

# RUTX10 Firmware Downloads

[Main Page](#) > [RUTX Routers](#) > [RUTX10](#) > **RUTX10 Firmware Downloads**

This page contains firmware files for RUTX10 devices. Look to the table below or the [changelog](#) to find download links.

To upgrade firmware using WebUI, follow the instructions in [RUTX10 Firmware](#).

## RUTX10

File	Type	Release date	Size	MD5	Changelog
<a href="#">RUTX_R_00.07.06.10_WEBUI.bin</a>	Latest FW	2024.04.04	24.6 MB	6ade4748118720d9f8c72524498acf69	<a href="#">Link</a>
<a href="#">RUTX_R_00.07.06.10_WEBUI.bin</a>	Mass production FW	2024.04.04	24.6 MB	6ade4748118720d9f8c72524498acf69	<a href="#">Link</a>
<a href="#">RUTX_R_GPL_00.07.06.10.tar.gz</a>	SDK	2024.04.04	80.1 MB	a6653437efd8ba12151579615a86b2f3	

**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

**Global RUTOS changelog can be found here:** [LINK](#)

\* This is universal changelog of RUTOS. Changes made to features that are not present in some devices, do not affect them.

### [RUTX\\_R\\_00.07.06.10](#) | 2024.04.04

- Global changelog for **R\_00.07.06.10** - [LINK](#)

### [RUTX\\_R\\_00.07.06.8](#) | 2024.03.25

- Firmware **R\_00.07.06.8** was removed due to an issue with inefficient memory allocation for LED control.

## [RUTX\\_R\\_00.07.06.6](#) | 2024.03.04

---

- Global changelog for **R\_00.07.06.6** - [LINK](#)

## [RUTX\\_R\\_00.07.06.5](#) | 2024.02.21

---

- Global changelog for **R\_00.07.06.5** - [LINK](#)

## [RUTX\\_R\\_00.07.06.3](#) | 2024.01.17

---

- Global changelog for **R\_00.07.06.3** - [LINK](#)

## [RUTX\\_R\\_00.07.06.1](#) | 2024.01.04

- **Fix**
  - **Services**
    - Fixed issue with NTPclient zombie processes

## [RUTX\\_R\\_00.07.06](#) | 2023.12.20

- **New**
  - **Network**
    - Added 802.11v BSS Transition Management and 802.11k Radio Resource Measurement
  - **Services**
    - Added OPC UA Server
    - Added the ability to set port for TACACS+ in PAM service
    - Added switch to enable using root certificate authority for MQTT alarms in Modbus Client services
    - Added new alarm action "Ubus event" in Modbus Client services
    - Added new input "Modbus alarms" in Data to Server service
    - Added wget ping subtype support in Events Reporting service
    - Added new I/O SNMP OID that returns numeric I/O state
    - Added TLS support for OverIP serial functionality
  - **WebUI**
    - Added Tailscale VPN support
    - Renewed user interface design
    - Added network interface name change functionality
    - Added last resort configuration option for multiwan policy rules
  - **System**
    - Added ability to enable/disable SSH access for specific users in System Users
    - API support
- **Improvements**
  - **Network**
    - Added two radio support on one SSID in Wireless
  - **Services**

- Expanded GRE VPN keep alive functionality to disable routes from unreachable tunnel
- Added PKCS#12 certificate container authentication method in IPsec VPN
- Added TLV message\_payload support for SNMP service
- Added Purple.ai configuration profile
- Replaced option "No leading zeros" with "Remove all zeros" in Over IP serial functionality
- Added reboot on storage device disappearance and re-appearance
- **WebUI**
  - Improved Events Log page loading by adding asynchronous pagination
  - Removed requirement for Diffie-Hellman parameters in OpenVPN service
  - Added improvements for creating OpenVPN IPv6 configurations
  - Added auto redirect after changing router's IP address or port
  - Added "Interface" dropdown for interfaces selection in Wake on LAN service
  - Increased Data to Server service MQTT topic length limit to 65535 characters
  - Added OSPF external routes section to Status page
  - Moved device menu entry "Reboot" to header menu
  - Moved WiFi scanner page to Services section
- **System**
  - Added Mosquitto CVE patch 2023-28366
  - Added Mosquitto CVE patch 2023-3592
  - Updated hostapd version to 2023-09-08
  - Updated cURL version to 8.4.0
  - Updated kernel version to 5.10.199
  - Updated Mac80211 version to 6.1.24
  - Added RMS data display to generated troubleshoot
  - Added downloaded Package Manager packages list to generated troubleshoot
  - Added process activity load list to generated troubleshoot
  - Changed default OPKG feed to use Teltonika's URL
- **Fix**
  - **Network**
    - Fixed DMVPN firewall rule creation issues
    - Fixed RUTX VLAN keep settings issue when WAN port configuration are overwritten with 1st vlan
    - Fixed Failover missing active rules when using multiple source and destination IP addresses
    - Fixed unstable Wireless mesh connection
    - Fixed low Wireless mesh throughput
    - Fixed concurrent Wireless STA and AP functionality on 5 GHz band
  - **Services**
    - Fixed SSH module enable in PAM service
    - Added minimum free space check when saving logs to flash in Logging service
    - Fixed "Set multiple coils" function sending too many bytes in Modbus Client services
    - Fixed multiple Events Reporting messages being sent when Firewall configuration is changed
    - Fixed VRRP instances advertising wrong virtual IPs
    - Added Hotspot information in SNMP MIB file
    - Fixed registered Hotspot Local Users showing random username
    - Fixed selection of MAC Auth for LAN interfaces in Hotspot service

- Fixed inconsistent Hotspot login behaviour when using MAC Auth with Password
- Fixed instance shutdown after last local user deletion
- Fixed RMS Hotspot data display for devices without WiFi support
- Fixed serial timeout not working in Over IP serial functionality
- Removed "Echo" option in Modbus TCP over Serial functionality
- Fixed CRC verification failing when CRC is correct in Modbus TCP over Serial functionality
- Fixed crash when getting unexpected messages from RTU in Modbus TCP over Serial functionality
- **WebUI**
  - Fixed side menu style issues when Japanese language is used
  - Fixed displaying of vendor names in Topology page
  - Fixed language packs being selectable when still in Package Manager queue
  - Added ability to configure IPv6 BGP peer
  - Fixed RelayD configuration issues after keep settings
  - Fixed realtime graphs responsive design issues
  - Fixed Network Shares users deletion
  - Fixed not all LAN interfaces shown in dropdown in Hotspot service page
  - Fixed wireless realtime data to show signal as unavailable with no connected clients
  - Fixed WiFi scanner disconnecting AP users
  - Fixed setup wizard errors in Wireless configuration page
- **System**
  - Patched FRR CVE-2023-38406
  - Patched FRR CVE-2023-38407
  - Patched FRR CVE-2023-41358
  - Patched FRR CVE-2023-41360
  - Patched FRR CVE-2023-41909
  - Patched FRR CVE-2023-47234
  - Patched FRR CVE-2023-47235
  - Patched OpenSSL CVE-2023-3446
  - Patched OpenSSL CVE-2023-3817
  - Patched LibXML2 CVE-2023-39615
  - Patched LibXML2 CVE-2023-45322
  - Patched FFMPEG CVE-2021-28429
  - Patched FFMPEG CVE-2022-48434
  - Patched dnsmasq CVE-2023-28450
  - Fixed running out of space when SSHFS is mounted in /tmp while generating troubleshoot
  - Fixed WebUI access after upgrading from legacy RutOS version

## [RUTX\\_R\\_00.07.05.4](#) | 2023.11.09

### • Improvements

- **WebUI**
  - Improved asynchronous pagination in events log pages
  - Optimized Overview page load
  - Added resource loading cancellation after switching to different page

## [RUTX\\_R\\_00.07.05.3](#) | 2023.10.30

- **New**
  - **System**
    - Added support for GD5F2GM7 and GD5F2GQ5 GigaDevice NAND flashes

## [RUTX\\_R\\_00.07.05](#) | 2023.10.19

- **New**
  - **Network**
    - Added "shared.m2m.ch" APN for Swisscom IoT operator to APN database
    - Added "gamma" APN to auto-APN database
    - Added "soracom.io" APN for Soracom operator to APN database
    - Added "simbase" APN to auto-APN database
    - Added "pnd" APN for Pond IoT to auto-APN database
    - Added "spitfire1" APN for Spitfire operator to APN database
    - WDS support for wireless bridging
  - **Services**
    - DLMS Client package
    - 7zip package
    - TincVPN package
    - Added router uptime and mobile connection uptime data parameters to SNMP
    - Custom MQTT publisher/subscriber topics definition support
    - Alternative configuration file upload support for MQTT Broker service
    - Device Provisioning Service support for Azure IoT Hub service
  - **WebUI**
    - Firewall status page
    - Page search feature
    - Network Topology page
    - "Allow insecure connection" option for MQTT TLS protocol in Data to Server service
    - Package Restore feature Enable/Disable option
    - Hotspot client connection/disconnection trap option for SNMP service
    - Added Events log trap option for SNMP service
    - Confirm dialog when cancelling a verified package in Package Manager
    - "Bridge ALPN" option for Bridge configuration in MQTT Broker service
    - New subtypes of events that specify a specific port on "Events Reporting" and "SNMP Trap rules" pages
    - Specific firmware packages repository link in Package Manager page
    - Ability to enter decryption passphrase for encrypted private keys
    - "Reconnect" button in RMS page
    - New event "Device startup completed" in Events Reporting service
    - Port status and configuration page
    - IP6 table configuration option for DHCPv6 protocol in Network -> WAN page
    - Wireless interface QR code generator
    - Channel analysis page Status -> Wireless -> Channel Analysis
    - Disabled direct network interface deletion when it is associated with a wireless interface
    - Limited to a single section configuration and added IP address field for Relayd service
    - "Fast roaming" configuration for Wireless service in Client mode

- Updated Status->Network->Wireless page to display interfaces as cards and added ability to filter connected clients by selected interface
- **System**
  - Mechanism to rebrand WebUI using GPL
  - Possibility to create web applications with closed-source GPL
- **Improvements**
  - **Network**
    - Moved FRR VTYSH package to package manager
    - Made newly created Firewall Traffic, NAT rules and Port Forwards disabled by default
    - Improved Interfaces to enable IPv6 DHCP server when mobile v6 or v4v6 PDP type is set
    - Improved IPSec performance throughput
    - Added automatic reconfiguration when switching between wireless interface modes
    - Added automatically generated name option for new network
  - **Services**
    - New reworked Data to Server
    - UPNP moved to package manager
    - Added IPv6 support for Modbus TCP Server/Client services
    - Refactored Azure IoT Hub service
    - Improved resiliency to timeouts in Modbus Client service
    - Added PDU data type to Modbus read requests
    - Added new formatters for MQTT alarms in Modbus Client service
    - Added main section to make test functions independent in Modbus Client service
    - Improved WAN IP register reading time in Modbus service
    - Sped up default profile and profile template generation for Profiles functionality
    - Optimized profile change time for Profiles functionality
    - Added IPv6 support for Stunnel VPN
    - Added MAC blocking for client connections after set amount of failed login attempts in Hotspot service
    - Improved TCPdump by allowing to capture packets from any interface
    - Added OSPF support for DMVPN
    - Updated Hotspot password hashing to sha512
    - Added I/O pin name to trap notification message
  - **WebUI**
    - Reorganized menu
    - Updated header design
    - Split Interfaces configuration in Advanced mode into two pages: WAN and LAN, identically as in Basic WebUI mode
    - Moved Interfaces IPv6 configuration into separate tab
    - Added client/server status information in OpenVPN instance overview page
    - Added more IPv6 information to interface status in Interfaces page
    - Removed "Custom delegated IPv6-prefix" field from DHCPv6 configuration in Interfaces page
    - Disabled DHCPv6 interface editing while in basic mode
    - Refactored custom DHCP options into separate modal
    - Added automatic start and end IP allocation for DHCP server configuration in Interfaces
    - Added client/server status information in L2TP VPN page

