M!DGE3 - Release Notes

Release 2.1.6.0

2023-03-13

- 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 username 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)
    - *Diagnostic* > *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)