Release Notes

Firmware 6.5.0

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on 9th October, 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**: 6.5.0
- **Release Date**: October 8, 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

VLAN Tagging

Added *VLAN* tagging (IEEE 802.1Q) support. The *PPPoE* parameters *VLAN Tagging* and *VLAN ID* were replaced with the option to use a VLAN as the PPPoE Interface.

Sites Blocking

A new configuration page *Sites* has been added under the *Firewall* section. Here, you can define site (URL) addresses to be blocked by the Firewall.

Secondary DNS Server

Added configuration for a *Secondary DNS Server* to the *Ethernet*, *Mobile WAN*, *PPPoE*, and *WiFi Station* configuration pages.

NTP Configuration

The following NTP Configuration options have been added: *Tertiary NTP Server*, *Maximal Polling Interval*, and *Enable fast initial synchronization*. For descriptions of these new items, refer to the *Configuration Manual*.

Note: Not available for ICR-2000/2400/2500/2600 platforms.

Syslog Configuration

Added more Syslog Configuration options:

- Ability to send *Mark Messages* for syslog availability checks.
- Ability to forward syslog messages via TCP and SSL/TLS, optionally with certificate-based authentication (the Secure Syslog Router App has been integrated into the firmware).

Note: Not available for ICR-2000/2400/2500/2600 platforms.

Improved Password Fields

All password fields in the GUI now have an "eye" icon to toggle password visibility. Additionally, fields for password generation now include a colored bar indicating the password complexity.

Last Login State

Added information about the last successful and failed logins. This is displayed after each SSH login and also in the *Security Information* section on the *General Status* page, where specific details about the last logged-in user, the login timestamp, and the number of failed login attempts are shown.

Free Space Indication

A new line, *Free space*, has been added to the *Status* → *General* section under *System Information*. This row provides information about the free space available for RouterApps and user data. Similarly, the free space for RouterApps is indicated on the *Customization* → *Router Apps* page.

Active Connections Page

Added a *Connections* status page showing a list of active connections. The page can be accessed via a link at the bottom of the *Network Status* page.

Ed25519 SSH Key

Added support for the Ed25519 SSH key, which provides better security and shorter creation times. This is now the default for the *FirstNet* models.

CA Certificate for Automatic Update

To enhance security, options to configure CA certificate validation for *Automatic Update* have been added.

Session Timeout Handling

Added auto-redirection to the login page when the HTTP *Session Timeout* expires.

Warning on Inactive JavaScript

A warning has been added to the Web GUI when JavaScript is disabled or unsupported by the web browser. It is highly recommended to enable JavaScript when accessing the Web administration.

Device Management Information (DMI)

Product identifiers have been added to the standard `/sys/class/dmi/id/*` tree.

New `os-release` Variables

New system variables have been added to `/etc/os-release` :

- The `VARIANT` variable indicates a specific product variant, for example, `1N` for the *FirstNet* models.
- The `ICR_FEATURES` variable can contain system flags that are utilized by the system, such as `HAS_INSECURE_OPTIONS` , `HAS_INTEGRITY` , or `HAS_LARGE_STORAGE` .

Logging Enhancement

Added more logging of administrative actions to syslog, including firmware upgrades and configuration backup/restores.

Encrypted Firmware Support

Added support for encrypted firmware images on the *FirstNet* models. Currently, such files are distributed only for individual projects and are not publicly available on the Engineering Portal.

Added Favicon

Added a favicon to the Web administration, allowing easier identification of the page among other open tabs.

Changed

User Management Enhancements

Significantly enhanced user management for better security across all platforms:

- User-related configuration options have been merged into a single dialog: *Manage Users* for admin roles and *Modify User* for user roles.
- Passwords must follow configurable complexity levels (very weak, weak, good, strong). Standard platforms require at least 6 characters (very weak). The *FirstNet* models require at least 12 characters (good).
- Passwords can be configured to expire after a default time period.
- Users currently logged in can only change their password after entering the previous password.
- Default user passwords and passwords set by the admin are expired by default and must be changed upon first login.
- Password change notifications can be delivered via email or SMS.
- Account lockout after unsuccessful login attempts now applies to SSH and potentially other login methods.
- Two-factor authentication can be configured using a QR code.
- The uploaded file for the *Secret Key* is now limited to 512 bytes.

PAM Service Updates

Renamed *PAM* service configuration to *Authentication Configuration* and added multiple options:

- The fail-lock parameters (*Lock Account After*, *Count Fails For*, *Unlock After*) are required on *FirstNet* models. It is optional for other platforms.
- Desired password complexity (*Force Password Complexity*).
- Delay between two login attempts (*Delay After Fail*).

WiFi AP Channels

Enhanced WiFi AP Channel selection:

- *Auto* channel selection (ACS) is now supported and enabled by default, except for SmartStart, SmartFlex, and SmartMotion routers.
- The selection box only includes channels supported by the WiFi module and the selected *Country Code*. Note that after changing the country code, you must click *Apply* to see the corresponding channels.

