

M!DGE3 - Release Notes

Release 2.3.6.0

2026-05-11

- Main component versions:
 - CNF version: 33
 - Web client version: 1.80.0
- Important Warning:
 - Step-by-step upgrade required: When upgrading the firmware (FW) from a version older than 2.2.6.0, the unit must first be upgraded to version 2.2.6.0 or 2.2.9.0, and only then to version 2.3.4.0 (or higher).
- New features:
 - Interfaces:
 - 5G Connectivity Support: Integrated the Telit FN990A28-HP cellular module, enabling worldwide certified 5G support on Midge3 units. The list of supported bands is available in the datasheet and the user manual
 - Security:
 - SSH Security Hardening: Strengthened SSH server (dropbear) security by disabling selected algorithms to address CVE-2025-14282.
 - Enhanced Connection Limiting: Improved system resilience by reducing the maximum number of unauthenticated SSH connections per IP (from 5 to 3) and total concurrent connections (from 30 to 10). The authentication timeout has also been reduced from 300 s to 10 s.
 - Scripting Logstorm Protection: Implemented a protective mechanism against system log flooding from user scripts. This ensures that one aggressive script cannot inadvertently block or impact the performance of other scripts.
 - MQTT SSL/TLS Security: Implemented support for SSL/TLS encryption to ensure secure MQTT communication.
 - Credential Auto-fill Prevention: Disabled browser auto-filling for credential configuration fields to enhance security and prevent accidental data overwrites during configuration.
 - Web interface:
 - Advanced Menu Enhancements: Expanded the Advanced menu with new event types for improved system tracking and diagnostics.
 - Firmware Module Visibility: The Status section on the *Settings > Device > Firmware > Upload* screen has been expanded to include a list of all available firmware modules.
 - Expanded Event Logging: Added several missing event types to the *Settings > Device > Events* screen, including *Going to Sleep*, *Modem internal fault*, and *Extension module firmware installed*.
- Fixed bugs:
 - Advanced NetConf Validation: Enforced advanced unit configuration validation even when configuration changes are performed via the NetConf interface.
 - Scripting Configuration UI: Fixed Advanced menu items related to Scripting configuration to ensure consistency.
 - Scripting Table Integrity: Resolved an issue where scripts could insert incomplete table rows into the configuration. All new rows are now required to be complete (all columns present), preventing potential display errors in the web UI.
 - Web interface:
 - Firmware Activation Feedback: Fixed and improved user feedback mechanisms when a firmware activation error occurs.
 - Unrecoverable Error Display: Corrected the error handling logic to ensure the proper error page is displayed in the event of an unrecoverable system error.

- Remote FW Activation: Resolved the issue preventing successful firmware activation when connected via a Remote connection.
- Known issues:
 - Cellular Statistics History Reset: Due to the expansion of cellular module statistics (supporting the new 5G module for Midge3), existing statistical history tables for cellular interfaces will be cleared during the firmware upgrade.
Workaround: None.
 - MQTT Licensing Requirement: The MQTT gateway and protocol are operational only if a **MASTER** software key is installed on the device. Even if a valid MQTT-specific key is present, the functionality will remain inactive or in an error state without the MASTER key.
Workaround: Ensure that a valid MASTER software key is installed to enable MQTT functionality.

Release 2.3.4.0

2026-03-05

- Main component versions:
 - CNF version: 32
 - Web client version: 1.79.0
- Important Warning:
 - Step-by-step upgrade required: When upgrading the firmware (FW) from a version older than 2.2.6.0, the unit must first be upgraded to version 2.2.6.0 or 2.2.9.0, and only then to version 2.3.4.0 (or higher).
- New features:
 - System
 - Cellular module Firmware upgrade: Enhanced the system's firmware update capabilities to include support for upgrading embedded cellular modules directly via the standard web interface.
 - Integrated Python Scripting: Introduced a native Python-based scripting engine (previously referred to as SDK) for custom logic execution. The unit provides a comprehensive API, allowing scripts full access to all internal device functions and parameters.
 - FQDN support for key Services: Selected configuration parameters now support entering target addresses as FQDNs in addition to standard IP addresses (applicable for OpenVPN, NTP, and ICMP ping).
 - MQTT Broker & Bridge support: Added native MQTT broker support with MQTT bridge configuration capability for seamless data forwarding between multiple nodes and integration into higher-level IoT systems.
 - Web interface
 - Enhanced menu navigation: Refined the main menu appearance for better orientation, now supporting up to 4 levels of hierarchy.
 - Improved Sleep mode configuration: Key Sleep mode settings have been moved to *Settings > Device > Unit > Sleep mode* for easier access (previously available only in the Advanced screen).
 - UI Refinements: Various fixes for component labels, layouts, and element states (enabled/disabled).
- Fixed bugs:
 - Service interface connectivity: Fixed an issue where NETCONF was unavailable via the service interface.
 - SIM Profile switching: Resolved an issue where a physically damaged SIM card could prevent the system from switching to a functional SIM profile.
 - ETH5 consistency checks: Fixed a bug that caused "minor" error messages to be displayed during configuration consistency checks when the ETH5 interface was active.
 - Remote FW Activation reporting: Fixed an issue where the web client incorrectly reported an application error during remote FW activation from older versions.

