AirLink OS 4.1

RELEASE NOTES

About AirLink OS 4.1

This release of AirLink OS 4.1 is 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
- Security
- 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.

Sierra Wireless has tested and validated upgrading to AirLink OS 4.1 from the following releases:

- 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 installed before they can be upgraded to AirLink OS 4.1. Direct upgrade to AirLink OS 4.1 from AirLink OS 3.1 and earlier is not supported.*

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.

Note: The LPWA radio module firmware update can take five minutes.

New Features and Enhancements

EM9190 and EM7690 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 03.09.11.00
- AT&T: 03.09.11.00
- FirstNet: 03.09.11.00
- T-Mobile: 03.10.07.00
- Generic: 03.10.07.00
- Bell: 03.09.11.00
- Telus: 03.09.11.00 (not certified)
- Rogers: 03.10.07.00
- Telstra: 03.04.03.00
- Softbank: 03.09.03.00
- Docomo: 03.10.07.00
- KDDI: 03.10.07.00

XR90/XR80 with new EM9190 radio modules: Supports additional 5G SA and NSA bands n7, n8, n12, n20, n25, n38, n40, n48 (plus LTE B43).

Indicated bands are supported on XR80/XR90 routers manufactured with an IMEI starting with “351”. Routers with an IMEI starting with “350” do not support these bands.

Added APN, ICCID and PLMN information and carrier-certified radio modem configuration for Softbank, Docomo and KDDI.

T-Mobile, Rogers and Generic Radio Module Firmware has been updated to prevent the n41 band issue described in this bulletin.

EM7411 and EM7421 Radio Module Firmware

Carrier Firmware Matrix:

- Verizon: 01.14.20.00
- AT&T: 01.14.13.00
- FirstNet: 01.14.13.00
- T-Mobile: 01.14.03.00
- Generic: 01.14.13.00
- Sierra (EM7411): 01.14.03.00
- Sierra (EM7421): 01.14.07.00

Networking

XR80/XR90: Removed the LPWA interface from the default “WAN” zone. The zone “WAN (No LPWA)” has been removed, and has been replaced with the “WAN” zone in existing rules for ACL input/output interfaces, watchdog references, and Multi-WAN policy egress interfaces.

Note: User rules that used the “WAN” zone in AirLink OS 4.0 will automatically use the new “WAN” zone, and so will not include the LPWA interface. System rules that previously used the LPWA interface will continue to do so.

Added the ability to display external modem information for HPUE modems connected through Ethernet. This feature has been validated with API version 2.3.56.

Added DHCP Option 119 UI support when creating a LAN segment under Networking > Zone Settings > LAN Segments > CREATE LAN SEGMENT > Domain Search List.

Enhanced IP Passthrough configuration. When IP Passthrough is enabled on an interface and its Destination Allocation Mode is set to Select From List, only devices connected to the selected interface or set as the passthrough destination on another interface will appear on the list.

Cellular	
	Added the ability to add and edit a SIM PIN as a security mechanism to prevent SIMs being used in unauthorized devices. After you have set the PIN for the SIM, the SIM PIN is required any time you need to update the SIM configuration.
	Added slow flashing red/yellow LED state to indicate a SIM and Radio Module Firmware mismatch.
	Removed MIMO options from the Cellular Configuration screen. 5G and LTE CAT-20 XR Series routers can only be used with 4x4 cellular antennas.
Wi-Fi	
	XR90/XR80: Added “virtual dual band” WI-Fi WAN capability.
	Added Simple Captive Portal to offer a customizable landing page for Wi-Fi users.
Ethernet	
	Added an alert to recommend WAN AUTO DETECT be disabled before deploying into the field, and that the Ethernet ports are manually configured for LAN or WAN.
VPN	
	Added a new Source NAT firewall rule.
	Added the ability to select and prioritize the VPN tunnels.
	Added IPsec Status under Networking > IPsec Status .
AirLink OS	
	Enhanced radio module firmware management with: • Ability to store only one image when it is shared across two or more radios • Automatically add new radio module firmware to the Radio Module table after a software upgrade that adds a new carrier for the current SIM • After upgrade, the radio uses the new RMFW appropriate for that SIM (if Network Operator Switching is enabled).
Logging	
	Doubled the size of the audit logs partition in order to capture events over a longer period of time. These logs do not auto-rotate.

