Release Notes

Firmware 6.4.5

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
This document was issued on 31st July, 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.

Firmware Release Information

- **Version**: 6.4.5
- **Release Date**: July 22, 2025
- **Target Devices**: ICR-1602, ICR-1642, ICR-1645
-  **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.

Part II.

Description of New Features, Changes, and Fixes

Added

Secondary DNS Server

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

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.

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.

Added Favicon

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

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.

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.

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.

Wireguard MTU Configuration

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

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

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 8 characters (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 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.

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.

HTTPS Ciphers

Disabled CBC-related ciphers in the HTTPS service. These ciphers are considered insecure.

`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.

`OpenSSL` Software

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

`OpenSSH` Software

Upgraded `OpenSSH` to version 10.0., mainly due to *CVE-2024-6387* (high). This fixes several minor security vulnerabilities and a temporary connection rejection after a previous session expired unauthenticated.

`strongSwan` Software

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.

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.

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.

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.

Kernel Logging

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

User Administration Update

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

List Behavior

Firewall rules list 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.

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.

Fixed

WiFi Connectivity

Fixed WiFi connectivity issues on multiple platforms, including ICR-1600, 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.

HTTP 404 Pages

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

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.

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, 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.

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.

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.

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.

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.
- Fixed *Invalid input* error on *NAT* and *NAT6* pages when logged in with the default password.