RUT142 Firmware Downloads

This page contains firmware files for RUT142 devices. Look to the table below or the changelog to find download links.

To upgrade firmware using WebUI, follow the instructions in RUT142 Firmware.

RUT142

File	Type	Release date	Size	MD5	Changelog
RUT14X_R_00.07.08_WEBUI.bin	Latest FW	2024.07.18	10.94 MB	d1ffc6c9ea03ed72ae19cd2a9226b354	Link
RUT14X_R_00.07.07.2_WEBUI.bin	Mass production FW	2024.06.12	10.81 MB	d4b58673b82519672e697166dd673b8a	Link
RUT14X_R_GPL_00.07.08.tar.gz	SDK	2024.07.18	19.01 MB	1448083901e707a9bf00c8c1d0e2bb56	

Note: packages for Package Manager are independent from firmware and can be downloaded in the Package Downloads page.

FW checksums

Checksums for firmware files can be found **here**.

Changelog

RUT14X_R_00.07.08 | 2024.07.18

- **New**
  - **Network**
    - DNS: added inherited server status to configuration page
    - HTTPS DNS Proxy: added new HTTPS DNS Proxy package to package manager
  - **Services**
    - Data to Server: added 'Lua script' data input
    - Hotspot: added Single Sign-on (OIDC) authentication mode
    - Hotspot: added Walled Garden blocklist functionality
    - IPsec: added initial XFRM support
    - MQTT Modbus Gateway: added JSON message type format
    - OpenVPN: added DCO support
  - **System**
    - API Core: added option to configure api session timeout
    - Certificates: added "Let's encrypt" certificate generation
    - PAM: added RADIUS external user support
    - UI Core: added data analytics support
    - Update Firmware: added warning message about device being temporarily

unreachable on firmware update

- **Improvements**
  - **Network**
    - DNS: separated field "DNS forwardings" into two: one for simple server forwarding other for domain-specific
    - DNS: moved "DNS Forwardings", "Listen interfaces", "Exclude interfaces", "Local service only", options to advanced tab
    - Firewall: improved protocol field in all firewall pages by making that "All" value would be mutually exclusive with any other value
    - Multi WAN: improved interface status representation when using load balancing
    - Network: added more options for "IPv6 assignment length" field
    - VLAN: added ability to configure VLAN 0
    - Wireless: added warning when user configures mesh on radio with automatic frequency channel
    - Wireless: added support for wireless MAC-filter MAC ranges
    - Wireless: changed Radius Accounting port is not required when configuring access point with enterprise encryption
    - Wireless: refactored radio configuration page layout
    - Wireless: refactored assignment of wireless interfaces MAC addresses, STA interface will always use fixed address
  - **Services**
    - Azure IoT Hub: added DPS symmetric key attestation support
    - Azure IoT Hub: added Direct Method support
    - Azure IoT Hub: added Plug and Play integration
    - Azure IoT Hub: added link to "Data to Server" page
    - Data to Server: added support for multiple filters
    - Data to Server: improved HTTP output hostname definition with automatic protocol specification in URL
    - Data to Server: improved MQTT input connection handling
    - DNP3 Client: added option to enable/disable service
    - Dynamic DNS: added Lookup hostnames support
    - GRE: increased Inbound and Outbound key limit to 4294967295
    - Hotspot: adjusted hotspot user manager page to display active and inactive user sessions
    - Hotspot: changed local users to be stored with other types of users
    - Hotspot: added 'noc2c' option for enabling client isolation, option is enabled by default
    - IPsec: added certificate warning message
    - Modbus Server: added mobile last month and last week usage registers
    - Mosquitto: added large package size check for MQTT clients
    - MQTT Modbus Gateway: improved mosquitto reconnect time and service will try to recover few times before exiting
    - MQTT Publisher: improved MQTT connection handling
    - OPC UA Client: added security modes
    - OPC UA Server: added security modes
    - OPC UA Server: added service status display
    - OpenVPN: added support for decrypting private key when uploading a configuration file
    - OpenVPN: improved instance status state
    - OpenVPN: added options to specify an IP address pool for dynamic assignment to clients

