Release Notes

Firmware 6.5.1

ICR-OS

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on 27th November, 2024.

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**: 6.5.1
- **Release Date**: November 28, 2024
- ❗ **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

Minimum Severity Syslog Configuration

The *Minimum Severity* setting has been added to the *Syslog* service configuration across all platforms. This feature allows administrators to optimize the volume of system log messages, improving manageability and performance.

USB Ports Disabling

The ability to disable USB ports has been extended to all platforms for enhanced security. Previously, this functionality was only available on ICR-4400 devices.

Postinstall Scripts

Support for *postinstall* scripts has been added to RouterApps. These scripts can now be executed:

- After a RouterApp is installed.
- During the first startup of a RouterApp following an update.

Changed

NAT64 Configuration

- NAT64 is now disabled by default. An option to explicitly *Enable NAT64* has been added to the *IPv6 NAT Configuration*. Previously, NAT64 was always enabled by default.
- A default firewall rule for NAT64 has been introduced. This rule is disabled by default.

NAT64 Implementation Replacement

The Ecdysis NAT64 implementation has been replaced with the NAT64 implementation provided by *Jool*. Ecdysis had been unmaintained for over 10 years. The Jool implementation introduces slightly different behavior:

- Only incoming traffic can be translated using NAT64; traffic originating from the router will not be translated.
- Jool uses netfilter instead of a virtual network interface, so there is no longer a NAT64 interface.
- A `null0` virtual interface and a relevant entry in the routing table have been added to ensure the routing table always contains an entry matching the NAT64 prefix.
- Jool drops all incoming packets with a source IPv6 address matching the NAT64 prefix. It is not recommended to enable NAT64 on multiple routers configured in series.

`hostapd` and `wpa_supplicant` Improvement

The configuration for `hostapd` and `wpa_supplicant` has been fine-tuned for improved performance. Changes include:

- Reduced WiFi re-scanning delay to 30 seconds when WiFi follow STA is enabled.
- Added proper disconnection from the WiFi network when stopping the WiFi station.
- Prevented connections with incorrect settings by ignoring outdated WiFi scan results.
- Introduced failsafe termination for `hostapd` if it fails to shut down in time.
- Enabled background radar detection.
- Fixed failures when stopping the AP-STA daemon.
- Added support for Operating Channel Validation (excluding the Laird SU60-SIPT).

Certificates Update

The `ca-certificates` bundle has been updated to the version released on 2024-09-24.

`curl` Update

The `curl` utility has been updated to version 8.11.0, addressing several minor security issues.

User Administration Update

The *User Administration* page has been renamed to *Manage Users* for improved consistency.

Fixed

Emergency Factory Reset

Fixed the *Emergency Factory Reset* issue. In routers running firmware version 6.5.0 with a `Pxxxxxxxxh` password, the emergency factory reset incorrectly initialized the default password to `PN/Ah` .

Certificate Configuration

Resolved an issue with the *Certificate* field in *HTTP Configuration*, which now properly accepts a full certificate chain. Previously, only the first certificate was loaded, while additional chain certificates were ignored.

SSH Public Key

Fixed the display of the configured *SSH Public Key* on the *Modify User* page. In firmware version 6.5.0, this field was incorrectly shown as empty even when a key was configured.

User Keys Reset

Fixed removal of SSH and two-factor authentication keys after a configuration reset. Previously, the user-uploaded keys were not removed.

Syslog Restart

Improved the reliability of Syslog service restarts. In some scenarios under firmware version 6.5.0, the Syslog service failed to restart after being stopped.

Cellular Modem Communication

Enhanced the robustness of QMI and MBIM communication. Previously, cellular communication could become indefinitely blocked when a faulty cellular module failed to respond to commands.

WiFi Issues

Resolved multiple WiFi-related issues:

- Fixed auto WiFi channel selection (ACS) for SG901-1059B and TI WL1837MOD in SmartStart, SmartFlex, and SmartMotion products.
- Corrected failures during restarts of the AzureWave AW-CM358 module on ICR-2000 devices.
- Restored the ability to use WiFi channel 13 on ICR-4400 devices with the Compex WLE900VX-I module.

DNS64

Addressed an issue with DNS64 address resolution when only an IPv4 network was available, but the destination supported IPv6. In previous firmware versions, the NAT64 address was always returned without attempting to resolve the IPv6 address via IPv4. The router now prioritizes resolving the IPv6 address and only falls back to NAT64 if the destination supports IPv4 exclusively.

Cellular Connections to IPv6

Fixed cellular connections to IPv6-only APNs. Previously, even when the *IP Mode* was set to IPv6, the device incorrectly reported itself as IPv4v6 to the cellular network.

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.