- RS485 Performance: Optimized and accelerated the Rx/Tx switching timing on the RS485 interface.
- Serial Protocol Stability: Adjusted the Buffer Flush Timeout behavior for all serial protocols on the COM port to resolve non-standard protocol states and improve reliability.
- Known issues:
 - Scripting configuration via NetConf: Providing an incomplete table row via the NetConf API (e.g., missing mandatory parameters) causes a display error in the web client UI.
Workaround: When configuring Scripting via the NetConf API, all list items must be specified (e.g., for a script instance, you must include `name`, `arguments` and `note`).
 - Remote FW Activation via Remote Access: FW activation cannot be performed through the Remote Access service when upgrading from version 2.2.9.0 or older.
Workaround: To perform the activation, use a direct IP connection to the remote station or call the corresponding API function (e.g., via a Python script).

Release 2.2.9.0

2025-11-07

- Main component versions:
 - CNF version: 29
 - Web client version: 1.75.1
- New features:
 - Ethernet phytter drivers updated

Release 2.2.6.0

2025-10-14

- Main component versions:
 - CNF version: 29
 - Web client version: 1.75.1
- Warning:
 - When upgrading the firmware (FW) from a version older than 2.2.0.0, the unit must first be upgraded to version 2.2.4.0 and only then to 2.2.6.0 (or higher).
After upgrading to version 2.2.4.0, an invalid configuration may be detected - the situation described in the Release 2.2.0.0, section Known issues will occur.
If an invalid configuration is detected during the upgrade to version 2.2.6.0 (stricter validation), this upgrade is rejected - see the section Fixed bugs.
- New features:
 - Interfaces
 - New Cellular module (Telit ME310G1-WW) supporting LTE Cat M1/NB1/NB2 Worldwide certified is now available.
 - For more universal use of the unit (e.g. for Internet access), the Network interface, VLAN and Wi-Fi configuration has been expanded to include the option to set the MTU.
 - System
 - NetConf API can now be enabled/disabled and redirected to another TCP port
 - Security
 - Security components are updated
 - When downloading a firmware package from www.racom.eu, a checksum (SHA-256 algorithm) of this package is now available, allowing you to check the integrity of the downloaded file.
 - Routing
 - The Babel protocol is now equipped with two configurable filters to improve the stability of the dynamic protocol in narrowband networks. The first filter allows you to prevent the import and

- retransmission of poisoned rules. The second filter allows you to prevent the import and retransmission of rules with a user-configurable highest permissible metric.
- Diagnostics
 - New menu Diagnostics > Information > Device > System services - now provides information about the status of system services
 - To facilitate diagnostics and increase security, it is now possible to enable firewall rule logging
- Web interface
 - Configuration items will display the Default value of the given item after clicking the item name with the mouse. If the item has been modified (orange colour = prepared in Changes), its Current value in the device is also displayed.
 - The InfoArea component used to list Status information now allows line wrapping. This way, the user can adapt the Status report to the current display size.
 - New window Diagnostics > Information > Device > System services - now provides information about the status of system services
 - Refresh button now reloads all configuration data from the connected unit. This is now equivalent to logging out and logging back into the unit.
 - The order of configuration items in the Configuration changes dialog is now stable. The previous version listed the order of items partially randomly in certain cases.
 - Modal dialogs can now be closed by pressing the Escape key or by clicking outside the area of the window
 - The Wi-Fi configuration screen has been expanded to include the option to enter the Hide SSID parameter
- Fixed bugs:
 - Fixed the malfunction of generic configuration validation for some data types. Validation was incorrect in firmwares 2.2.2.0, 2.2.3.0 and 2.2.4.0
 - The configuration validation now takes place as part of uploading new firmware. In case of invalid configuration, the new firmware version will be rejected. The new firmware can be installed after correcting the invalid configuration items. This prevents a unit with an invalid configuration from going to a safe factory setting after upgrading to a new firmware.
 - “Boot configuration error” event is deprecated (it can no longer be raised)
 - Re-reading the SIM card in case of incorrect reading. Solves the problem where under certain circumstances the cellular module got disconnected from the network and it was not possible to reconnect it until the entire station was rebooted or unit configuration has changed.
 - NTP service updated (Crash when bringing up net interface fails - fixed; NTP messages are not sent with preferred source address - fixed)
 - Increased request size limit from the web client to 128 MB. When the limit is exceeded, the user is notified with an error message.
 - Fix instability under high Ethernet load
 - TCP time stamp is disabled to prevent obtaining the uptime value
 - Event log: Fixed the display of the configuration settings of the given event at the moment of its occurrence. Only events that are relevant to the given HW and SW configuration of the unit are now displayed.
 - Fixed APN name validation for Cellular interface to prevent entering illegal characters
 - Fixed setting of default values of the monitoring configuration - previous version caused a website error
 - When creating a local Certification Authority, it is now mandatory to fill in the Location attribute
 - Web interface
 - Web command timeouts for Tamper Reset and Station Reboot have been extended to 100 s
 - By normal manipulation with the web client, it was possible to achieve a state where the user configured a Local station thinking that he was configuring a Remote station. Now fixed
 - After activating the firmware via Remote access, the connection to the Remote station will now be maintained

- Fixed: Diagnostics > Monitoring: "Unexpected error" may occur when calling the "Reset monitoring to defaults" function.
- In the event of a partial failure to update data on the Status page (consisting of several requests), the value of the Status data Last refresh timestamp is set to "Undeterminable"
- The historical data download button now correctly indicates the completion of the download not only for all tables, but also for an individual table
- StringSelectType component is fixed to load credentials properly and display loader while loading credentials.