- Added "MTU" field to L2TP client configuration page
- Added CHAP, PAP and MSCHAP-v2 authentication fields to L2TP instance configuration
- Added more detailed IPsec VPN status information
- Encryption AES-256-CBC added as default in OpenVPN
- Added "Authentication algorithm" support to OpenVPN configuration with static key mode
- Added GRE (DMVPN) VPN tunnel source support to any instead of specific interface
- Improved Hotspot landing page theme package removal
- Added upload and download theme functionality to Hotspot Landing page
- Improved ZeroTier VPN bridge configuration
- Added ability to adjust order of rules in Firewall page
- Added IPv6 RAW table to be displayed in Status -> Firewall
- Improved file upload component's visual appearance
- Change "Allow anonymous" option default value to 0 in MQTT Broker
- Added option to specify "Client ID" in MQTT Publisher
- Added functionality to select specific interface in Web Filter service
- Allowed to select FTP server subfolder in Traffic Logging service
- Renamed various service master/slave naming convention in config files, package names and webUI to client/server
- Added "Create static" button in Status -> Network -> LAN which bind DHCP lease for device
- Removed redundant "Action" option in Periodic Reboot
- Added DFS channel marking in Network -> Wireless
- Show wireless MAC address even when interface is inactive in Status -> System page
- Merged Multi AP configuration to wireless interface edit modal
- Added automatic network switch to bridge if selected in Wireless configuration
- Added default encryption for newly created wireless interfaces
- Simplified "802.11r Fast Transition" configuration options in Wireless interface configuration
- **System**
  - Updated kernel version to 5.10.188
  - Updated UCI version to 2021-10-22
  - Updated SSHFS version to 3.7.1
  - Updated FRR suite to 8.4.2
  - Updated cURL version to 8.2.0
  - Updated TCPdump version to 4.99.4
  - Updated C-ares version to 1.19.1
  - Updated iproute2 version to 5.19.0
  - Updated libubox package version to 2021-08-19
  - Added CVE patch CVE-2023-2650
  - Added additional firmware information in CLI prompt banner
  - Connection mode LED now blinks on data transfer
  - Changed "routername" to "devicename" in system config file
  - Made all clients get disconnected out once dropbear service is disabled
  - Improved firmware downgrade restrictions for certain regions
  - Device name is now displayed in browser tab when in WebUI login page
  - Added NF conntrack information in generated troubleshoot archive

- **Fix**

- **Network**

- Fixed UDP Broadcast Relay service crashing on start without physical network device
- Fixed wrong or empty WAN state info
- Fixed connection tracking for main interface in Failover
- Fixed Wireless AP and STA functionality for 5GHz band
- Fixed Wireless scanning issue with certain configuration
- Fixed Wireless transmit power changing without user input after saving different country code
- Fixed clients isolation functionality in Wireless
- Fixed Wireless STA authentication failure in case of channel change
- Fixed Multi AP startup when changing Multi AP configuration in Wireless
- Fixed client connection to EAP Wireless network

- **Services**

- Fixed reconnecting to inactive connections for Modbus Server service
- Fixed Modbus Client response after reboot write request
- Fixed Modbus Server to show error when trying to get operator name without SIM
- Updated Modbus Client to handle large numbers of schedule rules, when frequency is set to schedule (Daini)
- Fixed "Input" rule displaying incorrect and missing ports in Network -> Firewall -> Traffic Rules
- Fixed WireGuard VPN endpoint resolving problem
- Peer cache is no longer deleted when ZeroTier service is restarted
- Fixed RMS data collection about the list of devices connected to WiFi
- Fixed showing incorrect Internet state in RMS
- Fixed WiFi client info display in RMS
- Implemented error handling when device is blocked or unrecognized by RMS
- Fixed L2TP client sometimes not adding routes on successful connection
- Fixed NTP time sync with browser functionality in some edge cases
- Fixed reinstalled packages" verification when device name is changed
- Fixed an issue where signal query would return invalid value instead of error in case of no signal in MQTT Publisher service
- Fixed OpenVPN firewall rule creation for both IPv4 and IPv6
- Fixed OpenVPN server crash loop after changing authentication from TLS to Static Key
- Fixed IPsec VPN connection problem with small lifetime values
- Fixed IPsec "Default Route" not working when Flow Offloading is enabled
- Fixed an issue where system directory could be used as a mount point in SSHFS service
- Fixed IP block feature to unblock an OpenVPN IP address on successful authentication
- Fixed package installation process bug when packages have different architecture names
- Added "bearer token" authentication functionality in Dynamic DNS
- Fixed MQTT Broker "local\_port" option keep settings migration
- Remove public keys when key-based authentication is disabled in Access Control
- Fixed "Parity" field "Mark" and "Space" options being ignored in DNP3 Serial services
- Corrected SNMP MIB file syntax according to standards
- Fixed returned port count in SNMP



- Fixed disabled CLI remote access taking up a session slot
- Fixed user deletion in Network Shares service
- Fixed router reboot inconsistencies after Storage Memory Expansion
- **WebUI**
  - Fixed empty events cards in Overview page when no content is available
  - Fixed modal form inputs not clearing upon closing after nested modal is saved
  - Fixed select menu closing when selecting custom option
  - Fixed multi select expanding table row when adding new values
  - Fixed global section caching after deleting a section in a table
  - Fixed unpredictable search logic in tables
  - Fixed interfaces reordering by metrics in Failover page
  - Removed ability to select ports on ICMP and ESP protocol in Failover page
  - Fixed wrong status when interface is disabled in Failover page
  - Fixed firewall zone and rule creation/deletion on VPN configuration creation/deletion
  - Fixed STP enabling issue in Interfaces
  - Fixed EIGRP status info in Dynamic Routes
  - Fixed issue with custom DHCP options where you could not have multiple values per rule
  - Fixed Routing/NAT Offloading section display in Network -> Firewall -> General Settings when device is not supported
  - Fixed SSH/HTTP/HTTPS/ICMP setting in Network -> Firewall -> Attack Prevention page
  - Fixed failing Firewall rules with united protocol formats
  - Fixed zone select component not closing options menu when selecting an option in Firewall pages
  - Fixed memory leak when cancelling file uploads on Chromium-based browser
  - Fixed group settings saving by removing deprecated ":section" routes in Administration -> User Settings -> System Users
  - Fixed allowing IDs above 247 in Modbus Client service
  - Fixed selecting SIM in Modbus Client service Alarms
  - Fixed Modbus Alarm telephone number limit
  - Fixed to show available options for test requests on error in Modbus Client service
  - Fixed Modbus Alarm I/O pin display values
  - Fixed issue when creating instance named "gre" does not show in GRE VPN
  - Remote endpoint field now allows underscore character in IPsec VPN
  - Fixed ZeroTier wrong service status display in Status -> Services
  - Fixed problems with L2TP/PPTP VPN firewall rules automatic creation
  - Fixed problem related to the enable/disable toggle in OpenVPN instance overview page
  - Added fixes for key-direction missing problem when uploading OpenVPN config file
  - Fixed login page read-only inputs after custom user logout
  - Fixed issue when double clicking firmware upgrade cancel button returned error
  - Fixed Package Manager prompt message to appear when package requires network restart
  - Fixed showing in queue packages when they contained special symbols in the Package Manager page
  - Fixed various visual Side Widget bugs
  - Fixed Data to Server DNP3 filter from flash display
  - Fixed incorrect source data displayed in Realtime Data -> Connections table

- Fixed memory expansion confirmation prompt title
- Fixed incorrect configuration saving in Hotspot 2.0 service
- Disabled password hashing for new user creation in Hotspot service
- Fixed Hotspot landing page themes saving bug
- Fixed test email sending to more than one recipient in Events Reporting page
- Fixed VLAN OID values in SNMP service
- Output proper error message in case of hardware not being supported in Firmware Upgrade
- Fixed being able to open side widget when user does not have read access
- Fixed profile creation when current configuration is not present
- Fixed wrong protocol data display in "Access control" page
- Fixed LAN interfaces not showing up before WAN interfaces in Status -> Realtime Data -> Traffic
- Fixed incorrect Bluetooth details modal size
- Updated to display "MAC address" on device details page
- Fixed disabling DLNA service when USB drive is removed
- Fixed error when user has no write permissions in Speed Test page
- Updated Network -> Wireless interface add and delete button visibility in basic mode
- Fixed Wireless Multi AP incorrect SSID list after removal of an instance
- Fixed MAC address filtering in Network -> Wireless page to list only connected WiFi devices
- **System**
  - Patched CVE-2023-0386 vulnerability
  - Patched CVE-2023-0464 vulnerability
  - Patched CVE-2023-0465 vulnerability
  - Patched CVE-2023-2602 vulnerability
  - Patched CVE-2023-3772 vulnerability
  - Patched CVE-2023-3773 vulnerability
  - Patched CVE-2023-4128 vulnerability
  - Patched CVE-2023-33476 vulnerability
  - Patched CVE-2023-28484 vulnerability
  - Patched CVE-2023-29469 vulnerability
  - Patched CVE-2023-31490 vulnerability
  - Patched CVE-2023-36369 vulnerability
  - Patched CVE-2023-40283 vulnerability
  - Patched CVE-2023-48174 vulnerability
  - Delayed Custom Scripts execution on boot, after storage devices are mounted
  - Fixed Custom Scripts permissions after save
  - Changed certificate expiry calculation mechanism to fix Y2K38 bug
  - Fixed downloading of certificates that have a space in their name in Administration -> Certificates -> Certificates Manager
  - Fixed Events Log database rotation to prevent log partition space exhaustion
  - Fixed duplication and sorting of all events IDs in Events Log
  - Fixed FOTA crash when current hours is with leading 0
  - Fixed crontab job removal after disabling FOTA
  - Changed Mosquitto build options to not include cJSON library
  - Fixed device name resetting to default upon refresh in Administration
  - Fixed backup upload validation with memory expansion

## [RUTX\\_R\\_00.07.04.5](#) | 2023.07.24

- **Improvements**
  - **Network**
    - Added metric field support in BGP Route-maps page

## [RUTX\\_R\\_00.07.04.4](#) | 2023.06.26

- **New**
  - **Network**
    - Travelmate package for captive portal redirection
- **Improvements**
  - **Services**
    - Improved UPNP lease file validation
    - Improved DLNA 'Database directory' field validation to not allow ', ` and spaces
  - **System**
    - Device name is now displayed in browser tab when in login page
- **Fix**
  - **Network**
    - Patched CVE-2023-32233 vulnerability
    - Fixed an issue with Multi AP service remaining enabled when disabling
    - Fixed default networks in WAN firewall zone and possibility to add a network that is not yet created
  - **Services**
    - Fixed connection establishment for RMS MQTT service
    - Implemented partial restart when connection with RMS server fails
    - Fixed device name resetting to default upon WebUI page refresh
    - Fixed being able to set device name without passing validations
    - Fixed WireGuard port change in firewall traffic rule when modifying instance port

