SIERRA WIRELESS IS NOW SEMTECH®

AirLink OS 5.3

RELEASE NOTES

About AirLink OS 5.3

AirLink OS 5.3 is a minor release for the AirLink XR90, XR80, XR60 and RX55 routers. 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.

Change of Behavior Notices

Type	Component	Description	Target Version	Action
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. 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.
Obsolete	Wi-Fi	WEP is no longer supported as of AirLink OS 5.1 due to its security issues. 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.

Type	Component	Description	Target Version	Action
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. 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. If additional channels are required, consider enabling DFS Channels.

Upgrade Path Matrix

Semtech has tested and validated upgrading to AirLink OS 5.3 from the following releases:

- 5.2.46
- 5.1.78

Your routers must have AirLink OS 4.0.23 or later installed before they can be upgraded to AirLink OS 5.3. Direct upgrade to AirLink OS 5.3 from AirLink OS 3.1 and earlier is not supported.

If the router is running AirLink OS version...	Upgrade to...	Notes
5.2.46	**5.3**	
5.1.78	**5.3**	
5.0.x	**5.2.46**	
4.1.x	**5.1.78**	Downgrading from AirLink OS 4.1 to an earlier build is not supported.
4.0.23	**5.0.86**	
3.0.35 **3.1.24** **3.1.26**	**4.0.23**	
2.1.30	**3.1.26**	Downgrading from 3.0 to 2.1 is not supported.
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.

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

AMM Integration	
	Added support for AirLink OS routers on AM/AMM, enabling on-premise management for mixed fleets of MGOS, ALEOS, and AirLink OS-powered routers.
	Added support for router registration.
	Added support for software upgrade and downgrade.
	Added support for router template configuration.
	Added support for stats, maps and tracker.
Cellular	
	Added support for displaying the cellular RF bandwidth parameter at Status/Monitoring > Cellular > BANDWIDTH. **Note:** *The AirLink RX55 does not display cellular RF bandwidth info due to an EM74xx radio module limitation.*
	XR60: Added support for Anterix bands.
	XR60: Added a setting to disable band 8 from being used to connect to the network.
Logging	
	Moved DHCP client (dhclient) messages from Info to Notice log level.
Telemetry	
	Added the ability to disable the TAIP Checksum for TAIP Reports.
	Added the ability to detect and display the use of the J1979-2 protocol on the CAN bus under System > Status/ Monitoring. **Note:** *This feature is available for diagnostic purposes. J1979-2 CAN bus protocol is not supported in AirLink OS 5.3.*
Networking	
	Added Client DHCP feature to provide the ability to reference the router by a configurable name rather than an IP address (DHCP Option 12).
VPN	
	Added an OpenVPN status page under Status/Monitoring > Networking
	Added support for root certificates with username and password as authentication method for OpenVPN.
Location	
	Location Reports can now be configured to report RMC, GGA, and VTG NMEA sentences with a "GP" talker ID (e.g. GPRMC, GPGGA, GPVTG). This setting can be configured in Services > Location > Reporting.

EM9190 and EM7690 Radio Module Firmware

Carrier Firmware Matrix:

- AT&T: 03.14.10.04
- FirstNet: 03.14.10.04
- Bell: 03.14.10.01
- Generic: 03.17.04.00 (EM9190)
- Generic: 03.14.10.04 (EM7690)
- Rogers: 03.14.10.01
- Telstra: 03.10.07.00
- Telus: 03.14.10.00
- T-Mobile: 03.14.10.01
- Verizon: 03.17.04.00
- Softbank: 03.17.04.00 (EM9190 only)
- KDDI: 03.17.04.00 (EM9190 only)
- DOCOMO: 03.17.04.00 (EM9190 only)

EM9293 Radio Module Firmware

Carrier Firmware Matrix:

- AT&T: 02.15.01.00
- FirstNet: 02.15.01.00
- Bell: 02.17.08.00
- Generic: 03.04.10.01
- Rogers: 02.17.08.00
- Telstra: 02.17.08.00
- Telus: 02.17.08.00
- T-Mobile: 02.15.01.00
- Verizon: 02.17.08.00

EM9291 Radio Module Firmware

Carrier Firmware Matrix:

- AT&T: 02.15.01.00
- FirstNet: 02.15.01.00
- Bell: 02.17.08.00
- Generic: 03.04.10.01
- Rogers: 02.17.08.00
- Telstra: 02.17.08.00
- Telus: 02.17.08.00
- 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:

- Generic: 4.7.1.0
- Generic: 4.6.9.4

Bug Fixes

Cellular	
	Resolved an issue where LPWA radio module firmware was not downgraded and upgraded consistently during AirLink OS software downgrades and upgrades.
	XR60: Resolved an issue where the EXPANSIONS table (intended for XR90 and XR80 routers) appeared under Status/Monitoring > System > Device Information.
Wi-Fi	
	Added an alert and recovery mechanism to resolve an issue where the router could lose connection to a client interface.
	Resolved an issue where there was no notification that the AP was not using the configured channel after connecting to a client on a different channel.
Networking	
	Resolved an issue where QOS upload limits were not working for policies based on local LAN segments as source addresses.
	Resolved an issue where UDP stream stoppages during router initialization resulted in audio interruptions.
Serial	
	Resolved an issue where UDP PAD responses were not returned on the same interface where the inbound traffic was received.
Location and Telemetry	
	Resolved an issue where telemetry messages that display read strings (such as the VIN) needed to be placed in double quotes so whitespace can be seen.
	Resolved an issue where MIL status was not reported for the J1939 CAN bus, only for the J1979 CAN bus. The telemetry data item "J1979 MIL status" has been renamed "MIL status," and status is reported for both J1939 and J1979.
	Resolved an issue where disabling ALMS LwM2M also disabled Telemetry.
ALMS	
	Resolved an issue where an XR80 stopped communicating to ALMS via LwM2M after an upgrade to AirLink OS 5.2.46.
	Resolved an issue where VPN status information was not shown consistently.
VPN	
	Resolved an issue where Extended Captive Portal and OpenVPN would not work when both were enabled.
Apps	
	Resolved an issue where the container could not be restarted after the router firmware was updated through "Switch to Backup Image".

Known Issues

Cellular	
	XR60: An issue exists where the ENABLE BAND 8 setting appears on a multi-APN virtual interface, and can appear enabled when the setting is disabled on the parent interface. When the ENABLE BAND 8 setting appears on a multi-APN virtual interface, the parent interface setting is used.
	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 Mbps 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	
	An issue exists where a router with Dual-Band Client Connection enabled does not reliably connect to hidden SSIDs that contain spaces in their names.
	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.
	An issue exists on the XR80 or XR90 with Dual-Band Client Connection enabled being unable to connect to a Remote AP having an SSID on each band with the same name.
	RX55/XR80: An issue exists where some Pixel 6 phones keep connecting to and disconnecting from the 5 GHz Wi-Fi (WPA2) access point.
	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, after making a Multi-WAN interface priority configuration change, the existing connection does not transition to the higher priority interface. For example, traffic may continue on a cellular interface even though the router enters into range of a Wi-Fi AP.
An issue exists where Quality of Service is not able to set separate download Bandwidth Policies for an interface where the configured Interface Service Policy bandwidth is supported. QoS does not allow priorities to be assigned to the different download policies.
An issue exists where it is possible to attempt to create and delete a WAN Service under Networking > General > WAN Services > WAN SERVICES TABLE, although these changes cannot be saved.
An issue exists after a software downgrade and upgrade where the Firewall > Network Address Translations table introduces errors when creating a template in ALMS. Ensure that you perform a full synchronization before creating a template in ALMS.
An issue exists where a /24 subnet is created when IP Passthrough is enabled, regardless of the subnet prefix length setting configured in the IP Passthrough feature. As a result, the IP Passthrough Network and Broadcast addresses can fall outside of the specified setting.
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.
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.
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.

	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 configuration setting in a template for a disabled feature could cause 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 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.
AMM	
	An issue exists where WAN link status cannot be viewed on AMM when the router is in Multi-APN mode.
	An issue exists where ALMS Multi-WAN policies and ALMS-related log messages are present when the router is configured for AMM mode. When the router is in AMM mode, ALMS services and Multi-WAN policies refer to LWM2M communication to the AMM.
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	
	An issue exists where disabling and enabling UDP PAD Auto-answer mode requires the idle timeout to expire before serial data is sent to the PAD client.
	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.
	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