

Release Notes

Firmware 6.4.0




Abstract

This document encompasses the following key sections:

- **Firmware Update Instructions:** Guides users through the firmware update process, ensuring 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:** 6.4.0
- **Release Date:** February 7, 2024
-  **Compatibility and Distribution:**

It is important to note that this firmware version is not intended for mass production. Due to the implementation of many fundamental changes, it is highly recommended to thoroughly test the new firmware before considering its deployment in a production environment.

For comprehensive compatibility details and distribution guidelines, see the [Firmware Compatibility Chart](#) document published with the specific firmware version.

Firmware and Product Documentation Notice

- **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
	General Update Instructions and Notices	5
	FirstNet Firmware Specific Notes	5
II	Description of New Features, Changes, and Fixes	6
	Added	7
	Changed	11
	Fixed	14
	Security	16
III	Known Issues Related to the Firmware Version	17

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.
- **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

Router Apps Online Installation

The introduction of Advantech's new feature, the online Router Apps installation, marks a significant advancement in router management. This feature streamlines the process of adding Router Apps to Advantech routers, making it more efficient and user-friendly.

Users can access the Router Apps through the router's web interface, specifically under the *Customization* → *Router Apps* section. By default, the connection to the public Advantech server is enabled. Upon connection, clicking the *Load Available Apps* button will present a variety of Router Apps, each accompanied by a brief description.

The online Router Apps installation represents a significant enhancement in the user experience for Advantech router users. It consolidates the installation process into a single, intuitive platform, eliminating the need for manual downloads and installations. This not only saves time but also ensures that users can effortlessly explore and utilize new Router Apps, thereby enhancing the functionality of their Advantech routers. For more details about this feature, see the *Configuration Manual* of your router.

WiFi Scan Display Improvements

The display for the WiFi Scan (*Status* → *WiFi* → *Scan*) has been updated to enhance user interaction with a more intuitive design. For improved clarity, detailed information about each network is now collapsed and can be viewed by clicking on the *More Information* link. Additionally, each network now features a signal strength icon and a *Connect* button, directing users to the *Configuration* → *WiFi* → *Station* page. Here, relevant fields are pre-populated, simplifying the network connection process by entering authentication details.

Online Firmware Update

With the advent of the online installation feature, updating the router's firmware online is now possible, eliminating the need for manual downloading and installation. The firmware is downloaded in a similar manner and from the same server as the Router Apps, making it imperative to maintain a functional connection to a server that supports online installation, as outlined in the previous section.

The firmware update process is conducted on the *Administration* → *Update Firmware* page. On this page, click the *Check for updates* button; information regarding the availability of a new firmware version will be displayed, accompanied by a button to download and install it.

Passwordless Console Login

There is a new feature enabling you to log in to the router via SSH without a password, using the SSH Public Key. Note that only users with the Admin role are permitted to log in to the router with SSH. For detailed information about public key generation and the entire configuration process, see the *Configuration Manual*, section *Administration* → *Users* → *Passwordless Console Login*.

CPU & Memory Usage Information

This update introduces a valuable feature for monitoring system performance. Users can now view real-time information regarding CPU and memory usage. This information is readily accessible on the *Status* → *General* page, specifically within the *System Information* section.

For convenience and to ensure up-to-date information, there is an option for automatic updates. By clicking the *Refresh* button located in the upper right corner of the GUI page, users can enable the interface to update these values dynamically.

RTC Setting from Web UI

The recent enhancement to the Real Time Clock (RTC) feature introduces a convenient way to synchronize the router's clock with the user's web browser time. By simply clicking the *Apply browser time* button (*Administration* → *Set Real Time Clock*), users can ensure the router's internal clock matches the current time displayed in their web browser. This improvement facilitates an easy and efficient method to maintain accurate time settings on the router.

SIP ALG Support

The most recent firmware update introduces support for SIP ALG, an abbreviation for *SIP Application-Layer Gateway*. This feature is a significant enhancement for users who rely on multimedia sessions, such as internet telephony calls, facilitated by the Session Initiation Protocol (SIP).

