

RUT142 Firmware Downloads

[Main Page](#) > [RUT Routers](#) > [RUT142](#) > **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_00.07.10_WEBUI.bin	Latest FW	2024.10.10	11.06 MB	b9221c013f8057499da7468a61eabc35	Link
RUT14X_R_00.07.08.2_WEBUI.bin	Mass production FW	2024.08.12	10.94 MB	4a9f5bee75c08beb09237b15c63be785	Link
RUT14X_R_GPL_00.07.10.tar.gz	SDK	2024.10.10	19.45 MB	70a625753622da2f14029f68438ee5b6	

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_00.07.10](#) | 2024.10.10

- **New**
 - **Network**
 - Wireless: added noise value calculation
 - **Services**
 - AWS IoT Core: added service
 - BACnet: added ability to configure several BIP interfaces, to set network numbers and preconfigure BDT entries for BBMD
 - Console: added service status information display
 - DLMS: added service status information display
 - DNP3 Client: added service status information display
 - DNP3 Outstation: added service status information display
 - Modbus Client: added service status information display
 - Modbus Server: added service status information display
 - Modbus TCP over Serial Gateway: added service status information display
 - MQTT Modbus Gateway: added service status information display
 - NTRIP: added service status information display
 - OPC UA Client: added service status information display

- OPC UA Server: added variable "rut_wan_type" which shows if WAN is on a wired or a mobile network
 - OPC UA Server: added service status information display
 - RMS: added SOCKS5 proxy support
- **System**
 - Certificates: added SCEP certificate generation method
- **Improvements**
 - **Network**
 - Curl: added unix socket support
 - Firewall: added most options to basic mode for all firewall pages
 - Firewall: added all firewall pages to basic mode
 - Interfaces: increased interface metric maximum value from 10000 to 4294967295
 - Multi WAN: added rules table to basic mode
 - Network: improved performance under stateless single-directional traffic (RFC2544)
 - Static Routes: added page to basic mode
 - VRRP: added page to basic mode
 - Wireless: added interface status message when DFS CAC is in progress
 - Wireless: added most options to basic mode
 - Wireless: added SSID creation and deletion to basic mode
 - **Services**
 - DLMS: added meter COSEM object scanning
 - DNP3 Client: made menu names more consistent
 - Hotspot: added "Coova-Chilli-SSID" (28) Vendor Specific Attribute for Radius
 - IPsec: improved 'Remote endpoint' validation to allow '%any', '%any4', '%any6' values and netmask
 - IPsec: added ability to use certificates from Certificate Manager
 - L2TPv3: added Tunnel ID and Session ID validation to avoid creating multiple tunnels with the same parameters
 - Modbus Client: updated Modbus Client menu position
 - Modbus Server: updated Modbus Server menu position
 - Python3: changed python3-light package libraries
 - Tinc: added options to set the tunnel's IP address
 - Tinc: added a port option to listen for incoming connections and the ability to specify a port for outgoing connections
 - Wireguard: added tunnel source mode selection
 - Kernel: updated version to 5.15.165
 - Python3: updated version to 3.11.7
 - Strongswan: updated version to 5.9.14
 - **System**
 - Access Control: refactored 'General', 'Security' and 'PAM' Web pages
 - Auto Reboot: added support for multiple hosts/URLs in Ping/Wget Reboot
 - Backup: encrypting backup does not require 7zip package anymore
 - Certificates: split "Let's Encrypt" certificates into multiple files
 - Troubleshoot: added dynamic routes debugging information
 - WebUI: added ability to open new page in new tab without entering user credentials
 - WebUI: improved SDK example application
 - Glib2: updated version to 2.80.5
 - Ncurses: updated version to 6.5
- **Fix**

