RUT301 Firmware Downloads

This page contains firmware files for RUT301 devices. Look to the table below or the changelog to find download links.

To upgrade firmware using WebUI, follow the instructions in RUT301 Firmware.

RUT301

File	Type	Release date	Size	MD5	Changelog
RUT301_R_00.07.08_WEBUI.bin	Latest FW	2024.07.18	10.44 MB	6a8014d5b18a82cd3871cbefc4fc01c2	Link
RUT301_R_00.07.07.2_WEBUI.bin	Mass production FW	2024.06.12	10.44 MB	c1ddf715d6d2cacda4389d562293576d	Link
RUT301_R_GPL_00.07.08.tar.gz	SDK	2024.07.18	18.19 MB	3ea1e58a69e7524c5bac2cc83218d018	

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

RUT301_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
    - Input/Output: added ability to configure gpio debounce timer and changed default gpio debounce timer value from 200 ms to 10 ms
    - 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
  - **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
    - Input/Output: added custom name support in I/O status page
    - 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**
        - 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
        - Network: fixed overriding MAC address for interfaces that are bridged
    - **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

        - I/O Juggler: fixed improper dout action config handling
        - I/O Juggler: updated profile change action
        - Input/Output: allow unselecting all Post/Get access methods
        - 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
        - Overview: fixed issue when devices without WiFi send additional request without data
        - 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
        - Memory Expansion: fixed enable validation
        - 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

RUT301_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

RUT301_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
    - Uboot: fixed firmware recovery update via uboot on Windows
- **CVE Patches**
  - CVE-2024-31948

RUT301_R_00.07.07.1 | 2024.05.03

- **New**
  - **Network**
    - WebUI: added internet status tracking configuration and overview widget
    - LAN: added a new IPv6 LAN status page
    - Static Leases: added a new IPv6 Static Leases page
    - WebUI: added custom domain name resolve option in “DNS” configuration page
    - Failover: added additional connection flush options
    - VRF: added initial Virtual Routing and Forwarding support
  - **Services**
    - Post/Get: added I/O invert support

        - DLMS Client: added persistent TCP connections
        - Events Reporting: added unexpected shutdown event
        - Modbus Client: added 64bit data types
        - IPerf3: added iPerf3 to Package Manager
        - DNP3 Outstation: added I/O objects
        - Hotspot: added domain and subdomain options for external landing page
    - **System**
        - WebUI: added the ability to generate random passwords for password input fields
        - WebUI: added reset to “Factory defaults” option
        - System: changed firmware certificate verification tool
        - IP Block: added time-based login attempt blocking
        - WebUI: added firmware update notification support
        - PAM: added the ability to set port for TACACS+
        - Logging: added multiple remote syslog servers support
- **Improvements**
    - **Network**
        - Static Leases: added possibility to use MAC with wildcard
        - Topology: changed network devices scanning application
        - WebUI: improved design of Status - LAN page
        - DHCP: simplified DHCP configurations in other pages and moved full DHCP configuration to a separate page
        - DHCP: removed default disabled server configuration for WAN interface
        - WebUI: simplified data entry of DNS forwardings by separating hostname and IP address fields
        - BGP: added Virtual Routing and Forwarding (VRF) support
        - BGP: added multiple BGP instance support
        - WebUI: adjusted responsive design breakpoints
        - Dnsmasq: updated dnsmasq to version 2.89
    - **Services**
        - Wireguard: added option to bind tunnel to a specific interface
        - OPC UA Client: added limits (10 servers, 20 groups, 50 nodes per server, 50 values per group)
        - DLMS Client: increased maximum count of connection sections to 30
        - DLMS Client: added short name referencing
        - SNMP: set strict default community access when IPv6 address is used
        - SNMP: improved sysName OID to set device's hostname
        - Mosquitto: updated package version to 2.0.17
        - Hotspot: moved MAC blocking option from Access Control to Hotspot page
        - WebUI: added MAC authentication support when using RADIUS authentication mode
        - WebUI: moved licenses to footer
        - OpenVPN: added the bridge option for selecting the network device to be bridged with
        - OpenVPN: added possibility to create more than one TAP client
        - SSTP: updated package version to 1.0.19
    - **System**
        - WebUI: added more strict password requirements for restoring backup
        - SMTP: added option to either not verify SMTP server or upload SMTP server's CA file to verify authenticity
        - WebUI: Added the ability to choose the ROOT CA when using certificates from the device