## [RUTX\\_R\\_00.07.04.3](#) | 2023.05.11

- **Improvement**
  - **System**
    - Removed SSH RSA key generation
    - Added SSH ECDSA key generation
- **Fix**
  - **Network**
    - Fixed clients being unable to connect to wireless AP when multi AP configuration is empty
  - **System**
    - Fixed an issue on bootloader web recovery hanging with certain firmware sizes

## [RUTX\\_R\\_00.07.04.2](#) | 2023.04.18

- **New**
  - nftables support
- **Improvement**
  - **WebUI**

- Improved Overview page performance
- **System**
  - Changed hostname to router name
  - Updated OpenSSL to version 1.1.1t
  - Updated CA certificates to version 20211016
  - Updated libiwinfo to version 2022-08-19
- **Fix**
  - **Network**
    - Fixed Port-based VLAN ID calculation issue
    - Fixed Ethernet interfaces showing incorrect transferred data values
    - Fixed EEE disable issue that caused reduction in data transfer speed
  - **Services**
    - Fixed event text for configurable inputs/outputs on I/O Juggler
    - Fixed I/O PIN3 value not changing via MODBUS TCP
    - Added I/O status request error handling in various WebUI pages when the I/O service is booting up
    - Fixed OpenVPN enabling/disabling when using Password or TLS/Password authentication modes
    - Fixed OpenVPN keep alive setting migration issue
    - Fixed PPTP server name setting migration issue
    - Fixed missing WebUI issue caused by Email Relay installation
    - Fixed NTP's Operator Station Synchronization memory leak issue
    - Fixed test email validation
  - **System**
    - Fixed libcares vulnerability CVE-2022-4904
    - Fixed frr vulnerability CVE-2022-37035
    - Removed ability for non root users to edit scripts that get executed as root

## [RUTX\\_R\\_00.07.04.1](#) | 2023.03.24

- **Fix**
  - **Network**
    - Fixed Data Limit issue

## RUTX\_R\_00.07.04 | 2023.03.07

**Note:** Firmware version **RUTX\_R\_00.07.04** was removed from downloads list due to issues with Mobile Data Limit functionality not working correctly when Software offloading is enabled.

- **Improvements**
  - **WebUI**
    - Improved data persistence between page refreshes
    - Improved page navigation behavior
    - Improved redirect logic to open configuration edit modals
  - **Network**
    - Made Software Flow Offloading Enabled by default
    - Changed default WiFi AP cipher to CCMP (AES)
    - Added the logging of MAC addresses rejected by a WiFi AP
  - **Services**
    - Added MQTT support to I/O Juggler
    - Added a frequency option 'schedule' Modbus Master

- Added pagination to Events Reporting overview
- Added limit to Events Reporting rule list
- Added email logging for Events reporting
- 'Sync with browser' button in the NTP page now also synchronizes the time zone
- Added a limit of 30 for NTP instances
- Made Networks selections in the 'Traffic Logging' page to display interface choices dynamically
- Added "make before break" option to IPsec configuration
- Added MODBUS TCP connection handling layer to MQTT-MODBUS Gateway
- Improved MODBUS Master connection handling to reduce connection count
- Updated modbus request error messages
- Added OpenVPN server ip block support
- Added MQTT support for MODBUS Master alarms
- Added the possibility to get the device's Ethernet port data via SNMP
- Improved error messages in the Serial Utilities page
- **System**
  - Updated bash to version 5.1.16
  - Added detailed FW update failure error message to Events Log
  - Improved firmware upload/validation error messages
  - Updated Turkish language support
  - Added protocol column to IP block page
  - Added "vpns.log" file to the Troubleshoot package
  - Added Wireguard tunnel information to the Troubleshoot package
  - Updated default admin group access rights
- **Fix**
  - **WebUI**
    - Fixed Services page not displaying data after Thingworx package is installed
    - Added DNP3 to the 'Status > Services' page
  - **Network**
    - Fixed interface priority change issue
    - Fixed a Custom Firewall Rule editing issue
    - Fixed DMZ configuration saving while it is disabled
    - Fixed Port Scan script execution failure
    - Fixed Firewall zone duplication issue
    - Fixed disabled WiFi interface after factory reset
    - Fixed WiFi interface creation with SAE mixed encryption
  - **Services**
    - Fixed the listing of slow USB devices such as HDDs
    - Fixed DNP3 serial master not working when Stop bits are set to 2
    - Fixed DNP3 requests not deleting along with instance
    - Fixed DNP3 memory leak occurring after spamming the test request button
    - Fixed Serial Over IP related Firewall rule setting
    - Fixed I/O Scheduler overlapping instances issue
    - Fixed Input/Output image pin colors
    - Fixed issue that causes ADC subscribers to receive notifications for when ACL is active
    - Fixed WiFi Hotspot landing page uploaded theme image display
    - Fixed WiFi Hotspot trial user deletion issue
    - Fixed WiFi Hotspot service crash when associated WiFi interface is not up
    - Fixed WiFi Hotspot password request by SMS

- Fixed WiFi Scanner starting process when the WiFi interface is disabled
- Fixed Data To Server JSON format %n, %N and %s flag issues
- Fixed Events Reporting email data clean
- Fixed Events Reporting missing config selections
- Fixed GRE Tunnel's 'Tunnel source' field validation when the source is custom
- Fixed IPsec instance deletion after removing DMVPN package
- Fixed IPsec migration via Backup file when DMVPN is configured
- Fixed IPsec naming issue when the includes an equals sign
- Fixed L2TP client to use correct interface on failover events
- Fixed L2TP over IPsec connection dropping issue when connecting from a Windows client
- Fixed MODBUS database size limiting issue
- Fixed MODBUS MQTT Gateway client ID input
- Fixed MODBUS TCP Slave RSSI value
- Fixed MODBUS test button returning errors when several non-connected devices are configured
- Fixed NTP Etc/GMT+1 and Etc/GMT-1 time zones
- Fixed OpenVPN password validation when no CA certificate is uploaded or 'custom' template is selected
- Fixed OpenVPN Static Key configuration saving by making Static key upload required
- Fixed OpenVPN TLS client creation issue while LAN is down
- Fixed Package Manager displaying non-existent packages
- Fixed Package Manager errors showing up after successful installations
- Fixed Periodic Reboot entry duplication after a power cycle
- Fixed PPTP 'Client to client' option not being applied after save
- Fixed receiving excessive device state emails after a reboot is initialized over RMS
- Fixed WebUI unavailability after unsuccessful package install
- **System**
  - Fixed vulnerabilities CVE-2022-3524, CVE-2022-3566, CVE-2022-3567, CVE-2022-39188, CVE-2022-45934, CVE-2022-47929
  - Fixed bash vulnerability CVE-2022-3715
  - Fixed CGI-IO file download vulnerability CVE-2022-38333
  - Fixed libxml2 vulnerability CVE-2022-40304
  - Fixed libcurl vulnerabilities CVE-2022-43551 and CVE-2022-43552
  - Improved file upload logic
  - Fixed GPL firmware compilation with selected Tinc package
  - Fixed OpenVPN Static Key migration via keep settings issue
  - Fixed NTP time zone name setting migration when the name contains whitespaces
  - Fixed language setting issue
  - Fixed integer validation on industrial services
  - Fixed LAN port LEDs staying on after being disabled

## **RUTX\_R\_00.07.03.4 | 2023.02.09**

- **Fix**
  - **Services**
    - Sanitized tcpdump storage location
  - **Network**
    - Fixed CVE-2023-32349 vulnerability

## [RUTX\\_R\\_00.07.03.3](#) | 2023.01.25

- **Fix**
  - **Network**
    - Updated init sequence

## [RUTX\\_R\\_00.07.03.2](#) | 2023.01.13

- **New**
  - **System**
    - Japanese language
- **Fix**
  - **Network**
    - Fixed VLAN option setting when changing VLAN ID

## [RUTX\\_R\\_00.07.03.1](#) | 2023.01.03

- **Improvements**
  - **System**
    - Remove front-end certificate validation
- **Fix**
  - **Services**
    - Fixed libxml2 vulnerability CVE-2022-40303
    - Fixed an IPsec Phase one & two setting migration issue
    - Returned missing udp\_client\_count option to Over IP mode
  - **System**
    - Fixed JSON key parsing; keys can now be any printable character sequence
    - Fixed memory leak in 'session' module
  - **WebUI**
    - Fixed file pretty name parsing

## [RUTX\\_R\\_00.07.03](#) | 2022.12.16

- **New**
  - **Network**
    - Firewall DMZ page
  - **Services**
    - Java package
    - SFTP server support
    - OPC UA client
    - Hotspot registered users management page
  - **System**
    - Portuguese language
    - Spanish language
    - Turkish language
    - Email Relay package
  - **WebUI**
    - New Web menu design
- **Improvements**
  - **Network**

- Updated modem handling, attachment, tracking and connection establishment processes
- Added the possibility to select multiple ports in all firewall port fields
- Added 'Match' traffic by type option to firewall traffic rules
- Added DNS servers and routing table fields to the Wireguard page
- Improved generating network topology
- Moved Relayd, UDP Relay & Static Leases to the Interfaces menu section
- Update Firewall Traffic Rules page with DSCP and MARK options
- Added keepalive, holdtime and connect timers to BGP configuration
- Added 'Use gateway metric' to network protocols web interface
- Added more DHCPv6 client events to system log
- Moved IP Filter rules from Modbus TCP Gateway and Over IP services to Firewall page
- Added individual WiFi toggle support
- Added error message when DFS channel is selected during scanning
- Added wget tracking method to WAN Failover
- Added interface checks to remove inaccurate Failover events from the Event Log
- **Services**
  - Added OpenVPN IPv6 Web support
  - Added format button for each USB device in USB Tools General page
  - Reduced waiting time during storage device setup for Memory Expansion
  - Optimized Storage Memory Expansion package size
  - Replaced ntfs-3g with kernel-mode driver
  - Added USB to Serial support for Modbus, MQTT Modbus Gateway, NTRIP, DNP3
  - Added CSP headers to Hotspot Landing Page
  - Added hotspot user script validation
  - Improved logging of disconnecting client devices
  - Implemented Hotspot 'forget' method, which removes user from DB by MAC
  - Updated Zerotier web interface
  - Added IPsec Flush connection option on tunnel initialization
  - Added MODBUS slave regfile validation
  - Added delay, number of timeouts, always reconnect options to MODBUS Master service
  - Added DMVPN Phase 2 and Phase 3 support
  - Added synchronization counting to NTP client
  - Expanded the data that is sent to the Cumulocity cloud with device log, mobile data usage and GPS data
  - Added 'Unregister' button to RMS page
  - Added new data monitoring options to SNMP: configuration state of wireless, smart queues & VLANs
  - Updated Zerotier package to version 1.10.1
  - Added automatic package removal upon failed installation in Package Manager
  - Added option to describe custom routing table and MTU auto counting to Wireguard VPN
  - Added IP blocking to MQTT Bridge for failed login attempts to prevent bruteforce attacks
  - Updated sqm-scripts to version 1.5.1
  - Improved MODBUS Master service: added multiple datatypes, added multiple register reading for alarms
  - Added monthly reboot option to periodic reboot function
  - Added support for multiple custom option selection to SSTP configuration



