

UPDU Firmware Release Notes

Riedo Networks Ltd, Switzerland

Revision: 3.4.1-2b5cb066

Date: December 5, 2024

Release 3.4.1

This is a maintenance release fixing two bugs which can potentially affect UPDUs with switchable outlets:

- When switching outlets on or off, the web-interface can, in some situations start to misbehave and show other unrelated outlets in a blinking state.

Note that this only affects how these outlets are shown on the web interface, it has no effect on the physical state of the outlets on the PDU.

- Per-outlet power-on delay settings used during outlet sequencing are not applied as specified.

Enhancements

- Renew built-in updu.io certificate (valid until 2026-01-05)

Bugfixes

- Outlet-sequencing: Fix power-on delay configuration (#1290)
- Switchable outlets: Fix potential bogus relay state (#1286)

Release 3.4.0

This release adds the following major changes:

- Outlet sequencing: UPDUs with switchable outlets can be configured to sequentially power on outlets after a power outage in order to reduce inrush currents. Refer to the `Outlet Sequencing` chapter in the `CLI Reference Manual` for more details.
- A new command option `show config backup` is available which allows to export a full backup of all available settings of a given UPDU. By using the output of this command, a UPDU can be configured independently of the currently present configuration.

As always, the output of the command can be entered (pasted) into the `configuration` context on the CLI.

- The web-interface now supports downloading and restoring backup files. This new feature is available on the `Maintenance` page. Refer to the notes below for details.
- A new set of user energy counters has been added. These counters can be reset at any desired time and are available in the CLI. Refer to the `Energy` section in the `CLI Reference Manual` for details.
- The web-interface has been enhanced to configure user roles. These settings are available from the `Users` page and allow fine grained permission control for both local and remotely authenticated users.
- Changes to the CLI configuration: In order to add support for the settings backup and restore feature, a few changes to the CLI configuration syntax were required. Some of these are breaking changes where others are extensions of existing commands. Refer to the notes below for details.

NOTE: Regarding *Configuration backup & restore*:

The content of the backup exported via the web-interface as well as printed on the CLI using `show config backup` are identical. A backup can thus also be restored on either interface.

Also note that backups are plain text and are not restricted to a device. However, certain settings vary depending on the UPDU model (e.g. different outlet configurations) and occasionally, new firmware releases will introduce additional settings and change previous settings. Care must thus be taken when restoring backups on different devices or newer firmware versions.

Should a restore on either the web-interface or the CLI fail, consult the `CLI Reference Manual` included in every firmware release for the documentation of the settings.

NOTE: Regarding *Changes to the CLI configuration*:

As a first note, there is nothing to be done when upgrading the firmware as all settings are migrated automatically. If you have used scripted configuration via the CLI or kept local templates, these may have to be adjusted.

The easiest solution in this case is to upgrade the firmware of a device and obtain a new configuration by using `show config backup`. Using this approach will also ensure that the scripts make use of the newly introduced options to restore configurations in the most reliable way.

NOTE: Blast-RADIUS Mitigation

This firmware release contains changes to mitigate the Blast-RADIUS vulnerability (CVE-2024-3596). The UPDU RADIUS client always sends the `Message-Authenticator` attribute and by default requires this attribute to be present in responses from the RADIUS server. Should the RADIUS server not support sending the attribute, it is required to disable this verification on the UPDU, or the authentication will fail. Please consult the `RADIUS Authentication` section in the `CLI Reference Manual` for instructions.

New features

- Web: Roles management (create, delete, configure permissions)
- CLI: Add "show config backup" variant (#1223)
- Web: Config backup / restore functionality (#1195)
- Add user resettable energy counters (#1200)
- Add outlet sequencing (#2053)
- Modbus/TCP: Add monitoring active conditions counters (#1180)
- Modbus/TCP: Add outlet switching (#1179)

Enhancements

- Renew built-in updu.io certificate (valid until 2025-12-01)
- Web: SNMP Notification recipients community field validation (#1252)
- Batch CLI: Control access to main context (#1259)
- CLI: Suppress "configure" notices on non-interactive sessions (#1257)
- CLI: Truncate large prompts (#1260)
- Auth: Add Blast-RADIUS mitigation (#1209)
- SNMP: ADD ObjectPath OID (#1218)
- CLI: Add "detach" option to "acl" configuration command (#1223)
- CLI: Replace SNMP "notify-host" by "notify" (#1223)
- CLI: Replace SMTP "notify-recipient" by "notify" (#1223)
- Add "show outlets switchable" CLI command (#1228)
- Use relay state reported by the POMs (#1224, #1248)
- CLI: Add "accounts replace" option (#1240)
- CLI: Replace "users" command with "accounts"
- CLI: Add "clear-duplicate" to object name command (#1223)
- Backup/restore: Ensure user has CLI_ACCESS and is not modified (#1223)
- Batch CLI: Support multiple line endings (#1241)
- CLI: Add delimiters for certificate data entry (#1242)
- POM/PIM: Upgrade firmware to 3.11.0
- System: Simplify fatal error handling (#1213)
- Disable background MPU map (#1214)
- Serial: Clear FIFO on errors
- Display: New display drivers
- SSH: Enable strict key exchange extension support (#1198)
- Network: Upgrade stack to 2.4.2 (#1112)

Bugfixes

- Flash: Fix potential lockups (#1267, #1271)
- Identify: Fix "stop" regression (#1272)
- CLI: Consider '#' and '!' inside tokens not as comment delimiters (#1222)
- Fix per-outlet powercycle-delay persistence (#1235)
- Fix typo in "change datetime" command
- Fix rare TRNG problem (#1210)
- Flash: Disable AHB prefetch (#1205)
- Monitoring: Remove leftover mutex unlock (#1208)
- Time: Fix UTC and Localtime conversion (#2043)

Release 3.3.1

This is an internal maintenance release used for producing new UPDU models. A few bugfixes have also been back-ported to this patch release.