Templates	
	Reformatted identifiers for the following settings so that partial templates can be supported across a fleet of routers: • SIM Database/SIM Templates • GRE Tunnels • IPsec Tunnels • Wi-Fi Client • LDAP/RADIUS/TACACS+ • User accounts • Certificate Store • Firewall and Port Forwarding Rules *Note: If you configure routers using templates, ensure you create new templates based on AirLink OS 4.1, especially if you need to configure any of the settings listed above.* *Note: For features that have been updated as above, configuration identifiers are no longer editable, such as VPN names and SSIDs. For example, after manually creating an SSID in the Client SSID Database, you cannot change the SSID (to fix a typo or rename the SSID, for example). You must delete the entry and recreate it.*

Bug Fixes

Templates
Resolved an issue where certificate .pem file content was not added to a template.
Resolved an issue where a template created from the current configuration included some LPWA “Known SIM” configuration items, which caused errors when the template was applied to another router. LPWA SIM settings are no longer included by default in the default template.
Resolved an issue where a “Reset to template” (under Reset Configuration Type) setting inside a template could not be applied on ALMS.
Resolved an issue where configurations could be created or deleted while in template mode. Now only modifications of existing settings are allowed in template mode.
Resolved an issue where selecting an setting inside a table for a template would occasionally cause the template to fail when applied.
Resolved an issue where, using the “Create from current configuration” option on the same router with the same configuration, the number of fields in the template did not stay consistent when creating the template on different occasions.
Resolved an issue where it was possible to enter Dataset mode while in Template mode.
Resolved an issue where the Web UI could crash after creating a template from the current configuration and then deselecting several fields.
Resolved an issue where the UI in template mode would still receive data updates, forcing the end user to verify that the desired data was still in the template. Now UI data is not updated from the router or AirVantage when the UI is in template mode.

Resolved an issue where WAN Outputs could not be changed in a User Policy showing under the System Policies table when using the “Modify a template from local file” option.
Resolved an issue where, in template mode, the UI showed the template checkbox disabled (and thus not clickable) on a disabled field.
Resolved an issue where applying a template created from a current configuration containing multiple features could take a long time, with any “Undo” actions being slow to respond to clicks.
Resolved an issue where template file contentswere inconsistently exported.
Resolved an issue where the router failed to recover its radio module firmware after a template was applied to the router at the same time it was undergoing an AirLink OS software downgrade. In general, do not launch multiple operations (such as software downgrade and apply template) simultaneously on the same router.
Resolved an issue where a template checkbox was displayed for the installed radio module firmware in the Radio Module Image Management > Radio Module Firmware table. The setting was not intended to be selectable.
Resolved issues with saving template files by preventing any changes to settings from AirVantage or the local UI while in template mode, and not adding settings that are at factory default to the template.
Networking and Connectivity
Resolved an issue where it was possible to create and then misconfigure a new LAN segment, resulting in an error that could not be resolved by editing, deleting or re-creating the LAN segment.
XR80/XR90: Disabled some messages for the FTP, SIP, PPTP and NAT-T protocols from hardware acceleration to resolve issues with NAT traversal in some cases.
Resolved an issue where, in a Multi-WAN scenario involving at least three WAN interfaces (including a Cellular interface with IPv6 only enabled), a lower priority route could be used even when higher priority interfaces are available.
Resolved an issue where, when IP Passthrough is used, the gateway provided to the LAN-connected device was not within the subnet of the IP address provided to the LAN device.
Resolved an issue where the Edit option was available for all Multi-WAN rules, when the Edit option is only applicable to Signal Strength rules.
Resolved an issue with IP Passthrough where the targeted Ethernet port toggled on and off when a host MAC address target was unavailable.
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.
Resolved an issue where, after upgrading AirLink OS, the LPWA watchdog rule link validation could be incorrectly enabled.
Resolved an issue where, when the masquerade option was disabled or re-enabled on a WAN interface, the change did not take effect for existing flows from Ethernet or Wi-Fi LAN hosts sending traffic over the WAN interface.
Resolved an issue where, after upgrading to AirLink OS 3.1 to AirLink OS 4.0, Masquerading was enabled by default on all WAN interfaces for IPv4 traffic. This issue does not apply when upgrading from AirLink OS 4.0 to AirLink OS 4.1.