- Added PKCS12 certificate chain support to OpenVPN
- Improved MQTT to support multiple port listening, multiple bridge connections, notification settings and added support for custom configuration file
- Added QoS selection to MQTT Modbus Gateway
- Improved RAM usage during upload and installation of packages via Package Manager
- Updated curl to version 7.86.0
- Added brute-force prevention measures to Post/Get
- Added automatic private and public key generation to Wireguard VPN
- Added multiple Remote source IP support to IPsec
- Added the possibility to configure multiple IPsec phase 1 and phase 2 proposals
- Added functionality to rotate log file when log is saved to Flash memory
- Improved performance while fetching packages on repeat visits to the Package Manager page
- Updated Dbus to version 1.13.18
- **System**
  - Added a 'test mail' button to the Administration -> Recipients page
  - Added option to clear blocked IPs in the Access Control page after reboot
  - Updated Web Request-Response core logic
  - Added certificate validation to all services that support certificate upload
  - Updated URL protocol validations
  - Removed profile update requests during Save & apply
  - Optimized profile switching logic
- **WebUI**
  - Added bootloader version to the Device section in the System page
  - Added configuration page shortcuts to Overview page widgets
  - Added tooltip in Overview that show free, used and total RAM/Flash values on mouse cursor hover
  - Updated network interfaces protocols web interface
  - Updated 404 page to include navigation menu
- **Fix**
  - **Network**
    - Fixed CVE-2023-32350 vulnerability
    - Fixed jumbo frames MTU issue
    - Added the 'Any' choice to source & destination IP address field in NAT rule edit
    - Fixed NHRP web interface issues
    - Fixed WAN interface configuration interfering with LAN
    - Fixed mac80211 vulnerabilities CVE-2022-41674, CVE-2022-42719, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722
    - Fixed wireless interfaces connections not reestablishing after disabling & enabling again
    - Updated DFS radar detection patterns for Japan
    - Fixed Wired WAN connectivity issue when Failover interfaces are disabled
    - Fixed Failover fallback issue
  - **Services**
    - Fixed Printer service starting issue
    - Fixed Printer service boot issues
    - Fixed DLNA service reload issues on USB drive insert/remove
    - Fixed relay state switching
    - Fixed Save & Apply issue with ADC/ACL type condition on I/O Juggler

- Added I/O restart on configuration profile change
- Fixed I/O voltage range display for power socket pins
- Fixed SMNP OID for I/O state
- Fixed Hotspot connected user list maximum upload/download value limits
- Fixed incorrect connected Hotspot user information in RMS JSON
- Removed unnecessary field from the Port Mirroring page
- Fixed Hotspot issues related to specific connected phones
- Fixed Wireless AP enabled by MODBUS TCP Master not showing in Wireless clients
- Fixed WiFi Scanner hostname validation issues
- Fixed dbus vulnerability CVE-2020-35512
- Fixed dnsmasq vulnerability CVE-2022-0934
- Fixed ext4 vulnerability CVE-2021-3428
- Fixed kernel vulnerabilities CVE-2021-3669, CVE-2021-4203, CVE-2022-1353, CVE-2022-3435, CVE-2022-20008, CVE-2022-30594
- Fixed libxm12 vulnerability CVE-2022-29824
- Fixed Linux vulnerabilities CVE-2021-4148, CVE-2022-0480, CVE-2022-1055, CVE-2022-0886, CVE-2022-2663, CVE-2022-36879 for v5.4
- Fixed MQTT DoS vulnerability CVE-2021-41039
- Fixed privoxy vulnerability CVE-2021-44542
- Fixed python3 vulnerability CVE-2022-42919
- Fixed strongswan vulnerabilities CVE-2021-41991, CVE-2021-45079
- Fixed uboot vulnerabilities CVE-2022-30552, CVE-2022-30790
- Fixed switching between RMS connection types while the device is unregistered
- Fixed reload issues in website blocking feature
- Fixed IPsec PSK secret required field validation
- Fixed bandwidth limiting after QoS is enabled for the first time
- Fixed Dropbear issues when logging in over IPv6
- Fixed Modbus status in Status -> Services page
- Fixed Azure IoT Hub application issues when sending large volumes of data
- Fixed Azure IoT Hub MQTT password validation
- Fixed DMVPN configuration migration issue
- Fixed DMVPN duplicate select options, added suffix to mobile interfaces to use IPv4
- Fixed DMVPN IPsec connection issue
- Fixed DMVPN mobile interface 'Keep settings' migration issue
- Fixed Dynamic DNS long hostname text display issue
- Fixed Events Reporting memory leak issue
- Fixed Events Reporting not triggering after flipping an I/O slider
- Fixed FOTA cron job not starting after factory reset
- Fixed IPsec local firewall option parsing
- Fixed IPsec tunnel creation issue when compatibility mode is used and the tunnel name contains an underscore
- Fixed L2TP, PPTP, SSTP state display in the Status -> Services page
- Fixed NTP pool hostname validation
- Fixed OpenVPN certificate remove with Static key and TLS authentication methods
- Fixed OpenVPN configuration saving issue when using HMAC key authentication
- Fixed OpenVPN custom dev name transformation to correct format
- Fixed OpenVPN device name setting logic when uploading config from file
- Fixed OpenVPN instance status display

- Fixed OpenVPN TAP (bridged) configuration detection
- Fixed Qos configuration saving issue occurring after instance deletion
- Fixed RMS JSON incorrect WAN state and IP information
- Fixed RMS step access issue in the Setup Wizard page
- Fixed SNMP issues after reboot while using a Hotspot
- Fixed SNMP generating MIB files for devices in accordance with to their hardware
- Fixed SNMP traps not working after SNMP is installed from server
- Fixed SSTP client route creation issue
- Fixed UPNP secure mode not turning off issue
- Fixed Wireguard route to endpoint issue
- Fixed manual package installation for queued packages
- Fixed NAT Rules dependency from IPsec web instance
- Returned usleep utility
- Updated Australian and South African NordVPN server IP addresses
- Fixed paired bluetooth devices appearing nameless
- **System**
  - Fixed LED operation while device is in bootloader state
  - Fixed certificate signing issues
  - Fixed Telnet, CLI access blocking after max invalid tries
  - Fixed FW upgrade with 'Keep settings' while low free space is available
  - Fixed backup file duplication issue
  - Fixed network device handling in system
- **WebUI**
  - Fixed Hotspot interface display
  - Fixed side widget accessibility during first login
  - Fixed file upload issues
  - Fixed drag and drop issue in the Traffic Rules page
  - Fixed protocol display in the overview of the Interfaces page
  - Fixed blocked IP settings migration during a FW upgrade with the 'Keep settings'
  - Fixed login errors after browser tab restoration
  - Fixed redirect to newly set IP address after Interface configuration
  - Fixed firmware upgrade verify spinner not closing
  - Fixed an issue with file upload via drag and drop

## [RUTX\\_R\\_00.07.02.7](#) | 2022.09.12

- **Fixes**
  - Fixed CVE-2022-1012 memory leak vulnerability
  - Fixed CVE-2022-37434 kernel vulnerability
  - Fixed interface option reset after VLAN ID change
  - Removed memory leak on port events
  - Fixed WiFi Scanner out of range crash when iterating collected data

## [RUTX\\_R\\_00.07.02.6](#) | 2022.08.24

- **Fixes:**
  - Fixed Serial-symlink dmesg messages
  - Fixed OpenVPN tls-auth and tls-crypt option names

## [RUTX\\_R\\_00.07.02.5](#) | 2022.08.12

- **Improvements:**

- Updated curl to version 7.83.1
- Updated firmware validation error messages
- Added multiple source IP address support to the Port Forwards page
- Added CSP headers Hotspot WebUI landing page
- Optimized CORE distribution for packet handling
- Fixes:
  - Lixed EEE link advertisement
  - Fixed CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208 curl vulnerabilities
  - Fixed CVE-2022-30065 busybox vulnerability
  - Fixed file upload path traversal
  - Removed Data to Server limit to process less than 10 instances
  - Fixed Data to Server 'out of memory' crashes when database is full or has a large amount of data
  - Fixed OpenVPN dev setting logic
  - Fixed OpenVPN updating from legacy issue that caused IPv6 not to work
  - Fixed modal tabs navigation when editing wireless interface with non-english languages

## [RUTX\\_R\\_00.07.02.4](#) | **2022.07.20**

- Improvements:
  - Added default password change warning message before firmware downgrade
- Fixes:
  - Fixed CVE-2022-2068 vulnerability
  - Fixed Hotspot login via landing page issue
  - Fixed possible I2C bus lock-up issue when upgrading firmware from 02.xx versions

## [RUTX\\_R\\_00.07.02.2](#) | **2022.06.27**

- Improvements:
  - Updated FSTools package to version 2022-05-03
  - Added security headers to web requests
- Fixes:
  - Fixed CVE-2019-12900 libbz2 vulnerability
  - Fixed CVE-2022-23303 hostapd vulnerability
  - Fixed CVE-2022-29581 Linux kernel vulnerability
  - Fixed CVE-2022-29458 ncurses vulnerability
  - Fixed CVE-2022-1292 c\_rehash script command injection vulnerability
  - Fixed race condition for wireless configuration initialization

## [RUTX\\_R\\_00.07.02.1](#) | **2022.06.06**

- Fixes:
  - Fixed IGMP Proxy menu item not appearing after package installation
  - Fixed MODBUS write requests

## [RUTX\\_R\\_00.07.02](#) | **2022.05.23**

- **New features**
  - Overview side widget

- IGMP Proxy
- Privileged Access Management (PAM)
- AWS Greengrass support
- HTTPS certificate and key upload feature
- SSH public keys edit box
- License page
- Bluetooth EYE sensors support
- DNP3 data for Data to Server

## • Improvements

- Updated busybox to version: 1.34.1
- Updated curl to version 7.79.1
- Added iptables filter package for string filtering
- Added CHAP authentication for L2TP VPN
- Added IPv6 support for L2TPv3 VPN
- Added EAP-MSCHAPV2 authentication method for IPsec VPN
- Added IPv6 support to Auto Reboot
- Added 'Save to flash' and 'Test configuration' button to DNP3 configuration page
- Updated SNMP version 5.9.1
- Added OpenSSL authentication options to SNMPv3
- Added support for OSPF redistribution options and OSPF neighbors
- Added password field to BGP Peers page
- Extended BGP "AS" field validation to accept integers up to 4294967295
- Added "DHE+RSA" to OpenVPN cipher selections
- Increased OpenVPN max password length from 128 bytes to 512 bytes
- Made HMAC key direction initial value dependent on the role of the instance (client or server)
- Made HMAC key and HMAC authentication key upload fields required
- Added DES to IPsec encryption algorithms selections
- Added special character support for CHAP secrets
- Added validation requirements for PPTP user list username field
- Added option to manually enter Public key in Wireguard configuration
- Made generating Wireguard keys possible only while in auto mode
- Added Events Log database to troubleshoot archive
- Added RFC1918 filter field
- Added the possibility to unblock multiple blocked devices at once
- Added 'Port' column to blocked login attempts table
- Added Speedtest server refresh
- Updated Speedtest server list
- Added asterisk option to Site Blocking
- Added MD5 and SHA256 checksums to package validation page
- Changed certificate requirements to only require client key file if client certificate is used
- Added pagination and data retention between table pages
- Added pagination functionality to tables when there are more than 10 records
- Improved table sorting by saving user provided sort settings in the browser
- Improved drag and drop functionality
- Added the possibility to drag and drop files onto upload components
- Moved 'Root CA' from the 'Access Control' page to the 'Certificates' page
- Added 'Strict-Transport-Security' response header for HTTPS
- Added 'breadcrumbs' to modal windows