WiFi PSK File

Removed the *PSK file* option from the *WPA PSK Type* in the Wi-Fi Station configuration. Use the *256-bit secret* option, which behaves exactly the same.

WiFi AP Options

For *FirstNet* models, the *Extra Options* configuration option was removed from Wi-Fi AP and WiFi Station configuration pages due to security concerns.

Default Settings Changes

Changed default settings for better security. These settings can be modified via Web administration:

- Enabled both IPv4 and IPv6 firewalls by default, allowing all traffic originating from the default network 192.168.1.0/24.
- Disabled SNMP by default.

NAT Configuration

Added the possibility to configure *FTP Helper* and *PPTP Helper* ports in the IPv4 and IPv6 NAT configuration. Previously, the helpers were enabled on all ports, which might disrupt non-FTP or non-PPTP traffic.

ICMP Redirects

Disabled handling of ICMP redirects (accept_redirects) for higher security.

Syslog Limit

Changed Syslog *Size Limit* units from lines to kibibytes (KiB). The lines were previously limited to 1024 characters, so this should not affect the maximum file size.

SSH Ciphers

Disabled SHA1-related ciphers in the SSH service. These ciphers are considered insecure. The same restricted set of ciphers now applies to the SSH client as well.

`passwd` Command Enhancement

Switched to a full implementation of the `passwd` command, which now offers more options.

HTTP Header Security

Modified the *Content-Security-Policy* HTTP header for better security: Removed the `unsafe-eval` option, so the execution of the `eval()` function is now prohibited. Executing JavaScript from a string poses a significant security risk.

NTPv4 Implementation

Switched to a standard NTPv4 implementation based on ntp 4.2.8p18.

Note: Not available for ICR-2000/2400/2500/2600 platforms.

Linux Kernel Upgrade

Upgraded to Linux Kernel version 6.1.90, fixing a few minor security issues.

`OpenSSL` Software

Upgraded OpenSSL to version 3.0.15 to address a few minor security issues.

`OpenSSH` Software

Upgraded `OpenSSH` to version 9.8, mainly due to CVE-2024-6387 (high).

`OpenVPN` Update

Updated `OpenVPN` to version 2.6.12 to fix a few minor security issues.

`strongSwan` Update

Updated `strongSwan` to version 5.9.14.

`hostapd` and `wpa_supplicant` Update

Updated `hostapd` and `wpa_supplicant` to version 2.11 and optimized the configuration for more reliable connectivity.

IPsec Ciphers

Disabled DES, 3DES, and MD5 encryptions in *IPsec* configuration on *FirstNet* models for better security.

RouterApp Initialization

Modified the RouterApp defaults invocation to be called after the first startup of the device as well.

SSH Key Generation

Moved SSH key generation to device startup to make the initial setup of the SSH service faster.

SSL Security Improvements

Moved `/usr/ssl/*` to `/etc/ssl/*` for better consistency with the FHS and enhanced security on the *FirstNet* models.

Welcome Page

Modified the welcome page to display only when a `/var/data/*/.welcome` file does not exist.

Firmware Update Process

Modified the `fwupdate` command to delete the source `.bin` file during the upgrade when stored in `/tmp` . This is to preserve more space for the upgrade.

WiFi Database

Integrated the Wi-Fi regulatory database into the Linux Kernel image.

Kernel Logging

Increased the size of the Linux Kernel ring buffer for better logging.

GPRS Options

Removed unsupported GPRS options for ICR-2041, ICR-2441, and ICR-3241 routers.

Deprecated

`gsmsms` Command

The `gsmsms` command is deprecated and will be removed in version 6.5.0. The `sms` command should be used instead.

Fixed

WiFi Connectivity

Fixed WiFi connectivity issues on multiple platforms, including ICR-3200, ICR-4100/4200, and ICR-4400. Additionally, the issue where the WiFi connection failed when clicking *Connect* on the *Status* → *WiFi* → *Scan* page for SSIDs with leading or trailing space characters has been resolved.

Reboot Fix

Fixed device reboots that occurred when startup took more than 60 seconds, such as during the generation of large keys.

HTTP 404 Pages

Fixed the display of HTTP 404 pages. These are now only shown to authenticated users for security reasons.

Mobile WAN Status

Fixed the missing mobile WAN status on ICR-2734 (PLS83-EP).

IPv6 Firewall

Fixed the IPv6 firewall to allow DHCPv6 traffic.

IPv6 Autoconfiguration

Fixed the condition to start SLAAC IPv6 autoconfiguration. It now correctly starts only when the network mask is 64 bits.

Admin Access

Fixed access for `admin` users to `/var/data` .

Automatic Update

Increased the randomness of the dynamic *Automatic Update* window.

Concurrent SSH Key

Avoided concurrent SSH key generation when invoked multiple times.

Users Restore Robustness

The robustness of the user restore process has been enhanced. If a corrupted backup would result in a broken admin account, a standard admin account with a default password will be restored.

Firmware Update

Enhanced the robustness of firmware upgrades to prevent malicious users from injecting custom files into the upgrade process.

`jq` License

Fixed the version of `jq` in the list of licenses.

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.