Resolved an issue where pings sent from a specific WAN interface (not the Default WAN) were reported as receiving no response and packet loss in ALMS, when in fact the ping responses were received but were dropped because the echo reply packet size did not match the echo request packet size.
Resolved an issue where starting a ping from a source interface part of a bridge was not possible.
Resolved an issue where a kernel panic and subsequent reboot could occur when the only active WAN interface(s) on the router are multi-APN virtual interface(s) and Wi-Fi LAN clients were connected to the router in Wi-Fi Access Point mode.
Resolved an issue where, when a WAN link went down, link validation correctly applied to the link when the link re-connected. However, link validation was also done for other links that did not go down. This caused some unnecessary policy route changes because links were temporarily marked as “not validated.”
Resolved an issue where the UDP PAD server did not work when using the IP Passthrough cellular feature and when LISTEN FOR CONNECTIONS (AUTO-ANSWER) was enabled.
Cellular
Resolved an issue where, after switching configurations from multi-APN to single-APN, the Cellular interface stopped passing traffic.
Resolved an issue where, after a switch to backup image (downgrading AirLink OS) along with a re-install of the backup firmware to update the radio module firmware table, the radio module firmware table contained multiple entries for the same carriers applicable to the backup firmware and the previous firmware.
Resolved an issue where the “SELECT A FIRMWARE” list shown in the Create Radio Module Firmware screen contained firmware that was already installed on the router.
RX55 with EM7421: Resolved an issue where the Cellular LED was flashing red when the Adapter Status was connected and the radio module firmware table showed invalid data after upgrading and downgrading AirLink OS.
Resolved an issue where EM9190 radio module measured transmit power was higher than expected with Smart Transmit applied.
Resolved an issue in Multi-APN mode where the default APN was connected even when it wasn't included in the APN list.
XR80: Resolved an issue where, after disabling a Cellular interface, the Media Status remained “up” and Adapter Status remained “Connected”.
Resolved an issue where ALMS could persist in reporting the cellular Adapter Status as “No Service” when the cellular interface is connected and reporting the correct status to ALMS.
Resolved an issue where, after a firmware upgrade from 3.0.xx or 3.1.xx to 4.0.xx (up to 4.0.23), the Radio Module Firmware upgrade for the XP Cellular interface did not occur until the router was rebooted.
Configuring different Preferred Technology settings for two Multi-APN virtual interfaces causes “No Service” on the first virtual APN to be configured.
For XR90/XR80 configured with Cellular Multi-APN mode, an issue exists where, after an upgrade, a reset to factory defaults, and a template application, the Cellular LED may flash red even though the Cellular interfaces (including Virtual interfaces) are connected and passing traffic. To restore the Cellular LED behavior, disable/enable the Cellular interface or reboot the router.