- Improved initial WebUI loading after login
- Added Hotspot configuration profiles
- Added local Hotspot user password hashing
- Added Hotspot password encoding option
- Improved Hotspot related firewall rule setting
- Improved WiFi Scanner enable switch to toggle 2 and 5 GHz instances separately
- Removed CHAP authentication protocol for WiFi Hotspots due to incompatibility with hashed passwords
- Added ubus support to Hotspot
- Changed default port name of WiFi devices for 'Topology state' Events Reporting rule
- Added error code 5 for reserved SAMBA user names
- Added Mobile data and SMS limit features for external modem
- Added I/O SNMP trap
- Added ISO 8601 time format to I/O Juggler's '%ts' parameter
- Added device name parameter '%pc' to I/O Juggler
- Added PPPoE VLAN priority support
- Made VRRP ping section dependent on main instance
- Added 'WAN to LAN' switch

#### • Fixes

- Fixed CVE-2021-20322, CVE-2021-4197, CVE-2022-1011, CVE-2022-0847 kernel vulnerabilities
- Fixed CVE-2022-28391 busybox vulnerability
- Fixed CVE-2018-16789 shellinabox vulnerability
- Fixed CVE-2021-44543, CVE-2021-44542 privoxy vulnerabilities
- Fixed CVE-2021-43618 GNU Multiple Precision Arithmetic Library vulnerability
- Fixed zlib backport security issue
- Fixed Wireguard firewall zone assignment
- Fixed queued packages disappearing from list after FW upgrade with keep settings
- Fixed error message display for multiple input validation rules
- Fixed incorrect DHCP validation range for start and limit fields
- Removed 'Bring up on boot' option from network interface configuration pages
- Fixed coma-separated DHCP options disappearing after save
- Fixed exclude and listen interfaces
- Fixed 'Use broadcast flag' option saving
- Fixed firewall zone assignment when creating new interfaces
- Fixed OpenVPN 'Netmask' and 'IP address' field validations
- Fixed OpenVPN TAP configuration saving issue
- Fixed OpenVPN switching to TUN mode when uploading a configuration from file
- Fixed dynamic BGP route state display
- Fixed BGP peer enable in edit page
- Fixed issue when no L2TP client instance could be bound to IPsec
- Fixed firewall rule and zone behavior related to config section creation
- Added default value for L2TPv3 netmask, which is now written to config after save
- Fixed passthrough option saving to IPsec file
- Fixed DMVPN issue where instance configuration could not be saved
- Fixed Wireguard peer could not be saved issue
- Fixed NTP client time synchronization after factory reset
- Fixed device time display with selected time zone
- Fixed MODBUS TCP indexation missing bracket issue
- Fixed initial MODBUS TCP request count validation

- Fixed PIN 3/4 direction switching over MODBUS TCP
- Fixed MODBUS data to MQTT socket closing issue when connection fails
- Fixed MODBUS alarm configuration deletion
- Fixed DNP3 master not working after FW upgrade with 'keep settings'
- Fixed DNP outstation not returning error messages
- Added missing SNMP objects: mobile IP, data sent/received today
- Fixed MQTT Publisher 'Remote address' field validation
- Fixed long interface name support for Azure IoT Hub
- Increased maximum Azure IoT Hub 'Connection String' length to 4096 characters
- Fixed missing sent/received data issue
- Fixed URL input field length validation
- Fixed admin login issue after upload of backup from a device with older firmware versions
- Fixed MAC address formatting in Events reporting messages
- Fixed Events reporting DHCP lease message spam, when no new lease is added
- Fixed logging crashing after downloading Troubleshoot file
- Made Wake on LAN visible only on devices with Ethernet ports
- Fixed Traffic log file transfer to FTP server
- Fixed Web Filter service reloading after a host list file is uploaded
- Fixed access denied messages when sending JSON-RPC requests from root user
- Fixed error message display about duplicated intervals in Profile scheduler
- Fixed FW upgrade with 'keep settings' migration issue for Access Control's 'Fail count' and 'Device port' fields
- Corrected OSPF Routing card values, value positions and names
- Fixed global secret instances not being removed when there are no IPsec instances
- Fixed uploaded file remove icon not staying in position on hover
- Fixed Overview card collapse issue that made it unresponsive after too many clicks
- Removed WAN6 interface from the Overview page
- Fixed Cumulocity connection issue
- Hidden phone groups menu
- Added multiwan support for Wireguard default route
- Fixed wireless signal strength display when no clients are connected
- Fixed loss of connectivity for clients when router is in STA+AP mode
- Added validation that prevents automatic connection to first unencrypted WiFi AP when using MULTI AP
- Fixed Wifi Scanner data not being stored in certain scenarios
- Fixed WiFi scanner not turning on after FW upgrade with 'keep settings'
- Fixed Hotspot user group limit not resetting on specified time
- Removed an RMS error message when no Hotspot users were created
- Fixed Hotspot landing page image upload issue
- Fixed I/O Juggler external modem recognition
- Fixed flash driver reformatting after memory shrink
- Fixed DLNA package installation issue
- Changed Media Directories field to be required
- Fixed SAMBA fields value display
- Fixed relay output value display in I/O Juggler condition page
- Fixed I/O Juggler's WiFi rule not enabling or disabling WiFi interfaces
- Fixed I/O Juggler's double delete issue on I/O Juggler action and condition instances
- Fixed I/O Juggler's incorrect I/O status messages
- Fixed paired Bluetooth device RSSI display after reboot

## [RUTX\\_R\\_00.07.01.4](#) | 2022.02.25

- **Improvements**

- Increased Port Forwards rule max name length
- Added a new '%it' parameter for UTC time in ISO 8601 format to I/O Juggler

- **Fixes**

- Added missing bracket to the end of MODBUS messages
- Fixed preserving the contents of /etc/luci-uploads/ after FW upgrade with the 'Keep all settings' option
- Fixed IPv4-Gateway column showing empty values in the Status -> Routes page
- Fixed firewall extra option validation
- Fixed Hotspot enable button validation
- Fixed usage of custom headers in I/O Juggler HTTP action
- Fixed 'verify' option parsing for I/O Juggler
- Fixed OpenVPN server configuration with password authentication
- Fixed NTP interval length validation
- Fixed network interface enable after Drag & Drop
- Updated NTP client interval to 24h

## [RUTX\\_R\\_00.07.01.2](#) | 2022.01.04

- **Improvements**

- Removed L2TP section title prefixes

- **Fixes**

- Fixed IPsec crashing issue using mobile
- Fixed FW flashing when chip is in unknown state
- Fixed CPU usage percentage display in the Overview page
- Fixed FOTA timeout issue when server does not respond
- Fixed installation of backup packages

## [RUTX\\_R\\_00.07.01](#) | 2021.11.18

**Note:** Firmware version RUTX\_R\_00.07.01 released on 2021.11.18 was removed due to an issue with IPsec tunnel while using mobile connection.

---

- **New features**

- Load Balancing Rules
- 802.11s based wireless mesh network support
- Multiple Wireless AP feature
- RUTX series support without STM32
- Tinc VPN
- German language support

- **Improvements**

- Updated base to OpenWrt version 21.02
- Improved WebUI functionality when multiple browser tabs are open
- Updated kernel to version 5.4.141
- Updated mtd-utils to version 2.1.2
- Updated busybox to version 1.33.1



- Updated ubus to version 2021-06-3
- Updated ubox to version 2020-10-25
- Updated rpcd to version 2021-03-11
- Updated opkg to version 2021-06-13
- Updated fstools to version 2021-01-04
- Updated wwan to version 2019-04-29
- Updated ethtool to version 5.10
- Updated uhttpd to version 2021-03-21
- Updated ppp to version 2020-10-03
- Updated odhcpd to version 2021-07-18
- Updated hostapd to version 2020-06-08
- Updated dropbear to version 2020.81
- Updated dnsmasq to version 2.85
- Updated netifd to version 2021-07-26
- Updated firewall3 to version 2021-03-23
- Updated libjson-c to version 0.15
- Updated libevent2 to version 2.1.12
- Updated mac80211 to version 5.10.42-1
- Updated wireless-regdb to version 2021.04.21
- Updated binutils to version 2.35.1
- Updated gdb to version 10.1
- Updated strace to version 5.10
- Updated trace-cmd to version 2.9.1
- Updated valgrind to version 3.16.1
- Updated ath10k-ct-firmware to version 2020-11-08
- Updated procd to version 2021-02-23
- Updated iw to version 5.9.8
- Updated iproute2 to version 5.11.0
- Updated iptables to version 1.8.7
- Updated nettle to version 3.6
- Updated libpcap to version 1.9.1 rel3
- Updated elfutils to version 0.180
- Updated cryptodev-linux to version 1.11
- Updated linux-firmware to version 20201118
- Updated util-linux to version 2.36.1
- Updated openwrt-keyring to version 2021-02-20
- Updated mtd to version rel26
- Updated fwtool to version 2019-11-12
- Updated ca-certificates to version 20210119
- Updated wireguard-tools to version 1.0.20210223
- Updated iwinfo to version 2021-04-30
- Updated ipset to version 7.6
- Updated gre to version rel12
- Updated wolfssl to version 4.7.0
- Updated ustream-ssl to version 2020-12-10
- Updated uclient to version 2021-05-14
- Updated readline to version 8.1
- Updated mbedtls to version 2.16.11
- Updated libusb to version 1.0.24
- Updated libunwind to version 1.5.0
- Updated libubox to version 2021-05-16

- Updated libnl-tiny to version 2020-08-05
- Updated libnftnl to version 1.1.8
- Updated libiconf-full to version 1.16
- Updated libbsd to version 0.10.0
- Updated gmp to version 6.2.1
- Updated ulogd to version rel6
- Updated sqm-scripts to version 1.5.0
- Updated ntpclient to version rel14
- Updated nmap to version 7.80
- Updated curl to version 7.77.0
- Updated zerotier to version 1.6.5
- Updated xtables-addons to version 3.13
- Updated xl2tpd to version 1.3.16
- Updated stunnel to version 5.59
- Updated strongswan to version 1.0.13
- Updated sstp-client to version 1.0.13
- Updated pptpd to version rel5
- Updated openvpn to version 2.5.3 rel2
- Updated ntpd to version rel3
- Updated net-snmp to version rel2
- Updated mosquitto to version 2.0.11
- Updated miniupnpd to version 2.2.1 rel 3
- Updated etherwake to version rel5
- Updated libzip to version 1.7.3
- Updated libpgp-error to version 1.39
- Updated glib2 to version 2.66.4
- Updated libnetfilter-conntrack to version 1.0.8
- Updated libnetfilter-log to version rel3
- Updated lzo to version rel4
- Updated nghttp2 to version 1.43.0
- Updated openvpn-easy-rsa to version 3.0.8 rel3
- Updated iperf to version rel2
- Updated iperf3 to version 3.10.1
- Updated e2fsprogs to version 1.45.6
- Updated fuse to version 2.9.9
- Updated udprelay to version 2020-02-26
- Updated qmicli to version 1.28.2
- Updated pcre to version 8.45
- Updated libsmpp34 to version 1.14.1
- Updated libiwinfo to version 2.1
- Added netifd library for additional information related to network interfaces
- Updated openssl to version 1.1.1l
- Updated privoxy to version 3.0.32
- Added ACL reload method for sessions
- Added 'Advertisement interval' field to the VRRP configuration window
- Added a PPTP-to-WAN Zone Forwarding rule when default route is enabled on PPTP client
- Added email user group validation for sendind test emails with Events reporting
- Added an event logging feature for Ping Reboot events
- Improved file/section deletion logic: now files are also deleted after deleting a related config section