- **Network**
 - Firewall: fixed automatic priority option change
 - Wireless: fixed BSSID show for interface in Client mode
 - Wireless: fixed hostapd ubus call timeout after wireless configuration change
 - Wireless: fixed reporting disconnection from external AP when device in STA+AP mode
 - Wireless: fixed missing rx frame types needed for wifi scanner
- **Services**
 - BACnet: fixed communication issues between the ports
 - BACnet: added all available default baud rates
 - BGP: fixed AS field to allow duplicate values
 - BGP: fixed Access list filters not applying fully
 - DLMS: added all available default baud rates
 - DMVPN: fixed DMVPN GRE instance disappearing when creating new IPsec instance
 - DNP3 Client: removed unnecessary max length display for test response field
 - DNP3 Client: renamed TCP Station to TCP Client in the API documentation
 - DNP3 Client: added all available default baud rates
 - DNP3 Outstation: added all available default baud rates
 - GRE: fixed interface not showing up in OSPF and RIP selections if it is off
 - Hotspot: fixed blocklist not working when no addresses are provided
 - Hotspot: fixed uploaded custom landing page file permissions
 - Hotspot: fixed certificates to be required to enable https redirect
 - IPsec: fixed IP rule not appearing after network restart
 - IPsec: fixed duplicate port values in IPsec firewall rules
 - Ledman: fixed issue when power LED turns off when rebooting device
 - Modbus Client: added all available default baud rates
 - Modbus Client: added missing API docs for Modbus test request
 - Modbus Server: added all available default baud rates
 - Modbus Server: fixed firewall rule staying enabled when app is disabled
 - Modbus Server: fixed firewall rule creation
 - NTRIP: added all available default baud rates
 - OpenVPN: fixed the configuration after disabling the use of external services
 - Over IP: added all available default baud rates
 - SNMP: fixed Hotspot OIDs' hssID and hssUsername display
 - Tinc: fixed adding routes to remote subnets
 - Tinc: fixed configuration generation issues when creating multiple network and host instances
 - Tinc: fixed issues with route creation when using IPv6 addresses in tunnel configuration
 - Tinc: fixed validation for uploading key files
- **System**
 - Backup: fixed uploading backup with memory expansion enabled
 - CLI: fixed some private IPs being incorrectly determined as public
 - JSON-RPC: fixed login "Access Denied" error
 - WebUI: added API required values validation when enabling BACnet, DLMS, DNP3, Modbus, MQTT, NTRIP services
 - WebUI: fixed 'Memory' status card progress bars visuals
 - WebUI: fixed search bar suggestions after removing packages
 - WebUI: fixed showing data in modals for users with only read permissions
 - WebUI: fixed custom SDK pages not loading correctly

- **CVE Patches**

- CVE-2021-3520
 - CVE-2021-44540
 - CVE-2021-44541
 - CVE-2024-4032
 - CVE-2024-6119
 - CVE-2024-6232
 - CVE-2024-6923
 - CVE-2024-7264
 - CVE-2024-42225
-

[RUT14X_R_00.07.09.4](#) | 2024.10.02

- **Improvements**

- **Services**
 - NTP Client: changed default NTP servers

- **Fix**

- **Services**
 - NTP Client: fixed NTP server usage to work with next in line server if current server does not respond
-

[RUT14X_R_00.07.09.3](#) | 2024.09.27

- **Fix**

- **Network**
 - Multi WAN: fixed ipsets not getting deleted correctly when Multi WAN gets restarted
-

[RUT14X_R_00.07.09.1](#) | 2024.09.13

- **Improvements**

- **Services**
 - Python3: updated version to 3.11.7
-

[RUT14X_R_00.07.09](#) | 2024.09.03

- **New**

- **Network**
 - Firewall: added ability to configure NAT rule action
 - Firewall: added additional TTL target for firewall rules
 - Realtime Traffic: added historical traffic charts
 - Realtime Traffic: added overall quality measurement to wireless signal charts
 - Wireless: added option to enable 802.11w Management frame protection when using non-WPA3 encryption
- **Services**