Release 2.2.4.0

2025-05-30

- Main component versions:
 - CNF version: 28
 - Web client version: 1.74.2
- New features:
 - Security
 - When logging into the unit for the first time (or after Restore factory settings or Total purge), the user is prompted to enter a username for the admin role and a unique user password. All units from this firmware version onwards do not contain a default username and default user password at all.
 - The default security setting for entering a new password has been increased to support entering stronger passwords
 - Firewall L3 Input and Output have been expanded to include the ability to configure Source and Destination addresses; Output to include the definition of output interfaces; Input, Output and Forward to include the ability to specify a Policy filter (for better interaction with IPsec)
 - Expanded IPsec Traffic selector settings to include the ability to choose a method for creating automatic rules against traffic leakage (possibility of interaction with Policy filters on the Firewall)
 - IPsec has been extended with Transport mode
 - Firmware downgrade is now not allowed by default
 - Interfaces
 - New Cellular module supporting LTE Cat M1/NB1/NB2 (ANATEL certified, incl. bands 410 and 450 MHz) is now available
 - Wi-Fi interface now allows configuration with a hidden SSID
 - Wi-Fi interface now allows use of ACS functionality
 - Diagnostics
 - The "Test event" default settings was updated not to trigger all possible actions
 - Web interface
 - Searching in the Advanced menu now allows you to enter a search term from the browser address bar (can be used, for example, to create a web link for a specific search)
 - Russian translations have been removed from the user interface
 - Added new keyboard shortcuts for faster menu navigation (Diagnostic overview)
 - Event log now displays the configuration settings of the given event at the moment of its occurrence
 - The "Test event" configuration has been expanded to include the option to trigger the Alarm output
- Fixed bugs:
 - GRE L3 did not allow setting the Tunnel mask /31
 - Fix: For the /31 and /32 masks, special IP addresses (the first and last address of the range) are not checked and these addresses can be used.
 - Correction of the ICPM ping call result list

- Fixed PPPoE: when the link is active, the assigned client IP address was not visible in the Settings > Interfaces > PPPoE > Status menu
- The response to the ICMP timestamp request is now blocked because this type of request is reported as a possible vulnerability
- Enhanced checking of Wi-Fi parameter configuration according to the parameters of the selected region. In the previous version, it was possible to configure parameters that were not allowed in the given region
- Fixed the indication of the VPN status LED, which in some cases (after changing the tunnel configuration) did not match with the actual tunnel status
- Fixed the Wi-Fi interface Mask configuration check, which incorrectly accepted the value /0
- Fixed the SSID name validation where the apostrophe character should not be allowed
- Fixed the non-functional indication of successful completion of firmware activation if it was executed via Remote access
- Fixed the alignment of buttons in the Diagnostics > Monitoring menu
- User names can now contain all Unicode characters
- Known issues:
 - Diagnostics > Monitoring: "Unexpected error" may occur when calling the "Reset monitoring to defaults" function.
Workaround: Click "Acknowledge and Reload" button to clear the error message and load the Monitoring menu.

Release 2.2.2.0

2025-02-28

- Main component versions:
 - CNF version: 26
 - Web client version: 1.73.0
- New features:
 - System
 - The Event log entry now also includes the current settings of some configuration items (SNMP, AO, DO1, DO2, SMS, HS)
 - Security
 - Added the option to check firmware and configuration integrity (SETTINGS > Device > Configuration > Configuration checksum; SETTINGS > Device > Firmware > Firmware local > Firmware checksum)
 - Keys that are no longer supported by current browsers (ED25519, ED448, EC P-224, EC P-521) have been removed from the web certificate generator in the station
 - Diagnostics
 - Monitoring of ICMP frames is supplemented with a list of ICMP codes
 - For diagnostic purposes, a Test event has been added that can be triggered manually (SETTINGS > Device > Events)
 - List of ARP tables of neighbors (DIAGNOSTICS > Information > Interfaces > Ethernet > Neighbours)
 - Serial protocol
 - PPP protocol and PPPoE client now support configuration of Idle timeout (ADVANCED > Generic > com_X_protocol > Protocol_PPP > Idle timeout to reconnect [s]; Advanced > Generic > PppoeClient > Idle timeout to reconnect [s])
 - PPP dial up connection - solving missing DNAT in Narrow band LTE module

**Note**

To be able to initiate communication from the Center to the Remote when using a Narrowband LTE module (Extension module mPCIe-M or mPCIe-O), it is necessary to use FW version 2.2.2.0 or higher.

