# M!DGE2 Release Notes
## Firmware version 4.4.40.xxx

## Release 4.4.40.107, patch 1495
## 2021-02-26

### *New Functionalities*

**Higher M!DGE2 performance (HW Rev B02)**
The maximum CPU clock is increased from 600 MHz to 1 GHz, improving performance and throughput in several applications. CPU clock is adaptive (lower at high temperature and for low performance applications).

**SNMP improvements**
The SNMP EngineID is now configurable.

**GUI improvements & Toby module firmware update**
A warning will alert the user if a WWAN module is running a firmware version which is known to be outdated and should be replaced with a newer one.
Up-to-date Toby module FW is on our website in M!DGE2 download section. Run the module FW upgrade from the menu “System – Modem Firmware Update” and choose “WWAN” module. Upload the FW to the unit. Upgrade can also be performed remotely via cellular network with several minutes’ connection drop. If you prefer, do the update via CLI.

**Additional status information on Toby-L2 LTE module**
The signal to noise ratio of the LTE connection is made available via CLI, SDK, SNMP and web interface.

### *Security Fixes*

**libmodbus security bug fix**
CVE-2019-14463: out-of-bounds read fixed
CVE-2019-14462: out-of-bounds read fixed

**OpenSSL security bug fix**
CVE-2020-1971: Fixed NULL pointer deref in OpenSSL

**Security enhancement**
M!DGE2 web interface has been enhanced to be more robust against various XSS attacks. M!DGE2’s bash CLI has also been hardened.

### *Fixes*

**Switching between WWAN interfaces using two different SIM cards and one Toby module**
Switching between SIM1 and SIM2 profiles (within one Toby LTE module) was not possible in FWs 4.4.40.104 and 4.4.40.105. This was fixed.

**Password change did not apply on SNMP users**
In some situations, the SNMP user password was not applied with a change of the user’s system password. This was fixed.

**/bin/login spamming logs**
On some devices it could happen that a failing call of /bin/login spammed the logs if no serial interfaces were configured as login console.

**SMS with a special "@" character**
No character in SMS after the 1st occurrence of "@" sign was sent. This was fixed.

**RS232 Login Console**
It was not possible to use the primary RS232 interface as Login console. This was fixed.

**GUI improvements**
New table layout for Firewall menu. Clear button was deleted.
Configurations with several IPsec tunnels which were configured with expert-mode could lead to wrong tunnel status shown in the web interface.
GRE tunnel keys were treated like passwords in the web interface and shown as asterisks. This was wrong, because GRE tunnel key is not a secret, but only an identifier.
Changing the shell of a user was not applied unless the user's current password was provided and changed at the same time. This was fixed. Now changing the shell of a user only requires the admin password for confirmation, but no user password or changed user password.
The bridging status page was not accessible to non-admin users.
The maximum file size for WWAN firmware-update files was increased to 45 MB. This should be sufficient to perform most FW updates directly via web interface without the need for an external web or FTP server.
Setting the MTU of a bridge device BR1 or BR2 failed with an error message. This was fixed.
The MTU was not applied correctly to soft bridge devices.

**Enable fast NTP synchronization after boot**
Due to a misconfiguration, the NTP client took up to 10 minutes to synchronize after the boot. This was fixed.

**L2TP tunnels cannot be bridged**
It was not possible to bridge L2TP tunnels to soft bridges BR1 and BR2. This was fixed.

**GUI: WPA-Enterprise Identity**
Setting the RADIUS identity had no impact to the configuration. The identity was always set to the hostname of the Router. This has been fixed.

**Local services not accessible with IPsec**
In some scenarios with multiple IPsec connections, it could happen that local services like the web interfaces were not available via IPsec. This was fixed.

**Unstable IPsec connection**
In some use cases with several parallel connections, IPsec was quite unstable due to timing issues on tunnel establishment. This was fixed.