Resolved an issue where new radio module firmware was installed on the router (with Cellular Interfaces disabled and no SIM card) during a software upgrade, but not applied to the radio module after the interfaces were enabled. The router required a reboot for the radio module firmware to be installed on the radio for the interfaces to begin using the new firmware.
Resolved an issue where, in rare circumstances, with repeated networking or VPN configuration changes, it was observed that a Cellular interface could indicate that it is connected, but have no IPv4 address or WAN functionality.
Resolved an issue where the Cellular Configuration UI was missing after resetting the router to a template that disabled the Cellular interfaces.
Moved the “Cellular_manager: Transaction Timeout for AT+KSREP?” message to debug level so that it is not logged by default.
Wi-Fi
Resolved an issue where the router’s own AP SSIDs appeared in the SCANNED SSIDS list.
Resolved an issue with the router in WAP-2 Enterprise Client mode where the router would not connect when the SSID and credentials were too long.
Resolved an issue where WPA2-Enterprise could be configured without a RADIUS Server on additional SSIDs.
RX55: Resolved an issue where Wi-Fi Signal Bars sometimes read 0 after reconnecting when RSSI was good.
Resolved an issue where, after setting a Wi-Fi interface IP Assignment Method to “static” and not configuring a DNS server (as required by such a configuration), traffic could flow normally over the interface but eventually disconnect unexpectedly.
XR80: Resolved an issue where, when moving from AP + Client to only Client enabled, connecting on wpa3 failed until the router was rebooted.
RX55: Resolved an issue where the router did not connect to a WPA2-PSK SSID with SHA256 and PMF required.
Resolved an issue where it was possible to enter an SSID name over 32 characters long.
Resolved an issue where the XR80 router could not connect to an access point with a hidden SSID.
Resolved an issue present in AirLink OS 3.1 where “Wi-Fi_recovery” messages flooded the logs.
RX55: Resolved an issue where non-ASCII characters were not displayed properly in the Scanned SSIDs list.
RX55: Resolved an issue where Ethernet LAN to Wi-Fi throughput could be lower than expected on DFS channels.
Resolved an issue where a laptop could not connect to Wi-Fi using WPA2 Enterprise, with authentication passing through an IPsec VPN to a RADIUS server.
Resolved an issue where, after enabling the DISABLE APS ON CLIENT ASSOCIATION feature, the feature could not be disabled using the Enable/Disable button until the timer had expired.
XR80: Resolved an issue where the router did not connect to a remote AP configured to use WPA3 as its authentication type.
Location and Telemetry
Resolved an issue where unsupported settings were displayed under Services > Telemetry > MQTT.

Resolved an issue where GNSS custom reports were not being sent to their server at the remote end of a VPN tunnel.
Resolved an issue where telemetry data from the router did not pause and resume when the LPWA connection was lost and recovered.
Improved message filtering to resolve an issue where unrealistic location fixes were reported by the GNSS module.
Resolved an issue where the GNSS State under Services > Location stayed in the “Firmware Upgrade Complete” state and a location fix could not be obtained after a GNSS firmware upgrade.
Resolved an issue where Location Reporting sent NMEA reports that were flagged as invalid.
Resolved an issue where it was possible to interrupt a GNSS firmware update with a user-initiated reboot of the router.
Resolved an issue where an inaccurate Trip Report may have resulted from an improper shutdown of the router during the trip.
Resolved an issue where Custom Reports configured to GENERATE THIS REPORT AT POWER OFF were not sent to the MQTT server when the router was powered off.
Resolved an issue where GNSS sometimes did not report at the expected intervals, resulting in inaccurate Trip Reports.
Apps
Fixed an issue that prevented deleting a container volume when it included nested folders created by the container application.
Fixed an issue where the container image failed to load when it contained files included in folder with no user write permission.
Resolved an issue where, when using an archive to populate a container volume in Apps > Container Applications > Volumes > Create Container Volume > Upload archive, the content of the archive was extracted at each device boot, possibly overwriting changes made to that content by some application.
Resolved an issue where, after applying a template that enables Container Applications and creates an image to be pulled from a registry, the router failed to pull the image.
Resolved an issue where a race condition temporarily prevented a new Volume from being created and added while editing a Container Application.
Fixed an issue for container applications which led to incorrect file permissions for the application image files, and difficulties to use non-root user from within the container application.
Fixed an issue which led to container application images being incorrectly setup: when having several image layers; it could led to file modifications not taken into account properly: file deletion, file permission change, file addition or content change could be inconsistent.
Fixed an issue where, after disabling Container Applications at Apps > Container Applications > General Status, running applications continued to run.
Resolved an issue where some system resources were not cleared after disabling Container Applications, leading to unnecessary flash usage and potential errors.
AirLink OS
Resolved an issue where it was not possible to re-install the previously active firmware on the router after a roll-back to a previous version occurred.

