirVantage.
Resolved an issue where changes in Cellular WAN status were reported after a delay of several minutes.
Resolved an issue where Remote Location Report Sentences were reset to default after upgrade from AirLink OS 4.1 to 5.0.
Resolved an issue where WAN Status changes could be missed and not sent to AirVantage.
Resolved an issue in Location Reporting where ports that had been removed from the Destination Ports list were still sent reports.
Resolved an issue where Remote Location Reports that are configured with UDP had random source ports every time a report is sent out.
Resolved an issue where Telemqtt did not shut down properly when all MQTT Reports were deleted.
Resolved an issue where an erroneous location could be reported in an AMR report.
RX55/RV55: Resolved an issue on radio-based GNSS devices where gnssmgr could undergo multiple start/stop cycles on boot.
Resolved an issue where the GNSS location map appeared in the local UI but might not appear in the ALMS UI due to a lag in satellite count data being provided to ALMS.
XR60: Resolved an issue where the antenna short warning was erroneously displayed.
Resolved an issue where location fixes became inaccurate after several minutes when the router could not receive GPS data.
Templates
Resolved an issue with creating and applying templates containing a LAN segment for a Wi-Fi interface with Client mode. LAN Segment is now templatable for a Wi-Fi Client interface. As a general recommendation, when selecting configurations from tables to be exported to a template, select an entire table row. New configurations can have conflicts with certain pre-existing configurations on target devices. An example is Wi-Fi configurations where a radio is being changed between AP and Client modes. Another is when selecting configuration changes made on system firewall rules.
Resolved an issue where, in template creation mode, it was possible to enter and save passwords that violated minimum/maximum length and character restrictions, causing errors when the template was applied.
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. ▪ DHCP Reservation > Fixed IP Assignment
Resolved an issue where actions such as changing the Local User password, reboot, software update, reset to factory default, or ping/traceroute commands could take effect and apply to the router while in Template mode, and these actions persisted after leaving Template mode.
Apps
Resolved an issue where omitting the 'lanSegments' config.json option would prevent the container from starting.

	Resolved an issue with uploading a Docker image locally. ▪ Starting with AirLink OS 5.1, Docker 25.0.3-built images can be uploaded locally on the device. ▪ Recommend using 24.0.9 or earlier Docker version to build images that will be locally uploaded on AirLink OS 5.0 or earlier firmware. ▪ AirLink OS 5.0 and AirLink OS 5.1 have been tested to confirm that image pull from the registry works also for Docker 25.0.3 images.
	Resolved an issue where the LAN Segment on which the container was running was not retained after a template is applied to the router.
Logging	
	Resolved an issue where the Radio Module Logging filter could not be applied on XR60.
	Resolved an issue where the complete audit logs were not displayed after selecting “All Lines” as a display filter.
Certificates	
	Resolved an issue where expired certificates could show as valid until the router was rebooted.
	Resolved an issue where a certificate, private key, and root certificate added during the template creation process were not applied to a router from the template.
System	
	Resolved an issue where router login failed using TACACS+ authentication after upgrade from AirLink OS 3.1.26 > 4.0.23 > 4.1.31.
ALMS	
	Resolved an issue where an ALMS firmware update operation applied to multiple routers must be fully completed for all routers before you can access a single router's AirLink OS configuration UI through ALMS.

Known Issues

Cellular	
	An issue exists where a virtual APN interface selects the previous APN even though different APNs are given in the SIM Template database.
	An issue exists where, in rare cases, after upgrading from AirLink OS 4.0.23 to 4.1, information about the Cellular interface was not shown in the UI. To resolve, refresh the browser window.
	XR60: An issue exists where the cellular WAN connection was lost during tests when 90 clients (Wi-Fi and Ethernet) were connected with 800 Mps aggregate throughput for mixed applications.
	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/XR60: An issue exists with Wi-Fi Access Point configured with WPA2 Enterprise security mode where failover to a second RADIUS authentication server doesn't occur when the shared secret for the secondary RADIUS authentication server differs from the shared secret for the primary RADIUS authentication server.
	RX55/XR60: An issue exists where the Wi-Fi Client cannot connect to a hidden SSID. Ensure that any SSIDs to which you want the router to connect are visible to the router.
	Although a Timeout field appears in the RADIUS authentication server configuration, the setting is not used in AirLink OS.
	XR60: An issue exists where a Client mode interface only supports 2.4GHz + 5GHz for scanning. This will be remedied in a future release.
	XR80: An issue exists where changing channel on Wi-Fi AP 5GHz doesn't change the channel, and the router continues broadcasting on channel 161. The workaround is to disable and enable the AP.
	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.
	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. Semtech recommends configuring channel separation as wide as possible on Access Points. Configuring adjacent channels is not recommended.
Networking and Connectivity	
	If IP Passthrough is enabled on a cellular interface, and the cellular interface's APN settings changed from single to multiple (or vice versa), disable IP Passthrough before making the APN mode change. After the APN settings are changed, then re-enable IP Passthrough if desired on the cellular interface. Failing to disable IP Passthrough before changing APN modes can result in a state that can only be recovered by a reset to factory defaults.