- Web interface
 - Status panel now shows relative time since last Refresh
 - In cases where "password" did not refer to user login, the parameter name was changed to "passphrase"
- Fixed bugs:
 - Fixed the propagation of configuration changes from the web client to the NETCONF interface
 - Fixed unnecessary restarts of the Cellular service when booting the unit and using SIM1
 - Implemented checking of unauthorized IP addresses: The lowest address according to the given mask is not allowed on any interface. The highest address according to the given mask is not allowed on interfaces with broadcast enabled.(LAN, VLAN, radio, GRE L3, OpenVPN L3, PPP, WiFi AP)
 - Fixed the Event export format included in the Diagnostic Package to comply with RFC 4180 (fixed incorrect interpretation of the separator character ',' in some cases)
 - Improved the stability of Cellular service startup after FW upgrade
- Known issues:
 - GRE L3 does not allow setting the Tunnel mask /31. If the unit configuration contains this setting - do not perform FW upgrade.
Workaround: Change the Tunnel mask to a value wider than /31 before the FW upgrade.

Release 2.2.1.0

2024-11-29

- Main component versions:
 - CNF version: 25
 - Web client version: 1.72.0
- New features:
 - System
 - Wi-Fi Extension module supporting Wi-Fi Access point operation is now available
 - Security
 - Configuration backup files and User accounts can now be downloaded and uploaded encrypted
 - Remote access can now be enabled/disabled for the whole unit or for the individual interfaces
 - Diagnostics
 - Cellular interface service can now run in debug mode to support advanced diagnostics
 - Web interface
 - Security > Credentials modal dialogues improved
 - Diagnostics > Overview information can now be downloaded
 - Security > Policy screen implemented as a single point of File download and upload protection configuration
 - Diagnostic tools can now be started using Enter key
- Fixed bugs:
 - Diagnostic package was extended by some missing logs
 - IPsec tunnel VPN LED indication fixed
- Known issues:
 - After installing FW version 2.2.0.0 and higher, a full configuration validation is now performed each time the unit is booted. After installing this newer FW version, when the station is started for the

first time, a situation may occur that the saved configuration does not pass full validation (this situation can occur if the configuration was updated in a way other than using the web interface). Even in this case, **the unit starts correctly** and works as it did before installing the new FW version. An invalid configuration is indicated to the user by the system event "Boot configuration contains errors" (SYS LED indicates Alarm). The notification area contains an error message with a detailed description of the configuration items that did not pass validation. These invalid entries must be manually corrected (changed to a value that passes validation). It is only possible to change the configuration of the unit (save the new configuration) when all invalid entries have been corrected.

- PPPoE: when the link is active, the assigned client IP address is not visible in the Settings > Interfaces > PPPoE > Status menu.

Workaround: The client address can be found in the Diagnostics > Information > Interfaces > Ethernet > Network Interfaces menu.

Release 2.2.0.0

2024-08-30

- Main component versions:
 - CNF version: 24
 - Web client version: 1.70.0
- New features:
 - System
 - New NETCONF API supporting reading and modifying the Device > Configuration. This configuration data is defined by the YANG model.
 - Security
 - Unit configuration is fully validated. Validation is triggered at unit start-up and at any configuration change during operation.



Note

Until now, the configuration was fully verified only in the web interface. If the configuration was updated in another way, the current configuration may not be valid. In this case follow the instructions below in the Known Issues section to ensure a smooth FW upgrade.

- For compatibility reasons, the OpenVPN tunnel now allows the use of legacy SHA1 ciphers.
- Serial protocol
 - IEC 101 supports RTU reset
 - PPP protocol supports TETRA terminal connection.
- Routing
 - DHCP server implemented. Up to 16 instances of DHCP servers can run simultaneously on different interfaces. The server can also assign static IP addresses.
 - DNS forwarding service implemented. DNSSEC is supported.
 - Link manager is extended by the possibility of switching back-up routes to PPP and PPPoE.
 - PPP protocol supports Masquerade.
- Diagnostics
 - VPN status LED now indicates OpenVPN and IPsec status.
- Fixed bugs:
 - Fixed occasional incorrect ICMP ping termination
 - Correction of Cellular connection registration if the cellular network supports only 4G technology
 - The PPP protocol now allows you to use an empty username and password.
 - Web interface
 - Firmware activation when using Remote access may result in an error - fixed.

- Unification of system log names (tools/logs)
- Known issues:
 - After installing FW version 2.2.0.0 and higher, a full configuration validation is now performed each time the unit is booted. After installing this newer FW version, when the station is started for the first time, a situation may occur that the saved configuration does not pass full validation (this situation can occur if the configuration was updated in a way other than using the web interface). Even in this case, **the unit starts correctly** and works as it did before installing the new FW version. An invalid configuration is indicated to the user by the system event "Boot configuration contains errors" (SYS LED indicates Alarm). The notification area contains an error message with a detailed description of the configuration items that did not pass validation. These invalid entries must be manually corrected (changed to a value that passes validation). It is only possible to change the configuration of the unit (save the new configuration) when all invalid entries have been corrected.