Enhancements

- Support for additional MCB types
- Prevent firmware downgrades for certain PDU models.

Bugfixes

- Fix rare TRNG problem (#1210)
- Serial: Clear FIFO on errors
- Flash: Disable AHB prefetch (#1205)
- Remove leftover mutex unlock (#1208)

Release 3.3.0

This release adds the following major changes:

- The identify function is now also available on the web-interface. Use the icon next to the object name on the Analyzer page to start an identification on the UPDU.
- Infrastructure for storing the UPDU factory configuration in the measurement modules. This provides additional functionality for *Remote Meter UPDUs* (see note below) and simplifies in-field controller replacements.

NOTE: Regarding *Remote Meter UPDUs*:

When a *Control Unit* (RN3009) boots after being connected to a different *Remote Power Meter* (e.g. RN3013, RN3023), the new setup is detected and has to be acknowledged by the operator via the local user interface in order to take the specifics of the new *Remote Power Meter* into account. This detection is performed during startup, thus a software reboot or power-cycle of the *Control Unit* is required after connecting a different *Remote Power Meter*. The *Remote Power Meter* can remain powered during this process.

New features

- Time: SNTP server configuration through DHCP (#1168)
- Add 'show config hide-secrets' command (#1048)
- Dim LEDs on the measurement modules when display is blank (#1129)
- CLI: Add ping command (#1109)
- Web: Add identify object functionality (#1182)
- CLI: Add the command `show branches` (#952)
- Monitoring: Add branch state monitoring (#952)

Enhancements

- Web: Display RCM RMS and DC values on two separate columns (#1196)
- Renew built-in *.updu.io HTTPS certificate (valid until 2025-07-20)
- System: Ensure main thread stack size is also checked (#1191)
- Longer module poweroff after "reboot modules" (#1171)
- E3BUS: Stop probing daisy-chained devices on OCU buses after failures (#889)
- New QSPI memory drivers
- Reboot-surviving RAM: selective cache flush (#1172)
- E3BUS: Probe first device on OCU bus with more retries (#1171)
- Speed up factory reset (#1173)
- POM/PIM: Upgrade firmware to 3.10.0
- FRAM object store (#1166)
- RS485: Improve ring buffer handling (#1165)
- Reduce boot time (#1132)
- Upgrade RTOS to version 3.6.0 (#1034)
- Bootloader 1.1.2: Reset UART before starting firmware (#1093)
- Bootloader 1.1.1: Print bootloader slot (#1149)
- Bootloader 1.1.0: Speed-up application firmware verification (#1136)
- Improve event infrastructure (#1154)
- Renamed commands "monitor log" to "monitor enable log" and "monitor log off" to "monitor disable log" (#1038)

Bugfixes

- Syslog: Fix potential delay when disabling syslog (#1187)

Release 3.2.0

The major changes in this release are:

- Web settings persistency: The web-interface has been modified to handle the persistency of settings akin to the command line interface. Refer to the notes below for more details.
- New products support: The firmware now fully supports the new UPDU with Combo Outlets (combined C13/C19) as well as support for differential pressure sensors.

NOTE: Regarding the changes to the web-interface settings persistency:

Changed settings on an UPDU are applied immediately upon validation. On the CLI this happens after any configuration line where as the web-interface applies settings with the `Apply` button.

Applied settings are not automatically persisted. They will be lost after rebooting or power-cycling the device in question. Only after an additional action they are persisted. On the CLI, this is achieved by using the `write` command and the web-interface now features a similar `Write` button. Both interfaces show friendly reminders to make sure settings are persisted before logging out.

This mechanism allows administrators to prevent lockouts by scheduling a reboot before changing critical settings. For example: A reboot scheduled to happen in 5 minutes allows to change network settings without risking a device to become unreachable due to a misconfiguration. Should any modification cause a connection loss, the scheduled reboot will revert changes to the previously persisted state. When all settings are changed as desired and are working properly, they can be persisted and the scheduled reboot can be cancelled.

