SIERRA WIRELESS IS NOW SEMTECH®

# AirLink OS 5.2

## RELEASE NOTES

# About AirLink OS 5.2

This release of AirLink OS 5.2 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.

**Warning:** *An issue exists when downgrading XR80 or XR90 routers with serial numbers starting with 'FF' or 'FG' (that have EM9190 radio modules installed) to AirLink OS 5.0.86 or prior—this issue does not exist with XR80 or XR90 routers with other serial numbers. If you have downgraded AirLink OS to 5.0.86 or prior, the LPWA radio may not connect. If this occurs, please upgrade to either AirLink OS 5.1.78 or 5.2 to restore service.*
*If upgrading does not restore service for the LPWA radio, and you have ensured the XR80/XR90 is activated in ALMS and the router has a connected LPWA antenna and is located in an area where service is available, please contact Semtech technical support.*

**Warning:** *AirLink OS 5.2 introduces the EM9293 radio module for AirLink XR80 Gen2 and XR90 Gen2 routers. Software downgrade to AirLink OS versions earlier than 5.2 is prevented on these routers.*

# Change of Behavior Notices

| Type | Component | Description | Target Version | Action |
|---|---|---|---|---|
| Obsolete | Wi-Fi | WEP is no longer supported as of AirLink OS 5.1 due to its security issues.<br>Semtech expects this will not affect any users, as WEP is currently only supported in the RX55 and fails to connect to WEP-based APs today. | 5.1 | If using WEP, modify your AP to use a supported security mode. |
| Behavior change | Wi-Fi | AirLink OS 5.1 removed the indoor/outdoor switch that could enable the 5170–5350 MHz 5GHz Wi-Fi frequencies (DFS channels) for Australia, EU, and UK routers.<br>AirLink OS 5.2 restores the switch, although it only enables the 5170–5250 MHz range. | 5.2 | When upgrading from 5.0 to 5.2 with the switch enabled, the switch will remain enabled. A notification will indicate that the 5250–5350 range is no longer acceptable for regulatory compliance.<br>If additional channels are required, consider enabling DFS Channels. |
| Behavior change | Wi-Fi | The Client Isolation default setting will change to Enabled. | 7.0 | No action required. |
| Deprecation | Apps | 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.<br>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. |

# New Features and Enhancements

| | |
|---|---|
| **Cellular** | |
| | Added the ability to configure a Monitor Rule to act as a connection lost trigger for Auto SIM Switching. |
| **Wi-Fi** | |
| | Reintroduced the indoor/outdoor switch to allow the 5170-5250 MHz 5GHz Wi-Fi frequencies for Australia, UK, and EU-based models. |
| **Container Applications** | |
| | Added support for configuring the RAM limit for each container. The default RAM limit is 100 MB, and the upper limit is restricted to the router model's RAM limit. |
| **Security** | |
| | Changes required for AirLink OS 5.2 to comply with the cybersecurity requirements for Radio Equipment Directive (RED) EN 18031-1:2024 and EN 18031-2:2024. |
| | Additional security updates. |
| **Telemetry** | |
| | MQTT now supports communication over TLS. |
| | Added a new MQTT configuration option for customers to use serial number as the MQTT Client ID. The default Client ID is now blank, instead of the previously used "swi". |
| **System** | |
| | Added a setting to clear all user-generated data from the router with a reset to factory defaults. |
| **EM9190 and EM7690 Radio Module Firmware** | |
| | **Carrier Firmware Matrix:**<br>▪ AT&T: 03.14.10.04<br>▪ FirstNet: 03.14.10.04<br>▪ Bell: 03.14.10.01<br>▪ Generic: 03.14.10.04<br>▪ Rogers: 03.14.10.01<br>▪ Telstra: 03.10.07.00<br>▪ Telus: 03.14.10.00<br>▪ T-Mobile: 03.14.10.01<br>▪ Verizon: 03.14.10.00<br>▪ Softbank: 03.10.07.00 (EM9190 only)<br>▪ KDDI: 03.10.07.00 (EM9190 only)<br>▪ DOCOMO: 03.10.07.00 (EM9190 only) |
| **EM9293 Radio Module Firmware** | |
| | **Carrier Firmware Matrix:**<br>▪ AT&T: 02.15.01.00<br>▪ FirstNet: 02.15.01.00<br>▪ Generic: 02.15.01.00<br>▪ T-Mobile: 02.15.01.00<br>▪ Verizon: 02.17.08.00 |

| EM9291 Radio Module Firmware |
|---|

**Carrier Firmware Matrix:**

- AT&T: 02.15.01.00
- FirstNet: 02.15.01.00
- Bell: 02.15.01.00
- Generic: 02.15.01.00
- Rogers: 02.17.08.00
- Telstra: 02.17.08.00
- Telus: 02.15.01.00
- T-Mobile: 02.15.01.00
- Verizon: 02.17.08.00

