Release Notes

Firmware 6.6.1

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on April 23, 2026.

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**: 6.6.1
- **Release Date**: April 24, 2026
-  **Compatibility and Distribution**:

  Due to the significant changes introduced in the 6.4.x, 6.5.x and 6.6.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

I Firmware Update Instructions **5**

Router App Integration Warning 6

FirstNet Firmware Specific Notes 6

II Description of New Features, Changes, and Fixes **7**

Added 8

Changed 10

Deprecated 13

Fixed 14

III Known Issues Related to the Firmware Version **16**

Part I.

Firmware Update Instructions

Router App Integration Warning

Important Notice:

Several Router App functions have been integrated directly into the firmware since version 6.6.0. Existing Router App configuration is not converted during the upgrade. Users must reconfigure the corresponding functionality in the firmware and then uninstall the related Router Apps. The same feature must not be enabled simultaneously in both the firmware and the original Router App.

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

VXLAN Tunnel Support Introduced

VXLAN tunnel support has been introduced, enabling the creation of isolated Layer 2 networks across multiple sites.

Dynamic DNS Functionality Extended

Support for additional *Dynamic DNS* protocols has been added, extending traditional *DynDNS*:

- HTTPS transport support has been added to *DynDNS*, including optional custom CA support.
- Support for RFC 2136 DDNS has been added (except for ICR-20,24,25/2600).
- *DynDNS* menu and status items have been renamed to *Dynamic DNS*.

LLDP Service Implemented

The *LLDP* (Link-Layer Discovery Protocol) service has been implemented to enable automatic discovery of neighboring devices, simplifying network management and troubleshooting (except for ICR-20,24,25/2600).

Secondary Ping Target for Mobile WAN Added

Support for configuring a second *Ping IP Address* in *Mobile WAN Configuration* has been added. The SIM card is switched if none of the configured addresses are reachable.

GNSS Configuration Extended

The *GNSS Configuration* has been enhanced:

- Support for filtering forwarded NMEA sentences has been added.
- The maximum number of remote targets has been increased from 4 to 10.

SIM Management Features Extended

The *Manage SIM* administration has been enhanced:

- The currently selected *SIM Card* is now indicated on the *Unlock/Unblock SIM* and *Set SMS Center* pages.
- A *Switch SIM* command has been added when *Create connection to mobile network* is disabled in *Mobile WAN Configuration*.

Router Apps Status Page Added

A dedicated *Router Apps* status page has been added, providing a quick overview of installed Router Apps.

SNMP Part Number Object Added

The SNMP *infoPN* (1.3.6.1.4.1.30140.6.12) object has been added to provide the device Part Number.

File Import Buttons Introduced in Web Interface

Load From File buttons have been added to *User's Scripts* in the Web GUI and to the *Accept/Deny List* in *WiFi AP Configuration*.

Operator User Role Introduced

A new user role *Operator* has been introduced. Users assigned to this role can access the Web administration only to manage their own credentials. This role is intended for special-purpose Router Apps.

System Report NTP Sources Added

The System Report has been extended to include a list of *NTP Sources*.

status hw Hardware Information Extended

The `status hw` command has been extended to display additional hardware details, including the number of cellular modules, Digital Input/Output, Serial Ports, Bluetooth interfaces, and PoE PSE/PD support.

DNS Command-Line Tools Added

The `dig` and `nsupdate` command-line tools have been added to support DNS operations.

Terminal Usability Tools Added

The `clear` and `watch` tools have been added to improve command-line usability.

Per-CPU Statistics in top Enabled

Support for per-CPU statistics has been added to `top`, toggleable via the `c` key.

grep Context Support Added

Support for `grep` context arguments has been added, including `-A`, `-B`, and `-C`.

Hostname Utility Added

The `hostname` tool has been added for printing the device hostname.

xterm-256color Terminfo Support Added

The `xterm-256color` terminfo definition has been added to improve compatibility with advanced command-line tools.

Changed

Network Status Page Extended

The *Network Status* page has been enhanced:

- *Backup Routes* now include WAN IP and IPv6 addresses.
- An *LLDP Neighbors* list has been added (except for ICR-20,24,25/2600).
- The link to the *Connections* list has been moved to the main menu.

Web Administration User Experience Improved

The Web Administration interface has been improved:

- The *Factory Reset* button has been moved from the *Reboot Now* page to a standalone page under *Restore Configuration*.
- The briefly displayed *User has been logged in* page has been removed to speed up login. This may affect users accessing the Web Administration via automated tools such as `curl`.
- Address fields in *Firewall Configuration* have been extended to fully display IPv4 ranges and IPv6 addresses.

IPsec Tunnel Configuration Updated

The *IPsec Tunnel Configuration* has been updated with the following changes:

- The default *IKE Protocol* has been changed from *IKEv1* to *IKEv1/IKEv2*.
- *IKE Reauthentication* is now also enabled for the *IKEv1/IKEv2* protocol.
- IPsec rekeying and reauthentication times have been modified so that *Key Lifetime* is strictly the rekeying time and *IKE Lifetime* is strictly the reauthentication time.
- Default *Key Lifetime* increased from 3600 to 7200,sec (2,hours), and default *IKE Lifetime* from 3600 to 28800,sec (8,hours).
- *Rekey Margin* renamed to *Lifetime Margin*, and *Rekey Fuzz* to *Lifetime Fuzz*.

Automatic Update CA Handling Simplified

The *Use Custom CA Certificate* checkbox has been removed from *Automatic Update*. To use a custom certificate, fill in the *CA Certificate* field directly.