New features

- Web: Add scheduled reboots (#1123)
- CLI: Inform users about unsaved changes (#1116)
- Web: Keep track of dirty settings. Stop persisting configuration right away when applying settings. Show "Unsafe configuration" notice instead. (#1115)
- CLI: Add "change datetime" command, allow SNTP enable/disable (#1108)
- CLI: Add "change password" command (#1102)
- UI: Add configurable LED brightness (#1081)
- Sensors: Add differential pressure monitoring

Enhancements

- Renew built-in *.updu.io HTTPS certificate (valid until 2025-04-12)
- Auth: Add "change-credentials" permission (#1101)
- POM/PIM: Upgrade firmware to 3.8.1
- Sensors: Add power fault detection (#1063)
- Auth: Configurable LDAP receive buffer size (#1021, #1105)
- CLI: Add command 'show frequency' (#926)
- Auth: Use generic TLS/non-TLS socket abstraction for LDAP (#1019)
- CLI: Add power factor to the "show power" command (#1043)
- E3BUS: Improve internal API error handling
- Isolate generic RNXBoot image handling functions (#1083)
- Firmware image handling refactoring
- Auth: Split configuration in smaller structures (#1052)
- SNMP: Add amperage rating for power objects (#1077)
- Sensors: Add dynamic power handling (#1047)

Bug fixes

- CLI: Add server names validation (#1025)
- Auth: Properly set auth type for all methods and show on user profile page (#956)
- CLI: Fix parsing of fixed point numbers in the range -1..0 (#1092)
- Sensors: Fix bad sign of values in the range -1..0 (#1090)
- Web: Don't show watch config buttons for outlets without metering license (#1082)

Release 3.1.0

The major changes in this release are:

- SMTP Notifications: The notification system has been enhanced to support sending emails via SNMP. Up to three recipients can be configured to receive monitoring and audit messages from a single outgoing address.
- TACACS+: User authentication against a TACACS+ server is supported as an additional remote authentication service.
- Modbus/TCP Security: Encryption and optional authentication is now supported by the embedded Modbus/TCP server.

NOTE: With the addition of Modbus/TCP Security, a new configuration option `default-role` has been added to the Modbus/TCP settings. Existing plain Modbus/TCP configurations must configure this setting with a role including at least the `modbus-read` permission. Should it be required to switch outlets, the `modbus-write` permission must additionally be granted to the configured role. Consult the `Modbus/TCP Configuration` chapter from the `CLI Reference Manual` for more details.

New features

- Notification: Add notifications by email (#1031)
- Modbus/TCP: Add Security protocol support (#1030)
- Modbus/TCP: Add Read Device Identification command support (#916)
- Auth: Add TACACS+ support (#1003)
- Network: Add per interface DHCP hostname override (#1017, #1024)

Enhancements

- Renew built-in *.updu.io HTTPS certificate (valid until 2025-01-04)
- E3BUS: Improve logging of missing modules (#967)
- Boot: Improve PDU power cycle behaviour
- POM/PIM: Upgrade firmware to 3.6.1
- System: Avoid NOR Flash interface reconfiguration
- PDU: Optimize PDU node internal memory usage
- CLI: Add nodes electrical capabilities to `show wiring` output
- CLI: Improve `show module info` output for active PIM (#764)
- Support for Combo-Outlet POM (#920)
- UI: Show per inlet power for dual-inlet PDUs (#1014)
- Upgrade: Refactor upgrade API (#977)
- Log: Add audit log message for sensor attach/detach (#973)
- Network: Improve configuration error handling (#1028)
- Heap: Use complete free space as heap (#979)
- CLI: Remove deprecated "dns-server" interface configuration command (#1032)

Bug fixes

- Notification: Send missing early notifications (#1050)
- Bootloader: Fix rare boot lockup (#1041)
- CLI: Fix `snmp/delete notify-host` race condition (#1039)
- Console: Improve early log printing (#1041)
- System: Improve serial interface initialization (#1041)
- Console: Fix rare UART lockup (#1041)
- E3BUS: Avoid excessive logging (#1029)

Release 3.0.1

This is an internal maintenance release used for producing new UPDU models.

New features

- Settings: Support C14/C20 inlet connectors (#1055)

Bug fixes

- Fix factory dongle detection regression (#1027)

Release 3.0.0

The major changes in this release are:

- Network ACL: The network stack has been enhanced with configurable Access-Control-Lists (ACL). ACLs allow to restrict or grant access to services based on IP ranges. For detailed information on how to use this functionality, refer to the `CLI Reference Manual`. Please note that this firmware version does not yet allow ACL configuration via the Web-Interface.
- Configurable user roles: The device now supports freely configurable user roles. Multiple roles can be created and used for both local and remote users.
- New bootloader: A new bootloader has been developed and is active from this version. This new bootloader allows to significantly reduce the the time needed to perform future firmware upgrades.
- Syslog: The configuration on the CLI has been changed to allow enabling and disabling sending messages without clearing the current configuration. Additionally, syslog messages can be sent with timestamps corresponding to the local timezone in addition to the default UTC timestamps.

Due to this change in the configuration interface, the format of the configuration has slightly changed. The format is automatically migrated with the firmware upgrade and can be exported with the `show config` command on the CLI.

NOTE: It is not possible to downgrade to a previous firmware version once this version has been installed.

NOTE: When upgrading from an older version, the bootloader is upgraded automatically when the new firmware first runs. Do not power off the UPDU until the system is fully booted.