**SMS not working with shared modem configuration**
SMS were not sent if the first WWAN interface was down even if the configuration was that the first available module should be used.

**Link management**
A bug in the dial-in behaviour on link-groups that resulted in preventing a switchover from happening was fixed.

**Mail transmission failures fixed**
Some MTA servers did not process mails with attachments from our SDK. This was due to a duplicate line in the mail header which is strictly not allowed in SMTP protocol. The duplicate line was removed.

**SNMP: missing MIB**
The HOST-RESOURCE-MIB was unsupported by the Router. This has been fixed.

**Reboot triggered by igmpproxy supervision**
The system health supervision failed on some igmpproxy setups resulting in a device reboot.

## *Known Issues*

**Protocol server restrictions**
The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

- Only one Protocol server can be configured even in units with more RS232 interfaces. Use the Device server or SDK for 2nd serial interface functionality.
- If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to local M!DGE2' 1st LAN IP address). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

**"3G/4G only" preferred service-type**
This cellular connection option also allows 2G/Edge connection.

**Too large techsupport files**
It is not possible to download correctly too large techsupport file. Sizes up to 50 MB are recommended.

**IPsec & XAUTH**
IPsec cannot be configured with XAUTH option.

**Redundancy/VRRP**
It is not possible to enable Redundancy/VRRP.

**Discovery services other than LLDP**
It is only possible to configure LLDP discovery protocol, others are not configurable.

**Manual LAI**
Manual LAI configuration is available, but not working correctly.

**WAN with STP/RSTP enabled**
It is not possible to enable STP/RSTP while at least one LAN is set as WAN – the WAN is flapping all the time due to internal timing.

# Release 4.4.40.105, patch 1447
# 2020-10-22

## *New Functionalities*

**Port based DHCP addresses**
M!DGE2 supports port based DHCP address specification now.

**Certificate revocation list download for IPsec**
The IPsec daemon now tries to obtain the CRL file if a CRL location is defined in the installed certificate chain.

## *Security Fixes*

**Linux kernel security bug fixes**
CVE-2020-8428: A use-after-free in the Linux kernel could allow local users to run a DoS.
CVE-2020-10732: Uninitialized buffer might leak kernel data to user space on core dumps. The mainline bug fix was back-ported to the 4.4.40.x firmware.
CVE-2020-12114: Possible denial of service by corrupted mountpoint reference counter. The mainline bug fix was back-ported to the 4.4.40.x firmware.

**Curl security bug fixes**
CVE-2019-5482: A malicious TFTP server could cause a heap corruption in libcurl.
Libcurl can be tricked to prepend a part of the password to the host name before it resolves it, potentially leaking the partial password over the network and to the DNS server(s).
CVE-2019-5436: Possible TFTP receive buffer overflow fixed.
CVE-2019-5435: libcurl contains two integer overflows which if triggered can lead to a too small buffer allocation and a subsequent heap buffer overflow.

## *Fixes*

**Firewall rule blocked IPsec traffic from router**
In setups where all traffic but IPsec is blocked it could happen that packets from the router were unintentionally blocked as well, even though they were supposed to be sent via IPsec. This was due to a missing firewall rule that was present for forwarded traffic, but was missing in the outgoing chain.

**GUI improvements**
The web interface did not allow to disable Dead Pear Detection (DPD). This was fixed.
Due to a flaw in the GUI design it could happen that firewall rules could not be edited or deleted via web interface. This was fixed.
The web interface enforced the first WWAN interface to be permanent. This restriction was not needed and therefore removed.

**M!DGE2 services cannot be accessed via IPsec**
An issue with packet fragmentation prevented to access services (like web interface or SSH access) via IPsec. Routed data traffic was not affected. This issue was fixed. If you relied on this malicious behaviour as a feature, you should get in contact with our support to find a valid firewall configuration.

**Multicast packets, GOOSE, Profinet data not forwarded on M!DGE2**
Starting with FW release 4.3.40.100 multicast IP packets were not forwarded on switched Ethernet ports of M!DGE2. This was fixed.

