SIERRA WIRELESS IS NOW SEMTECH®

AirLink OS 6.0.0

RELEASE NOTES

About AirLink OS 6.0.0

This release of AirLink® OS 6.0.0 is available exclusively for AirLink EX400 and RX400 routers. AirLink OS 6.0.0 does not apply to AirLink XR90, XR80, XR60 and RX55 routers.

These release notes describe new features, bug fixes and known issues that apply to this release.

Change of Behavior Notices

Type	Component	Description	Target Version	Action
Behavior change	Wi-Fi	The Client Isolation default setting will change to Enabled.	7.0.0	No action required.
Behavior change	SMS	EX400: SMS Provisioning default setting will change to Disabled.	6.1.0	No action required.
Behavior change	Multi-WAN	WAN Policy Link Validation is no longer enabled by default.	6.0.0	No action required.

New Features and Enhancements

Cellular	
	Added a setting to disable band 8 (B8 for 4G LTE, N8 for 5G SA) from being used to connect to the network.
	Added a "Data Connection" timeout trigger to Auto SIM switching. This monitors when an interface gets stuck in "Connecting" state and automatically switches to an alternate SIM card after a configurable timeout.
	Under Status > System > Cellular, added the ability to display: ▪ SIM card EID (this is also visible when editing a SIM configuration in the SIM Database) ▪ NSSAI and Mapped NSSAI

	Added support for automatically updating, if configured, the radio module firmware image when the active profile changes on a multi-profile SIM card.
Wi-Fi	
	The term “Broadcast SSID” in Wi-Fi interfaces has been replaced with “Hide SSID”. Note that existing functionality and default settings remain equivalent to previous versions.
Templates	
	The Template menu now has an “Apply a replace template” option. Selecting this option (intended for templates created using “Create template from current configuration”) replaces all settings on the target device with the configuration provided in the template. Non-default settings in the template will modify those settings on the target device, and all other settings on the target device will return to their default configuration. **Note:** *Using “Apply a replace template” when connected to the router through a local connection resets the “admin” AirLink OS login password to the default password found on the device label. This is because templates do not contain the “admin” password.*
Networking	
	Renamed Multi-WAN System Policies to remove ALMS references. “ALMS Management Servers” is now “AirLink Management Servers IPv4”, for example. Management and Software Servers can originate from ALMS or AMM, depending on Device Management configuration.
VPN	
	When configuring IPsec VPN tunnels, the configuration menu no longer allows manually entering an IP address or FQDN for **Peers**, **Local Subnets**, **Remote Subnets**, **Exempt Subnets**, and **Secondary Peer for Failover**. You can select a pre-configured IP/Network, FQDN or Zone for these settings, or create these elements from the tunnel configuration menu.
Power Management	
	Reorganized the System > MCU section with Voltage Threshold and Power Management sections into one System > Power Management section with Standby Mode subsection and structured Triggers table under it.
AirLink OS	
	Renamed the Notifications CLEAR button to CLEAR ALL and added “Acknowledge” and “Acknowledged” tool tips for individual alerts.
	Added color-coding to indicate: ▪ when a value changes on the device. The corresponding field in the UI flashes orange for half a second to reflect the update. ▪ time-sensitive information, such as location data. Current “live” values are shown in green text; stale values are shown in red text. In the case of location data, a value is considered stale after a location fix is lost for two or more seconds.
	Changed Status/Monitoring section title to Status.

Revised the user interface to enhance readability and navigation:

- Enhanced search:
  - Search keywords can now be entered in any order
  - Search by label or value
  - Added Search History
- Added "EXPAND ALL/COLLAPSE ALL" and "Show more/Show less" functionality to view or hide full configuration menus
- Pages have been split into smaller sections under separate tabs
- Added icons and collapsibility to the left navigation bar
- Added links to quickly navigate between related configuration and status pages

Removed audible alerts for notifications.

Enabled three-digit version numbers for AirLink OS releases. The new software version number follows the pattern *major.minor.patch* to help improve readability and communication.

You can now drag and drop configuration items (such as IP/Network items that appear as New IP/Network in configuration fields) to reorder values.

Each item now has copy, edit and delete options contained in its own menu (accessed by clicking ⋮).

ALMS

The Fast-Changing Rule is not activated automatically after adding a data point in ALMS. After clicking a "cloud" icon to add a data point to the Fast-Changing Rule, you must select the options to activate the rule and to add the data point to the rule.

Added the ability to retrieve and download NMEA logs in ALMS.