New features

- Log: Add “show log bootloader” command (#986)
- Console: Print log messages during booting (#989)
- Roles: Add support for user-configurable roles (#853)
- Network: Add ACLs to control incoming traffic (#928)
- Web: Retrieve roles dynamically (#960)
- Bootloader: New bootloader with failsafe update

Enhancements

- LDAP: Improve LDAP message framing (#1016)
- Syslog: Add `syslog [enabled|disabled]` configuration command (#984)
- Syslog: Allow logging with localtime timestamps (#978)
- Network: Upgrade stack to 2.3.0 (#959)
- Time/SNTP: Allow tracing (#953)
- Doc: Refactor CLI Reference Manual (#569)
- Log: Crash information is logged after a software crash (#173)

Bug fixes

- LDAP: Fix memory leak when using TLS (#1015)
- Flash: Fix bug in the flash driver (#992)
- SSH: Fix SSH exec crash when a connection is closed prematurely (#1005)

Release 2.10.2

This is a maintenance release fixing a critical bug affecting all UPDU models with the firmware versions 2.9.0, 2.9.1, 2.10.0 and 2.10.1: When a UPDU is configured with the HTTPS webserver disabled, booting with one of the affected firmware versions causes the UPDU to enter a crash loop which cannot be resolved without on-site maintenance.

If you are running 2.9.0, 2.9.1, 2.10.0 or 2.10.1, make sure the HTTPS webserver is enabled. DO NOT DISABLE IT! If it is disabled, enable it and save the configuration.

Bug fixes

- Web: Fix crash when booting with "https disabled" (#994)

Release 2.10.1

This is a maintenance release fixing a critical bug on RN3003, RN3014 and RN3009 affecting the web client. After upgrading to 2.10.0, users can no longer log in to the web client. Other functionality is not affected by the problem.

Devices which are in this condition can be upgraded to 2.10.1 with the RNX PDU Tool.

Bug fixes

- Web: Fix /api/nodes bug with some PDUs (#963)
- Web: Add support for System Power metric (#964)

Release 2.10.0

The major changes in this release are:

- Modbus/TCP Server: A basic Modbus/TCP server is added to give access to all measurement values. The `show modbus` CLI command shows the Modbus/TCP register map. The server is disabled by default.
NOTE: The current implementation does not have any security features. Thus upon service activation, the server listens on all active network interfaces and data can be accessed by any client with access to the physical network. Future firmware versions will implement access control settings and optional security.
- Unit Identification: The `identify` CLI command helps to avoid mistakes when doing maintenance. It shows an on-site engineer what PDU, module or outlet to work on by blinking the outlet LEDs of the object in question.
- System Power Monitoring: A PDU powered by Power over Ethernet now triggers a `WARNING FAILOVER` condition and causes monitoring notifications to be sent.

New features

- CLI: Add "clear dns-cache" (#954)
- Web: LDAP settings (#934)
- CLI: Add "identify" command (#897)
- Web: Add "preserve network" option to factory reset (#891)
- Monitoring: Notify when the system is PoE powered (#915)
- Modbus/TCP: Add Modbus/TCP server (#879)
- Web: Display local time in page header
- Web: Hide sensitive information like SNMP communities and shared secrets in settings (#846)
- Basic support for optional POMs (#878)
- SNMP: Add sending traps for audit events (#811)

Enhancements

- DNS: Allow debugging with "trace enable dns" (#951)
- Log: Log identify operations to the audit log (#942)
- Web: Reduce JSON generation memory consumption (#947)
- UI: Slightly reduced button brightness (#941)
- Monitoring: Improve "System Power" log message (#921)
- Network: Add link speed and duplex mode to "show interface" (#888)
- UI: Refactor LED handling (#932)
- UI: Show ongoing identify operation on display (#931)
- SNMP: Add ComposedName (#881)
- Web: Warn about insecure connection on login page. Show secure URL if available. (#817)
- POM/PIM: Upgrade firmware to 3.5.0
- Power-cycle POM upon non-user initiated reboot (#925)
- Sensors: Improve robustness (#868, #899, #923)
- SNTP: Increase max poll interval to 24h (#902)
- CLI: Improve "section" output filter (#918)
- UI: Allocate off-screen draw buffer from heap
- Log reboot reason (#909)
- Network: Enable storm-protection on ETH1/ETH2 (#392)
- Auth: Add configurable order of authentication methods (#861)

Bug fixes

- CLI: Fix "show rules" line truncation (#937)
- CLI: Fix custom time offset displaying (#945)
- CLI: Fix static IPv6 gateway command (#939)
- UI: Add missing per-phase current to overview page on 3L PDUs (#936)
- Add missing malloc return value checks (#910)

Release 2.9.1

This is a maintenance release fixing problems around the authentication using the LDAP protocol. It adds support for a formerly refused optional object in the LDAP response, allows for larger LDAP packets, and improves LDAP debug messages allowing to easier debug LDAP problems.

Further on, measurement values responsible for non-OK conditions are added to the monitoring log messages.

Enhancements

- Monitoring: Add measurement value to message (#911)
- LDAP: Add raw data capture (#917)
- LDAP: Improve debug messages (#912)

Bug fixes

- LDAP: Accept (but ignore) SearchResultReference (#929)
- LDAP: Dynamically grow receive buffer (#927)
- LDAP: Fix bad command used in LDAP documentation (#913)

Release 2.9.0

This release adds the following major changes:

- LDAP authentication: It is now possible to authenticate users against a remote LDAP server.
- Custom SSL/TLS certificate support: Users can now configure their own certificates which are used by the built-in webserver.
- Web client: New configuration options previously only available in the CLI are now also possible in the web client: monitoring, webserver settings. Further on, current and past monitoring conditions are shown on a dedicated page.
- RSTP disabled in the factory defaults: The Rapid Spanning Tree Protocol is disabled in the factory default settings. See below for more information.

