Template:Networking rut2xx firmware change log

☐

Contents

RUT2_R_00.07.04.2 | 2023.04.18

- **New**
    - nftables support

- **Improvement**
    - **Network**
        - Added PDP profile registry and LTE SMS format functions & management for the Verizon network
        - Improved SIM detection algorithm
        - Improved Multi-APN connection establishment time
    - **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 IPv4, IPv6 mobile connection restarts
- Fixed operator scanning when mobile interface is disabled
- Fixed data limit and tracking when software flow offloading is enabled
- Added network reload call before bringing the mobile interface up
- Fixed Port-based VLAN ID calculation issue
- Fixed PDP context authentication when using special characters
- **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 wrong timezone returned issue in Operator Station Synchronization & Timezone Synchronization
    - Fixed MODBUS TCP Slave memory leak issue when requesting mobile parameters
    - 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
    - Fixed an issue with mobile metric setting migration from legacy FWs to RUTOS
    - Removed ability for non root users to edit scripts that get executed as root

[RUT2_R_00.07.04.1](#) | 2023.03.24

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

[RUT2_R_00.07.04](#) | 2023.03.07

- **Improvements**
    - **WebUI**
        - Improved data persistence between page refreshes
        - Improved page navigation behavior
        - Improved redirect logic to open configuration edit modals
        - Updated the 'Status -> Mobile' page
        - Updated interface card in the Overview page
        - Separated Sent and Received data bars on the chart in the Mobile Usage page
    - **Network**
        - Added an info message displayed when a faulty SIM card is inserted
        - Added ResIOT operator's APNs to the APN database
        - Improved mobile connection re-establishment after reboot
        - Improved mobile connection recovery in cases where it was lost unexpectedly
        - Improved 'Deny data roaming' operation when switching between operators
        - 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 an error message when trying to send an SMS from the 'Send Messages' page with no SIM card inserted
- Changed the behavior of setting the 'Write to config' flag in the 'mobileoff' SMS rule
- Added argument support for the 'Execute custom script' SMS rule
- 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
    - **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
        - Updated DFOTA notification to show "More info" only when the update is forced

- **Fix**
    - **WebUI**
        - Fixed MAC address showing on mobile interfaces
        - Fixed mobile cell ID displaying in hexadecimal
        - Fixed mobile data limit card creation in the Overview page
        - Fixed modem widget disappearing from the Overview page
        - Fixed Services page not displaying data after Thingworx package is installed
    - **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 call function when VoLTE is disabled
        - Fixed VoLTE control when IMS is not enabled
        - Fixed mobile IPv6 IP checking when the device didn't get a correct IP address
        - Fixed APN authentication when using empty credentials
        - Fixed manual APN selection from list
        - Fixed disabled WiFi interface after factory reset

- Fixed WiFi interface creation with SAE mixed encryption
  - **Services**
    - 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
    - Added limitations on message size and quantity of email messages in Email to SMS
    - Fixed SMTP HELLO value parsing issue
    - Fixed SMS message window reset button
    - Fixed not being able to save empty 'Message text' field in Auto Reply
    - Fixed multi-part SMS concatenation
    - Fixed multi-part SMS processing
    - Fixed SMS error message on 'Mobile Data Reset' action
    - 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
- Fixed LED animation during firmware upgrade
- Fixed settings migration issue that caused unreachable Internet after upgrade from a legacy FW version
- Fixed an issue with OpenVPN TAP configuration migration from legacy FWs
- 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 LED indications when PDP type is IPv6
- Fixed issues with PDP type and SMS limit period migration via keep settings

[RUT2_R_00.07.03.4](#) | 2023.02.09

- **Fix**
  - **Network**
    - Changed generic modem restart method
    - Fixed mobile page VoLTE switching issues
  - **Services**
    - Sanitized tcpdump storage location
  - **System**
    - Fixed legacy backup upload
    - Fixed upgrade from legacy FW issue with keep settings

[RUT2_R_00.07.03.3](#) | 2023.01.25

- **Fix**
  - **Network**
    - Fixed disabled WiFi interface after factory reset

[RUT2_R_00.07.03.2](#) | 2023.01.13

- **New**
  - **System**
    - Japanese language

- **Improvements**
  - **Network**
    - Optimized mobile netifd script installation