	Resolved an issue where the name of the Current Template was not properly displayed under Admin > Reset Settings.
	Resolved an issue where ALMS customers were not notified when they did not have the required server.notification rights to receive data updates.
	The log-in window legal banner feature will allow only HTML tags related to text formatting. Other tags will not be rendered.
	Resolved an issue with inconsistent display of configuration errors in the “modifying settings” status bar.
	Resolved an issue where the log-in window displayed incorrectly after firmware upgrade or reboot.
	Resolved an issue when commands were put into a configuration edit page.
	Dashboard Data Usage pie charts now show WAN TX bytes and RX bytes.
	Resolved an issue where some edit pages would cause errors (showing modified fields) after being opened and updated with no changes made to settings.
	Resolved an issue where logging into AirLink OS in two browser tabs caused unexpected behavior. You can now log into AirLink in only one browser tab or window.
	RX55/XR80: Resolved an issue with Edge browsers where items in a dropdown menu could not be selected after clicking the arrow icon.
	Resolved an issue with inconsistent behavior in Dataset Mode, where the status bar displayed added items differently depending whether they were added from a table by clicking “Add Table to Dataset” or by selecting individual columns in the same table.
	Resolved an issue where the Time > NTP > Update Interval was shown as a decimal value instead of hours/minutes/seconds.
	Resolved an issue where a UI glitch could occur after selecting a WAN interface in the USER-DEFINED POLICIES section of the Multi-WAN configuration menu with a narrow window (approximately 1300 px).
VPN	
	Resolved an issue where the IPSec Tunnel Dead Peer Detection timer value could not be changed to a non-default value.
Extended Captive Portal	
	Resolved an issue where the Extended Captive Portal client used a different WAN interface than the WAN interface configured for captive portal.
Logging	
	Resolved an issue where the message “The interface mss.mode is read as empty. Cannot create ACL rule” was misreported at the “Error” level for non-cellular interfaces. This message is now logged at the “Debug” level.
Hardware	
	Resolved an issue where disabling the Voltage Threshold settings (MCU > Voltage Threshold) did not cause the router to use its default Standby Voltage, Resume Voltage and Delay settings. The router continued to use the settings that were set previously.

Security

General
Added extra input validation on some Captive Portal settings.
Deprecated aes256-ctr and aes128-ctr ciphers.
Updated OpenSSL to 3.0.

Known Issues

Cellular
5G SA bands are not available when using Telus radio module firmware.
An issue exists where, after entering the SIM PIN, the SIM PIN field indicates an incorrect entry with the text “SIM PIN should be 4 to 8 digits long”, although the entry is valid and can be saved to the router.
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.
An issue exists where the option “5G-SA Only” appears in the Preferred Technology menu when the router has a non-5G radio module.
RX55: During throughput testing for low packet sizes, the router occasionally entered an Out of Memory state and rebooted.
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 the radio disconnected from the 5G network, stayed connected to LTE, but reported that the Service Type was NR5G (NSA) with a 5G band.
An issue exists where, when an XR Series router is connected to a 5G network, LTE primary band info is not shown under System > Radio Module.
RX55: When adding EM7411 radio module firmware to Radio Module Image Management, a validation error indicates the addition will exceed the maximum number of entries in the table. The error message appears even when there are available entries in the table. Despite the error message, the radio module firmware is added to the device when there are available entries in the table.
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
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.
An issue exists where Auto Channel selection can select a channel that is not on the available channels list when the XR80/90 Access Point is set for the EU Region with DFS channels enabled. To resolve, disable AUTO-CHANNEL and manually select a channel from the list.
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, after an XR series router Client fails to connect to an XR series router Access Point, the XR series router Client does not automatically try to connect to another access point. To resolve, assign non-equal priorities to the SSIDs of the remote access points.
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.
XR80/XR90: Do not support connecting to WPA-PSK-TKIP networks.
RX55: Does not support connecting to a Cisco 9117AX access point when configured to broadcast a WLAN on 2GHz and 5GHz bands with WPA2.
AirLink routers configured with PMF (802.11w) Required do not support connecting to some access points (such as Aruba) using WPA2 Enterprise.
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.
In general, in any Wi-Fi application, 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

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.
After changing the Ethernet interface IP address assignment from DHCP to Static and assigning a static IP address, a reboot is required before the interface can pass traffic.
An issue exists where a device connected to the router via Ethernet does not get a new LAN segment IP address after the LAN segment on the Ethernet port has changed. To ensure the IP address of the device is updated, do either of the following: • Disable and re-enable the Ethernet port from the UI. • Disconnect and then reconnect the Ethernet cable to the device.
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.
An issue exists where USBNet may stop working on a Windows 10 device. To recover the link, reboot the router.