- Improved package deletion logic
- Added the possibility to configure multiple reboot times in one Reboot Scheduler configuration instance
- Updated 'External system log server' field validation to accept IPv6 addresses
- Added redirect to Overview page after login
- Added WebUI session timeout after user inactivity
- Added placeholder text to dropdown menus
- Improved multi-select design and functionality
- Added Unix timestamp, local ISO time, UTC time to Modbus
- Added info message when selected file cannot be uploaded
- Improved IPsec throughput
- Added IPsec "Compatibility mode" configuration support
- Made SNMP 'Community name' option editable
- Added new configuration options to the Failover feature
- Changed Failover page availability from Advanced only both advanced and basic
- Made Failover Interfaces table rows draggable when in 'Load Balancing' mode
- Changed Failover page 'Ratio' fields to a smaller size
- Added 'Duplicate passwords are not allowed' error message to Hotspot landing pages
- Added 'Allow password duplicates' field to the Hotspot configuration page
- Improved wireless frequency option layout
- Added external modem support for the 'Mobile Usage' graph
- Added pagination, search bar and easier device selection to the Bluetooth page
- Added I/O support to SNMP
- Removed ubus list method due to security reasons
- Added MODBUS "%I, %T, %S, %r, %n" support to MODBUS Data Sender
- Removed search engine site crawling
- Improved IPsec "Local/Remote source" validation
- Added Firewall "all" and "custom" protocol options
- Added Backup file size limit of 2 MB
- Improved basic/advanced mode changing
- Improved Wireguard "IP Addresses" field validation
- Added language download support from language selection section
- Added PPTP "Client to client" configuration support
- Made DDNS "username", "password", "host" fields optional
- Added SSTP "Default route" configuration support
- Added support for PL2303GC serial to USB chip
- Added bgscan feature to wpa\_supplicant
- Optimized Wireless device status information requests in all WebUI pages

#### • **Fixes**

- Made RMS 'Connect' button disabled when a connection attempt is already in progress
- Added validation for TLS Clients 'Private network' option
- Fixed the validation range for MTU fields
- Fixed removing firmware image file after leaving the firmware upgrade page
- Fixed network selection list for Traffic Logging - added all available LAN networks
- Fixed DHCP Options validation
- Fixed configuration profile date display
- Fixed blank page after invalid URL in login page
- Fixed TR-069 related firewall rule loading
- Fixed remote subnet netmask validation issues for the GRE Tunnel configuration
- Fixed WebUI section toggle

- Fixed package installation modal layout
- Fixed current page values showing up in login page username field
- Fixed the possibility to create section with a name that is already in use in the same config file
- Fixed OpenVPN username and password deletion when deleting configuration instance
- Fixed session closing issue for the user whose password was just changed
- Updated MODBUS credential validation
- Updated MQTT credential validation
- Fixed DNS 'Rebind protection' setting when switch is disabled
- Updated libgcrypt to version 1.9.3 to fix CVE-2021-33560
- Fixed CVE-2021-33624, CVE-2021-29648 vulnerabilities
- Fixed DHCP 'Lease time' and 'Unit' option saving over the Setup Wizard LAN page
- Fixed Reboot Scheduler not removing crontab file after disabling the rule
- Fixed OpenVPN 'Extra options' field validation to allow a space character
- Added table drag and drop functionality to the Firewall's Traffic Rules page
- Fixed DNP3 Outstation crash caused by non-void function returning no value
- Fixed RMS 'Copy' button functionality
- Fixed incorrect loading after saving Failover configuration
- Fixed escaping '#' symbol from hotspot username and password fields
- Fixed I/O Juggler hour condition interval issue
- Patched CVE-2021-40528 vulnerability
- Patched CVE-2021-40490 vulnerability
- Patched CVE-2020-16120 vulnerability
- Fixed VLAN section creation
- Returned Interfaces "Port priority" option
- Fixed missing Content-Type header to initial WebUI response
- Fixed RIP information parsing in status page
- Fixed OpenVPN IPv6 netmask validation
- Fixed SNMP Trap Settings Host/IP field validation
- Fixed Cumulocity authentication reset
- Fixed Events Reporting rule saving

## **RUTX\_R\_00.07.00 | 2021.07.16**

### **• New features**

- New WebUI based on Vue.js 2.6.12
- RutOS updated to OpenWrt 19.07.7 base
- DNP3 Master and DNP3 Outstation

### **• Improvements**

- Updated firewall to release 3
- Updated kernel to version 4.14.221
- Updated uhttpd to version 2020-10-01
- Updated xtables-addons to release 9
- Updated mwan to version 2.8.14
- Updated pcre to version 8.44
- Updated curl to version 7.74
- Updated sqlite to version 3.33
- Updated ncurses to version 6.2
- Updated OpenSSL to version 1.1.1k
- Added full MODBUS register address expansion specifier for Data to Server
- Added full MODBUS register address legend

- Added Client ID option for the MQTT protocol in Data to Server
- Improved Data to Server sleeping accuracy
- Improved Data to Server username validation; now space is allowed
- Added firmware version OID to the SNMP service
- Added IP address family option field to the SNMP page
- Added SNMPv6 section to the SNMP Communities page
- Renamed the 'System -> Users' page to 'System -> System Users'
- Moved password changing option to the 'System -> System Users' page
- Switched to ar8216 driver
- Added IPsec XAUTH support
- Improved OpenVPN updown, init scripts to write info about instance in JSON
- Added AES-256-GCM encryption support to OpenVPN
- Added extra configuration parameters to DMVPN
- Added PSK conversion to DMVPN and single PSK types
- Improved Package Manager package installation, deletion and dependencies
- Improved Package Manager download process over FOTA
- Added new Input/Output values manageable over RMS
- Added IPv6 traffic logging
- Made 'Network -> Failover' and 'Network -> Interfaces' page data draggable on multiple browsers
- Added Input/Output Post/Get URL parameter t\_time changing delay and time to seconds or milliseconds
- Added support for multiple USB to Serial adapters
- Added option to send SMS warning messages to Hotspot users authenticated with SMS OTP when specified amount of data is used up
- Added option to switch back to primary SIM card after timeout
- Improved I2C communication
- Added peer groups to BGP access list dropdown
- Added TCP MD5 authentication support for BGP
- Added option to switch back to primary SIM card after timeout
- Improved I2C communication
- Added peer groups to BGP access list dropdown
- Added TCP MD5 authentication support for BGP

#### • Fixes

- Added glib2 patch to fix CVE-2019-13012 vulnerability
- Added ntfs-3g patch to fix CVE-2019-9755 vulnerability
- Added WolfSSL patch to fix CVE-2021-3336 vulnerability
- Added Busybox patch to fix CVE-2018-1000500 vulnerability
- Added netifd, odhcp6c IPv6 routing loop on point-to-point links patches to fix CVE-2021-22161 vulnerability
- Fixed Android clients IPsec MTU/MSS size
- Fixed wrong IPsec DPD value saving
- Changed IPsec PSK maximum length to 128 symbols
- Fixed SSTP remaining up after package removal
- Fixed DMVPN crypto\_proposal write to config
- Fixed I/O Juggler's SMS sending to correct group
- Fixed I/O Scheduler's relay state issue
- Added I/O direction check while changing IOs via I/O Post/Get
- Fixed float endianness mismatch on some devices MODBUS TCP Master, MODBUS Serial Master

- Fixed UPnP issue that caused config changes to apply only after service restart
- Fixed WebUI files caching when upgrading firmware
- Fixed WebUI date display format
- Fixed MODBUS returning incomplete MAC address data
- Fixed 'Over IP' serial type's UDP issue in client mode
- Fixed DLNA connections count total in statistics page
- Fixed WiFi Hotspot's Walled Garden issues
- Fixed WiFi Hotspot data logging issues
- Fixed P2P group information processing vulnerability in wpa\_supplicant
- Added validation to Walled Garden Address list field
- Fixed wrong VRRP IP address writing to file
- Fixed DLNA connections count total in statistics page
- Fixed JSON-RPC issue that caused incorrect state returns

## [RUTX\\_R\\_00.02.06.1](#) | 2021.02.10

### • Fixes

- Added dnsmasq patch CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687
- Fixed PPTP server interface naming
- Fixed correct client PPTP interface name selection for route creation
- Fixed adding helper to firewall's wan zone when enabling PPTP configuration
- Added package size checking when manually installing a package
- Fixed 'New Firmware Available' message display after firmware upgrade

## [RUTX\\_R\\_00.02.06](#) | 2020.12.31

### • New features

- External Quectel modem support
- WPA3 WiFi encryption

### • Improvements

- Updated base to OpenWrt 19.07.4
- Added Phone Groups as possible SMS recipients to SMS Post/Get
- Added PSK support for MQTT Broker/Publisher
- Changed Output Scheduler structure
- Removed limitation of one configuration per Input
- Added multiple modem support for TR-069
- Fixed parsing user uploaded custom OpenVPN configuration files containing carriage returns
- Added iptables conntrack flush on WAN Failover if IPsec is enabled
- Optimized package responsible for sending/receiving GRE Tunnel keepalive packets
- Added extra error checking to Package Manager when downloading packages
- Added data usage info for both SIM cards to RMS
- Added logging to syslog when Ping/Wget Reboot "Action" is set to 'None'
- Improved display of configuration tables when a lot of information is shown
- Renamed MODBUS strings to uppercase
- Added redirect to configuration page after a new configuration is created with the 'Add' button
- Added option to create a Configuration Profile from current configuration
- Added data validation to Profiles Scheduler fields
- Replaced the Firewall 'Helpers' page with conntrack helper configuration for each

firewall zone

- Increased dynamic list maximum amount of values to 50
- Added the possibility to save email accounts without entering email username and password
- Unified device access password validations
- Expanded DDNS validation for domain input to accept emails
- Added the possibility to ignore DFS channels when automatic channel selection is performed (for 5 GHz WiFi)
- Removed unsecure WPA-PSK and WPA-EAP encryption support
- Improved Hotspot Landing page address validation to accept a trailing slash
- Removed unnecessary warning message in the Hotspot page
- Disable Wireless device & interface configurations when WiFi device is in 'pending' state
- Removed unused 'Expiration time' option in the Hotspot page
- Refactored GPS code
- Split VLAN configuration page into two separate ones: 'Port Based' and 'Interface Based'

- **Fixes**

- Fixed IPsec Passthrough subnet/ip value parsing to make it dynamic for leftsubnet
- Fixed occasions when error messages overlap buttons
- Fixed I/O state saving after revert back to original state
- Fixed IPsec connection after reboot
- Fixed bridged interface configuration for L2TPv3
- Removed trailing newlines in returned SNMP strings
- Fixed Events Reporting waiting to send email before rebooting
- Fixed MQTT MODBUS Gateway not working when topics have special characters
- Swapped pin3 and pin4 values in MQTT Publisher
- Added an 'IP4Table' option to advanced interface configuration
- Fixed an issue where User Scripts were being deleted after device reboot
- Fixed various WebUI validation bugs, typos, option hints & alignments
- Fixed a bug that caused an internal sever error after logging in with a username that contained special characters
- Fixed crashes that occur after configuration files are not correctly generated
- Fixed a Firewall Port Forwarding bug which caused an internal sever error when no 'Protocol' was selected
- Fixed changing WebUI mode bug while current page is accessed with POST method
- Fixed password allowed lengths and tooltips
- Fixed mountpoint display
- Fixed WiFi SSID validation
- Fixed keeping Hotspot Walled Garden address list after firmware upgrade
- Fixed internal server error upon opening the 'Wireless' Status page while WiFi device band is set to 'Auto'