Besides this, the release adds support for new UPDU models featuring more than one inlet.

Rapid Spanning Tree Protocol (RSTP)

Support for the Rapid Spanning Tree Protocol was added in release 2.2.0 and was disabled by default. Later, in release 2.7.0 this protocol was enabled by default. Starting from this release (2.9.0), RSTP is again disabled in the factory default settings.

This change means the following:

- New UPDUs shipped to customers with release 2.9.0 of the firmware have RSTP disabled. Users can of course enable it via the CLI or the web interface.
- When 2.9.0 is installed, a factory reset will disable RSTP if this was previously enabled. Please check the documentation on the `factory-reset` command in the UPDU CLI Reference Manual for more information, as it is possible to do a factory reset and preserve the network settings.

IMPORTANT INFORMATION: The factory default settings only affect new products that have not been configured yet. Existing products are only affected when a factory reset is performed. In other words, for existing products, if you have saved the settings at least once before upgrading (e.g. using the `write` CLI command or by applying settings in the web client), upgrading the firmware to any newer release (including 2.9.0) will not change the behavior of the UPDU, i.e. RSTP will stay enabled or disabled as it was configured before the upgrade.

Upgrading via the Web Interface

When upgrading UPDUs individually via the web interface, note that the web client of earlier firmware versions may not always confirm the firmware upgrade even though it was successful.

In the following situations, an upgrade confirmation is shown:

- You are upgrading from version 2.8.0 over an encrypted connection using the `updu.io` domain. In this case the Location reads something like `https://a-b-c-d.updu.io`, where a-b-c-d is the IP address (a.b.c.d) of the PDU.
- You are upgrading from any version over an unencrypted HTTP connection: If this is the case, the URL starts with `http://`.

When you are upgrading over an encrypted HTTPS connection and address the UPDU by its IP address or by some other local name, the fact that version 2.9.0 includes a renewed SSL/TLS certificate may cause your browser to block the web client from accessing the UPDU after the upgrade is done. In this case, please try to reload the web page after about 2-3 minutes.

Starting from version 2.9.0, a custom SSL/TLS certificate can be configured to cover such situations.

Downgrade

The changes done in this release necessitate blocking downgrades to earlier versions. It is therefore not possible to downgrade once release 2.9.0 of the firmware is installed.

New features

- Disable RSTP in the factory defaults (#880)
- CLI: Add "show rules" and "show conditions" commands (#874)
- CLI: Add "reboot switch" command (#866)
- Auth: Add LDAP support (#812)
- Web: Add custom SSL/TLS certificate support (#852)
- Web: Monitoring configuration (#818)

Enhancements

- POM/PIM: Upgrade firmware to 3.4.1
- Power: Log presence of 5VAUX after booting (#896)
- Web: Reduce upgrade timeout and add reload button on failure (#894)
- Web: Reload web client when webserver settings change (#893)
- Web: Clear TLS cache when SSL/TLS certificate change (#892)
- Renew built-in *.updu.io HTTPS certificate (#886)
- Web: Disregard redirect to HTTPS when HTTPS is disabled (#876)
- Web: Improved cookie settings (#277)
- CLI: Allow disabling/enabling monitoring rules (#813)
- Web: Add firmware version to Home page (#850)
- CLI: Add "show config all" to show certificate data (#858)
- Renamed RCM AC to RCM RMS (#843)
- Web: Disable updu.io redirect with custom SSL certificate (#860)
- POM: Improve reliability of inter-module communication
- CLI: Context help showing available timezones (#847)
- LOG: Sanitize log characters to 7-bit ASCII (#824)
- Web: Increase https connections if http is disabled or redirected (#829)
- Web: Add optional HTTP Strict Transport Security (#830)
- Web: Allow tracing (#802)
- Upgrade network stack to 2.2.0 (#800)
- Optimize SSH public key RAM usage (#809)

Bug fixes

- Web: Fix firmware upgrade response not sent back (#883)
- SNMP: Fix powerfactor of aggregated meters (#875)
- Web: Fix upgrade confirmation from pre-2.8.0 versions (#859)
- Settings: Fix premature settings write (#864)
- Monitoring: Fix potential bogus UNKNOWN conditions after booting (#844)
- OVP: Fix erroneous OVP failure for PDUs without RCM (#839)
- Web: Fix negative uptime (#831)

Release 2.8.0

This release adds these major changes:

- New RNX-UPDU-MIB2 SNMP MIB added: The new MIB is structured around the physical properties of a PDU and gives a more straightforward access to most information than the old MIB. The old MIB is still present but can be disabled in the configuration. The old MIB file was renamed to `RNX-UPDU-MIB1.mib`.
- Sensor and RCM objects: Monitoring, names and descriptions were added for Sensor and RCM objects.
- SNMP Notifications: Monitoring messages can now be sent in the form of SNMP Traps and Informs.
- Web User Interface: The Web UI now gives access to more features of the PDU, such as RADIUS settings, SSH keys, licenses, system log.

