

Release Notes

Firmware 6.6.0




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:** 6.6.0
- **Release Date:** December 17, 2025
-  **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 10
 - Deprecated 14
 - Removed 15
 - Fixed 16

- III Known Issues Related to the Firmware Version 18**



Part I.

Firmware Update Instructions

Router App Integration Warning



Important Notice: Several Router App functions have been integrated directly into the firmware. 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

Ethernet Port Control Introduced

Added an *Enable Port* option to the *Ethernet* configuration of all products.

ETH0 Configuration Expanded on Routers with Switched Ports

Extended configuration options for the switched ETH0 port on ICR-25xx/26xx and ICR-44xx:

- Added *Enable Ports* option for each individual port.
- Extended *Media Type* selection to individual ports.
- Added *VLAN Filtering*, allowing switch ports to forward only VLAN-specific traffic.

Quick Setup Workflow Introduced

A *Quick Setup* page is now shown after first login to guide users through initial configuration.

Router App Features Consolidated

Functionality from several Router Apps has been consolidated into the firmware:

- *Geolocation* and *GNSS* added to *General Status*, with SNMP-based location reporting and a new *GNSS Configuration* page for location tracking. This replaces the former *GPS Router App*.
- SMS actions have been linked to digital input state changes, support for variables has been added to *Digital Input SMS*, and a new *Inputs/Outputs Configuration* page has been introduced for managing digital outputs and the USR LED. This replaces the former *IO Control* and *USR LED Management Router Apps*.
- An *Events Configuration* page introduced for triggering SMS, e-mails, SNMP traps, or scripts based on specific events. This replaces the former *Event Notificator Router App*.
- A *Reboot Schedule* configuration added for automated, user-defined router reboot times. This replaces the former *Daily Reboot Router App*.
- Mobile WAN *Operator* selection enhanced to support comma-separated lists, enabling attachment to any listed PLMN. This serves as a *PLMN Whitelist* and replaces the corresponding Router App functionality.

Firewall Functionality Enhanced

Enhancements to firewall configuration:

- *Input Interface* and *Output Interface* selectors expanded to show all interfaces and standard zones.
- Rule descriptions stored as `iptables` comments for improved traceability.

Subnet-Specific Child SA Support Introduced

A new option to create a separate child SA for each subnet has been made available in the *IPsec Tunnel Configuration*.

HTTP Security Controls Strengthened

Security Level selection has been introduced in *HTTP Configuration*. Higher levels disable weak ciphers, and regenerating certificates may be required.

S1 Router Upgrade Conversion Implemented

Configuration conversion after firmware upgrades is now performed automatically on S1 routers.

Web Interface Guidance Expanded

Web administration enhancements include:

- RouterApp announcements are now displayed in the top-right corner, providing clear visibility for messages such as WebAccess/DMP notifications.
- Help text added throughout, including range hints for numeric fields.
- Tooltips enriched with configuration file item names.

Non-ASCII Input Warning Introduced

A warning is shown when non-ASCII characters are entered, as such input is not supported.

Status Command Set Extended

The `status` command suite has been expanded:

- `status geolocation` and `status gnss` introduced.
- `status hw` added to display hardware features.
- `status sim` added to report SIM statistics.

Bridge Management Commands Provided

The `bridge` command has been introduced for advanced bridge device control.

Wake-On-LAN Support Enabled

The `ether-wake` command is now available to generate WOL packets for remote device activation.

System Report Details Expanded

System Report improvements include:

- More detailed VLAN reporting.
- Inclusion of *Crash Log* and *Crash Dump Storage Statistics*.

Diagnostic Data Export Enabled

A *Save Diagnostic Data* option has been added to the *System Log* page for collecting debugging information.

PCAN-USB Adapter Support Introduced

External [PCAN-USB](#) adapters are now supported on RBv3 and all ICR-4xxxx products.

Configuration Item Summary Included

A list of configuration items is now included as part of the firmware release documentation.

Changed

WiFi Country Selection Structure Changed

The WiFi *Country* selection has been separated into a standalone page, providing a single country setting for all WiFi APs and STAs.