**No default route on WWAN with custom APN**
There was a customer setup with a private APN where we failed to establish the default route over WWAN. The issue was fixed. Working APN setups are not affected by the fix.

**CLI improvements**
The CLI status did not show SWI information for the second PDP context.

**SCEP enrolment did not work with Windows PKI**
Certificates provided by a Windows PKI were not installed correctly. This has been fixed.

**Certificate chains from SCEP server**
Certificate chains installed via SCEP did not work with IPsec.

**IPsec tunnel, wrong IP Source address**
In a specific situation with multiple WANs and dynamic routing, it could happen that M!DGE2 could try to establish an IPsec tunnel with a wrong source IP address (from a wrong WAN interface). This was fixed.

**BGP, IPsec default parameters**
Most of default parameters were changed to match the default values in RipEX2 radio.

**AT commands failure**
In some rare situations, internal AT commands could be handled wrongly. This was fixed by a new Toby module firmware 16.19. Contact our support team for a download link.

**STP is disabled by default**
STP could cause some troubles if not configured correctly within the network. STP was disabled by default, but it is possible to configure it and use it on LAN interfaces.

**Telnet is disabled by default**
Telnet is disabled by default. SSH is suggested to be used.

## *Known Issues*

**Protocol server restrictions**
The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

- Only one Protocol server can be configured even in units with more RS232 interfaces
- If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to local M!DGE2' 1st LAN IP address). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

**Switching between WWAN interfaces using two different SIM cards and one Toby module**
Switching between SIM1 and SIM2 profiles (within one Toby LTE module) is not possible in FWs 4.4.40.104 and 4.4.40.105. For such functionality, please use FW 4.4.40.101.

# Release 4.4.40.104, patch 1416
# 2020-05-14

## *New Functionalities*

**IPsec improvements**
IPsec tunnels can be enabled and disabled individually now.

**Prevent down-grade to incompatible version**
If you want to downgrade to an older release, you may have to install intermediate releases. Normally that's the latest release of the major version of the desired software. The Update process will detect the release number of the uploaded image and prevent installation of invalid releases.

**IPsec**
The number of configurable IPsec tunnels was increased to 10.

**GUI improvements**
It is now possible to configure whether status messages should appear on the web interface login page.
The system log level settings can now be changed more convenient in the web interface.
It is now possible to import IPsec expert mode files with encrypted keys via the web interface.
Routers with Toby-L2 LTE modules now show LTE band information on the WWAN status page.

**SDK improvements**
M!DGE2 can now be set to a low power sleep mode from SDK.

**STP and RSTP**
STP and RSTP is now supported.

**Improved user access rights**
The user access management was improved. It is now possible to grant native shell access to additional admin users or to disable shell access for a user.

**Additional GRE tunnel parameters**
It is now possible to configure tunnel keys for GRE to allow a gateway to distinguish between GRE packages from different connected end devices.

**Additional BGP settings**
The BGP setup allows to configure additional parameters for time-out, hold-time and weight.

**Maximum number of static DHCP hosts increased**
It is now possible to configure up to 70 static DHCP host entries.

**Asymmetric routing is available**
Asymmetric routing is when a packet takes one path to the destination and takes another path when returning to the source. These data were dropped by M!DGE2 firewall. It could cause temporary issues if RipEX Backup paths were configured in the network. It can be controlled now via CLI. The required parameter is "*firewall.invalid_ip*".

## *Security Fixes*

**Security fixes in 3rd party and open source packages**
CVE-2018-15599: *dropbear* contained a user enumeration vulnerability
CVE-2020-8597: *pppd* remote code execution in EAP code

## *Fixes*

**ublox Toby-L2 SMS handling**
While receiving big SMS messages, the evaluation of the SMS message index could lead to wrong results.

