

Release Notes

Firmware 6.6.2



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:** 6.6.2
- **Release Date:** July 28, 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	4
	Router App Integration Warning	5
	FirstNet Firmware Specific Notes	5
II	Description of New Features, Changes, and Fixes	6
	Added	7
	Changed	9
	Removed	11
	Fixed	12
III	Known Issues Related to the Firmware Version	14

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

GNSS Constellation Selection Added

Support has been added for selecting which *Constellations* are used in *GNSS Configuration*, and the *GNSS* status has been improved to display satellites from all enabled constellations. By default, GPS and Galileo are enabled.

exFAT File System Support Added

Support for the *exFAT* file system has been added, enabling the use of USB flash drives formatted in Microsoft Windows.

Security Information Extended with Last Factory Reset and SSH Fingerprint

Security Information in *General Status* has been extended with *Last Factory Reset* and *SSH Fingerprint*.

Debug Severity Dialog Added for Mobile WAN Debugging

A dialog has been added, allowing users to set the *Syslog Minimum Severity* to *Debug* directly when enabling *Mobile WAN* debugging.

Insufficient HTTPS Certificate Warning Added

A warning has been added stating “*The current HTTPS certificate is insufficient for the selected Security Level.*” to remind users to *Generate a new certificate*.

File Extension Indicator Added to Router Apps Page

A *File Extension* indicator has been added to the *Router Apps* page.

USB Port Information Extended

Information about the USB port has been extended:

- The USB port count (0 or 1) has been added to `status hw`.
- USB device information has been added to `status usb`.
- USB port status has been added to `status ports`.
- A list of *USB Devices* has been added to the system `report`.

eSIM Profile Management Tool Added

The `esim` tool has been added for eSIM profile management on EC25-EUX, RG255C-GL, and RM520N-GL. It is currently available through the command line only; Web GUI support will be added in the next release.

tcpdump Enabled on -S1 Devices

The `tcpdump` tool has been enabled on -S1 devices as well. On these devices, the command is limited to `/tmp`; use the `-Z` argument to drop root privileges.

taskset Command-Line Tool Added for ICR-4xxx

The `taskset` command-line tool has been added to ICR-4xxx routers for managing CPU affinity.

eMMC Support Extended for Larger Erase Blocks

Support for eMMC has been extended to include devices with erase blocks larger than 512 KiB.

Changed

Emergency Reset Data Wiping Extended to All Devices

The scope of *Emergency Reset* has been extended to clear all user data (`/var/data`), Router Apps (`/opt`), and device certificates (`/etc/certs`) on all devices. Previously, this applied only to -S1 devices.

Maximum Firewall Rules Increased

The maximum number of *Firewall* rules has been increased from 32 to 64.

Reboot Process Improved

The reboot process has been improved:

- The `reboot` command has been changed to properly shut down running services first.
- A `halt` command has been added that performs a shutdown, then turns off the PWR LED, and waits 100 seconds so the router can be safely unplugged.

SSH Key Restore Respects Configured Key Type

Restoring the SSH key has been changed to respect the configured *Key Type* in *SSH Configuration*. Previously, RSA-2048 was always used (ED25519 on -S1 devices).

Linux Kernel Updated to 6.1.175

The router has been upgraded to Linux kernel version 6.1.175. This brings upstream security patches and stability improvements.

CA Certificates Bundle Updated

The *ca-certificates* bundle has been updated to the version dated 2026-05-14.

OpenSSL Updated to 3.5.7

OpenSSL has been upgraded to version 3.5.7 to address [CVE-2026-28390](#), [CVE-2026-31789](#), [CVE-2026-34182](#), [CVE-2026-34183](#), [CVE-2026-45445](#), and [CVE-2026-45447](#) (high), and [CVE-2026-2673](#), [CVE-2026-7383](#), [CVE-2026-9076](#), [CVE-2026-28387](#) to [CVE-2026-28389](#), [CVE-2026-31790](#), [CVE-2026-34180](#), [CVE-2026-34181](#), [CVE-2026-42764](#), [CVE-2026-42766](#) to [CVE-2026-42770](#), and [CVE-2026-45446](#) (medium).

OpenSSH Updated to 10.3

OpenSSH has been upgraded to version 10.3 to address [CVE-2026-35385](#) (high), and [CVE-2026-35386](#), [CVE-2026-35387](#), and [CVE-2026-35414](#) (medium).

