M!DGE/MG102i Release notes

Firmware version 4.1.40.xxx

Release 4.1.40.102
2018-08-15

IMPORTANT: ECC Conversion
The flash on M!DGE and MG102i routers provides an automated error correction using ECC. We changed the ECC length from 1-bit ECC to 4-bit ECC which provides better error correction. On the first boot after the software update has been performed, the data on the flash memory are automatically converted to use the new ECC setup. While this conversion is being performed, the LED diodes are "on" for about 30 seconds. If you switch back to an older software release like 4.0.40.x, the migration is reverted.
We tested updates and downgrades to and from 4.0.40.x and 3.8.40.x. Updates to or from older versions are not supported. If you run an older release or want to downgrade to an older release, you are advised to migrate via 4.0.40.x as an intermediate release. To revert the migration on downgrade, the SPL boot loader release 4.1.40.x stays in place. It can be downgraded in a second software update process initiated from the target release after the first reboot.
Software updates with recovery images require special attention. You must not use recovery images 4.0.40.x and older for systems running 4.1.40.x and newer. If you want to use recovery images, please contact our support at support@racom.eu.

IMPORTANT: Update to 4.1.40.x is failing (Exiting with code 3 Unsupported Model or Family)
The software version 4.1.40.x requires a minimum software version installed to update from. Therefore, the update will fail if you do not have the correct software installed. Previous updater would recognize this software Image as not meant to be installed on this router model.
Please use the newest Software depending on your currently installed major software version (>=3.7.40.114, >=3.8.40.112, >=4.0.40.109) and then update to the newest 4.1.40.x software.

New Functionalities

OpenVPN pushed IP address
It is possible to apply the network settings pushed by OpenVPN server for a TAP device.

Consider only 3G/4G networks for WWAN data link
It is possible to restrict a WWAN interface to connect only on 3G or 4G networks.

Provide same USB drivers for all platforms
For our products, different drivers for external USB serial or USB Ethernet adapters had been shipped. We now provide the same drivers for all our routers. Please refer to our manual for detailed description of supported 3rd party hardware.

GUI improvements
A change of the IP of the WLAN AP in dual-mode operation did not automatically change the DHCP range appropriately.
A SIM card which required a PIN did show "unknown" for pin protection in overview and "error" on SIM state until the correct PIN was applied.
The web GUI does not offer HW flow control on internal serial ports which do not support this.
The current IPsec status shown in the web interface was inconsistent at different locations. The status is shown identical everywhere now.
A WAN interface on a disabled LAN port would show as "dialing" in the overview. That was fixed. It shows "disabled" now.

With too many VLAN interfaces, the GUI showed inconsistent data.
WLAN networks which do not match on channel selection in WLAN dual mode are not selectable anymore in the web GUI.
The uptime of OpenVPN clients is shown in UTC in the web interface. That is explicitly mentioned now.

Better help text on CLI
The help text for CLI was missing a parameter on firmware update.

New SNMP field showing the activation time of a new software update
Software update via SNMP is done in two steps: First the new release is updated, second is the activation of the previously updated software release. So far, only the time stamp of the download could be obtained via SNMP. Now also the activation time stamp can be requested via SNMP.

WLAN client TLS version
It is now possible to configure the preferred TLS version for each WLAN client network if WPA-EAPTLS is configured.

SDK improvements
It is possible now to perform an incremental configuration update from the SDK now. This corresponds to the option "missing config directives will be ignored" in the web GUI.

Allow individual SSL settings for WPA-EAP-TLS
It is possible now to set up individual SSL settings for WLAN with WPA-EAP-TLS setup. Please contact our customer support if you need this feature.

Support for new configuration version 1.11
The new software release supports conversion of configuration files with version ID up to 1.11.

Fixes

Kernel warnings in the logs of AP with lots of WLAN clients
In situations with many WLAN clients, the AP sometimes showed warnings like "could not get mac80211 beacon" in the logs. This was fixed.

OpenVPN server does not restart after configuration update
After uploading a configuration with new OpenVPN expert mode file, the OpenVPN server was not automatically restarted and did not apply the changes.