SIP ALG plays a crucial role in the management of SIP traffic, especially in networks utilizing Network Address Translation (NAT). It aids in the establishment, modification, and termination of SIP-based multimedia sessions. By inspecting and modifying SIP packets as necessary, SIP ALG ensures that they navigate through NATing firewalls without issues. This is particularly important in environments where SIP traffic must pass through a firewall or router that performs NAT.

Working Directory in Shell Prompt

The latest update to the Advantech routers brings a user-friendly enhancement to the *BusyBox* shell prompt, commonly used for the console environment. This improvement involves displaying the current working directory within the shell prompt. This new feature significantly enhances user experience by making navigation within the *BusyBox* environment more intuitive.

Follow WiFi STA Radio Settings

The introduction of the *Follow STA radio settings* parameter in the Wi-Fi Access Point (AP) configuration marks a significant advancement in network adaptability. This new parameter, when activated, changes the behavior of the Wi-Fi AP to dynamically align its radio settings with those of a foreign AP to which the Station (STA) is connected.

By default, this parameter is disabled, meaning the AP operates as it traditionally has. In this default mode, the AP maintains its predetermined radio settings regardless of the STA's connection status. However, when the *Follow STA radio settings* parameter is enabled, it allows the AP to automatically adjust its radio settings – such as frequency, channel, and other relevant parameters – to match those of the foreign AP currently connected to the STA.

This feature is particularly useful in environments where the AP needs to be flexible and adapt to various network conditions. It ensures a more seamless and efficient network experience, especially in scenarios where the STA frequently connects to different foreign APs with varying configurations.

SNMP Custom Field

In the latest update to the SNMP (Simple Network Management Protocol) configuration, a new and flexible feature has been introduced: the Custom field. This addition complements existing parameters such as *Name*, *Location*, and *Contact*, offering users the ability to input and manage data as per their specific requirements.

The Custom field provides enhanced versatility in SNMP configurations. Users can utilize this field to store and manage additional information that is pertinent to their network management and monitoring needs. This could include unique identifiers, specific configuration details, or any other data that aids in more effective network management. The introduction of this field is a significant step towards offering more customizable and adaptable network management tools.

Profile SNMP OID

The SNMP (Simple Network Management Protocol) OID (Object Identifier) structure in the router has been enhanced with the addition of a new read-only OID, .1.3.6.1.4.1.30140.6.10, labeled as *infoProfile*. This OID is specifically designed to represent the current configuration profile of the router.

The *infoProfile* OID can assume one of four values: *standard*, *alt1*, *alt2*, or *alt3*. These values correspond to the standard configuration profile and three alternative configuration profiles, respectively. This feature allows for easier monitoring and management of the router's configuration state via SNMP.

SNMP for Binary Inputs

The SNMP (Simple Network Management Protocol) configuration has been further enhanced with the addition of entries for the binary inputs BIN2 and BIN3. This update extends the SNMP monitoring capabilities to these specific binary inputs, allowing for more comprehensive network management and monitoring.

PPPoE Configuration Enhancement

Maximum Segment Size Clamping feature has been incorporated into the PPPoE Configuration settings, serving an essential function in boosting network efficiency and stability. By dynamically adjusting the TCP packets' Maximum Segment Size (MSS) to match the Path Maximum Transmission Unit (PMTU) of the network, it ensures enhanced data flow. This feature is activated by default, promoting optimal transmission efficiency.

OpenVPN Security Level

The *Security Level* option has been incorporated into the OpenVPN configuration settings. This option allows for the configuration of the security level, offering these five options: *Weak*, *Low*, *Medium*, *High*, and *Very High*. For more details, see the *Configuration Manual*. It is strongly recommended to set the option to at least *Low* to meet the minimum security requirements.

Syslog Configuration Enhancements

The Syslog configuration now supports specifying a hostname in the *Remote Host* address setting, with DNS translation refreshed every 60 minutes. Furthermore, the display window for syslog output has been expanded from 30 to 50 lines, improving visibility of log entries.