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.
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.
RX55: The throughput for the UDP traffic over the Cellular interface can be low, especially for small packet sizes.
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 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 where any Multi-WAN rules that apply to IPsec Policies for Client Tunnels are removed after the router reboots. To avoid this issue, and if it is acceptable to use the VPN WAN priority system wide: 1. Set WAN INTERFACES to “default” under Networking > VPN > Configure. 2. Edit the WAN Output(s) to match the desired WAN priority for the default policies “Default IPv4 Traffic” or “Default IPv6 Traffic” under Networking > Multi-Wan Policies > System Policies. 3. Add Multi-WAN rules to the “Default IPv4 Traffic” or “Default IPv6 Traffic” policies.
An issue exists where, when VPN tunnels are disabled or in a “Connecting” state, clicking the REFRESH button on the Networking > IPSec Status page produces a Command execution alert in the UI.
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.
When the XR90 is used as the VPN server, the tunnel can be established, but bi-directional ping traffic does not work. Please contact Sierra Wireless for assistance with this issue.
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.
An issue exists where, when editing an IPsec Tunnel configuration, a WAN interface that has been disabled appears in the WAN INTERFACES list as “Value not available”.
The minimum VPN failover time is approximately 48 seconds, regardless of DPD timeout.
With an IKEv2 LAN-to-LAN tunnel established, if the primary VPN server goes down and Dead Peer Detection (DPD) fails over to a secondary server at the same time as a WAN interface switch occurs, the tunnel may repeatedly connect/disconnect as DPD erroneously detects failures on the secondary server.
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. If this occurs, run the software update again.
An issue exists 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). To display the names correctly, reboot the router.
An issue exists where, after a software upgrade from AirLink OS 3.x to 4.0, the HL8700 (LPWA) radio module firmware is not updated to 4.6.9.4. The radio module firmware is updated when the AirLink OS software is upgraded again.
An issue exists where, after a software upgrade, the Radio Module Image Management table is full and 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 a 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.
An issue exists where a template created from the current configuration can include the “system-defined” LAN segment created when IP Passthrough is configured; this template can cause errors when applied to other routers. To resolve the issue, review any “Templated System LAN Segments” included when creating a template, and manually exclude the LAN Segment associated with the IP Passthrough configuration (this LAN Segment will use the same “IPv4 Pool Starting Address” and “IPv4 Pool Ending Address” values).
While in Template mode, actions such as changing the Local User password, reboot, software update, reset to factory default, or ping/traceroute commands can still take effect and apply to the router, and these actions will persist after leaving Template mode.
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: • Smart Reporting • LAN Segments • DHCP Reservation > Fixed IP Assignment • DMZ • Network Watchdog > Monitoring Rules • Multi-WAN
AirLink OS
An issue exists where it is 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.
An issue exists under Diagnostics > Radio Module Log, where non-cellular radio WAN interfaces are listed in the Radio menu.
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.
XR90: An issue exists where, after disconnecting an XP cartridge and performing a software upgrade, the disconnected cartridge still appears as installed under System > Radio Module Image Management.
ALMS
An issue exists where, under Networking > Diagnostics > IP Capture, the in-progress button continues to spin after an IP capture is completed.
Cellular interfaces and virtual interfaces are unsorted in the Hardware Interfaces and Status Monitoring pages in ALMS.
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 ignition status may not be reported to ALMS. This affects AMR Trips Reports, where different trips are merged because of missing ignition start and end markers. The issue exists for routers running AirLink OS 3.x with Telemetry Service enabled that were upgraded to version 4.0.x. Note that Telemetry Service is disabled by default in AirLink OS 3.0 and later, so routers upgraded from AirLink OS 3.x to 4.0.x with Telemetry Service disabled before the firmware upgrade are not affected. To resolve the issue, please contact Sierra Wireless for assistance, or reset the router to factory default settings after upgrading to 4.0 or later.
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
An issue exists where it is possible to configure “privileged” ports 1 to 1023 for TCP PAD operation and other services. Such services will not work on these ports.
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.
An issue exists where the remote splash page does not download due to WAN unavailability after a router reboot. When the router has established a WAN connection, to prompt the router to download the remote splash page, disable and re-enable the Simple Captive Portal, or wait for the Server Interval to expire.

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.