Custom factory default configuration does not apply
There have been situations where a custom factory configuration could not be applied. This was fixed.

SDK improvements
The SDK function `nb_can_setattr` failed if the optional parameter restart was different from 0.
The SDK function `nb_cert_read` returned an error string instead of empty string if the requested certificate was missing. This was fixed.
On parallel call of `nb_config_get` from different SDK scripts the function might return wrong data occasionally. This was fixed.
The SDK function `nb_cert_enroll` returned 0 on error case. That was fixed.
The SDK function `nb_cert_install` failed to install certi1cates from local files. This was fixed.

GUI improvements
IPsec expert mode file download from the web interface sometimes failed.
The certificate site for WLAN interfaces was not displayed when dual mode was configured.

Invalid IPsec expert mode files
Depending on how the client certificates for the IPsec expert mode files were generated, it was possible that the client could not connect to the IPsec server.

Authorities certificates were not used for all HTTPS downloads
Some functions where data are downloaded from a server, the "Authorities" certificates were not used. E.g. it was not possible to update WWAN module firmware via HTTPS.

SNMP: Upload of current configuration to server failed
An upload of the current configuration to a server failed when triggered via SNMP. That was fixed.

HTTPS server did not restart after configuration update
When a configuration with new certificates for the HTTPS server was uploaded, the server did not apply the new certificates automatically.

Modem emulator phone book entries could not be deleted
Deleting a phone book entry from the modem emulator resulted in an error message. This was fixed.

Security updates in 3rd party software package PHP
The following security issues were fixed in PHP software package: Stack-buffer-over2ow while parsing HTTP response (CVE-2018-7584), Out-Of-Bounds Read in timelib_meridian() (CVE-2017-16642), remote denial of service in PHP PCRE (CVE-2016-1283).

Stability problems with Software Releases version 4.1.40.100 and 4.1.40.101
During the software update process and in normal operation the device can go into an undefined state with version 4.1.40.100 and 4.1.40.101. This was fixed. Please do not use these software versions.

IPsec with PSK authentication fails to provide expert mode file for download
While configuring an IPsec connection the GUI showed the error message "IPsec: No valid ZIP file." even though the configuration was OK.
Even though the web GUI showed a download link for expert mode files on IPsec with PSK authentication, the download failed with the error message "Unable to create IPsec clients file". That was fixed.

Fix of OpenSSL security related bugs
A cache timing vulnerability on generation of RSA keys was discovered in OpenVPN. This issue was fixed. For detailed information refer on CVE-2018-0737.

WLAN going down on bridge configuration
Applying a configuration where a WLAN-AP interface is bridged with a VPN interface required a system reboot. This was fixed.

WLAN automatic channel selection could select SRD channels
In Release 4.1.40.101, a WLAN-AP configured with ACS does not omit channels which are reserved for short range devices. This was fixed and SDR WLAN channels 149, 153, 157, 161 and 165 are no longer used.

Secondary WAN interface does not switch off
If an interface with higher priority comes up, the current WAN interface with lower priority is not switched off. The routing and data transfer are switched to the new interface though.

Wrong settings for link supervision after change of WAN link priority
After changing the priority of two WAN interfaces, the link supervision settings were applied to the wrong WAN link.

WLAN selection priority ignored on WPA-Enterprise
If WPA-EAP-TLS was configured for one WLAN client setup, the priority for that configuration was always set to 1, meaning that this network was selected with high priority independent of the configured priority.

Known Issues

SDK function `nb_cert_install` returns no error on failing installation from local file
If the source of an installed certificate is file:///... the SDK function `nb_cert_install` will always return 0 - even if the installation failed. This is a known issue and will be fixed as soon as possible.

IP Passthrough
IP passthrough is not working as expected. The functionality will be fixed as soon as possible.