The Troubleshooting Package, previously only available when locally connected to the router, can now be retrieved in ALMS.

Enhanced software update using the AirLink OS configuration UI in ALMS with:

- the ability to search by both name and release version
- additional "Processing Software Update" notification regarding the operation in progress.

SMS

SMS Provisioning is disabled by default on the RX400.

I/O

Reorganized the System > I/O section, moving Analog Inputs Values and Transformed Values from I/O Configuration to Status > I/O.

Logging

Added the ability to mark Regular Logs with a customizable message to help improve troubleshooting.

EM8695 Radio Module Firmware

Carrier Firmware Matrix:

- AT&T: 01.01.01.00
- Generic: 01.01.01.00
- T-Mobile: 01.01.01.00
- Verizon: 00.01.16.00

Bug Fixes

Cellular	
	Resolved an issue where the Auto-SIM switch feature did not work consistently under some circumstances.
	Resolved an issue where temperature would be incorrectly logged for virtual cellular interfaces.
	Resolved an issue where a virtual APN interface selected the previous APN even though different APNs were given in the SIM Template database.
Wi-Fi	
	Resolved an issue where the negotiated security mode for a Wi-Fi Client was not being properly displayed. Now the security mode that is actually being used between the Client and remote AP will be displayed.
	Resolved an issue where logs did not include a “Channel Available Check (CAC) complete” message when an Access Point had an SSID configured on a DFS channel.
	Resolved an issue where, under certain conditions, the primary RADIUS Authentication Server did not fail over to the secondary server.
	Resolved an issue where the Wi-Fi client would not connect to a higher priority IPv6 Access Point.
	Resolved an issue with an unclear error message regarding the maximum number of SSIDs in the Client SSID Database.
	Resolved an issue where the Wi-Fi client had to be enabled before a manually configured SSID could be added to the interface.
Ethernet	
	Resolved an issue where non-default Ethernet link speed settings did not persist across reboots.
Networking	
	Resolved an issue where, after making a Multi-WAN interface priority configuration change, the existing connection did not transition to the higher priority interface.
	Resolved an issue where Quality of Service was not able to set separate download Bandwidth Policies for an interface where the configured Interface Service Policy bandwidth was supported.
	Resolved an issue where it was possible to attempt to create and delete a WAN Service under Networking > General > WAN Services > WAN SERVICES TABLE, although these changes could not be saved.
	Resolved an issue where a /24 subnet was created when IP Passthrough was enabled, regardless of the subnet prefix length setting configured in the IP Passthrough feature.
	Resolved an issue where, if IP Passthrough was enabled on a Multi-APN cellular interface, and the cellular interface's APN settings changed from single to multiple (or vice versa), the router’s IP Passthrough segment was shown as invalid.
	Resolved an issue where Network Watchdog link validation failed when configured without an IPv4/IPv6 FQDN/IP host.
	Resolved issues that were observed with high-speed traffic passing through the USBNet interface (USB port used as a network interface) at times, where the USBNet interface was dropped on USB-connected Windows PCs, requiring a router reboot to recover.
	Resolved an issue with network disconnects in IP Passthrough mode by improving IP Passthrough logic to handle cellular network provider-initiated disconnects.

	Resolved an issue where WAN Policy Link Validation caused excessive Cellular interface restarts. WAN Policy Link Validation is no longer enabled by default.
Serial	
	Resolved an issue where disabling and enabling UDP PAD Auto-answer mode required the idle timeout to expire before serial data was sent to the PAD client.
Location	
	Resolved an issue where labels for some Telemetry items relating to Cellular were misleading.
	Resolved an issue where NMEA Log download was only available when NMEA Logging was enabled. NMEA Log download is available when NMEA Logs are present on the device.
ALMS	
	Resolved an issue where some settings remained enabled while an ALMS operation was in progress.
	Resolved an issue when using a CSV file in ALMS to configure AirLink OS routers where the file application failed with an unnamed “Bad data type” error.
	Resolved an issue where uploading a new dataset file would overwrite the existing dataset name.
	Resolved an issue where, under Networking > Diagnostics > IP Capture, the in-progress button continued to spin after an IP capture was completed.
VPN	
	Resolved an issue where IPsec tunnels in AirLink OS did not use UDP encapsulation when there is no NAT between the VPN server and the VPN client (both endpoints use routable IP addresses). AirLink OS 6.0.0 adds an option to force UDP encapsulation for this case (“Force” is the default setting).
	Resolved an issue where a FIPS mode IPsec tunnel restarted continuously when Multi-WAN policy was configured.
	Resolved an issue where the Status/Monitoring Dashboard displayed an incomplete list of VPN tunnels or stale VPN tunnels associated with each WAN interface.
Simple Captive Portal	
	Resolved an issue where both IPv4 and IPv6 traffic was not passed after a client with dual IP stack support was authenticated on the portal.
AirLink OS	
	Resolved an issue where errors existing in the router’s configuration prevented a dataset from being created and saved.
	Resolved an issue where the router’s Reboot Now, Reset Settings and Software Update operations could be launched when there were unsaved configuration changes.
	Resolved an issue where scientific notation (e) and arithmetic operators (- and +) could be entered for Wi-Fi SSID priority.
	Resolved an issue where pressing ESC did not close the Search bar while viewing the configuration in ALMS.
Templates	
	Resolved an issue where, 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 ALL had to be manually selected when creating the template.