**IPsec tunnel configuration failed**
It could happen that IPsec was not correctly activated after installing a user-configuration file. This could happen with special configuration settings. If IPsec came up after applying a configuration (most scenarios), then you were not affected.

**GUI improvements**
The required RSSI value for mobile interfaces was set to 100 dBm automatically without customer interaction.
NTP Server did not allow to set up access from world (0.0.0.0/0).
IPsec network configuration allows to configure overlapping networks for local and remote side now.
File format of tcpdump debug traces from the web interface was improved.
It could happen that a software update failed with a generic error message if the software image download failed. Now, in such cases, the web interface will show a more helpful error message.
It was not possible to configure a firewall rule with dedicated incoming and outgoing interface.
The web interface returned an error if some special characters like quotes were used inside an email password.
Disabled radio buttons where not shown as disabled. Nevertheless, it was not possible to change their values.
Logs from SDK scripts did not wrap with the page width of the web interface.

**ublox Toby-L2 $I^2S$ communication**
The $I^2S$ communication could fail while using a ublox Toby-L2 module.

**Toby-L2 initial registration**
While using a Toby-L2 module, the initial registration could fail when no 2G connection was available.

**Authentication in SMS control SDK script**
The SMS control SDK script which is enabled by default in every M!DGE2 unit did not accept the ‘admin’ password until un-storing and storing its password was done. For all already configured M!DGE2 units, a factory-reset must be applied for the functionality to be fully operational or that unstore/store procedure.

**Software downgrade via USB stick failed**
In factory state, the downgrade to Releases prior 4.2.40.x failed.

**SDK improvements**
The function *nb_syslog()* did not clean an internal buffer correctly which could lead to corrupted log messages.
Due to an erase condition, mails sent from the SDK on a high rate could get lost before they were sent.

**Possible LTE connection loss**
Devices with Toby-L2 LTE modules faced sporadic connection losses. In some cases, the connection could not be re-established until reboot. This was fixed.

**Bring up several LTE connections with switch-over links**
Switch-over links should come up if their permanent master link disconnects. This did not work correctly if there were several permanent WWAN links with switch-over configured.

**Configuration via USB stick could fail**
Due to a time-out issue, it could happen that consecutive configuration steps via USB stick failed. This would only affect you if you use one USB stick with some base configuration and then apply another configuration with a USB stick on top without rebooting between these steps. You can apply consecutive configurations via USB stick one after the other now.

**IPsec improvements**
In some situations, it was not possible to reach the configuration web interface of a local router because traffic was erroneously routed via the IPsec tunnel. This was fixed.

**Link supervision timeout prevents switch to better link**
If link supervision was enabled, the link management did not change to a better link before the supervision timeout was reached. Even if the link was obviously down. This was changed so that a better link would be taken into account directly once being sure the old one was lost.

**Low LTE throughput**
Due to a failure in the TCP window management, the LTE throughput was very low. This was especially an issue in longer TCP sessions like big file downloads or VPN connections.

**USB-Ethernet adapter not working**
Due to an internal misconfiguration, USB-Ethernet adapters were not shown in the IP setup of the web interface.

**Reset of GNSS module could fail**
There had been situations where the GNSS supervision failed to reset a GNSS module correctly. In that case, no GNSS fix was available until the next system reboot.

**Installing a software release could lead to loss of stored factory configuration**
After installing a new software release, the factory configuration manually stored by the customer was lost.

## *Known Issues*

**Protocol server restrictions**
The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

- Only one Protocol server can be configured even in units with more RS232 interfaces
- If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to local M!DGE2' 1st LAN IP address). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

# Release 4.4.40.101, patch 1354
# 2019-12-12

## *New Functionalities*

**GUI improvements**
Redundant settings for HTTP, HTTPS and telnet were removed. These services are now managed via Services setup.

**SDK improvements**
New function *usleep()* provides sub second sleep intervals.
New API function to *nb_syslog_p()* for logging to different log levels.