Release 4.1.40.101
2018-02-27

IMPORTANT: ECC Conversion
The flash on M!DGE and MG102i routers provides an automated error correction using ECC. We changed the ECC length from 1-bit ECC to 4-bit ECC which provides better error correction. On the first boot after the software update has been performed, the data on the flash memory are automatically converted to use the new ECC setup. While this conversion is being performed, the LED diodes are “on” for about 30 seconds. If you switch back to an older software release like 4.0.40.x, the migration is reverted.
We tested updates and downgrades to and from 4.0.40.x and 3.8.40.x. Updates to or from older versions are not supported. If you run an older release or want to downgrade to an older release, you are advised to migrate via 4.0.40.x as an intermediate release. To revert the migration on downgrade, the SPL boot loader release 4.1.40.x stays in place. It can be downgraded in a second software update process initiated from the target release after the first reboot.
Software updates with recovery images require special attention. You must not use recovery images 4.0.40.x and older for systems running 4.1.40.x and newer. If you want to use recovery images, please contact our support at support@racom.eu.

IMPORTANT: Update to 4.1.40.x is failing (Exiting with code 3 Unsupported Model or Family)
The software version 4.1.40.x requires a minimum software version installed to update from. Therefore, the update will fail if you do not have the correct software installed. Previous updater would recognize this software Image as not meant to be installed on this router model.
Please use the newest Software depending on your currently installed major software version (>=3.7.40.114, >=3.8.40.112, >=4.0.40.109) and then update to the newest 4.1.40.x software.

New Functionalities

Terminal Server
Generally, a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to M!DGE/MG102i over the local area network (LAN), or even over the cellular network. It is a virtual substitute for devices used as serial-to-TCP(UDP) converters. It is possible to configure two Terminal servers.

Limit bandwidth per WiFi client
In AP mode the maximum bandwidth may be limited per Wi-Fi client.

GUI improvements
On interfaces which show a minus symbol to remove entries (i.e. firewall rules), the corresponding setting was deleted immediately. This is now safeguarded by an alert to prevent accidental removal of settings.

Firmware blobs
To comply with RED, it is not possible to load unsigned firmware blobs any more. All firmware blobs are signed now.

Timezone update
The timezone list has been updated to version 2017c.

SNMPv3 engine ID configuration
Engine ID for SNMPv3 traps can be configured now.

WLAN drivers
The WLAN drivers have been updated to a newer version.

Bridge VLAN interfaces
Software bridge devices BR0 and BR1 were added to the options provided for bridged VLAN interfaces. This allows VLAN interfaces to be bridged with WLAN and layer two VPN (TAP) interfaces.

Hayes AT Modem Emulator
Devices with serial interface provide a Hayes AT Modem Emulator. This can be used to replace an existing modem-based data-call applications. For further information read our case study.

WLAN SSID
The WLAN SSID configuration via webgui has been revised to allow more special characters.

Hostapd and wpa-supplicant updates
Hostapd and wpa-supplicant were updated to version 2017-08-24.

Regulatory Database
The wireless regulatory database is handled as firmware file now.

Mobile IP services
Starting with release 4.1.40.101, Mobile IP is activated by default and does not require an extra software license.

Fixes

IPsec expert mode configuration
Some files of the IPsec expert mode configuration were not installed correctly after the software update. That was fixed.

GUI improvements
There was a browser which showed the web interface incorrectly. Changes of the GUI CSS fixed this issue.
The RX/TX transfer rates in status view did not update when the link was disabled and no new data were transmitted. This was fixed and the displayed transfer rate will drop to 0 in that case.
Fixed display of alert messages.
The selection for bridged modems showed "none" as option. Nevertheless, this could not be selected. This was fixed. Selecting "none" as modem will disable the modem bridge.
The QoS setup overview showed wrong data after applying new settings. This was fixed.
When SIM cards were switched between WWAN modules, there was a misleading warning showing up. This has been fixed.
After configuration of a new WWAN interface it could happen that the new interface was not shown in the list of configured devices until the page was reloaded. This was fixed.

SSH server certificate download failed
The certificates which were provided for download from the web GUI were not in the correct format to reinstall them in another device. This was fixed.

SDK example script for SMS receive/transmit failed sometimes
The SDK example script on SMS receive/transmit had an error in the DIO handling. This was fixed. It was improved for better readability and cleaner code as well.

Boot loop after operator error on software update
We have seen devices to run into a boot loop after the administrator performed a configuration update after a partial software update. The bug fix would prevent any configuration updates via file upload until a pending software update was applied on reboot. Nevertheless, it is recommended to reboot the device after performing a software update.