- Events Reporting: added new firmware version notification event
 - SNMP: added Multiwan data module
 - **System**
 - WebUI: added notifications menu
- **Improvements**
 - **Network**
 - Ports Settings: added more PoE state symbols, colored disabled port differently and improved port status hint
 - Realtime Traffic: improved chart styles
 - Wireless: increased EAP authentication logging
 - Wireless: added various validations for network that is being used by wireless interface
 - Wireless: added insecure configuration warnings when configuring SSIDs
 - Wireless: updated wireless cards to display each radio device's signal quality and band data
 - Wireless: reduced time required for Fast Transition in STA mode
 - **Services**
 - Data to Server: added warning messages about insecure certificates for http_certfile and mqtt_certfile options in API and WebUI
 - DLMS: added SHA256 authentication
 - DLMS: improved COSEM group enable validation
 - GRE: reduced GRE keepalive packet buffer size
 - Hotspot: increased throughput performance
 - Hotspot: increased maximum length of 'Local users' username to 255 characters
 - Hotspot: added walled garden allowlist and blocklist
 - IPsec: added support for route based tunnel
 - L2TP: added field for custom options
 - SMPP: added timeout option
 - Web Filter: added hostname count message after successful file upload
 - **System**
 - Access Control: improved system user's access control rules logic
 - Access Control: added option to disable password auth for the root user
 - Administration: improved write/read access control options display to match menu path style
 - Backup: improved backup page by splitting it into backup and reset settings page
 - Side Widget: added port status widget
 - Update Firmware: changed firmware update log to include firmware version
 - WebUI: updated firmware and backup verification pages design
 - WebUI: improved global alerts display
 - WebUI: added confirmation prompt for disabling service in side widget
 - Kernel: updated version to 5.15.162
- **Fix**
 - **Network**
 - Devices: fixed configured VLAN 0 device cannot be selected in interface physical settings configuration
 - Network: fixed Ethernet switch port state change tracking logic
 - RelayD: fixed relayd assigning wrong interface to zone
 - Wireless: fixed station mode connection issues for 2.4 GHz radio in STA+AP mode
 - Wireless: fixed wireless status API response to contain separate interface information for multiple radio configurations
 - **Services**

- Azure IoT Hub: fixed the Azure IoT Hub deprecated endpoint to create Data to Server sections
 - Azure IoT Hub: fixed the Azure IoT Hub deprecated endpoint so that it does not create sections in GET request
 - Azure IoT Hub: fixed the deletion of Data to Server sections when an Azure IoT Hub section is deleted through the deprecated endpoint
 - DLMS: fixed OBIS code validation
 - Hotspot: fixed 'Hotspot network' input validation to only allow network mask from 16 to 30
 - OPC UA Client: fixed TCL file upload
 - OPC UA Server: fixed TCL file upload
 - OPC UA Server: fixed configuration migration
 - OpenVPN: fixed default firewall zone for tap interfaces
 - SNMP: fixed TELTONIKA-MIB wireless module crash
 - SNMP: fixed mobile network state display
 - SNMP: fixed default hssDwLimit, hssUpLimit, hssDwBandwidth and hssUpBandwidth values
 - **System**
 - API Core: fixed file deletion
 - Boot: fixed Teltonika logo in httpd recovery page when using Firefox
 - Package Restore: fixed automatic package re-installation after firmware upgrade
 - Troubleshoot: fixed troubleshoot not including all the log files when log to flash is enabled
 - User Settings: fixed page to show groups and users if the user has been granted access
 - WebUI: fixed overview page to display active wireless (WLAN) clients
 - **CVE Patches**
 - CVE-2021-32292
 - CVE-2022-40617
 - CVE-2023-49441
 - CVE-2024-0397
 - CVE-2024-3596
 - CVE-2024-5535
 - CVE-2024-8088
 - CVE-2024-26669
 - CVE-2024-26739
 - CVE-2024-26740
 - CVE-2024-36901
-

[RUT14X_R_00.07.08.2](#) | 2024.08.12

- **Fix**
 - **System**
 - Update Firmware: fixed inconsistent firmware download from FOTA
-

[RUT14X_R_00.07.08.1](#) | 2024.08.06

Note: This firmware version was removed due to an issue with FOTA firmware download.

- **Improvements**

- **Services**

- Zerotier: updated version to 1.14.0

- **Fix**

- **Network**

- Network: fixed default route not being added for PPPoE connections

- **Services**

- OPC UA Client: fixed connections not being closed after using testing functionality

- **System**

- WebUI: fixed SDK WebUI package compilation
-

RUT14X_R_00.07.08 | 2024.07.18

Note: This firmware version was removed due to an issue with FOTA firmware download.

- **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