Release 2.1.7.0

2024-06-07

- Main component versions:
 - CNF version: 23
 - Web client version: 1.69.0
- New features:
 - Security
 - IPsec is extended with modern AEAD ciphers providing encryption and integrity checking in one algorithm
 - IPsec is extended with the possibility of using a PPK key
 - Security components are updated (Dropbear, NTP, NetSnpmp)
 - Routing
 - The Babel protocol is extended with the ability to filter routing rules (Relay filter) in order to reduce the amount of Babel protocol overhead data transmitted over the radio channel.
 - Diagnostics
 - Improved Remote access error message in case of remote station not reachable
 - The web interface now provides the possibility of directly viewing the system logs of individual services
 - System
 - M!DGE3e support
 - Web interface
 - The GRE tunnel configuration is extended by the Tunnel Name
 - The console dump filtering setting on the Diagnostics > Tools page is now disabled when the command is running. The purpose is to ensure consistency between the filter settings and the listing currently in progress.
 - Implementation of new corporate graphics - logos and icons
 - Implementation of a new screen for PPPoE client settings: Settings > Interfaces > PPPoE client
- Fixed bugs:
 - Advanced Network interface name checking has been added, which will ensure checking the maximum length of the interface name even in the case of VLAN configuration
 - Configuration of Flow control (RTS/CTS) on the COM port is now disabled if the COM port is switched to RS485 mode
 - Fixed incorrect display of TCP header values in monitoring
 - Fixed FTP connection not working when using NAT
 - Web interface
 - Improved error message when remote device is unavailable
 - Modifying the names of some IPsec parameters

- Known issues:
 - Firmware activation when using Remote access may result in an error. The firmware is correctly activated, but the user is not correctly informed about it.
Workaround: Reload the web page

Release 2.1.6.0

2024-03-13

- Main component versions:
 - CNF version: 22
 - Web client version: 1.68.0
- New features:
 - Security
 - Added a config item to prevent FW downgrade
 - OpenVPN is extended by the possibility of authentication using user name and password
 - L2 Firewall has been expanded with Forward rules, which now enables full filtering of L2 forwarded traffic
 - Serial protocols
 - IEC 101 now supports spontaneous mode
 - System
 - The time in the RTC is periodically synchronized with the system time to increase the accuracy of the time stored in the RTC
 - Interfaces
 - PPPoE client is now available
 - Web interface
 - The L2 Firewall screen is redesigned: renaming Blacklist and Whitelist to Blocklist and Allowlist, adding a new Forward table.
 - New "Device incompatible" error screen in case the web client is not compatible with the unit
 - Highlighting the Status field on configuration screens
 - Credentials configuration expanded to include Certificate Subject Alternate Names (SAN) settings
 - The password input component has been expanded to include the option to copy to the clipboard and the option to hide/show the password
 - If the unit is unavailable at the same IP address after activating the new FW, an error message is displayed with information about the IP address change
- Fixed bugs:
 - Fixed false occurrence of "USB overcurrent" event when booting the unit.
 - Cellular
 - Fixed incorrect generation of "Cellular MAIN down" SMS notification
 - Fix rewriting of APN profiles from cellular network
 - Status screen: fix "Primary link down" event link to point to Link management Status
 - Fixed creating a trusted CA in the unit
 - DNAT rule for the EXT interface cannot be created – fixed
 - Fixed incorrect SNMP functionality when using a space in the "Security user name" parameter (used in SNMP v3).
 - Web interface
 - Fixed a bug when disconnecting from a remote device with older firmware
 - Fixed OpenVPN tunnel nested table configuration duplication feature
 - Fixed showing preferred cellular service in card view when using LPWAN on Settings > Interface > Cellular page
 - Fixed validation of Note item in Credentials configuration

Release 2.1.2.0

2023-12-15

- Main component versions:
 - CNF version: 21
 - Web client version: 1.66.0
- Warning:
- Due to the implementation of Security certificates storage, the “Credentials lost” event is triggered and SYS LED shines red (to indicate serious system alarm) when upgrading from FW version older than 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 or newer FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
 - Security
 - Any Special characters can now be used in IPsec passphrase
 - Several configuration parameters (Severity, SNMP and SMS notification, Threshold field for all Events) are updated to require higher level (security technician level) of access rights
 - New Settings > Security > Management access menu combining settings of Webserver, Remote access and Service USB
 - Serial protocols
 - IEC 101 extension providing time synchronization
 - Interfaces
 - New Cellular module supporting LTE Cat M1/NB1/NB2 (Global bands, incl. 450 MHz) is now available
 - Diagnostics
 - Most Status info panels are revised to provide more information
 - Web interface
 - Settings > QoS card-view is extended to show “Flow rate” units
 - Settings > Device > Software keys screen is extended to provide basic System information
 - Settings > Security > Credentials > Sign CSR > Choose File selection dialog now provides filtering by file extension
 - Settings > VPN > OpenVPN tunnel configuration can now be easily duplicated to create a new tunnel
- Fixed bugs:
 - OpenVPN Server status uses incorrect column labels - fixed
 - BGP – MD5 password length limit is now properly set to 80 characters
 - Fixed overflow of long filenames in some places in the web interface
 - Fix required credential type on Settings > Security > Management access > Remote access page
 - Security > Credentials download/upload buttons are hidden when using remote connection
 - Remote access dialog improved to wrap IP addresses correctly
 - Settings > Security > Credentials > Credentials Note is wrapped correctly to prevent text overflow
 - Fixed size of TLS protection shared key ID field on Settings > VPN > OpenVPN page
- Known issues:
 - DNAT rule for the EXT interface can not be created
Workaround: Select PPP protocol for any COM port.