Cellular Registration Timeout

A new configuration feature now allows for the customization of the cellular network registration timeout. Although the standard 2-minute timeout suffices for most scenarios, there are specific cases where adjustments are necessary. To cater to such needs, configuration options named `PPP_REG_TOUT`, `PPP_REG_TOUT2`, `PPP_REG_TOUT3`, and `PPP_REG_TOUT4` have been introduced. These options allow for configuring the registration timeouts for the first to the fourth SIM cards, respectively. Expressed in seconds, these settings offer precise control over the network registration timing. Adjustments can be made via the router console or incorporated into startup scripts, though they are not available through the graphical user interface (GUI).



For experts only. Incorrect usage can lead to system instability or malfunction.

Added `xxd` Command

The `xxd` program, a command-line utility for generating a hex dump of a given file or standard input, has been added to the firmware. For more information, see the [Command and Scripts Application Note](#).

Changed

Linux Kernel Upgrade

The most significant change in this firmware release is the substantial upgrade of the Linux kernel to version 6.1. This upgrade introduces a series of vital updates and modifications, pivotal for this transition.

Alongside the kernel upgrade, we are also introducing an updated version of Toolchains. This new version is freely available on the [Toolchains](#) page. It is utilized for compiling the source codes of Router Apps.



For Router Apps intended to run with the updated kernel, it is mandatory to use the new Toolchain for compilation. Likewise, older versions of Router Apps may not function correctly with the firmware containing the new kernel. Therefore, we strongly recommend updating all installed Router Apps in conjunction with upgrading your router to the new firmware.

Updated OpenVPN Software

The OpenVPN software in our system has been updated from version 2.4.12 to version 2.6.8. This update addresses the critical security risks identified as [CVE-2023-46850](#) (critical) and [CVE-2023-46849](#) (high).



Users should be aware of compatibility issues between OpenVPN versions 2.6 and 2.4, as well as between OpenSSL versions 1.1 and 3.0. Some features in OpenVPN 2.6 have been deprecated and will be removed in future releases, which may lead to compatibility problems. Users are advised to avoid using these deprecated features. For more detailed information and guidance, please refer to the *Configuration Manual*. In case of issues with setting up the OpenVPN tunnel, verify the *Security Level* settings, which can now be newly set, see the relevant section in this document.

Updated OpenSSL Library

We have updated the OpenSSL library in our firmware. The previous version 1.1.1, which will no longer be supported after September 11, 2023, has been replaced with the newer version 3.0.12. This upgrade enhances the security and functionality of our firmware. For detailed information about the changes in the new OpenSSL version, please refer to the [OpenSSL Changes](#) webpage.



The security strength of SHA1 and MD5 based signatures in TLS has been decreased. Consequently, SSL 3, TLS 1.0, TLS 1.1, and DTLS 1.0 are no longer functional at the default security level 1. Additionally, X509 certificates signed using SHA1 are disallowed at security level 1 and higher. Furthermore, compliance with RFC 5746 for secure renegotiation is now mandatory by default for SSL or TLS connections to be successful. This change is part of an ongoing effort to enhance security standards and protect against vulnerabilities.

System Password Storage

System passwords are now secured using the SHA-512 security algorithm, replacing the previous SHA-256 method.

WiFi `regdb` Update

The built-in regulatory database (`regdb`), which is a configuration API for 802.11 wireless networks in the Linux kernel, has been updated to align with the new kernel version. This update ensures that the `regdb` is fully compatible and optimized for the latest kernel enhancements. The regulatory database is crucial for managing wireless network settings in compliance with regional regulations. It contains information about allowed channels, power levels, and frequency use for wireless networking in different countries.

Enhanced `DynDNS` Status Report

A new line of information has been added to the `DynDNS` status page to report the state of `DynDNS` reconnection.

Limiting `/tmp` Filesystem Size

To protect system resources, the maximum size of the `/tmp` filesystem is set to 50% of the RAM size. Writing more data than this limit will result in a failure.

Updated `iproute2` Program

The `iproute2` program has been updated to version 6.1, providing necessary support for the new kernel version.

Updated `ethtool` Program

The program for displaying and modifying the parameters of network interface controllers, named `ethtool`, has been updated to version 6.5.

Updated `iw` Program

The program used for configuring and displaying information about wireless devices, referred to as `iw`, has been upgraded to version 5.19.

Updated `strongSwan` Software

We have updated the `strongSwan` software to version 5.9.13. This update has fixed [CVE-2023-26463](#) (critical) and [CVE-2023-41913](#) (critical).