BIND Updated to 9.18.49

BIND has been upgraded to version 9.18.49 to address [CVE-2026-1519](#), [CVE-2026-3039](#), and [CVE-2026-5946](#) (high), and [CVE-2026-3592](#) and [CVE-2026-5950](#) (medium).

curl Updated to 8.20.0

`curl` has been upgraded to version 8.20.0 to address [CVE-2026-5773](#) (high), and [CVE-2026-1965](#), [CVE-2026-3783](#), [CVE-2026-3784](#), [CVE-2026-3805](#), [CVE-2026-4873](#), [CVE-2025-5399](#), [CVE-2026-5545](#), [CVE-2026-6253](#), [CVE-2026-6276](#), [CVE-2026-6429](#), [CVE-2026-7168](#), [CVE-2025-9086](#), [CVE-2025-10148](#), [CVE-2025-10966](#), [CVE-2025-13034](#), [CVE-2025-14017](#), [CVE-2025-14524](#), [CVE-2025-14819](#), and [CVE-2025-15079](#) (medium), and [CVE-2025-15224](#) (low).

jq Updated to 1.8.2

`jq` has been upgraded to version 1.8.2 to address [CVE-2026-32316](#) (high).

sudo Updated on -S1 Routers

`sudo` on -S1 routers has been upgraded to version 1.9.17p2.

Bootloader Updated on ICR-2xxx

The 2nd level bootloader (AT91Bootstrap) on ICR-2xxx has been upgraded to version 4.0.12, and the DDR2 settings have been changed to be JEDEC compliant.

RM520N-GL Internal Communication Switched to QMI

The RM520N-GL internal communication has been switched from MBIM to QMI.

Removed

Huawei ME909s Support Removed

Support for the Huawei ME909s module, previously used in SL306, has been removed.

Fixed

File Download Throughput Improved for 5G ICR-4xxx

File download throughput has been improved for all 5G ICR-4xxx routers.

Default Password After Emergency Reset Fixed

An issue causing an incorrect default password after *Emergency Reset* has been resolved.

SNMP Trap Failure for Unknown GNSS Location Fixed

An issue causing SNMP trap failure when the GNSS location is not known has been resolved.

GNSS SNMP Response Codes Corrected

GNSS SNMP responses have been corrected to return `noSuchInstance` instead of `genError` when the location is unknown.

Supported Rates List Fixed on ICR-2xxxW

The list of supported rates on ICR-2xxxW (AW-CM358 Wi-Fi) has been corrected. This issue only occurred when transitioning from the 5 GHz to the 2.4 GHz band, since OFDM-coding rates are otherwise shared.

High-Severity Web Administration Vulnerability Fixed

A high-severity vulnerability in the web administration interface has been resolved ([CVE-2026-14339](#)). An unauthenticated remote attacker could send a POST request with an excessively large Content-Length to trigger a buffer overflow, allowing denial of service and potentially remote code execution.

IPsec IKE Lifetime Validation Fixed

IPsec IKE Lifetime validation has been corrected so that it is skipped for the IKEv1 protocol. Also, the field is now disabled when *IKE Reauthentication* is disabled.

IPsec Tunnel Setup Failure Fixed

An issue causing *IPsec* tunnel setup failure due to misconfiguration of another tunnel has been resolved.

Automatic Update Error on -S1 Devices Fixed

An error on -S1 devices occurring after applying *Automatic Update* configuration without a CA certificate has been resolved.

U-Boot Environment Reading Fixed

An issue when reading the U-Boot environment has been resolved. In some situations, this could cause SmartFlex routers to have incorrect MAC addresses.

Partial Configuration Restore Fixed

Partial configuration restore has been corrected so that it no longer affects the time synchronization configuration.

Cellular-Based Time Synchronization Fixed on 5G Networks

An issue affecting cellular-based time synchronization on 5G networks has been resolved.

ICR-2437 IPv6 Connectivity Fixed

Connectivity of ICR-2437 (Unitac ML620) with *IP Mode* set to *IPv6* has been fixed. The module does not support it, so the router now uses *IPv4/IPv6* instead.

SMS Retrieval Fixed on ICR-2437

SMS retrieval on ICR-2437 (ML620) has been fixed. Performance when retrieving multiple SMS messages has also been improved on any router.

PLMN Scanning Optimized

PLMN scanning has been optimized when multiple *Operators* are whitelisted.

Cellular Module Shutdown Sequence Improved

The cellular module shutdown sequence has been improved for a more graceful power-off.

Network Type Selection Fixed for Selected Modules

The *Network Type* selection list has been corrected for routers with EC25-AF, EC25-AFX, and EC25-J modules. Previously, GPRS was offered even though these modules do not support it.

HTTP Error Pages Content Fixed

The content of HTTP error pages has been fixed. In some situations, the pages were blank.

Web GUI Typos Fixed

Several typos throughout the Web GUI have been fixed.

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.