**GNSS dead-reckoning**
New configuration options to store and load GNSS DR calibration data to the GNSS module for faster DR learning and better DR data basis.

**SNMP service improvements**
System temperature is now provided on SNMP poll. The OID is *1.3.6.1.4.1.33555.10.40.50.0.*

**Added support for certificate chains for OpenVPN export mode configuration**
It is possible now to install certificate chains for OpenVPN using the expert mode configuration process.

**Netflow interface supervision for Ethernet and WWAN interfaces**
Netflow was introduced for WLAN interfaces and is now available for other device types like Ethernet and WWAN as well.

**MQTT Broker**
A MQTT Broker can now configured on M!DGE2 Routers providing MQTT service to the network.

**Key-parameter support for GRE tunnels**
GRE tunnels now support the Key-parameter which is used to separate different GRE tunnels between two end-points.

## *Security Fixes*

## *Fixes*

**Watchdog on failing SDK script did not work**
A change in the watchdog API was not properly handled by the SDK scripting engine. Resulting in watchdog to fail to restart the System on error. This was fixed.

**Problems on switch-over between WAN and WWAN**
Under rare conditions, the switch over between WAN and WWAN did not work as expected.

**GUI improvements**
The GUI failed to set some special characters like '&'.
If VLAN is configured on bridge devices, the bridge interfaces showed up several times in the web GUI. This was fixed.
Due to a mistake in the input sanity check, it was not possible to change some user options without changing the user's password. This was fixed.

For actions which require the current password which is normally stored only as salted hash, it is still required to provide the password, but this (new) password may be the same as the old one.
Due to a failure in string escaping functionality, some AT commands failed. This was fixed.
Fixed typo

**IPsec tunnels failed to start**
Due to timing issues on setups with several IPsec tunnels, some of these sometimes failed to start. The start procedure was changed to prevent this failure.

**Old configuration files failed to apply**
Some very old configuration files failed to apply with error message ’Unable to create backup’. This was fixed.

**Bridge interface lost on software update**
Software bridge interfaces (like BR1, BR2) might get lost on SW-Update and needed to be reconfigured after the update was finished. This was fixed and the bridge interfaces are preserved on software update.

**Storage date of last "Factory Default Config" is not updated on consecutive storage events**
If the function to store the current configuration as factory default is called several times, the timestamp of the latest store event is not updated. This was fixed.

**SDK improvements**
*nb_dio_count* failed to remove obsolete data resulting in wrong data. This was fixed.

**GNSS data show up delayed**
We have seen GNSS data to be delayed by some seconds due to a failure in buffer handling. This was fixed.

**4G-only WWAN connection failed to connect**
Under certain conditions, LTE modules failed to connect if 4G-only was selected even through LTE network was available. That was fixed.

**Unstable WWAN connection with LTE-First setting**
With LTE-First option, some LTE modules failed to establish connection under poor LTE conditions on software release 4.3.40.102. This was fixed.

**The LTE module could stay in 2G or 3G even though better service type is available**
This has been fixed.

**Connection tracking for FTP service missing**
On software releases since 4.3.40.100, the connection tracking for FTP was not configured correctly. This was fixed.

**TCP/IP connection not established when the connection is terminated inside M!DGE2 router**
This was fixed by changing of internal kernel parameters.

**Reboot with GNSS module**
The GNSS module in combination with 4.3.40.x causes rebooting of the M!DGE2 unit. This was fixed.

**Boot order of services**
In some rare combination of M!DGE2 services, the particular service did not come up correctly. The order of services has been improved.

**TCP establishment**
Some TCP sessions (ports) could not be fully established if this TCP was terminated in M!DGE2 while GRE over IPsec was established. This was fixed.

## *Known Issues*

**Protocol server restrictions**
The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

- Only one Protocol server can be configured even in units with more RS232 interfaces
- If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to local M!DGE2' 1st LAN IP address). If using VPN tunnels, mapping should be configured to these LAN IP addresses.