	An issue exists where Network Watchdog link validation fails when configured without an IPv4/IPv6 FQDN/IP host, and the interface restarts. Link Monitors that are created and applied against a dual stack interface (IPv4/IPv6) must have an FQDN that resolves to an IPv4/IPv6 address. If an IPv4/IPv6 address is preferred, an IPv4 address must be specified in the primary target, and an IPv6 address in the secondary target (or vice versa). Alternatively, the interface can be configured to be only single stack or link validation disabled completely.
	Issues have been observed with high-speed traffic passing through the USBnet interface at times (USB port used as a network interface), where the USBnet interface has been dropped on USB-connected Windows PCs, requiring a router reboot to recover. Please refer to the AirLinkOS online guide in the Hardware Interfaces / USB Interface section for information on setting up the required driver for using USBnet with Windows.
	Upgrade issue: An issue exists where Multi-WAN rules that are applied to IPsec tunnel policies are deleted after upgrading to AirLink OS 5.0.86 from 4.0.x or 4.1.x.
	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.
	QOS: DSCP packet marking does not work. Please contact Semtech 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.
	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	
	XR80 and XR90: The realized maximum throughput for FIPS IPsec tunnels is approximately 40 Mbps to avoid an internal system issue. This issue is not present for non-FIPS IPsec tunnels.
	OpenVPN tunnel names cannot include spaces. Names with underscores or hyphens are supported.
	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.
	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 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 in ALMS where, during an AirLink OS downgrade to a version earlier than 4.1, the "Install application" operation remains in progress after the downgrade was complete. To resolve this issue, confirm that the device is running the desired firmware, and then abort the operation.
Templates	
	When generating a template file from a system that uses dynamic System LAN Segments (as displayed in Networking > LAN Segments > System LAN Segments table), these must ALL be manually selected when creating the template.
	When creating a template with DHCP Relay configuration, the "IPv6 Address" field is not selected by default. Applying a template on the target device will fail if "DHCP Relay IPV6 Server Address" is configured and "IPv6 Address" is missing. You must manually add the "IPv6 Address" field if "DHCP Relay IPV6 Server Address" is configured.
	An issue exists where a disabled configuration setting included in a template as disabled causes an error notification when the template is applied.
	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 setting will fail when attempting to apply the template to a fleet of routers, if the routers have those settings previously configured: ▪ DMZ
AirLink OS	
	If the "Reset Configuration Type" setting is changed but not saved before clicking the "Reset Settings" button, the system will reset according to the previously saved "Reset Configuration Type". This is expected behavior as the "Reset Configuration Type" setting is not used until it has been saved.
	An issue exists where the AirLink OS local access URL https://airlink./ (as shown in some Quick Start Guides) 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
ALMS
ALMS currently does not support communication over IPv6.
An issue exists where a software update in ALMS fails when the router is power cycled while the software is being downloaded or installed.
An issue exists when using a CSV file in ALMS to configure AirLink OS routers where the file application fails with an unnamed "Bad data type" error. If you see this error, Semtech recommends using the AirLink OS UI or AirLink OS templates to configure these settings.
An issue exists where, under Networking > Diagnostics > IP Capture, the in-progress button continues to spin after an IP capture is completed.
Location and Telemetry
Semtech recommends that customers should not modify system-defined reporting rules, triggers, or datasets. Modified system-defined rules may not migrate correctly after upgrading to AirLinkOS 5.1. If you have modified system-defined rules, you must create user-defined rules/triggers/datasets and reset system-defined rules before upgrade. If a reporting rule status is "error: unable to load" after upgrade, you can resolve the issue by editing the trigger used by the rule (for example, the [System] Status Report Trigger under ALMS > Smart Reporting > On Change Trigger Conditions) and adding one or more datasets to the trigger.
After a direct upgrade from AirLink OS 4.1 to AirLink OS 5.1, any system trigger used in a user-defined reporting rule (under ALMS > Smart Reporting > Reporting Rules) will be changed. System triggers can no longer be used for user-defined reports, so a new trigger is automatically defined, but the new trigger uses a fixed period (15 minutes) instead of the "on change" system trigger that may have been used prior to the upgrade. Affected customers should review the settings for the new report trigger and adjust as required.
An issue exists where an HPUE external modem cannot report the modem's WAN IPv6 address. The transport of IPv6 traffic is not in any way affected.
An issue exists where Dead Reckoning options for Ignition Parking Mode are shown, and can be selected, for routers that do not support Dead Reckoning. For these options, the router will continue to report location fixes received while parked.
While using GNSS Remote Reporting with UDP transport, reports may be lost while WAN connectivity is unavailable
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.

Certificates
An issue exists where, when creating a template from scratch for a configuration that includes a generated certificate (for Wi-Fi or VPN, for example), after applying template to another router, the certificate appears as “Untrusted” in the Imported Certificates table. To avoid the issue, while in template-creation mode, go to System > Security > Certificates > Generated Certificates and de-select and select the certificate's checkbox again.
The Private Key field in certificate configuration behaves like a password during template creation. You must manually set the Private Key value to add it in the template file. The Private Key field is not automatically added when creating a template from current configuration.
Generated Certificates: An issue exists where using a dataset and CSV file in ALMS to set a custom common name for a device, when the USE SERIAL NUMBER FOR COMMON NAME field is enabled while creating the dataset (then later disabling USE SERIAL NUMBER FOR COMMON NAME in the CSV file), applying the CSV file fails. Semtech recommends that the USE SERIAL NUMBER FOR COMMON NAME setting always be disabled before using a CSV file to set a custom name for a device.
An issue exists where applying a template that includes generated certificate settings produces an internal error message in ALMS, although the template is applied correctly. To avoid the issue, when creating a template on a router with generated certificates that use Device Serial Number as common-name, edit all the generated certificates (using Device Serial Number as COMMON NAME) on the router (in the Certificate Signing Request settings menu) and de-select the COMMON NAME field before saving the template.