Release Notes

Firmware 6.5.2

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on 3rd March, 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**: 6.5.2
- **Release Date**: March 3, 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

DNSSEC Queries Support

The support for DNSSEC queries was added and router now enables LAN devices to query DNS records protected by cryptographic signatures.

IP Address Ranges Support

The support for IPv4 and IPv6 address ranges has been added to *Firewall* settings, allowing the *Source* or *Destination* address to be in format `192.168.1.100-192.168.1.200` .

`Any` in the IPv4 and IPv6 *Static Routes Interface* selection

Users can now, for example, set up static routes towards a GRE tunnel.

VRRP Interface configuration

Interface configuration to *VRRP* was added for enabling users to select *ETHx* or the Ethernet *Bridge*.

Wireguard MTU Configuration

Setting the MTU (Maximum Transmission Unit) in WireGuard is beneficial for optimizing performance, avoiding fragmentation, and ensuring stable connections.

Password Quality Indicator

Password quality indicator has been added into *L2TP* and *PPTP* Configurations. A password quality indicator helps users create stronger passwords.

Network Status Extended

Network Status was extended to display currently selected *Backup Routes*.

Implemented `service syslog reload`

The command `service syslog reload` was implemented to enable rotation of log files.

Changed

List Behavior

Several lists now hide unused items and support a larger number of entries. Initially, only two items are shown, but as the last item is filled, two more will automatically become visible.

- The maximum number of *Firewall* rules has increased from 16 to 32.
- The maximum number of *NAT* rules has increased from 16 to 64.
- The maximum number of *Static Routes* has increased from 8 to 32.
- The maximum number of *static DHCP leases* for Ethernet and VLAN has increased from 6 to 32.

WiFi AP Configuration

Updated WiFi AP configuration to prevent invalid parameter combinations from being displayed. Only valid options are now selectable.

- The *Channel* selection now only offers legal channels supported by the hardware. **To see the correct list, the *Country Code* must already be applied**.
- 5 GHz and 6 GHz channels are no longer available if the country code is set to 00. A warning is displayed, indicating that this is due to legal restrictions.
- Bandwidths with no available channels are no longer offered.
- Renamed the ill-named `WIFI_AP_HT40` setting item to `WIFI_AP_BANDWIDTH` .

NTPv4 Implementation

Internal NTPv4 implementation was changed (except for ICR-2000, ICR-2400, ICR-2500 and ICR-2600 router families). Ntp was replaced by chrony 4.6.1, which provides higher stability and reliability.

TCP Timestamps

TCP timestamps (set net.ipv4.tcp_timestamps=0) were disabled for security reasons.

IPv6 Address Fields Behavior

IPv6 address fields have been modified to accept uppercase characters in IPv6 addresses.

Sensitive Configuration Parameters

The removal of sensitive configuration parameters from reports has been improved. Now, only options ending with `PASS` , `PASSPHRASE` , and `PASSWORD` are removed. Previously, all options containing the substring `PASS` , including words such as `PASSIVE` , were removed.

GRE Pre-shared Key Display

The GRE Pre-shared Key is now displayed in plain text, as it is not considered sensitive information.

Removed

802.1X Option From WiFi AP Configuration

The *802.1X* option has been removed from the WiFi AP configuration because it was misleadingly named and enforced WEP encryption with static keys, which is highly insecure. The 802.1X protocol is still supported in combination with WPA encryption under the *WPA-Enterprise* options.

Fixed

Cellular Modem Failures

Previously, the cellular modem could restart under heavy load (when downloading large files), causing transmission failures. This issue affected PLS8, PLS83, MC7304, LM960, MPL200, EC25, BG96, and FM101 cellular modems.

WiFi Issues

Several WiFi issues have been fixed:

- Fixed authentication on ICR-2xxxW routers, particularly authentication using WPA3-PSK and to some AP, notably Ubiquiti UniFi 6 Lite.
- Fixed ability to set 6GHz WiFi channels 3, 5 or 7. Previously the error *Error during HOSTAPD configuration update.* was displayed.
- Prevented firmware reboot when connecting to a 5 GHz WiFi AP on ICR-2xxxW routers.
- Fixed WiFi STA termination on ICR-4400 devices. The bug caused termination of the first WiFi connection after calling `service wifi2 stop` or `service wifi restart` .
- Fixed visibility of the *WPA PSK Secret* in both WiFi AP and STA configuration.
- Fixed broken field validation JavaScripts on platforms limited to the `00` country code.
- Fixed automatic pre-filling of configuration fields after applying WiFi STA settings on ICR-2xxx routers. Previously, the fields were empty when the user clicked Back after applying changes.

NTP Avalability

Resolved an issue where NTP would be available after losing Internet connectivity. Previously, NTP would terminate upon connection loss and fail to start again.

NAT64 Availability

Fixed the availability of NAT64 on ICR-2000, ICR-2400, and ICR-2500/2600 router models.

SSH Session Timeout

Fixed the SSH logoff after session timeout. Previously the connections were always closed after 1 hour of inactivity regardless the *Session Timeout* value.

Keys Backup

Resolved an issue with backing up *SSH Public Keys* and *Secret Keys* for *Two-Factor Authorization*. These settings were previously missing from the *Backup Configuration*, causing them to be lost after a firmware upgrade.

GPS Module Termination

Fixed improper termination of the GPS module, which led to unexpected error messages and frozen location data.

Web Administration Issues

Fixed several Web administration issues:

- Fixed a malformed Content-Security-Policy header.
- Fixed broken field validation JavaScripts for non-admin users.
- Improved security and HTML validity. The pages are now more compliant with HTML standards and better check input values.

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.