        - WebUI: unified time format to ISO8601 across the entire WebUI
        - WebUI: added ability to choose imported certificate and key as 'Server certificate' and 'Server key' in 'Access Control'
        - WebUI: added 'Hosts' and 'IP Addresses' options for 'Simple' certificate generation and certificate signing
        - WebUI: changed firmware update option to server as a default option
        - WebUI: improved first login password change logic
        - Certificates: updated Root CA certificates
        - GPL: added offline package preparation command for GPL builds
        - Speedtest: added multiple connections support to improve accuracy
        - Kernel: updated to version 5.15.149
        - Libcap: updated package version to 2.69
- **Fix**
    - **Network**
        - Topology: fixed showing interfaces with assigned VLAN
        - WebUI: fixed static routing creation for GRE instance
        - Network: fixed DHCPv4 relay mode enabling
        - Failover: fixed Failover missing active rules when using multiple source and destination IP addresses
        - WebUI: fixed network and failover interface metric sorting synchronization issue
        - WebUI: fixed failover rule policy save issue with newly added WAN interface
        - Interfaces: fixed failover value for new WAN being taken from WAN that was just deleted
    - **Services**
        - Modbus Client: allow using negative floating point values in requests
        - Azure IoT Hub: fixed Data to Server minor WebUI dependency bugs
        - Data to Server: fixed DLMS data formating
        - Data to Server: fixed Network link state data display
        - DLMS Client: fixed segfault while reading profile generic COSEM object
        - DLMS Client: fixed profile generic entries reading
        - DLMS Client: fixed application memory allocation issues
        - SSTP: fixed route adding when default route is enabled
        - SNMP: fixed VLAN OID naming
        - OpenVPN: added fixes for instance status tracking functionality
        - OpenVPN: resolved uptime counting issues
        - PPTP: fixed PPTP instance deletion problem
        - Azure IoT Hub: fixed 'contentType' telemetry message parameter
        - Hotspot: fixed password validation for locally created users and signed-up users
        - Hotspot: fixed session invalidation after deleting registered user
        - Hotspot: fixed firewall rule creation
        - PPTP: fixed problem related with routes when failover is enabled
        - WebUI: fixed data loading error in Input/Output > Post/Get page
        - UPnP: updated package version to 2.3.4
    - **System**
        - Package Manager: fixed spinner message when restarting network after package upload or download
        - Package Manager: fixed supported devices check when installing a package from server
        - WebUI: fixed language install from uploaded package after upgrade with keep settings
        - WebUI: fixed an issue when a user was not logged out after changing profiles

        - Telnet: fixed segmentation fault during concurrent connections
        - CLI: fixed enter key issue on mobile chromium based browsers
        - System Users: fixed SSH session close after deleting user or disabling SSH access
        - Profiles: fixed profile migration with installed packages
        - WebUI: fixed Hotspot log page table search functionality
        - Speedtest: fix missing download speed on some servers
        - PAM: updated libpam to version 1.6.0
- **CVE Patches**
    - CVE-2022-4603
    - CVE-2022-23308
    - CVE 2022-45061
    - CVE-2023-0466
    - CVE-2023-6129
    - CVE-2023-7042
    - CVE 2023-24329
    - CVE 2023-27043
    - CVE-2023-42366
    - CVE-2023-46218
    - CVE-2023-46219
    - CVE-2023-46752
    - CVE-2023-46753
    - CVE-2023-48795
    - CVE-2024-2397
    - CVE-2024-25062
    - CVE-2024-27913
    - CVE-2024-22365

RUT301_R_00.07.06.10 | 2024.04.04

- **Fix**
    - **System**
        - Ledman: fixed memory leak

RUT301_R_00.07.06.8 | 2024.03.25

Note: Firmware **R_00.07.06.8** was removed due to an issue with inefficient memory allocation for LED control.

- **Improvements**
    - **Services**
        - IPSec: disabled libgmp in favor of openssl
        - IPSec: updated Strongswan to 5.9.6
- **Fix**
    - **Services**
        - IPSec: increased charon load timeout
        - IPSec: fixed loading of large private keys

RUT301_R_00.07.06.6 | 2024.03.04

- **New**
  - **Services**
    - Added domain and subdomain options for external landing page in Hotspot
- **Improvements**
  - **System**
    - Minified *.svg WebUI files to save space on the device
    - Removed unused easy-rsa package to increase free space
- **Fix**
  - **Services**
    - Fixed OverIP serial utility issue where after some time server mode can't accept incoming connections anymore

---

RUT301_R_00.07.06.5 | 2024.02.21

- Initial FW release for the RUT301 device