- **Fix**
  - **Network**
    - Shortened modem hang monitor timeout
    - Fixed VLAN option setting when changing VLAN ID

[RUT2_R_00.07.03.1](#) | 2023.01.03

- **Improvements**
  - **System**
    - Remove front-end certificate validation
  - **Network**

- - - Optimized mobile netifd script installation
- **Fix**
  - **Network**
    - Fixed modem communication validation
    - Fixed connection establishment in IPv6 only mode
  - **Services**
    - Fixed libxml2 vulnerability CVE-2022-40303
    - Fixed an IPsec Phase one & two setting migration issue
    - Fixed OpenVPN migration from legacy firmwares
    - Fixed not being able to create or edit PPTP instances after upgrading from legacy firmware
  - **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

[RUT2_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 option to select subnet parameters in mobile Passthrough/Bridge modes

- Added WhereverSIM operator APN and fr.lebara.mobi APN to APN database
- Added mobile connection state for IPv6
- Added individual WiFi toggle support
- Added error message when DFS channel is selected during scanning

- **Services**
  - 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
  - Added execute custom script SMS Utilities rule
  - Added receiver and transceiver mode support to SMPP
  - Added timezone synchronization with GSM operator option to NTP Client
  - 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 nd 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

- **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 an indication to the Interfaces page that displays when data limit is enabled
    - 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 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 mdcollect memory leak issue
    - Fixed data limit not resetting properly
    - Fixed incorrect mobile data usage calculations for multiple day periods
    - Fixed an Auto APN 'Keep settings' issue
    - Fixed data counting after mobile data limit has been reached
    - Fixed mobile band not setting correctly on first try
    - Fixed incorrect data limit conditions causing unwanted SIM switches
    - Fixed Passthrough DHCP lease time setting
    - Fixed mobile bridge mode issue when no DNS servers are supplied
    - Added new Operator Lists instance name validations
    - 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
    - Added wget tracking method to WAN Failover
    - Added interface checks to remove inaccurate Failover events from the Event Log
    - Fixed Wired WAN connectivity issue when Failover interfaces are disabled
    - Fixed Failover fallback issue
  - **Services**
    - Fixed GRE, MQTT broker, IP alias, MAC filter & Failover migration from legacy firmwares
    - 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 I/O Juggler SMS text message Save & Apply issue
    - 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 UCI SMS Rule return message to display new changes
- Fixed DNP3 issues when asking for modem temperature
- Fixed base64 encoding of SMS messages when forwarding to HTTP
- Fixed SMS sending issues when using multiple APN
- Added Gateway modem option to IP Block and WoL in SMS Rule edit
- Fixed unblocking IP addresses with an SMS message
- Fixed Mobile Utilities page not load properly on some occasions
- 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
- **System**
  - 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

[RUT2_R_00.07.02.7](#) | 2022.09.12

- **Improvements:**
  - Improved manual-auto connection mode

- **Fixes**
  - Fixed AT command for SMS storage usage
  - 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

[RUT2_R_00.07.02.6](#) | 2022.08.24

- **Improvements:**
  - Added 'home.vodafone.de' APN
  - Improved stability of device information storage

- **Fixes:**
    - Added SMSC type omitting when empty SMSC number parsed in SMS PDU mode
    - Fixed Serial-symlink dmesg messages
    - Fixed OpenVPN tls-auth and tls-crypt option names

RUT2_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
    - Increased custom APN Username & Password field maximum length to 64 symbols
    - Added auto switch to modem's SMS storage when SIM card storage doesn't exist
    - Improved mobile connection status handling
    - Added CSP headers Hotspot WebUI landing page

- Fixes:
    - 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 proccess 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 MAC and leasetime setting for Bridge & Passthrough modes
    - Fixed modal tabs navigation when editing wireless interface with non-english languages

RUT2_R_00.07.02.4 | 2022.07.20

- Improvements:
    - Added default password change warning message before firmware downgrade
    - Extended time period for device to make connection to operator
    - Reduced the number of modem reboots when changing mobile settings
    - Reduced excessive log output when no SIM card is inserted
    - Added modem restart prevention on modem init
    - Added disable RPLMN option in the SIM section of the SIM card config

- Fixes:
    - Fixed CVE-2022-2068 vulnerability
    - Disabled autoconnect on stop-network call
    - Fixed Hotspot login via landing page issue