Release 2.1.1.0

2023-10-31

- Main component versions:
 - CNF version: 20
 - Web client version: 1.65.0
- Warning:
- Due to the implementation of Security certificates storage, the “Credentials lost” event is triggered and SYS LED shines red (to indicate serious system alarm) when upgrading from FW version older than 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 or newer FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
 - Security
 - OpenVPN server and client are implemented. Every unit can act both as a server and/or client.
 - OpenVPN server related Events are implemented: OpenVPN client connected, OpenVPN client disconnected
 - OpenVPN client related Events are implemented: OpenVPN tunnel 1 down ... OpenVPN tunnel 4 down
 - When generating a new key for the web interface, only keys supported by current web browsers (RSA or OC) are allowed. The key fingerprints for the website and the keys from the certificate for the website are checked to check if they belong to each other.
 - The labels on the credentials screen have been improved to better match the described functionality.
 - The IPsec configuration overview has been extended with a “Note” field and “Management mode” field was removed to improve screen readability.
 - Entering passphrases is unified across the web client.
 - Firmware
 - Settings > Device > Firmware > USB screen is now available to configure USB flash drive firmware upgrade option.
 - Interfaces
 - Default MTU for cellular interface was changed to 1500 bytes.
 - SNMP
 - Settings > Services > SNMP > Status info section is now available.
 - The complete Engine ID value is now displayed in the SNMP Status.
 - MIB description fields updated to use “Username” and “User” labels correctly
 - The System uptime information is now available.
 - Diagnostics
 - Syslog can now be used to log all unit Events. Syslog enables logging to a remote server. Settings > Services > Syslog screen provides Status info and configuration options.
Note: A full copy of all events replaces the previous function copying only user login and logout events. The “Login attempt” parameter is removed. It is fully replaced by “Web interface login” and “Web interface login rejected” events.
 - New “Routing” and “COM” sections were added to the Status screen.
 - Status info section design was improved: Auto refresh provides more compact design; Download button offers the option of downloading the content of the status to a file.
 - System
 - Linux kernel updated to LTS version 6.1.38
- Fixed bugs:
 - PPP protocol does not work properly after a configuration change when flow control is active – fixed
 - Monitoring parameter “Include reverse” for COM and TS interfaces does not work – fixed
 - Remote access key configuration items are not properly translated – fixed
 - Different formatting of MAC addresses in Zabbix and MIB Browser – fixed

- The lowest possible value Cellular interface MTU was updated to work correctly for the Cinterion TX62W module
- Fixed diagnostic package generation to not include warning in case of GNSS module disabled
- When a new SW key is uploaded, the web interface does not display new available features correctly – fixed
- The "Sign CSR" button was incorrectly placed on the individual certificate tab. It is now moved correctly to the global context of the Credentials screen.
- Settings > Firewall > L3 and NAT screens were rearranged to be uniform with the rest of the web client.
- Diagnostics > Tools – Start and Run buttons are enabled also if there is valid data in the web store.
- Known issues:
 - OpenVPN Server status uses incorrect column labels. "Client address" and "Client port" should be used instead of "Server address" and "Server port".
 - In case of replacing the Remote access key with a different one the configuration update results in error message "Compatibility error ...". This is not a proper error message. The error is caused by the fact there is a different authentication key on both units at the moment of updating the authentication key on a remote unit and still having the old one on a local unit.
Workaround – Replace the Remote access key also on a local unit with a new one. Remote access should work correctly again using the new authentication keys.
 - Direct firmware upgrade from version 2.0.18.0 or older is possible in one of two ways
 - Upgrade firmware to version 2.1.0.0 prior to upgrading to 2.1.1.0 or newer
 - Use special upgrade package including the FWD abbreviation in its name. See the Firmware archive for download options.

Release 2.1.0.0

2023-07-28

- Main component versions:
 - CNF version: 19
 - Web client version: 1.62.0
- Warning:
 - Due to the implementation of Security certificates storage, the "Credentials lost" event is triggered and SYS LED shines red (to indicate serious system alarm) after the first FW upgrade to version 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
 - Firmware
 - Firmware package security against unauthorized modifications is improved by adding asymmetric encryption
 - Firmware can be upgraded using USB Flash drive
 - Interfaces
 - Serial ports COM1 and COM2 configuration was extended by the possibility to define 5 and 6 stop bits (in addition to the current 7 and 8 stop bits).
 - Routing
 - Link Management implemented – adding a simple way to implement backup routes and to backup IPsec tunnels.
 - Diagnostics
 - Default severity of several events was increased to get a better default unit status overview on the Status screen