## [RUTX\\_R\\_00.02.05.2](#) | 2020.11.19

- **Fixes**

- Randomized the global rate limiter to mitigate "SAD DNS" attack

## [RUTX\\_R\\_00.02.05.1](#) | 2020.09.30

- **New features**

- DLNA media server
- iptables NETMAP extension

- "Flush connections on" option for WAN Failover
- New firmware notifications
- Updated header logo from 'Teltonika' to 'Teltonika | Networks'
- 802.11r support
- WiFi Scanner
- SQM QoS
- USB Tools
- USB to Serial adapter support
- Auto format USB storage devices to NTFS
- Storage Memory Expansion

- **Improvements**

- Improved WebUI page loading speed
- Added Basic/Advanced mode selection in Setup Wizard
- Added a dropdown with a search function for time zone selection
- Added "copy to clipboard" button in Cloud Solutions next to MAC and Serial
- Added option to send all Modbus records in one packet
- Disabled IPV6 services on LAN by default
- Added password hashing in Post/Get pages
- Added a warning message about rebooting the device while certificate files are being generated
- Added status option to uploaded custom OpenVPN configuration file
- No longer showing "Enable OpenVPN config from file" option if "Enable external Services" is selected
- Added some missing placeholder values
- Added warning message about unsaved changes when leaving Auto Reboot, Periodic Reboot, Wireless pages
- Added port selection to SSTP configuration
- Changed Periodic Reboot service name to Reboot Scheduler
- Added table row highlights on hover
- Changed section name from 'Email users' to 'Email accounts' in the Recipients page
- Added network interface automatic assignment to firewall zones when interface protocol is switched
- Adjusted Azure validations
- Adjusted Local/Remote subnet field validations
- Adjusted Hotspot field validations
- Unified VPN overview section option names and titles
- Removed mandatory requirements for inter-zone forwarding source & destination options in Firewall zone configuration
- Added placeholder values for drop down options in Routing pages
- Increased maximum package upload size
- Removed mobile interfaces from Hotspot configuration
- Added "Passthrough subnets" option to IPsec configuration page
- Added package size checking when installing packages via Package Manager
- Optimized switching between Basic and Advanced WebUI modes
- Added missing services to Events Reporting page when selected Event is "Config change"
- Improved general web design, ordering and positioning
- Added word wrap in the Unsaved Changes page
- Centered 'Apply' button in the Profiles page
- Hid network interfaces with DHCPv6 protocol in Overview page while in Basic WebUI



mode

- Changed tcpdump "Select storage" option value from 'Internal storage' to 'RAM memory' in the System → Administration → Troubleshoot page
- Added more descriptive error messages when connection to FOTA server fails
- Updated "Local address" hint in l2tpv3 page
- Made ESSID value mandatory
- Added wireless device status display in Wireless Overview page
- Moved Hotspot2.0 to Services menu
- Added network selection option in Traffic logging page
- Reworked Q-in-Q configuration page
- Added the possibility to unpair all paired Bluetooth devices at once
- Improved Bluetooth device to pair selection
- Moved all USB related services to the 'Services -> USB Tools' page
- Added 'General' page to 'Services -> USB Tools'; the page contains a list of all USB devices and the option to safely unmount the devices
- Added 'passive-interface' and 'default-information' options to the OSPF configuration page
- Added NHRP dynamic route status page

#### • Fixes

- Fixed DDNS freeze issues
- Fixed Firewall Traffic Rules Source and Destination address field validations
- Started using more stable, builtin ar82xx switch driver
- Symlinking tty devices in one place
- Fixed period when sending packet curl timeouts in Modbus Data Sender
- Fixed "active SIM" register value retrieval after regression in Modbus TCP Slave
- Fixed Hotspot 'Trial access' function
- Fixed OpenVPN TLS Cipher display and added a limit to number of ciphers
- Fixed various WebUI validation bugs, typos & option hints
- Fixed DHCP lease range validation and value saving in Interfaces page
- Fixed error messages when creating interfaces with incorrect names
- Fixed various section toggling bugs
- Fixed username validation in SNMP page
- Fixed certificate file importing bugs & common name display in Certificates Manager page
- Fixed interface option related to IPv4 and IPv6 in Routing pages
- Fixed OpenVPN multi-line command that adds client specific parameters
- Fixed DHCP lease range validation in Basic mode
- Fixed incorrect sorting in dynamic tables
- Fixed routing table writing and deleting
- Fixed incorrectly displayed type when no protocol is selected
- Removed Wireguard interfaces from the Interfaces page
- Fixed SNMP user access mode display in SNMPV3 Users Overview page
- Fixed SNMP memory leak on chilli module
- Fixed MD5 and SHA256 checksum calculations
- Fixed DHCP-options field validation to allow separating parameters with commas
- Fixed Package Manager side menu entry updates right after package upload
- Fixed Wireguard port selection
- Fixed VPN zone status display
- Fixed lua errors when Start/End time option is empty
- Fixed incorrectly displayed OpenVPN protocol

- Fixed Lua errors in Profile Scheduler and Firewall Zones
- Removed */log* folder from Troubleshoot file directories
- Fixed endless spinner when applying profiles
- Fixed nil value in the Traffic Logging page
- Fixed "Units" option dependency on "Enable DHCP" option in the Setup Wizard's LAN page
- Fixed redirecting to login page after factory setting restore (reset)
- Removed Unsaved Changes notification when downloading Troubleshoot/tcpdump files from the System → Administration → Troubleshoot page
- Vulnerability fixes for Package Manager and Certificates Manager pages
- Fixed Firewall zone placeholder (removed "-- Please select --" and left "Unspecified")
- Fixed update from server option in the Firmware page
- Added missing error messages when password is invalid in default password change page
- Fixed "Lease time" option in the Setup Wizard's LAN page
- Fixed error 500 when accessing Advanced pages while in Basic mode
- Increased allowed character lengths for MQTT Broker and Data to Server
- Fixed XSS vulnerabilities in package manager and package file upload pages
- Fixed incorrect OpenVPN configuration saving
- Fixed NHRP lua error
- Removed "Wireguard" from Status → Services display if it is not installed
- Fixed wireless interface turning on/off in the Wireless page
- Added connected client number indication to the Overview page and Side Widget
- Fixed platform tags in the Wireless Device edit page
- Added checking if the device has 2.4/5 GHz wireless devices
- Added missing "Hotspot 2.0" service in the Status → Services page
- Fixed Hotspot login page signup fields and notifications
- Fixed incorrect JSON parsing, eternal spinner when unpairing devices & RSSI display in the Bluetooth page
- Removed Phone Groups page
- Changed BGP init start value from 60 to 95
- Fixed erroneous data usage display of external modem after it's been disconnected

## [RUTX\\_R\\_00.02.04.3](#) | 2020.07.31

### • New features

- Backup archive MD5 & SHA256 checksum calculation to help user identify altered backup archives
- Package signature check to verify that a package comes from Teltonika

### • Fixes

- Fixed CVE-2019-17367
- Fixed hiding of configuration pages that users of a specific group don't have read access to
- Fixed firmware upload script

## [RUTX\\_R\\_00.02.04.1](#) | 2020.07.02

### • New features

- USB Tools page with "USB to Serial" and "Printer Server" sections
- Relay control to Call Utilities
- 'Certificates' page for generating and managing TLS certificates

- 'Drag & Drop' support for Overview page tables
- 'Speed Test' feature
- AVL I/O support
- JSON formatting option for Data to Server
- During this release a new package was released - [WireGuard](#)

## • Improvements

- Added timeout and keep-connection options to Modbus TCP Slave
- Improved L2TPv3 functionality with VLAN
- Improved 'Profile Scheduler' with minute accuracy
- Reordered VPN configuration options
- Standardized section header styles
- Unified spelling of dropdown values
- Added information about 'Package Manager' packages before updating firmware
- Updated services management to Status → Services page
- Improved performance of firmware upgrades from server
- Improved security features related to file uploading and HTTP headers
- Changed RAM/flash memory units from MiB to MB
- Updated warning message and lease deletion message for static leasing
- Moved 'Country code' option to general tab
- General web responsiveness improvements

## • Fixes

- Fixed Enable/Disable function in Wireless page
- Fixed validation in Wireless interface edit page
- Fixed 'Wireless Scans' page table headers on smaller screens; changed 'Wireless Scans' page action button positioning
- Fixed BLE device data collection immediately after pairing
- Fixed missing data fields in Bluetooth device database
- Fixed symlinking tty devices in one place
- Fixed random 'I/O Juggler' crashes
- Fixed validations and option saving in OSPF page
- Fixed various element positioning bugs on smaller screens
- Fixed switching to advanced mode notification when accessing non existing pages
- Fixed validations in Traffic Logging page
- Fixed showing failover section only for interfaces with failover rules
- Fixed static leases redirect after saving
- Fixed empty dropdown values in 'I/O juggler' and 'Network Shares'
- Fixed interface IP address validation in DDNS page
- Fixed various spelling mistakes
- Fixed broken address option in the 'Troubleshoot' page
- Fixed dropdown select element double clicking issue
- Fixed basic/advanced mode switching with Microsoft Edge browser
- Fixed firmware upgrading bug when LAN interface with a changed name exists
- Fixed redirecting to the 'Interfaces' page when mode is changed from basic to advanced and user is in the 'LAN' or 'WAN' pages
- Fixed validation of custom header in 'Data To Server' page
- Fixed "Type" option error in Failover page
- Updated username and password validations
- Fixed profile change action in 'I/O Juggler'
- Fixed bidirectional GPIO change feature

## [RUTX\\_R\\_00.02.03.4](#) | 2020.06.15

- **Fixes**

- LED fixes
- Fixed config generation script

## [RUTX\\_R\\_00.02.03.1](#) | 2020.05.15

- **New features**

- Responsive WebUI design
- New Access Control window for managing IP access
- Attack Prevention page under Firewall settings
- New IPv6 options in WAN, LAN and VPN pages
- Hotspot Users Management page
- Progressive Web Application support and extra page caching when device is configured with a valid SSL certificate
- OpenVPN configuration file upload functionality
- Unsaved Changes page
- Bridge mode display in Overview page
- Input inversion buttons
- Dynamic switch port display in side widget
- Bluetooth data to server for RUTX devices that support Bluetooth
- WiFi traffic logging for RUTX devices that support WiFi
- Input/Output manipulator
- MQTT Publisher: added support to send I/O values
- Bluetooth: "ELA" sensors frame format support
- Bluetooth: available and paired devices pagination, ability to pair/unpair multiple devices at the same time
- Ability to install packages stored in backup file
- New Modbus TCP Slave register fields
- New Modbus Alarm redundancy options
- NTPD version 4.2.8p14