        - Over IP: added label to show how many servers a client is connected to
        - Over IP: connect on data feature will not disconnect immediately after data transfer but wait for inactivity timeout
        - Over IP: increased TLS handshake timeout to 10 seconds
        - SMPP: added brute-force prevention
        - SMPP: added TLS/SSL support
        - SNMP: changed interface module OID structure
        - SNMP: improved User-based Security Model (USM) brute force attack prevention measures
        - Stunnel: improved global instance settings dependencies
        - emailrelay: updated version to 2.4.1
        - OpenVPN: updated version to 2.6.9
        - stunnel: updated version to 5.72
    - **System**
        - Access Control: added certificate key length warnings
        - Access Control: adjusted access control when all pages are blocked
        - Access Control: added certificate file download for CLI to work on all browsers
        - API Core: implemented functionality to include warning messages for vulnerable certificates
        - Package Manager: added multi package actions
        - Package Manager: added status filter
        - Package Manager: moved package upload action to main page
        - Package Manager: added links to installed packages pages
        - Package Manager: refactored "Packages" page
        - Package Manager: updated opkg repository link to use https
        - RutOS: improved GPL example page to align with new software architecture
        - Troubleshoot: added support for multiple syslog servers
        - UI Core: added additional message with IP address to loading screen for scenarios when redirect to different IP address happens
        - UI Core: added toast message hiding when text is too long
        - Update Firmware: added 'Firmware version' data in screen after firmware upload
        - WebUI: added functionality to cancel loading screen if it takes 30 or more seconds
        - WebUI: removed all ubus method calls from webui
        - WebUI: improved language caching
        - WebUI: added password generator for first login modal
        - WebUI: added sticky position to side menu
        - WebUI: added default password hint to login error message
        - WebUI: added warning messages for low-security certificates
        - Kernel: updated version to 5.15.159
        - libexpat: updated version to 2.6.2
        - SSL/TLS: updated version to 3.0.14
        - vue: updated version to 3.4
- **Fix**
    - **Network**
        - Channel Analysis: fixed network list not being updated if a single scan fails
        - Devices: fixed missing API devices status endpoint permission
        - DHCP: fixed "DHCP option" allow empty input value
        - DHCP: fixed IPv4 leases being not correctly shown when NTP synchronizes time
        - DHCP: fixed DHCP error that occurred after changing the subnet of the LAN IP address in the setup wizard
        - Dynamic routes: fixed duplicated external routes cards

        - Firewall: fixed firewall zone validation when adding interfaces
        - Multi AP: fixed Multi AP not working with fast roaming
        - Multi AP: fixed switching to Multi AP mode fails due to encryption
        - Multi AP: fixed Multi AP configuration being deleted when switching mode on the same radio device
        - Network: fixed overriding MAC address for interfaces that are bridged
        - RelayD: fixed API error when "network" and "lan_mark" options are not present in a PUT request
        - Wireless: fixed wireless scan results sometimes not being returned
        - Wireless: fixed wireless status page not updating wireless SSID status after page is opened
        - Wireless: removed the ability to have different countries in radio configurations
        - Wireless: fixed interface delete when it's unassigned from the wireless interface in access point mode
        - Wireless: fixed backticks for WiFi SSID are not allowed in WebUI
    - **Services**
        - BACnet: fixed incorrect BACnet IP port used for sending responses
        - BGP: fixed route map sequence going out of range
        - BGP: fixed listen range field allowing multiple entries
        - DLMS: fixed DLMS test response format
        - DLMS: fixed COSEM group validation
        - DLMS: fixed API POST error for /dlms/devices/config endpoint
        - DLMS: fixed serial connection not working after reboot
        - DNP3 Client: fixed to allow reading objects past 255 index
        - DNP3 Client: fixed incorrect hints
        - DNP3 Outstation: fixed serial outstation starting issues
        - Hotspot: fixed uploading more than one custom theme
        - Hotspot: fixed creating Hotspot to SSID that is disabled
        - Hotspot: fixed displaying data limit columns and inputs
        - Hotspot 2.0: fixed Venue name and Operator's name field validations
        - IPsec: fixed connectivity issues when using WAN failover
        - IPsec: fixed the instance status when the local firewall option is disabled
        - Modbus Client: fixed test request option validation
        - Modbus Client: fixed alarm output action display values
        - Modbus Client: fixed incorrect period hint
        - Modbus Server: fixed APN register not clearing APN
        - Modbus Server: fixed 148 and 164 modbus registers
        - Modbus Server: fixed incorrect hints
        - NTRIP: fixed NTRIP NMEA generation timestamp and coordinates errors
        - NTRIP: fixed configuration reading with several instances added
        - OPC UA Server: fixed not starting while modem is down
        - OpenVPN: fixed displaying imported files from device
        - OpenVPN: fixed the private key decryption for cases when a password is used
        - OpenVPN: fixed data cipher migration
        - Over IP: fixed connect on data initiating TCP connection after few data transfers
        - SMPP: fixed username bypass problem
        - SMPP: fixed password validation
        - SNMP: fixed GSM mSignal OID value type
        - SNMP: fixed GSM module memory leaks
        - SSTP: fixed functionality when the default route option is not enabled
        - Web Filter: fixed whitelist not working for some hosts when using IPv6