- Security
 - Security credentials (keys and certificates) subsystem including safe credentials storage was implemented: Various types of security credentials can be generated providing also Upload, Download and Update option. Whole Security credential storage Download, Replace and Update option.
 - Various types of security credentials can be used in unit configuration: IPsec tunnels, Remote access authentication, Firmware distribution authentication, Web pages traffic encryption.
- Fixed bugs:
 - Serial port COM1 has a possibility to configure DSR/DTR signals despite that HW does not provide those signals – fixed.
 - PPP protocol reconfiguration stops proper protocol operation occasionally – fixed.
 - COM ports 2 and 3 disablers were fixed
 - GNSS detection in various system configuration fixed
 - Time zone “America/Port” parameters fixed
 - Logging to a remote Syslog server fixed
- Known issues:
 - Remote access key configuration items are not properly translated yet. The missing translation is:
 - UsAcc_RmtAccessClientKeySource ... “Source of Remote access client key”
 - UsAccRmtA_ClientPrivKeyId ... “Client private key ID”
 - In case of replacing the Remote access key with a different one the configuration update results in error message “Compatibility error ...”. This is not a proper error message. The error is caused by the fact there is a different authentication key on both units at the moment of updating the authentication key on a remote unit and still having the old one on a local unit.
Workaround – Replace the Remote access key also on a local unit with a new one. Remote access should work correctly again using the new authentication keys.
 - In case of replacing the Web server authentication certificate, the private key has to be generated using “RSA” or “EC” algorithms. Current web browsers do not support new “ED25519” and “ED448” algorithms. Validation of this configuration item is missing.
Workaround – use only “RSA” or “EC” algorithms when generating a new Web server private key.
 - When a new SW key is uploaded, the web interface does not display new available features correctly.
Workaround – logout and login again after SW key installation.
 - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings > Routing > Babel > Network > Interfaces* cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
Workaround - Use *Advanced > Routing > Babel > Interfaces > Babel interface passwords* configuration page for this initial update.

Release 2.0.18.0

2023-05-12

- Main component versions:
 - CNF version: 18
 - Web client version: 1.61.0
- New features:
 - SNMP
 - Several configuration items are now available (Enable/Disable status of: ETHx, COMx, TSx, Service USB, IPsec, GRE, QoS, FW, NAT, BGP, OSPF, BABEL, Cellular, Monitoring; ETHx link speed), read-only.
 - HW dependent configuration items are returned as “no such instance” in case they are queried

- Time stamp items data type “Counter32” changed to “Unsigned32”
- Serial protocols
 - PPP protocol implemented
- Security
 - SSH server updated to version 2022.83
- Fixed bugs:
 - SNMP
 - “System boot completed” notification is now generated properly
 - Sleep mode “Waking period” is now measured properly
- Known issues:
 - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings > Routing > Babel > Network > Interfaces* cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
Workaround - Use *Advanced > Routing > Babel > Interfaces > Babel interface passwords* configuration page for this initial update.
 - PPP protocol reconfiguration stops proper protocol operation occasionally.
Workaround – Restart the unit or make any serial protocol configuration change (causing serial protocol restart).
 - Serial port COM1 has a possibility to configure DSR/DTR signals despite that HW does not provide those signals.
Workaround – do not configure DSR/DTR on COM1.

Release 2.0.16.0

2023-02-24

- Main component versions:
 - CNF version: 17
 - Web client version: 1.59.2
- New features:
 - System
 - GNSS implemented – time synchronization, position
 - Sleep mode – wake on Sleep input implemented
 - Interfaces
 - Network interface (Ethernet bridge) can be configured without any Ethernet port attached
 - Diagnostics
 - NTP status extended
- Fixed bugs:
 - Cellular interface
 - Cellular interface naming in Statistics fixed
 - Monitoring
 - Ethernet interface monitoring did not work correctly in case only one direction (Tx or Rx) was enabled. Fixed: it is now possible to monitor either both directions or one direction only.

Release 2.0.14.0

2022-12-16

- Main component versions:
 - CNF version: 16
 - Web client version: 1.58.0

- New features:
 - System
 - Sleep low power mode implemented
 - Sleep mode related event implemented
 - OTH-W3-WIFI adapter driver implemented
 - Several Events were updated to provide a possibility of sending SNMP and SMS notification
 - Routing
 - Routing option to set Metric for each routing rule implemented
 - Babel – Network neighbor authentication implemented
 - IPsec – List of active IPsec associations and Traffic selectors in the Status field now provides better formatting
 - IPsec – Traffic selectors filtering rules are now extended by IP protocol option
 - Interfaces – Cellular interface
 - Default MTU changed to 1430 Bytes
 - Cellular connection down event implemented
 - Security
 - Security subsystem updated (StrongSwan)
 - Firewall
 - L3 Firewall Input – Block list implemented
 - Diagnostics
 - Monitoring output enriched by translation of several EtherTypes
 - List of *Diagnostics > Information > SMS* messages is now sorted to show newest records first
 - Firmware upgrade screen now provides more information about installed FW and version of FW in archive in order to find out which update files can be used for the unit FW upgrade
 - Web interface
 - Input field component size was optimized
 - All input fields are now validated on blur (after the input is completed)
 - *Diagnostics > Event* page Severity filter groups were updated
 - Monitoring File output is refreshed automatically
 - Notifications from Remote device are now identified by the Remote unit's name and/or address
 - User interface is redirected to Status page after successful firmware upgrade
 - Notification messages are sorted in descendent order in order to provide newest messages on top of the previous
 - *Diagnostics > Information > Static tab* renamed to *System* to better reflect its content
 - All dialog and modal windows updated to a new version of modal component
 - Activating firmware over Remote access is now supported. Firmware file to a Remote unit needs to be transferred using Firmware distribution service
 - New menu *Settings > Services*
 - SNMP and SMS configurations moved here
 - Timeout of all requests from web interface to a unit is now 120 seconds
- Fixed bugs:
 - Serial interface
 - SAIA S-BUS: The first answer was not transmitted if operating in a SavePlus mode – fixed
 - Monitoring
 - Known issue “Monitoring of the IPsec encrypted packets on the Cellular interface does not work correctly” – fixed
 - Monitoring activated on disabled ETH port led to recovery mode – fixed
 - Web interface
 - Various layout and disable field fixes (Attach to network interface, ETH ports)
 - Update of Web inactivity timeout parameter fixed
 - *Diagnostics > Tools > ICMP ping* Source address does not offer WWAN interface address as it was not correct in all circumstances