Updated OpenSSH Software

The OpenSSH software has been updated from version 8.8p1 to version 9.6p1. This update addresses the critical security risks identified as [CVE-2023-38408](#) (critical) and [CVE-2023-48795](#) (medium).

Updated curl Program

We have updated the curl program to version 8.4.0. This update has fixed [CVE-2023-38546](#) (low), [CVE-2023-38545](#) (critical), [CVE-2023-38039](#) (high), [CVE-2023-28322](#) (low), [CVE-2023-28321](#) (medium), [CVE-2023-28320](#) (medium), and [CVE-2023-28316](#) (critical). For more details about this release, see the [Curl Changelog](#) webpage.

Fixed Net-SNMP Software Security Issues

We have updated the Net-SNMP software to version 5.9.4 to fix security issues [CVE-2022-44792](#) (medium) and [CVE-2022-44793](#) (medium).

Fixed

Date in Emails

The latest firmware update rectifies an issue related to the router's email functionality, where previously, the date information was absent in the data section of emails produced by the router. This problem has now been effectively resolved.

WiFi Startup

The firmware update includes a crucial fix for the *hostapd* daemon, addressing a previously identified issue where a configuration error was causing the WiFi script to fail to start. This fix rectifies the problem, ensuring that the *hostapd* daemon initiates correctly and operates as intended.

VRF Support

The recent update to the kernel includes the addition of *CGROUP_BPF* in the Linux kernel, enabling support for Virtual Routing and Forwarding (VRF) configuration. The integration of *CGROUP_BPF* (Control Groups Berkeley Packet Filter) is a key enhancement for network administrators. It allows for more sophisticated and flexible management of network traffic. With VRF, it's possible to create multiple virtual routing tables within the same router. This facilitates the segregation of different network segments, allowing for more controlled and secure routing of traffic.

ETH2 Bridge MAC

The firmware update addresses a problem where an invalid MAC address appeared on the ETH0 interface, typically when bridged with the ETH2 interface. This correction guarantees that the MAC address on ETH0 is now valid and operates correctly, applicable exclusively to the v4 platform.

VRRP Ping

The issue with ping functionality in VRRP, where it only worked correctly for *Ping Interval* values less than 4250 seconds, has been resolved. Previously, for intervals over 4250 seconds, the ping occurred continuously, which is no longer the case.

SNMP for Serial Number

A fix has been implemented for an SNMP issue that caused the SNMP get for the serial number to become blocked after any system reboot, whether soft or hard. This problem was resolved after the first login on the WebGUI, but the fix now ensures uninterrupted SNMP functionality post-reboot.

Docker Container Availability Issue

The recent firmware update has successfully addressed the issue with the *Docker* Router App, which was previously unable to install containers. This problem stemmed from an unreachable repository, impeding the App's functionality. With this resolution, the *Docker* Router App can now seamlessly install containers, enhancing its usability and efficiency.

Ntpdate Issue

The *ntpdate* command has been updated to fix a buffer overflow issue, enhancing its security and stability.

WiFi Domain

The issue affecting Wi-Fi channels, which were not functioning despite being supported by the country code, has been resolved. Users can now configure channels without encountering problems. This fix is applicable only to ICR-3xxxW products.

Licenses List

The issue where the license page in the Web GUI did not display the full list of licenses, especially for Router Apps with many dependencies like Node-RED and their nodes, has been fixed.

SNMP Reporting

The issue where the SNMP item `mobileReportPeriod` (OID 1.3.6.1.4.1.30140.4.22) was not returning any value has been fixed.

Iptables Extensions Installation

We have resolved the issue with installing iptables extensions, which are essential for certain RouterApps, such as *NetFlow/IPFIX* RA.

Security

Password Protection in GUI

For security reasons, the graphical interface has been modified to prevent the copying of sensitive data, such as passwords, from any field into the clipboard, thereby securing the data from unauthorized access.

Fixed DoS Attack Crash

The firmware update resolves an issue where the *totd* daemon stopped functioning after a DoS attack on the router, affecting DNS address resolution.

Part III.

Known Issues Related to the Firmware Version

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 encountering this issue, 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's important 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 have any 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.