    - **System**
        - Administration: fixed repeated validation on cleared inputs and added validation when new password matches the old one
        - API Core: fixed API method validation during upload action
        - API Core: fixed error messages for POST method
        - API Core: fixed option list validation
        - Boot: fixed factory settings restore (firstboot) not deleting hidden files
        - Events Log: fixed refresh button in event log table
        - IP Block: fixed adding MAC addresses back to whitelist when unblocking all of them
        - Recipients: made phone number field required
        - Setup Wizard: fixed lan ip step not changing ip address
        - Troubleshoot: fixed system log and kernel log buttons to be enabled with read only rights
        - Update Firmware: fixed misleading "Firmware version" status of "N/A" to "FOTA service is disabled" when FOTA is disabled
        - Update Firmware: fixed issue when infinite spinner appears after updating device firmware from server without having internet connection
- **CVE Patches**
    - Patched CVE-2023-52425
    - Patched CVE-2023-52530
    - Patched CVE-2024-25629
    - Patched CVE-2024-28757

RUT14X_R_00.07.07.3 | 2024.06.25

- **Fix**
    - **Network**
        - WebUI: fixed port advertisement change
    - **System**
        - FOTA: fixed config when upgrading from older firmware with keep settings
- **CVE Patches**
    - CVE-2024-31950
    - CVE-2024-31951

RUT14X_R_00.07.07.2 | 2024.06.12

- **Improvements**
    - **Network**
        - Zerotier: added backup WAN interface blacklisting if WAN failover is enabled
    - **Services**
        - SNMP: added bruteforce attack prevention when using SNMP v3 user
        - L2TP: improved reconnect attempt logic
    - **System**
        - SSH: removed weak SSH algorithms
        - Telnet: moved to Package Manager
- **Fix**
    - **Network**

        - BGP: fixed instance migration issues
    - **Services**
        - DMVPN: fixed duplicate NHRP map entries creation
        - OpenVPN: added fixes for the insecure tls-cert-profile option usage
    - **System**
        - IP Block: fixed blocking of UDP traffic
        - Ledman: fixed WiFi LED indication when WiFi configuration is changed
        - Uboot: fixed firmware recovery update via uboot on Windows
- **CVE Patches**
    - CVE-2024-31948

RUT14X_R_00.07.07.1 | 2024.05.03

- **Improvements**
    - **System**
        - WebUI: improved first login password change logic
        - Certificates: updated Root CA certificates
- **Fix**
    - **Services**
        - Modbus TCP Over Serial Gateway: fixed gateway returning corrupted data with larger baud rates
- **CVE Patches**
    - CVE-2024-2397

RUT14X_R_00.07.07 | 2024.04.16

- Initial firmware release for RUT142