RUT2_R_00.07.02.2 | 2022.06.27

- Improvements:
    - Added ping to DNS IPv6 support
    - Added modem reset to default state after device FW upgrade
    - Modem init now checks NVRAM sensitive commands before setting
    - GSM output was made consistent
    - Updated FSTools package to version 2022-05-03
    - Added security headers to web requests

- Fixes:
    - Fixed CVE-2019-12900 libbz2 vulnerability
    - Fixed behavior of some gsmctl commands
    - 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 band locking issue
    - Fixed race condition for wireless configuration initialization
    - Fixed operator control issue

[RUT2_R_00.07.02.1](#) | 2022.06.06

- Improvements:
    - Improved GSM related messages in Troubleshoot logs

- Fixes:
    - Fixed IGMP Proxy menu item not appearing after package installation
    - Fixed default mobile network configuration generation
    - Fixed MODBUS write requests and Mobile Utils option setting

[RUT2_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
    - 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 mobile bytes sent and bytes received SNMP OIDs
- Added mobile LED turn off feature ('System -> Administration' page)
- Added 'iot.1nce.net', 'internet', 'VZWINTERNET' and Truphone APNs to APN database
- Updated mobile usage data point calculation logic
- Added the possibility to manually enter operator number
- Improved obtain mobile cell ID process
- Added modem restart if SIM card is removed during APN database fetching process
- Added unauthorized call logging
- Added space character support in SMS commands
- Disabled SMS modem storage configuration form when SIM is not inserted
- Changed SMS '%wi' parameter value to return IP address of any currently used WAN interface (not only wired)
- Added external modem SMS limit Overview card and widget
- Made in-use APNs visible next to mobile interface configurations (before clicking the 'Edit' button)
- Added duplicate value check for list configuration options
- Changed mobile card instance design
- Fixed 'Mobile Data usage reset' SMS rule
- Fixed the default state parameter of SMS list POST/GET command
- 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 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 mobile IPv6 display in Events Reporting status messages
- Fixed Bridge mode when DNS2 is not available
- Fixed PAP/CHAP username and password fields not saving in interface edit window
- Fixed sending email without secure connection for providers that support such an option
- Fixed 'N/A' parameter showing up in SMS Utilities monitoring status message
- Fixed Call Utilities Events Log message for reboot rule
- Fixed SMS command validation for no-authorization option
- Fixed MODBUS SMS alarms 'Enable' option saving
- Fixed running RMS with no SIM card inserted issue
- Fixed firmware available on server version checking issue
- Fixed CVE-2020-15078 openvpn vulnerability
- Fixed storage calculation for packages
- SMS Utilities: enhanced service security
- Fixed firmware deletion after leaving the page
- Fixed setup wizard redirect after LAN IP change
- Fixed various validation bugs, typos, option hints & alignments
- Fixed multiple IPv6 configuration field validations
- Fixed PDP logging for Verizon operator
- 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 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 APN migration if APN was selected from APN list on legacy firmware
- Fixed RIP configuration migration from legacy firmware versions

- Fixed Wireguard interface status setting migration from legacy firmware versions
- Fixed default config options for SSH and Web access SMS Utilities rules

[RUT2_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
    - Removed invalid network interface selections from the "Network" dropdown in the Wireless interface configuration page
    - Changed the logic of uploading files to the modem
    - Fixed second mobile interface creation issue
    - 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
    - Fixed connection to whitelist carriers
    - Fixed Passthrough mode when DHCP is disabled
    - Fixed 'Deny data roaming' feature
    - Fixed mobile blocking dependency on region
    - Disabled Ping To DNS functionality when Bridge/Passthrough mode is enabled

[RUT2_R_00.07.01.2](#) | 2022.01.04

- **New features**
    - DFOTA modem upgrade system for Quectel modems

- **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
    - Fixed mobile data limit display after profile change
    - Fixed Bridge mode without multi-APN
    - Fixed multi mobile interface checking
    - Fixed error handling when the modem is not responding
    - Prolonged autoconnect setting timeout

RUT2_R_00.07.01 | 2021.11.18

Note: Firmware version RUT2_R_00.07.01 released on 2021.11.18 was removed due to an issue with IPsec tunnel while using mobile connection.

- **New features**
  - RUTOS WebUI