Release Notes

Firmware 6.5.4

Abstract

This document encompasses the following key sections:

- **Firmware Update Instructions:** Guides users through the firmware update process to ensure a smooth and successful experience.

- **Description of New Features, Fixes, and Changes:** Provides detailed information about new features, enhancements, fixes for previous issues, and other significant changes included in the firmware update.

- **Known Issues Related to the Firmware Version:** Informs users about any existing issues or limitations with this firmware version, aiding in informed decision-making and preparation.

Firmware Release Information

- **Version**: 6.5.4

- **Release Date**: July 22, 2025

- ⚠ **Compatibility and Distribution**:

  Due to the significant changes introduced in the 6.4.x and 6.5.x releases, extensive testing of these major releases is strongly advised prior to their deployment in operational environments.
  For comprehensive compatibility details and distribution guidelines, see the *Firmware Compatibility Chart* document published with the specific firmware version.

Firmware and Product Documentation Notice

- **Firmware Versions in New Routers:** Not all new Advantech routers are shipped with this latest firmware release due to specific carrier or regional certifications. Check the *Firmware Compatibility Chart* document for the latest firmware information for your router model.

- **Router Configuration Information:** The most recent and detailed configuration information is available in the *Configuration Manual* for your router model.

- **Accessing Documents and Applications:** Visit the *Engineering Portal* at *icr.advantech.com* for product-related documents, applications, and firmware updates.

Contents

Part I.

Firmware Update Instructions

General Update Instructions and Notices

HTTPS Certificates:

- Following the release of firmware version 5.3.5, the router's HTTPS certificate format has been updated to enhance security measures. It is crucial to recognize that routers produced prior to this firmware version will not have their HTTPS certificates automatically updated during the firmware upgrade process.

- For manual HTTPS certificate updates, remove the existing certificate files found at `/etc/certs/https*` on the router. This action should be performed through an SSH connection. The certificates will be automatically regenerated in the new format upon the next reboot of the router.

FirstNet Firmware Specific Notes

Note: The following notes are specific to *FirstNet* products (ICR-3241..**-1ND** and ICR-4461..**-1ND**) and apply starting from firmware version 6.3.2, unless indicated otherwise.

- **Administration User Account:** Access via the *root* user for web or SSH logins is disabled. Utilize the *admin* account instead. The router label contains a unique password.

- **Disabled User Scripts:** Scripts set up through the GUI are unsupported. Scripts will convert to a Router App in updates to firmware version 6.3.7 or later. Note: Scripts will be deleted when updating to firmware versions from 6.3.2 to 6.3.6.

- **Different Default Settings:** Default router settings have been changed to improve security, deviating from standard configurations.

- **Password Complexity:** *very weak* and *weak* levels are not available for the password complexity setting on the *Configuration → Services → Authentication* page.

- **No FTP Support:** FTP configuration is removed from the GUI.

- **No Telnet Support:** Telnet configuration is removed from the GUI.

- **WiFi Security:** Support for WEP, WPA1, and WPA2-TKIP security protocols is discontinued.

- **OpenVPN Security Level:** Security levels *0 - Weak* and *1 - Low* are not allowed.

- **HTTP Restrictions:** Only HTTPS access is allowed with a minimum of TLS version 1.2.

- **MTU Settings:** The default MTU is set to 1342 bytes.

- **SNMP Restrictions:** SNMP write access is disabled.

- ***FirstNet* Router App Changes:** Some functionalities previously in the *FirstNet* Router App are now embedded in the firmware, focusing the app on monitoring the security status of *FirstNet* routers.

Part II.

Description of New Features, Changes, and Fixes

Added

Registration Timeout Setting Added

Added the *Registration Timeout* option to the *Mobile WAN Configuration*. Previously, this setting was only available via text settings as `PPP_REGISTRATION_TOUT` and `PPP_REGISTRATION_TOUT2` .

Changed

Sudo Version Updated

Upgraded `sudo` (available on -S1 platforms only) to version *1.9.17p1*, which addresses CVE-2025-32463.

CURL Version Updated

Upgraded *CURL* to version *8.14.0*, addressing several *minor security vulnerabilities* and improving overall stability.

Enabled NMEA Output on LE910

Modified the serial port configuration for the *Telit LE910C4-WWXD* module to *enable NMEA output*, allowing GPS data to be accessed via the serial interface.

Fixed

IPsec NAT Rule Handling Resolved

Resolved an issue where internal NAT rules were not properly removed after an IPsec Security Association (SA) re-keying. This previously led to IPsec connection failures following SA changes.

Verizon Connectivity on ICR-41/4271 Fixed

Fixed a connectivity issue affecting Verizon networks on ICR-41/4271 routers using the Telit FN990 module.

Telit FN990 Startup Timeout Resolved

Resolved a problem that caused startup timeout errors when initializing the Telit FN990 cellular module.

Router Apps: Version Sorting Fixed

Fixed an issue in the *Router Apps* section where versions were not sorted correctly during *Online Installation*.

Syslog Configuration Loading Resolved

Resolved a permission issue that prevented non-admin users from loading the *Syslog Configuration* page in the web interface.

Improved VRRP Shutdown Fixed

Fixed an issue with the shutdown behavior of VRRP (keepalived), ensuring proper termination of the service.

Part III.

Known Issues Related to the Firmware Version

ICR-3200 – WiFi Behavior Changed

Starting with firmware version 6.4.2, the Laird SU60 WiFi driver was upgraded to version 11.171.0.24. This update fixes several WiFi connectivity issues on these routers. It may also affect the behavior of the WiFi module in certain situations; for example, when used as both an AP and a Station, the AP will not accept any clients if the Station is not connected.

Firmware Update – Unexpected Filename

There is a known issue that occurs if the filename of the firmware intended for your router has been altered. This can affect both manual firmware updates and the Automatic Update feature. When this issue arises, the following warning message is displayed: *"You are trying to upload file 'xx.bin' but 'yy.bin' is expected. Are you sure to continue?"* To resolve this issue, please follow the instructions provided in Part I - Firmware Update Instructions of this document.

WiFi Configuration – Lost After Firmware Downgrade

Be aware that if you downgrade your firmware to a version earlier than 6.2.0, all existing WiFi configurations will be completely lost. It is crucial to back up your configuration before proceeding with such a downgrade.

ICR-3200 – Country Code for WiFi

In the initial firmware version for the ICR-3200 WiFi module, there is a limitation regarding the setting of the country code. Any modifications to the country code made on the configuration page will not take effect. This is because the country code for the WiFi module is pre-set during the manufacturing process, based on the intended region of product distribution.

SmartStart SL302 – Cellular Network Authentication

For the SmartStart SL302 router equipped with the Telit LE910-NA1 cellular module firmware version 20.00.522, there is a known limitation: It is not possible to use a username and password for authentication when connecting to the Mobile WAN network. This restriction specifically affects settings configured on the *Mobile WAN Configuration* page.
To check the firmware version of your cellular module, visit the *Mobile WAN Status* page in the router's web GUI, where it is listed under the *Mobile Network Information* section.