- Due to FCC regulations, NAM products do not expose this page; the *Country* is fixed to . Global products allow selecting (all countries) or .
- After changing the *Country*, users should review *HW Mode*, *Bandwidth*, and *Channel*. Invalid settings are disabled, but previous values remain until manually adjusted.
- During firmware upgrade, differing AP/STA *Country* settings are unified. Some radio settings may become invalid and must be reconfigured to restore AP/STA operation.

Default Forwarding Rule Revised

The default forwarding rule in *Firewall Configuration* has been revised to match all traffic with *Input Interface* in *LAN*. Since version 6.5.0, only traffic from the 192.168.1.0/24 subnet was matched.

IPsec Subnet Capacity Increased

The maximum number of Local and Remote Subnets in the *IPsec Tunnel Configuration* has been increased from 2 to 10. Unused entries are automatically hidden.

SMS Number Entry Method Updated

SMS Phone Number configuration now uses a single field accepting multiple comma-separated values, replacing the former three-field layout.

NTPv4 Implementation Unified

NTPv4 has been unified on ICR-20, 24, 25/2600 by adopting chrony 4.6.1, matching implementations used since 6.5.2 on other products.

NTP Configuration Extended

NTP Configuration now permits time synchronization using multiple backup sources: GNSS and/or Cellular network. Cellular network time sync is unavailable on SR303, SR305, and ST352 models.

Default NTP Polling Interval Increased

The default NTP *Maximal Polling Interval* has been increased from approximately one minute to approximately one hour.

Mobile WAN Credential Rules Tightened

Mobile WAN Configuration now disallows incomplete credentials; *Username* and *Password* must both be set or both left empty.

System Information Status Expanded

Enhancements to *System Information* include:

- *Part Number* added, and *Product Type* and *Product Name* moved to verbose mode.

Mobile Network Information Status Enhanced

Improvements include:

- Corrected *Model* name to display the full cellular module variant.
- Added *Firmware Release* identifier.
- Added *IMSI* and *SMS Center* number.

System Configuration Consolidated

Several settings have been reorganized under *System*:

- *Automatic Update* and *Authentication Configuration* moved under *System*.
- *Name*, *Location*, *Contact*, and *Custom* identifiers moved from *SNMP Configuration* to a new *Identification Configuration* page.
- A *Hostname* setting has been introduced.

Peripheral Ports Configuration Reorganized

The *Peripheral Ports* configuration has been consolidated:

- *Expansion Port* and *USB Port* moved under *Peripheral Ports*.
- *Binary Input/Output* renamed to *Digital Input/Output* across relevant pages.

SIM Management Options Consolidated

Set SMS Service Center, *Unlock SIM Card*, and *Unblock SIM Card* have been merged into a single *Manage SIM* menu item.

Web Interface Branding Updated

Updated the company logo in the Web administration interface to reflect current corporate branding.

Certificate Size Limit Increased

Maximum X.509 certificate size has been increased from 6 kB to 8 KiB.

Tunnel Interface Naming Updated

Interface naming has been updated:

- `usb0` and `usb1` are now consistently used for the first and second Mobile WAN.
- PPPoE renamed to `pppoe0`, L2TP to `l2tp0`, and PPTP to `pptp0`.

Automatic Update Scheme Hardened

The default URL scheme for *Automatic Update* has been changed to `https:`. Using HTTP now requires explicitly specifying the `http://` prefix.

Emergency Reset Functionality Expanded

Emergency Reset behavior has been enhanced:

- Account locks are now removed.
- Factory reset of the cellular module is performed.
- Configuration wiping security increased on ICR-2xxx-S1 and ICR-41xx/42xx devices.

Status Output Units Adjusted

`status` commands now report sizes in kibibytes (1024 bytes).

System Log Location Changed

System Log files on S1 routers have been moved from `/var/data/system` to `/var/log` to unify log storage locations.

Linux Kernel Upgraded

Upgraded to Linux kernel version 6.1.141, bringing upstream security and stability fixes.

CA Certificate Bundle Updated

The ca-certificates bundle has been updated to the version dated 2025-11-04.

OpenSSL Version Updated

OpenSSL has been upgraded to 3.5.4, as the 3.0.x branch approaches end-of-support. This may affect interoperability with older systems.

