Release Notes

Firmware 6.5.3

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on May 29, 2025.

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**: 6.5.3
- **Release Date**: May 28, 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

Cellular Synchronization with Date and Time Added

Added possibility to synchronize date and time with the cellular network (except for SmartFlex SR303, SR305 and SmartMotion ST352):

- For automatic synchronization, select *Synchronize clock with cellular network* in the *NTP Configuration* page.
- For manual synchronization, select *Query cellular module* in the *Set Date and Time* page.

Cellular Communication Log Added

Added logging of AT, QMI, and MBIM communication with the cellular module. To enable, check *Enable debugging* in the *Mobile WAN Configuration* and then increase *Minimum Severity* in the *Syslog Configuration* to *Debug*.

Mobile WAN Expert Configuration Options Added

Added expert configuration options for Mobile WAN, not shown in the GUI:

- Set `PPP_TOLERATE_NO_SIM=1` to disable module restarts if connectivity is enabled but SIM is missing. After inserting the SIM, the user must **reboot the router manually**.
- Set `PPP_TOLERATE_NO_SIGNAL=1` to disable module restarts if the signal has been lost. As a side effect, the SIM switching will not work.

Default APN for PLMN Added

Added default APN for PLMN 2320319, 23203189, and 90140571.

Terminfo Database for Router Apps Added

Added terminfo database file for easier integration of screen-oriented router apps, such as *Midnight Commander* or *Lynx*.

Changed

WireGuard Tunnel Subnets Capacity Modified

Increased the maximum number of *Remote subnets* in the *WireGuard* tunnel configuration from 4 to 32. Unused items are automatically hidden.

Added New Ciphers to IPsec Tunnel Configuration

Upgraded strongSwan to version 6.0.1 and added new ciphers to the *IPsec* tunnel configuration:

- `CAMELLIA256CCM128` and `CHACHA20POLY1305` added to *ESP Encryption*.
- DH groups `24 (modp2048s256)`, `28 (ecp256bp)`, `29 (ecp384bp)`, `30 (ecp512bp)`, `31 (curve25519)`, `32 (curve448)`, `36 (mlkem768)`, and `37 (mlkem1024)` added to *IKE DH Group* and *PFS DH Group*. The configuration fields now show also the group names.
- Fixed certificate validation, so the router will reject certificates that do not match the configured *Local ID* or *Remote ID*.

OpenSSH Upgraded

Upgraded OpenSSH to version 10.0. This fixes several minor security vulnerabilities and a temporary connection rejection after a previous session expired unauthenticated.

Carrier Options Modified

Modified *Carrier* selection options in the *Mobile WAN Configuration*:

- *Outside North America* is now available on all platforms and enables a global cellular configuration.
- Individual operators such as *AT&T* are listed only on products certified for the NAM region.
- *North America, Generic* is also available and enables a generic North America (PTCRB) configuration (when supported), or a global configuration.
- *Automatic detection* was renamed to *North America, Autoselect*. It now either selects a specific network operator configuration automatically or falls back to a generic North America configuration.

Web Administration Enhanced

Enhanced Web administration with a color stripe to distinguish between standard routers (green stripe) and S1 routers (orange stripe).

General Status Page Modified

Modified *System Information* on the *General Status* page to display the *Product Type* by default and the *Hardware UUID* only when *More Information* is requested.

Removed

TCP Settings from Expansion Port Removed

Removed *Use CD as indicator for TCP* connection and Use *DTR* as control of *TCP* connection settings from *Expansion Port Configuration* (except for SmartStart). These settings no longer apply to other products, as *DTR/DCD* signals are only available on SmartStart products.

Default APN for PLMN Removed

Removed default APN for *PLMN 26003*.

Fixed

ICR-27/2800 Cellular Lock-up Fix

Fixed cellular module lock-up on ICR-27/2800 occurring after a failed connection reconfiguration.

Follow STA Radio Settings Option Fixed

Fixed availability of the *Follow STA Radio Settings* option in the WiFi AP Configuration. It appears only when supported by the WiFi module, newly also on all ICR-41xxW/42xxW. It is now supported by all products, except SL3xx with SG901-1059B, and ICR-2xxxW with AW-CM358.

Handling of the PAP or CHAP Option Fixed

Fixed handling of the *PAP or CHAP* option in the Mobile WAN *Authentication* on ICR-2437 with ML620, and SL306 with ME909. The username/password was not set correctly in case *PAP or CHAP* was selected.

Network Selection and Attachment Optimized

Optimized network selection and attachment on ICR-2437 with ML620. The implementation now uses Unitac-specific AT commands recommended for better reliability and performance. This change works best with the latest Unitac firmware `0.3.4.1/ML620EUV14_RELEASE_20250516`.

Changing of APN Setting Fixed

Fixed changing of APN settings on ICR-4133/4233 with FM101. Previously a module restart was required in some situations.

NTP Time Sync Error Resolved

Fixed failure of the manual *Set Date and Time* operation when invoked via Query *NTP* server in firmware 6.5.2.

FTP Server Errors Resolved

Fixed occasional FTP server errors with message *failed to map segment from shared object* which could cause login failures.

Wrong WiFi Chipset Name Fixed

Fixed wrong WiFi chipset model name displayed for ICR-2xxxW with AW-CM358.

Web Administration Improvements

Fixed several issues of the Web administration:

- Fixed JavaScript error on Module Switching page of SmartMotion products.
- Fixed *Invalid input* error on *NAT* and *NAT6* pages when logged in with the default password.

Leading Zero MCC Handling (PLS83) Resolved

Fixed handling of *Mobile Country Codes* with leading zeros on products with *PLS83* modules.

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.