Release Notes

Firmware 6.4.2

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**: 6.4.2

- **Release Date**: Aug 1, 2024

- 🛑 **Compatibility and Distribution**:

  Due to significant changes introduced in 6.4.0 update, extensive testing of the new firmware is strongly advised prior to its deployment in operational environments, when upgrading from version 6.3.x.

  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.

- **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

`jq` Command

The firmware now includes `jq` command for a better manipulation of JSON files. Detailed usage instructions are available in the *Commands and Scripts* Application Note.

SSH Port Configuration

There is a new *Port* field available for the SSH server configuraton (*Configuration → Services → SSH*). The defaut listenig port which is 22 can be changed here.

Authentication Menu Highlighting

The *Two-Factor Authentication* menu item is now highlited red in case this type of authentication is not configured and enabled. This feature is implemented for *FirstNet* models.

Changed

WiFi Driver Update

Upgraded the Laird SU60 WiFi driver on ICR-3200 routers to version 11.171.0.24. This update resolves numerous WiFi connectivity issues on these routers.

Disabled WiFi WEP

Disabled WiFi WEP encryption on ICR-4100/4200 routers as the Atheros driver (ath11k) no longer supports it.

SSH Hardening

Hardened the SSH service on *FirstNet* models to meet all requirements of the *ssh-audit* tool. Specifically, the required RSA key size has been increased to 3072 bits, several insufficiently secure ciphers have been disabled, and the maximum session timeout has been reduced to 900 seconds.

Modified Filesystem Hierarchy

Modified the filesystem hierarchy to better comply with the *Filesystem Hierarchy Standard*:

- Added `/run` directory for run-time variable data. On all routers, this is identical to `/var` .

- Moved `/home/httpd` to `/usr/share/www` and added a symlink to the original location to preserve backward compatibility.

RouterApp Platform Check

Modified RouterApp selection to accept filenames corresponding to the current platform only. For example, ICR-4100/4200 routers (v4i platform) require names ending with `.v4i.tgz`

FRR RouterApp

Enabled `CONFIG_TCP_MD5SIG` in the Linux kernel. This allows the *FRR* RouterApp to set the TCP MD5 option.

RTC Menu Optimization

Improved usability of the *Set Real Time Clock* dialog. First, the *Administration → Two-Factor Set Real Time Clock* menu item was renamed to *Administration → Set Date And Time*. Next, added a radio button to choose between different methods, allowing users to set the current browser time, set it manually, or configure an NTP server address.

`u-boot` Updates

First, we upgraded `at91bootstrap` to version 4.0.8 and `U-Boot` to version 2021.04 on all ICR-2000 routers. Next, we upgraded `u-boot-tools` used to build all platforms to version 2021.04.

`popt` Library

Upgraded the internal `popt` library in ltib to version 1.7. Users who build custom `ltib` binaries need to rebuild the RPM database by invoking the following command:

`sudo rm -rf /opt/ltib && rm .lock_file .tc_test_gcc-icr* && ./ltib --hostck` .

Removed WiFi DFS channel

Removed WiFi DFS channel on ICR-1600 routers.

Fixed

High-volume Data Crash

Fixed a crash during high-volume data uploads via cellular network on some ICR-4100/4200 routers.

2FA on v4i

Enabled two-factor authentication on ICR-4100/4200 (v4i platform) routers, which was erroneously disabled.

PAM Login

Fixed an erroneous HTML text displayed when logging into the router if two-factor authentication failed. This issue occurred only when *Debug* mode was enabled on the *Configuration → Services → PAM* configuration page.

CPU Usage

Fixed the *CPU Usage* value in the *System Information* section. The firmware previously reported the average load incorrectly.

SSH Failure

Fixed an SSH failure that occurred after increasing the key strength requirements. This issue happened when the existing key length did not meet the new minimum requirements.

WiFi Setting

Removed broken links to WiFi settings displayed when the WiFi configuration was successfully updated, but not all APs or STAs were functioning correctly.

WiFi Status

Fixed Wi-Fi status cannot correctly display information on ICR-1600 routers.

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 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.