With this release, the self-signed HTTPS certificate was replaced by a updu.io wildcard certificate. UPDUs can now be accessed without any browser security warnings using the URL `https://a-b-c-d.updu.io`, where a-b-c-d is the IP address (a.b.c.d) of the PDU. The built-in webserver can be configured to automatically redirect to this URL. RNX operates public DNS servers to support the resolving, thus in order to use this feature, the browser used to access the PDU must be able to resolve public DNS records. This must be taken into account when enabling the automatic redirect from HTTPS to the updu.io hostname.

New features

- Web: Support redirects to HTTPS and to the updu.io domain
- SSH: Support ECDH key exchange (#746)
- CLI: Add "show snmp engineid" command (#805)
- Add SNMP traps (#804)
- Web: Show log
- SNMP: Add new updu-mib2 MIB (#661)
- Monitoring: Add sensor temperature and humidity rules
- Monitoring: Add RCM current rules (#790)
- Log monitoring messages on unknown values (#630)
- PDU: Add sensor objects
- Auth: Add RADIUS tracing (trace enable radius) (#784)
- CLI: Add trace command to enable/disable debugging (#786)
- Web UI: Manage SSH keys
- Web UI: Add RADIUS settings
- LOG: Add audit logging for user actions (#633)
- Network: Add support for configurable AutoIP fallback time (#775)

Enhancements

- Web: Hide failed login attempts, log login message (#824)
- Web: HTTP to HTTPS redirection is now the factory default
- Web: Use updu.io HTTPS certificate (#703)
- Monitoring: Reworded OVP_FAILURE to FAULT
- CLI: Change "show rcm" output (#613)
- PDU: Rename sensor names from AUXN to SensorN
- LOG: Configurable syslog facility (#599)
- CLI: Add user-defined object name to "show rcm" output
- PDU: Add RCM objects
- CLI: Allow factory-reset to preserve network settings (#779)
- CLI: Don't hide RADIUS and STP settings when disabled (#783)
- OVP: Add support for standalone OVP (#756)
- Web: Display message for unsupported user agents (#776)
- Web UI: Split settings up into separate pages
- SNTP: Insist longer during the initial synchronization (#774)
- UI: Show static IP addresses even if no cable is connected (#762)
- Make MIBs configurable (#189)
- Internal communication with metering modules is improved (#671)

Bug fixes

- Web: Fix POM/Outlet ordering on analyzer page (#826)
- SSH: Check for login permission on public key authentication (#823)
- Users: Fix role set to guest if no roles are set (#820)
- Web: Fix session handling when large domain cookies are present (#806)
- CLI: Reset "monitor log" on session disconnect (#801)
- Patch network stack to fix vulnerability: IP Fragment Reassembly (#799)
- SNMP: Fix upduRcmSensorQuality value always being ok(0) (#781)
- SNMP: Multiple set commands are not committed if one fails (#777)

Release 2.7.1

This patch release addresses a major vulnerability in the UPDU TCP/IP network stack which can lead to a denial of service. All versions of the UPDU firmware are affected by this vulnerability.

It also adds a number of internal features for the production of new UPDU models.

Bug fixes

- Patch network stack to fix vulnerability: IP Fragment Reassembly (#799)

Release 2.7.0

This release adds these major changes:

- RADIUS authentication: In addition to use local users, the UPDU supports user authentication against a RADIUS server.
- SSH public key authentication: By configuring public keys for local users, it is possible to connect with SSH without entering a password.
- RSTP enabled by default: The rapid spanning tree protocol introduced in release 2.2.0 of the UPDU firmware is now enabled by default (for new UPDUs or after performing a factory reset).
- The powercycle delay of switchable outlets can now be individually configured.

This release also adds functionality to limit access to selected features with a license. The only feature which currently requires a license is per outlet metering. UPDUs without the outlet metering license will no longer expose the per outlet measurements (e.g. the `show power` CLI command will indicate `n/a` on all outlets, as do the other interfaces). There should not be a different behaviour on UPDUs which were acquired with the outlet metering license.

If you have acquired the per outlet metering license with your UPDU but you see `n/a` on outlets, or if you would like to add the per outlet metering license, please get in touch with us.

New features

- Add SSH public key authentication (#706)
- Add SSH exec functionality (#707)
- Add "monitor log" CLI command (#539)
- Update MIB: Add upduMeterDataQuality object (#739)
- Add licensing functionality (#728)
- Add "Inlet" object (#726)
- Add "reboot modules" command (#715)
- Add configurable telnet and ssh session-timeout (#701)
- Make the powercycle delay configurable (#697)
- Add RADIUS support (#691)

Enhancements

- Web UI: Show description and edit it (#724)
- Hostname is now shown in the title bar of the display (main page) (#751)
- Enable RSTP in the factory defaults (#750)
- Upgrade network stack to 2.1.8 (#735)
- Turn off all Button LEDs when the screen is blanked (#731)
- Rename spanning tree "timers" command to "stp-timers" (#713)
- Add device name to SNMP SysDescr (#708)
- Increase SSH server stack size (#704)
- Use the heap for crypto and SSL functions (#699)

Bug fixes

- No longer scan for extra modules when booting (#671)

Release 2.6.2

Internal release.