| EM7411 and EM7421 Radio Module Firmware |
|---|

**Carrier Firmware Matrix:**

- AT&T: 01.14.22.00
- FirstNet: 01.14.22.00
- Bell: 01.14.13.00
- Generic: 01.14.22.00
- Rogers: 01.14.03.00
- Sierra: 01.14.03.00
- Telus: 01.14.03.00
- T-Mobile: 01.14.03.00
- Verizon: 01.14.24.00

| HL7800 Radio Module Firmware |
|---|

**Carrier Firmware Matrix:**

- AT&T/FirstNet: 4.7.1.4
- Sierra: 4.7.1.4

# Bug Fixes

| Cellular |
|---|
| Removed PLMN 315-010 from the T-Mobile list of networks so that the GENERIC radio module firmware is used by default when using private networks. |
| **Networking** |
| Resolved an issue with IP Passthrough mode where a specific type of network traffic could trigger a packet with an invalid source address to be sent from the cellular interface. These packets could result in cellular disconnects on some carriers. |
| **Serial** |
| Resolved an issue where inbound TCP PAD connections were not being established via a Host-to-LAN VPN. |
| **Location and Telemetry** |
| Resolved an issue where GNSS logging that indicated GNSS Location Fix acquisition or loss was missing. |
| RX55: Resolved an issue where GNSS Antenna Current and GNSS Antenna State could be selected for telemetry reports when the router does not support this capability. |
| XR60: Resolved an issue where Geolocation displayed the Country as “Unknown” after a location fix was acquired. |
| Resolved an issue where the default MQTT Client ID of “swi” caused MQTT disconnections. |

| | |
|---|---|
| | Resolved an issue where modified system-defined rules may not migrate correctly after upgrading to AirLink OS 5.1. If you have modified system-defined rules, you must create user-defined rules/triggers/ datasets and reset system-defined rules before upgrade.<br>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. |
| | XR60: Resolved an issue where the data required for ALMS AMR reports was not being uploaded in some cases. |
| | Resolved an issue where some MQTT reports were not sent. |
| **Software Upgrade/Downgrade** | |
| | Resolved an issue where ALMS communication could not be established following an AirLink OS firmware upgrade in some cases. |
| | Resolved an issue where downgrading AirLink OS software would not also downgrade the radio module firmware to the correct version. After downgrade, rebooting the router would update the router with the correct radio module firmware. |
| | Resolved an issue in ALMS where, during an AirLink OS downgrade to a version earlier than 4.1, the "Install application" operation remained in progress after the downgrade was complete. |
| **Certificates** | |
| | Resolved an issue where the Private Key field in certificate configuration was not added when creating a template from current configuration. |
| **Logging** | |
| | Resolved an issue with excessive error messages for the Wi-Fi Client 5GHz by lowering "Failed to set scan ESSID" log level. |
| **ALMS** | |
| | Resolved an issue where location data upload for the ALMS Tracker widget could be delayed. Configuration is supported to ensure that the required data is uploaded in a timely manner. |

# 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. |
| | 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. |

| Wi-Fi |
| --- |
| XR60: An issue exists where repeated configuration changes to add/remove Wi-Fi SSIDs on the XR60 AP may cause the SSIDs to stop accepting connections and passing traffic. A reboot of the XR60 after the configuration changes are complete will recover proper operation. |
| Although a Timeout field appears in the RADIUS authentication server configuration, the setting is not used in AirLink OS. |
| 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 |
| --- |
| An issue exists where a WAN interface that has IP passthrough enabled can be added to a Multi-WAN policy rule, which is an incompatible configuration.<br><br>In general, AirLink OS configuration changes (performed manually or using a template) can generate errors when they are blocked by incompatible configurations elsewhere on the router. |
| 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. |

| |
|---|
| 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. |
| IPv6 DNS Propagate fails for the Ethernet WAN interface. Manually configured DNSv6 servers are not propagated from WAN to HOST-PC on the LAN. |
| **VPN** |
| IPsec tunnels in AirLink OS do not use UDP encapsulation when there is no NAT between the VPN server and the VPN client (both endpoints use routable IP addresses). Carriers may sometimes drop raw ESP packets if they are not UDP encapsulated. An option to force UDP encapsulation for this case will be added in a future AirLink OS release. |
| CoovaChilli Captive Portal and OpenVPN are not compatible. You can configure only one or the other on the router; not both. |
| XR80 and XR90: The realized maximum throughput for FIPS IPsec tunnels is around 40Mbps 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. |
| 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. |
| **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. |

| | |
|---|---|
| **AirLink OS** | |
| | An issue exists where the AirLink OS local access URL https://airlink./ (as shown in older Quick Start Guides) does not work on computers running Ubuntu. Use https://192.168.1.1 instead. |
| **ALMS** | |
| | 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. |
| | ALMS does not support communication over IPv6. |
| | 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** | |
| | 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. |
| **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.<br>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. |
| | 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. |

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