Resolved an issue where, when creating a template with DHCP Relay configuration, the “IPv6 Address” field was not selected by default. Applying a template on the target device failed if “DHCP Relay IPV6 Server Address” was configured and “IPv6 Address” was missing.
Resolved an issue where a template created on a router with an enabled, operating Extended Captive Portal configuration failed when applied to a router that is at factory default.
Resolved issues where a device template created on a router containing the following setting would fail when attempting to apply the template to a fleet of routers, if the routers have those settings previously configured.
Logging
Resolved an issue where not all IP Capture settings were reset after a router reboot.

Known Issues

Cellular
An issue exists where certain cellular carriers permit network connection regardless of APN validity but restrict data traffic flow to authorized APNs only. Ensure that you configure the correct carrier-approved APN for your SIM card to connect to the network and pass traffic.
AirLink OS does not support multiple IPv6 addresses assigned via SLAAC/DHCPv6. Only the last IPv6 address will be used.
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 applying a CSV template containing an AP password will result in a “Bad data type” error. Set the AP password directly through ALMS to avoid/resolve this.
An issue exists where some settings with the label “IPv4/IPv6 Address or CIDR Range” require **both** an IP address and CIDR range (192.168.1.0/24, for example) in order to be validated.
Although a Timeout field appears in the RADIUS authentication server configuration, the setting is not used in AirLink OS.
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 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.
Ethernet
An issue exists where, after disabling the Ethernet interface in AirLink OS, the Ethernet port’s power LED can appear green (powered on) when a cable is connected to the port. However, after being disabled, the port does not have any network functionality despite the LED being on.
Networking and Connectivity
An issue exists where WAN IPv6 configuration parameters (Networking > General > WAN) for Ethernet and Wi-Fi WAN cannot be selected for a template.

An issue exists where creating a template from the current configuration does not automatically include the QoS Traffic Classifier in the Bandwidth Policy. To include the Traffic Classifier in the template, manually select the QoS "Traffic Classifier" items in the UI when creating the template. If a QoS Bandwidth Policy is defined and the Traffic Classifier is not manually selected, an error will occur when applying the template to a device.
An issue exists where the DDNS password setting does not correctly parse a password containing special characters, causing DDNS to fail when DDNS is enabled.
An issue exists where SNAT rules are not applied on LAN-side interfaces. This affects: ▪ user-configured SNAT rule entries that apply to LAN-side traffic ▪ container applications where the source IP address of container-initiated traffic will be the internal container's IP address instead of the corresponding router's IP address for the LAN segment used by the container.
When an interface has an IPv4/IPv6 address but the corresponding Network Watchdog rule has no IPv4/IPv6 address (or FQDN resolution to IPv4/IPv6) then the link validation will fail and the interface will eventually be restarted.
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
An issue exists where the IPsec Tunnel went down and could not re-establish when the router was passing bidirectional Multi-APN cellular traffic routed both through and outside the IPsec VPN tunnel.
An issue exists where a template containing an incomplete VPN tunnel configuration can be successfully applied to another router with no indication that the configuration is invalid.
OpenVPN tunnel names cannot include spaces. Names with underscores or hyphens are supported.
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
An issue exists where a template generated from a local connection to the router does not include the admin user password.
An issue exists where templates generated from ALMS include some default configuration values (for dataset definitions). Templates that are generated from a local connection to the router contain only non-default settings.
An issue exists where a configuration setting in a template for a disabled feature could cause an error notification when the template is applied.
Location and Telemetry
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.
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