Release 2.6.1

This is a patch release to address an important issue related to the newly added user-configurable object names.

IMPORTANT: If the web-interface of the 2.6.0 firmware version was used to set custom names to Outlets, it is required to perform one of the following actions before applying this update.

- Change and apply any configuration on the Settings page using the web-interface. E.g. Enable Telnet, click 'Apply', Disable Telnet, click 'Apply'.
- Connect to the console (via SSH or Telnet) and type 'write'.

If this is not followed, it is very likely that all Outlet name changes are lost after the reboot of the PDU.

Bug fixes

- Fix persistence of custom object names on web-interface

Release 2.6.0

This release adds these major changes:

- IPv6: Network interfaces can be configured with IPv6 addresses. There is support for static addresses, stateless address autoconfiguration (SLAAC) and DHCPv6.
- SNMPv3: SNMP is more secure thanks to SNMPv3. Along with this change, the user management has been extended to also include the SNMPv3 authentication and encryption information. SNMP version 2 is now disabled in the factory defaults.
- Local time: The local timezone of the UPDU can be configured, allowing the local time to be shown on the display and in log messages (see the `show log` CLI command).
- User-configurable object names: In addition to object descriptions, objects can now also be assigned a name. Names have to be unique and can be used to address objects, e.g. using the `outlet [on|off|cycle]` CLI command.

New features

- Add object description to SNMP (#694)
- Web UI: Display outlet names. Allow to edit them (#686)
- Web UI: Add user management.
- Add object name writing via SNMP (#684)
- Add object and configurable name to SNMP (#683)
- Add user configurable object name (#665)
- CLI: Add section output filter (#676)
- Add local time support (#642)
- Add IPv6 (#620)
- Add SNMPv3 (#311)

Enhancements

- CLI: Improve HOME/END key handling, add CTRL-L/R handling
- Disable SNMPv2 by default (#656)
- Improved SNMPv2 configuration syntax (#653)
- Add new "test rcm" command, deprecate "rcm test" (#650)
- Add snmp-read, snmp-write roles (#657)
- CLI: Always allow exit, end, logout (#669)
- Improve initial module discovery (#662, #672)
- CLI: Improve arguments TAB-completion (#514)
- CLI: Improve user configuration commands
- CLI: Allow TAB-completion for tokens containing whitespace (#658)

Bug fixes

- Fix log message timestamps to wrap after some 119h (#690)

Release 2.5.0

This release adds these major changes:

- Syslog support: All logged messages which can be seen with the `show log` command can now also be sent to a syslog server running on a remote system.
- Current and voltage alarming: For each measuring point in a UPDU, a set of four thresholds (critical low, warning low, warning high, critical high) can be configured for the voltage and current values. If a measurement crosses a threshold, a message is logged (and sent to the remote syslog server). See the section "UPDU Object Configuration" in the CLI manual for more information.

UPDU objects such as modules or outlets have been renamed or assigned a stable identifier. For example, outlets are called `OutletM.N` where `M` is the module number and `N` the outlet number as shown on the UPDU case (e.g. `Outlet4.3`). Consequently, the arguments to the `outlet [on|off|cycle]` CLI command changes from `outlet [on|off|cycle] 4.3` to `outlet [on|off|cycle] Outlet4.3`.

New features

- Add current and voltage monitoring (#619)
- CLI: Add "[include|exclude|begin] pattern" output filtering
- Add bootloader version to "show version" command (#622)
- CLI: Schedule reboot with "reboot in" command. (#307)
- Web UI: User profile page with password change.
- Add syslog support
- Add "show power description" and "show energy description" commands
- Add user-configurable object description (#610)
- Web UI: Show interface MAC addresses (#585)
- Web UI: Outlet power cycling (#500)

Enhancements

- Improve module upgrade speed
- Switch to umm-malloc heap. (#540 and #579)
- Add "show log utc" to show the log with UTC timestamps (#604)
- Add more information to "show version" output (#593)
- CLI: Improve TAB-completion to complete to the longest common prefix (#595)
- Improve settings save performance (#543)

Bug fixes

- Better support for the RN3003

Release 2.4.0

This release adds a Secure Shell server (SSH). The CLI, which is accessible through the AUX3 serial console and through Telnet, can now also be accessed through an encrypted SSH channel. As a consequence, Telnet is now disabled by default. It is strongly recommended to check that Telnet is disabled and if necessary, set Telnet to `disabled` after the upgrade.

For SSH, a reasonably recent SSH client is required (at least OpenSSH 7.3 or Putty 0.71).

In the CLI, commands can now be abbreviated to the number of letters that makes them unique (e.g. `sh co` for `show config`).

New features

- CLI: Allow command abbreviation (#527)
- Add SSH server

Enhancements

- Reduce network stack thread pool (#581)
- Increase HTTP connections stack size (#580)
- Renew built-in HTTPS certificate (#565)
- Increase memory reserved for the network stack (#542)
- Disable telnet in the factory settings (#578)
- Don't reconfigure IPv4 if nothing changes (#575)
- CLI: User configuration more user-friendly (#574)
- CLI: Terminate modes and sessions using CTRL-D (#563)

Bug fixes

- CLI: Allow demoted user to leave configuration mode (#577)
- Fix telnet connection close (#572)
- CLI: Optimize tab-completion redraw (#570)
- Fix network services shutdown to properly return resources (#566)
- Fix serial console blocking issue (#564)

Release 2.3.0

This release features a completely new command line interface with new commands. The CLI is accessible through the serial console on AUX3 and through telnet.