- **Improvements**

- Added HMAC configurations for OpenVPN
- Added AES ciphers support for OpenVPN
- Added DHCP lease range display in the Network → LAN page
- New Hotspot user signup page design and field validation
- Hotspot validation for local user authentication
- Moved wireless device configuration
- Added warning messages when deleting interfaces/configurations
- Added available FW on server status messages in FW upgrade page
- Changed UPnP redirect delete button style
- Changed functionality of reset button in the Firewall → Custom Rules page. Now fully resets to default
- Added hints on all value fields about field validation
- Removed modem traps if no modem is present
- Updated wireless information in side widget
- Optimized section toggling logic, removing all toggling associated flags required prior optimization
- Standardized section edit page headers in WebUI Services
- Improved the look of error pages and messages

- Updated Wiki links to [wiki.teltonika-networks.com](http://wiki.teltonika-networks.com)
- Disabled 'Clear data limit' button for inactive interfaces
- Reordered menu, moved 'Default configuration' to the Backup page, moved 'Diagnostics' to the Troubleshoot page
- Added credentials input fields to Data to Server
- Changed hint of 'Allow guest' in the Network Shares page
- Updated Periodic Reboot service status in the Services page
- Improved hint for incoming calls option
- Changed OpenVPN LZO option to a dropdown with an extra 'none' option
- Removed 'MAC auth' option from Hotspot with LAN interface
- Removed unnecessary 'Status' column and added "No users currently connected" message in the Hotspot Users Management page
- Added suggestion to create a profile if there are no profiles created in the Profiles → Scheduler page
- Filtered out unnecessary interfaces ending with \_4\_6 in firewall page
- Moved SIM switch to separate page and added check interval and retry count options
- Changed side widget button color to blue to make it more visible
- Added 'Dynamic List' option limit (20 elements)
- Improved stm32 recv message handling
- Modbus TCP test now allows reading more than 125 coils/inputs
- Reworked NTP page, separating general options from NTP specific ones

#### • Fixes

- Added validations for Wireless configuration advanced settings fields
- Added name validation in the Firewall → Port Forward page, fixed custom protocol value selection and display
- Added validation for GRE 'Remote subnet IP' option
- Fixed Schedulers' cells to be of equal width
- Fixed uploading backup from lower firmware version
- Fixed SSTP certificate upload function
- Fixed IPsec 'Aggressive' setting value saving in config file
- Fixed LAN settings static lease name validation
- Fixed descriptions in Access Control → Security page
- Fixed HTTP login while HTTPS session is still active
- Removed Bluetooth device from available devices section if it is in paired devices section
- Fixed real time CPU load in the Overview page
- Fixed multiusers correct group creation when upgrading from 2.00.2 FW to 2.01.1 FW with the 'Keep all settings' option
- Fixed advanced static routing display for all routes
- Fixed file upload error messages in backup page
- Fixed 'Select' option for Firefox browser
- Fixed RAM usage display in side widget
- Fixed access to non existing pages
- Fixed saving empty message field in Events Reporting rules
- Fixed I/O socket pinout
- Fixed Events Reporting send test email page display when email contains 2 new lines in a row
- Fixed LAN Overview section display
- Fixed early login page load after reboot or backup upload
- Fixed Package Manager notification displays
- Fixed PPTP and L2TP client configuration creation with same name

- Fixed static route removal if corresponding interface is removed
- Fixed Realtime Graphs → Traffic tab display
- Fixed OpenVPN username and password writing to file
- Fixed time zone sync between Setup Wizard & NTP pages
- Fixed WiFi interfaces table style when no interfaces are present
- Fixed DHCP lease range validation
- No longer write anything into Events Log when forcing reboot to prevent device hang-up
- Fixed restore settings when upgrading from Yocto base firmware on TRB1 targets
- Fixed launching stm32 autoflash script at early boot to avoid possible keep settings loss
- Removed certain Events Reporting options on devices that don't have the corresponding functionality
- Fixed recovery from lost connection for MQTT publisher, Modbus MQTT gateway
- Resolved using SHA512 bug for versions 02.01 or lower with additional (-b) parameter

## **RUTX\_R\_00.02.01.1 | 2020.01.15**

- New features:
  - Email to SMS
  - Static IP lease
  - SMS OTP and MAC auth in Hotspot
  - Hotspot logs
  - TOS in HotSpot
  - Custom URL parameters while using external landing page in Hotspot
  - Expiration time for Hotspot
  - Wireless status page
  - USB mount settings
  - Site blocking list from file
  - Events Reporting via Email
  - STunnel
  - Multi-User support
  - Mobile page
  - Operators control
  - Bluetooth passive device scanning
  - Hotspot 2.0
  - Modbus MQTT gateway
  - Package manager
  - RUT FOTA
  - TR-069
- Improvements:
  - Deleted OpenVPN forward rule on instance deletion
  - Improved "SMS Forwarding to Email" field validations
  - Rename IPsec fields from right/left to remote/local
  - Bluetooth style improvements
  - Applied same style on all scheduler templates
  - Renamed "Setup Wizard" steps
  - Renamed "IPv4 and IPv6 routes" headings
  - Renamed "User groups" to "Users & Recipients"
  - Added "Clear data limit" on a specific date
  - Enable/Disable all SMS-Utilities rules at once
- Fixes:

- Fixed WAN mobile interfaces reload
- Fixed parsing interface IP address in WAN
- Fixed OSPF "Hello Interval" field hint
- Fixed field validation on "Port Forward" create form
- Fixed display build date
- Removed "Bring up on boot" option
- Fixed Mobile page with additional USB modem
- Fixed creating SNAT rule without port
- Fixed SDK archive name

## **RUTX\_R\_00.02.00.2 | 2019.10.11**

- Fixes:
  - WiFi fix

## **RUTX\_R\_00.02.00.1 | 2019.09.27**

- New features:
  - Auto APN
  - MQTT
  - Web Filter
  - Dynamic Routes
  - GRE over IPsec
  - Wireless Hotspot
  - VRRP
  - HTTP POST/GET
  - Network Shares
  - VLAN multiple tags functionality
  - SMS HTTP POST/GET
  - SMS Forwarding
  - Auto Reply
  - SMS storage
  - Switch back to primary SIM
  - Email groups
  - Default VPN firewall zones
  - Support for XT25F128B spi-nor memory
  - Support for Bluetooth
- Improvements:
  - Updated Kernel to version 4.14.131
  - Updated Strongswan to version 5.8.0
  - Updated curl to version 7.60.0.4 (fixes CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890)
  - Updated mosquito to version 1.5.8
  - Updated dnsmasq to version 2.80
  - Updated iptables to version 1.6.2
  - Updated openssl to version 1.0.2s
  - Updated zlib to version 1.2.11
  - Updated hostapd to the 2018-05-21 version (fixes CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, CVE-2019-11555)
  - Updated fstools to the 2019-03-28 version
  - Updated procd to the 2018-03-28 version

- Updated rpcd to the 2018-11-28 version
- Updated ubox to the 2018-02-14 version
- Updated ubus to the 2018-10-06 version
- Updated uci to the 2019-05-17 version
- Updated Firewall to the 2018-08-13 version
- Updated netifd to the 2019-01-31 version
- Updated uhttpd to the 2018-11-28 version
- Switched to mac80211 WiFi driver
- Updated IPsec page
- Updated DMVPN page
- Updated Overview configuration page
- Fixes:
  - Fixed operator name parsing
  - Fixed serial reading
  - Fixed SIM card PIN code setting
  - Fixed I/O event handling
  - Fixed backup save after device restart
  - GPS init script fixes
  - IPsec page rework
  - Failover/Load Balancing mobile interface fixes
  - L2TP/PPTP/SSTP configuration fixes
  - TX power save setting fixes
  - Refactored profiles functionality
  - Added write to config option in Call Utilities
  - Wireless config migration fix
  - Firmware checksum fix

## **RUTX\_R\_00.01.06 | 2019.07.24**

- New features:
  - Added Wake on LAN feature
  - Added SSTP VPN support
  - Added mobile bridge feature
  - Added Status → Network page
  - Added SIM Switch feature
  - Added SMS Limit feature
  - Added save and restore SIM PIN code from flash
  - Added feature to monitor switch port events
  - Added Events Reporting send to RMS functionality
  - Added FOTA support for RUTX08, RUTX10, RUTX11
  - Added Modbus TCP master function
- Improvements
  - Added microcontroller version information
  - Updated Wireless page design and WiFi widget in overview page
  - Updated Overview widget style
  - Updated stm32 firmware
  - Updated LED logic
  - Changed check for new FW logic
  - WebUI style updates



- Fixes:
  - Fixed multiwan function. Changed firewall traffic control to routing rules control
  - NTP time zone display fix
  - LED functionality fix
  - Changed time function used for rollback timestamps
  - Login form updated and other fixes
  - Fixed firmware update checksum mismatch
  - lua error on map when GPS is disabled fix
  - Firmware update percentage and check box fix
  - LAN interface creation with short names fix
  - WAN state and IP print fixes
  - OpenVPN new port save in firewall rule fix
  - RUT FOTA bug fixes

## **RUTX\_R\_00.01.04.5 | 2019.06.14**

- Improvements:
  - Revert settings logic updated
- Fix:
  - Firmware update checksum mismatch fix
  - DHCP dnsmasq fix
  - Wireless improvements and bug fixes
  - Increased RMS HTTP Proxy resource limit

## **RUTX\_R\_00.01.04.1 | 2019.05.17**

- New features:
  - Add initial wireless support
  - Added SNMP support
  - Added Advanced Routing functionality
  - Added L2TP VPN
  - Added PPTP VPN
- Improvements:
  - Added signal strength logging and reporting to Events Log
  - Added authentic firmware check
  - OpenSSL updated to version 1.0.2r
- Fixes:
  - Wireless improvements and bug fixes
  - Fixed IPSec Phase 1 and Phase 2 keys lifetime not saving bug
  - Input Output improvements and bug fixes
  - Fixed router values sent from SMS utilities
  - WebUI style fixes
  - Fixed RMS proxy multiform submits

## **RUTX\_R\_00.01.03 | 2019.04.25**

- New features:
  - Adapted WebUI for RUTX08
  - Added DMVPN support
  - Added HTTP support

- Added SMS message input field validation and counter
- Added UPnP support
- Added GRE Tunnel support
- Implemented dynamic routing with BGP, OSPF, RIP, EIGRP and NHRP protocols
- Added manual network band lock support
- Added Events Log
- Added Events Reporting
- Improvements
  - Updated OpenVPN client count to 20
  - WebUI style updates
- Fixes:
  - Profile scheduler fixes
  - Mobile service crash fix
  - Ping Reboot IP field validation fix
  - LED functionality related fixes

## **RUTX\_R\_00.01.02 | 2019.03.19**

- New features:
  - Added configuration profiles
  - Updated WebUI style
  - Added Reboot button
- Improvements:
  - curl updated to version 7.64.0
  - openssl updated to version 1.0.2q
  - dropbear updated to version 2018.76
  - busybox updated to version 1.28.3
  - ustream-ssl updated to latest version
  - OpenVPN updated to version 2.4.6
  - OpenVPN-Easy-RSA updated to version 3.0.4
  - ubus updated to version 2018-10-06
  - uhttpd updated to version 2018-11-28
  - NTP updated to version 4.2.8p12
- Fixes:
  - Root CA validation and page style fixes
  - Hardware compatibility check fix
  - DDNS force IP renew fix
  - Site Blocking enable column fix
  - Don't show rules in Load Balancing mode when in failover page fix

## **RUTX\_R\_00.01.01 | 2019.02.05**

- New features:
  - Initial firmware release