Bridged WLAN
Sometimes Bridges with WLAN interfaces did not start. This was fixed.

GPS got stuck under certain condition
Sometimes the GPS module (issue was seen at ME909u) got stuck and would not produce a fix until system restart. This was fixed.

Memory leak in SMS send function
When sending via an SSH connection, temporary files were sometimes not deleted if the connection was interrupted too early by the SSH client. If that happened very often, */tmp/* directory could fill up with effect to the operating system. That was fixed.

Allow SSH login for additional admin users
Only the first three configured admin users were able to login via SSH and telnet. That was fixed.

Do not forward packages of local networks
Packets which belonged to networks of local interfaces were routed over IPsec links even though they were neither originated from, nor targeted to the router (iptables FORWARD chain). That was fixed.

SPL update failed
In very rare occasions it could happen that an update of the SPL boot loader failed. We have seen that on devices which were up for about one year without reboot. To guarantee a proper update, the updater will check the up-time and reject updates if the device has not been rebooted for a long time.

Disabled forwarding of DHCP offers
In setups with more than one WAN link, DHCP offers on one of the WAN links were sometimes forwarded to the other WAN interface. This behavior was not intended and got fixed by disabling forwarding on WAN links until the link is fully operational and all firewall rules apply.

File configuration update improvement
Some configuration files (e.g. VPN expert mode files or uploaded SDK scripts) were not deleted after configuration update even if the option "missing config directives will be replaced with factory defaults" was selected. This behaviour was changed. If you want to keep such files, select "missing config directives will be ignored".

GPS supervision
We have seen situations where the GPS failed to provide data, but the supervision did not trigger a restart of the GPS or of the router. The root cause for the missing GPS data was fixed as well as the behaviour of the GPS supervision in a GPS daemon failure state.

Voice daemon fails and triggers reboot
There have been situations where the voice daemon failed to start and triggered a system reboot. The voice daemon was fixed.

Group alias of nobody to nogroup added
There was a case where a customer relied on the existence of the system group nobody for advanced expert mode OpenVPN configuration. For backwards compatibility with the existing configuration, the group nobody was created as alias to nogroup.

SNMP users not created on configuration update
SNMP users were not created when applying a configuration file. Therefore, SNMP requests with these user credentials failed. This was fixed.

NTP time sync takes very long on initial configuration
We have seen situations where it takes very long (several minutes) to get a time sync via NTP on the first configuration from factory state.

MG102i port Ethernet 5 not turned off
Even when disabled port, Ethernet 5 was not switched off and still showed link activity. The port is now shut down correctly.

SDK improvements
Due to a failure in parameter check, nm_modbus_reply could fail even though the given parameters were correct. This was fixed.
In rare conditions nb_status returned NULL instead of data even though the request was legit. This was fixed.

Linux Kernel security bug fixes
CVE-2017-16525 Possible attack via crafted USB device in USB serial module
CVE-2017-16531 Possible attack via crafted USB device in kernel USB core
CVE-2017-16534 Possible attack via crafted USB device in kernel USB core
CVE-2017-16535 Possible attack via crafted USB device in kernel USB core
CVE-2017-1000410 Possible remote kernel information leak via Bluetooth L2CAP

VLAN packet loss
If there is an MTU set up on a LAN interface, VLAN packets which are routed over this interface will get lost if the VLAN’s MTU is not set up accordingly. This was fixed.

MTU setup of VLAN interfaces failed
MTU setup was applied to the wrong VLAN interface if there were different VLANs defined on different LAN interfaces. This was fixed.

Security bug fixes
CVE-2018-1000007 curl HTTP authentication leak in redirects
CVE-2017-8816 curl NTLM buffer overflow via integer overflow
CVE-2017-8817 curl FTP wildcard out of bounds read
CVE-2017-8818 curl SSL out of buffer access

IPsec expert mode configuration missing in configuration download
Uploading a configuration file that includes an IPsec expert mode configuration missed to start IPsec automatically. This has been fixed.
The IPsec expert mode files were not included into the configuration files that can be downloaded from the web interface. This was fixed.

Pitfalls

Known Issues