For more information refer to the CLI reference manual bundled with the release.

New features

- New UDPU CLI
- Serial console requires user authentication

Enhancements

- Web: Remove buttons to switch all outlets of a module (#562)
- Relay power cycle functionality (off, 5 s wait, on)
- Clamp max humidity to 99.9% (#510)
- Reformat SNMP SysDescr field (#504)
- Only upgrade POM/PIM when the version changes (#301)
- Disable logging to the console, add "show log" and "clear log" (#493)

Bug fixes

- Fix SNMP SysUpTime wrapping after 49.7 days (#534)
- Fix GreenPAK part-number readout (#511)

Release 2.2.0

New features

- Add spanning tree protocol support on ETH1/ETH2 (#455)

Enhancements

- Add "show version" shell command, remove "fw versions|details"
- Simplify settings load order (#494)
- Disable shell commands: resize, history, shell
- Add meter data expiration (#481)
- Upgrade RTOS to version 2.6

Bug fixes

- Improve IP settings validation (#434)

Release 2.1.0

New features

- Add support for PIMs connected via RS485
- Enable ETH3, including a default outgoing interface configuration option
- Add fallback to AutoIP when IPv4 is configured to DHCP (#411)

Enhancements

- Improve the “show power” and “show energy” output (#478)
- Improve the “show topology” output (#378)
- Add RCM screen if more than one RCM is found
- Show “N/A” in overview screen when no measurements are available (#440)
- E3BUS improvements (RX thread)
- Poll network interface state in web app (settings page)
- Add “show e3bus rtt” command (#360)

Bug fixes

- Fix “e3bus reset” blocking infinitely (#452)
- Fix potential TCP stack deadlock (#418)
- Detect missing and extra POMs
- Print error when the “relay” shell command is used on modules without relays (#379)
- Wake up screen when auto-off is disabled (#427)

Release 2.0.1

Bug fixes

- Fix the migration of pre-2.0 network settings causing ETH1 to be disabled (#433)

Release 2.0.0

New features

- DNS configuration per interface (#410)
- Rename "show uptime" shell command to "show time" and add current date & time (#354)

Enhancements

- Use CycloneTCP network stack (#346)
- Add hostname validation (#426)

Bug fixes

- Fix "rcm info" command failing and locking the shell (#424)
- Fix inconsistent parameters checking for SNTP configuration (#422)
- Fix web server settings not applied after a reboot (#386)

Release 1.4.3

Bug fixes

- Fix initial PoE PSE state (#409)
- Switch off POM module LEDs when booting (#401)
- Add "fw usbflash" shell command that is only available in factory mode.
- Add a no voltage threshold factory configuration defaulting to 20V (#241)
- Fix PoE/AC detection and refactor power manager (#370)

Release 1.4.2

Bug fixes

- POM: Fix LED timing (POM 2.1.2)(#393)
- Improve factory dongle robustness (#388)

Release 1.4.1

Internal release.

Release 1.4.0

New features

- Add support for RCM sensor
- Web UI:
 - Add network settings
 - New environment page showing sensor values (temperature, humidity)
- Long press on CANCEL/DOWN allow doing a factory reset

Enhancements

- `conf get net` command shows all network interfaces
- Separate link and IPv4 configuration (`conf set net [link|ipv4]`)
- Improve display responsiveness when in MODULE mode
- Improved display drawing speed
- Show static IP address even when Ethernet link is down
- POM:
 - While the button is pressed, the module LED is blue
 - LEDs are now driven independently of the ICM
- Add support for the factory dongle, remove `conf factory unlock` command
- Automatically reboot the ICM when resetting the settings via the shell

Bug fixes

- POM: Fix LED timing issues
- Fix values truncated instead of rounded in SNMP and on display

Information

- After installing this version it won't be possible to downgrade to a lower version
- New POM LED behavior:
 - Phase LED:
 - * While powering up, the phase LED shows red, then orange, and finally green
 - * red: Shows a critical condition:
 - GreenPAK not found or unsupported
 - FRAM not found or unsupported
 - Led-string problem (e.g. number of LEDs differs from the configured LEDs)
 - Missing calibrations
 - Permanent problem communicating with the ADCs
 - * orange: Shows a temporary condition
 - Both up- and downstreams are not OK
 - Powermeter task is in error state (tries to recover)
 - * green: All OK
 - Outlet LEDs:
 - * red: Voltage <50V
 - * green: Voltage is 230V +/- 10%
 - * blink red: Otherwise

Release 1.3.1

New feature

- Support for Manchester de-modulator revision 2 (GreenPAK).

Release 1.3.0

New features

- Support for environmental sensors on AUX ports
- Web UI:
 - Add settings page
- Local UI (display):
 - Add ENVIRONMENT screen
- Command line interface:
- Add "show sensor" command

Enhancements

- Increase serial console and telnet ringbuffer

Bug fixes

- Truncated SNMP community strings
- Wrong SEMC clock frequency

Known limitations

- ETH3 (100MB/s Ethernet) is disabled