Ethernet Performance Optimized

Ethernet performance has been optimized:

- The default `pfifo_fast` root queuing discipline has been replaced with `fq_codel` to improve latency and fair queueing. Because a root qdisc now already exists, users relying on `tc qdisc add` must use `tc qdisc replace`.
- CPU load distribution and packet processing efficiency have been improved on all ICR-4xxx devices.

Router Identification Length Reduced

The maximum length of *Router Identification* in *GNSS Configuration* has been reduced from 128 to 70 characters to improve compliance with the NMEA standard.

Maximum SSH Public Key Size Reduced

The maximum allowed size of the *SSH Public Key* in User Management has been reduced to 16 KiB.

SNMP OID for ICR-2452 Corrected

The SNMP OID for ICR-2452 routers has been changed to 1.3.6.1.4.1.3014.1.2452. Previously, the OID matched ICR-447x (1.3.6.1.4.1.3014.1.89).

Invalid Pages and Commands Hidden

Web pages and `status` commands not applicable to a specific product have been removed. For example, `status module` is no longer available on LAN routers.

CA Certificates Bundle Updated

The *ca-certificates* bundle has been updated to the version dated 2025-12-02.

Wireless Regulatory Database Updated

The wireless regulatory database has been updated to the version dated 2026-02-04, and the country codes list (UN M49) has been updated to the version dated 2026-03-09.

OpenSSL Updated to 3.5.5

OpenSSL has been upgraded to version 3.5.5 to address the following vulnerabilities: CVE-2025-15467 (critical), CVE-2025-69419 and CVE-2025-69421 (high), and CVE-2025-15468, CVE-2025-66199, CVE-2025-69420, and CVE-2026-22796 (medium).

OpenVPN Updated to 2.6.19

OpenVPN has been upgraded to version 2.6.19 to address CVE-2025-13086 (high).

Net-SNMP Updated to 5.9.5.2

Net-SNMP has been upgraded to version 5.9.5.2 to address CVE-2025-68615 (critical).

U-Boot Updated on ICR-41xx/42xx

U-Boot on ICR-41xx/42xx devices has been upgraded to version 2024.10.

Deprecated

WEP and TKIP Encryption Deprecated

WiFi *Encryption* algorithms *WEP* and *TKIP* have been deprecated and will be removed in a future release due to known security vulnerabilities that allow traffic decryption and unauthorized access. Users are strongly encouraged to migrate to *AES*.

Fixed

MBIM Communication on ICR-4261 Fixed

An issue causing MBIM communication failure on ICR-4261 with the RM520N-GL module (revision RM520NGLAAR03A03M4G_A0.300.A0.300) has been resolved.

IPsec Tunnel Stability with Multiple Subnets Fixed

An issue affecting the stability of IPsec tunnels with multiple subnets when *Separate Child SA for Each Subnet* is enabled has been resolved.

SIM Statistics Signal Values Fixed

An issue causing incorrect display of *Signal Min* and *Signal Max* values in *SIM Statistics* has been resolved.

GNSS SNMP Reporting Fixed

An issue affecting the reporting of GNSS information via SNMP has been resolved.

Remote SSH Access with NAT Fixed

An issue affecting firewall configuration when NAT enables *remote SSH access* and a custom *Port* other than 22 is defined in *SSH Configuration* has been resolved.

SSH Connection Handling Behavior Fixed

The behavior of the *SSH* service after opening three concurrent unauthenticated connections has been corrected to match the standard `MaxStartups 3:60:6` configuration.

Web Administration Issues Fixed

Several minor issues in the Web Administration have been corrected:

- The *Network Type* selection in *Mobile WAN Configuration* now displays only supported technologies.
- Fixed an issue where LTE bands above 100 were not displayed correctly in Mobile *Network Information*.
- Saving of *Registration Timeout* for the second SIM in *Mobile WAN Configuration* has been corrected.
- Display of SHA-1 *Authentication* in *SNMP Configuration* after upgrading from a previous version has been fixed.
- Updating of *NTP Configuration* on LAN routers has been corrected.
- Reliability of configuration saving during device shutdown has been improved.

Cellular Module Model Detection Fixed

Detection of the full *Model* name for EC25/EG25 variants has been corrected.

Region Assignment for Selected Devices Fixed

Incorrect region assignment has been corrected for ICR-3201 (Worldwide) and BB-SL302 (North America).

Telit GNSS Enhancements

Fixed Telit GNSS to also send GLL, GSV, and VTG NMEA sentences.

Default HTTPS Certificate Parameters Corrected

The default HTTPS certificate has been updated to include `CA:TRUE` and to permit `keyCertSign`.

Configuration Reset Scope Fixed

The *Configuration Reset* process has been corrected to also reset the `/etc/group` file.

Emergency Reset Double Reboot Fixed

An issue causing a double reboot in certain scenarios during *Emergency Reset* has been resolved.

Bluetooth Discovery Fixed

An issue causing Bluetooth discovery to stall in certain situations has been resolved.

WiFi and GNSS Auto-Detection Fixed on Older OEM Devices

WiFi and GNSS auto-detection has been fixed for OEM products manufactured before 2019.

gsmpwr Command Help Fixed

Incorrect usage help of the `gsmpwr` command has been corrected.

Crash Dump Creation from Privileged Processes Fixed

An issue preventing the creation of Crash Dumps from privileged processes has been resolved.

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.

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.