OpenSSH Version Updated

Upgraded to OpenSSH 10.2p1, addressing [CVE-2025-61984](#) and [CVE-2025-61985](#).

strongSwan Version Updated

Upgraded to strongSwan 6.0.2, ensuring compatibility with OpenSSL 3.5.

OpenVPN Version Updated

Upgraded to OpenVPN 2.6.15 to address [CVE-2025-2704](#).

AIDE Version Updated

Upgraded AIDE to 0.19.2 to address [CVE-2025-54389](#) and [CVE-2025-54409](#).

Pure-FTPd Version Updated

Upgraded Pure-FTPd to 1.0.52 to address [CVE-2024-48208](#).

jq Version Updated

Upgraded `jq` to version 1.8.1, resolving minor security issues.

Inode and Journal Configuration Changed

The ext4 system partition inode size has been increased to 256 bytes to ensure timestamp support beyond the year 2038, and the journal size has been unified across all platforms to 1 MiB.

Deprecated

OpenVPN Compression Deprecated

OpenVPN *compression* is no longer recommended and should be avoided. Enabling this option no longer activates actual compression; instead, it only enables compression framing so that the system can receive already-compressed packets from legacy peers.

LAN Status Command Deprecated

The commands `status lan X` are deprecated. Use the updated form `status ethX`, which reflects the current interface naming conventions.

PPP Status Command Deprecated

The commands `status ppp X` are deprecated. Use `status mwan X` instead, as it provides the proper status reporting for multi-WAN interfaces.

Removed

Legacy Configuration Restore Removed

Support for restoring configuration files from firmware versions older than 6.2.0 has been removed. Upgrading from older firmware is still possible, but certain configuration fields will be reset to their default values.

FTP Helper Settings Removed

The *FTP Helper* settings have been removed from S1 routers, as these models do not support FTP functionality.

Deprecated `gsmsms` Command Removed

The deprecated `gsmsms` command has been removed. Use the `sms` command as its replacement.

Fixed

ICR-2x5x NAM Classification Fixed

ICR-2x5x devices were corrected to be recognized as non-NAM products. This enables proper WiFi *Country* selection on these devices.

RS-485 Detection Fixed

Fixed RS-485 port detection on SR303 and SR304 routers equipped with two RS-485 ports (models SR303xx6xx and SR304xx6xx).

IPsec Operation After IP Change Fixed

Resolved an issue where IPsec failed after an IP address change (for example, following a SIM switch). Previously, SNAT and DNAT tables were not updated correctly, causing certain flows to drop.

ETH Status Reporting Fixed

Fixed Ethernet status reporting on ICR-44xx devices when *Bridged*. The *Bridged* state was not detected correctly and the *IP Address* field appeared as Unassigned.

SMS Support on ICR-2437 Fixed

Fixed SMS functionality on ICR-2437 devices equipped with the ML620 module.

SMS Delivery on Verizon Network Fixed

Fixed an issue preventing SMS messages from Verizon from being delivered to US-based recipients.

SNMP CPU Usage Reporting Fixed

Corrected the SNMP `statusCPUUsage` value to match the usage reported in the *System Information* status.

Timezone Reconfiguration Fixed

Fixed *Timezone* reconfiguration from the command line, including through WebAccess/DMP. Previously, a device reboot was required for timezone changes to take effect.

SSH Public Key Display Fixed

Fixed the display of the *SSH Public Key* on the *Modify User* page. Previously, only the first 256 characters were shown.

Static Routes Interface List Fixed

Fixed the *Interface* selector in the *Static Routes* configuration to display only currently available interfaces.

WiFi 40MHz Channel Filtering Fixed

Corrected filtering of 40MHz-wide *Channels* in the *WiFi AP* configuration for the 2.4GHz band.

Permissions for Firmware Update Page Fixed

Fixed permissions so that the *Update Firmware* page is no longer shown to non-admin users.

Configuration Restore Fixed

Fixed configuration restore so that settings are no longer modified when an empty file is provided.

System Report Process List Fixed

Fixed the System Report to include the list of running processes along with their full argument sets.

lpm -i Argument Validation Fixed

Fixed argument validation for the `lpm -i` command. Only values between 1 and 16777215 seconds are now accepted.

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.