- Status info fields extra refresh suppressed
- Sharing configuration files between RipEX2 and M!DGE3 minor fixes
- Return to *Settings > Firewall > SNAT* and *DNAT* screens from Notification area – fixed
- Web inactivity timeout calculation improved
- System
 - Unit RTC update is now blocked when Tamper is active
 - Known issue “Disabling HTTP protocol together with Ethernet configuration changes can lead to unit recovery restart” – fixed

Release 2.0.13.0

2022-09-13

- Available functionality:
 - COM2, COM3 expansion board
 - Cellular interface
 - World wide LTE module
 - Link testing
 - Profile switching
 - SMS - notification, statistics, status read
 - Ethernet ports: Disable; speed control
 - VPN tunnels:
 - IPsec
 - GRE L2 and L3
 - Static routing
 - BGP, OSPF and Babel dynamic routing protocols
 - Firewall: L3 (Input, Forward, Output) and L2 (Blacklist, Whitelist)
 - Source NAT (NAPT), Destination NAT (NAPT)
 - QoS
 - COM port protocols:
 - Async Link, COMLI, DNP3, DF1, IEC101, Mars-A, Modbus RTU, PR2000, RDS, Siemens 3964R, SAIA S-BUS, UNI, Transparent
 - Terminal server protocols:
 - Async Link, COMLI, DNP3, DF1, IEC101, Mars-A, Modbus RTU, Modbus TCP, PR2000, RDS, Siemens 3964R, SAIA S-BUS, UNI, Transparent
 - Real-time Monitoring of all interfaces
 - SNMPv3: Event log notifications; Following groups available to read: “System Group” MIB-II available, Event log; All statistics data;
 - Syslog incl. logging to a remote server
 - Time synchronization - NTP Server and Client
 - User interface - Additional Advanced generic menu for all implemented configuration features;
 - Diagnostic information:
 - Statistic counters for all interfaces
 - Detailed Event log with filtering options
 - Export option of all Statistics data and Event log to an external csv file
 - Historical statistics - ‘any’ required time interval
 - Differential statistics - short term interval
 - Status information available for the following modules: NTP; System information; Ethernet interfaces; Cellular interface; Static routing; IPsec; Supply voltage; Temperature measurement; NAT; Firewall L2, L3;
 - Auto refresh option for all Status fields
 - Status screen providing overview of Major and Critical events in last 7 days

- Status screen providing realtime information about system status
- Ethernet link down events
- Cellular interface - signal strength
- Unit HW values (temperatures, voltage) monitored, events triggered when threshold is reached, Hot standby switch over possibility on such an event
- Configurable Diagnostic package
- Diagnostic tools
 - ICMP ping available via web interface
 - Monitoring saved to a file; Monitoring direct record to a file
 - RSS ping diagnostic tool
 - Routing diagnostic provides next hop interface for the given IP address
- Unit service tasks
 - Factory settings - from web interface or by pressing HW button
 - Unit reboot - from web interface or by pressing HW button
 - Default configuration and Total purge available
- Remote access (fast remote configuration)
 - Indicated by a specific web browser tab icon (favicon)
 - Old firmware version (in the Remote unit) warning message
- Multiple user accounts
- Password complexity; Password lockout
- RADIUS authentication and authorization
- Service access via the USB port: USB/WiFi and USB/ETH adapters available; service address and DHCP range configurable
- Service access protocols (HTTP, SSH) can be disabled; Service access protocols (HTTP, HTTPS, SSH) default UDP port numbers can be changed
- Web interface localizations: English; Russian
- Web interface improvements (unsorted)
 - Notification center
 - Remote access with reconnect option
 - All the time displays (including monitoring) and inputs are now localized according to a configured Time zone
 - Help screen for configuration windows and Diagnostics - Statistics
 - Title bar indicates menu position and active Remote access connection
 - Automatic logout is performed when the “Web inactivity timeout” expires
 - Compressed communication to limit amount of transferred data
 - Firmware update can be done using smaller firmware patches (over an older installed FW version)