

EmberZNet SDK 6.4.0 GA

Silicon Laboratories, Inc.

September 15, 2018

1 Release Highlights

1.1 Version 6.4.0 GA:

- Beta low power support for DMP BLE + Zigbee
- Green Power Combo support (GPPB + Sink)
- RAIL support for GB Smart Metering Sub-GHz PHYs
- NVM3 support for Zigbee single protocol
- IAR EWARM 8.30.1 support
- Various bug fixes

2 Using This Release

This release contains the following

- Gecko SDK 2.4.0
- Zigbee stack EmberZNet Pro v6.4.0
- Zigbee Application Framework v6.4.0
- Zigbee Sample Applications

For more information about the Silicon Labs EmberZNet Pro stack see UG103.02 - Zigbee Fundamentals. If you are a first time user, see QSG106: Getting Started with EmberZNet Pro.

2.1 Compatible Software:

The Zigbee stack should be used in conjunction with the Silicon Labs Simplicity Studio V4 development platform. Simplicity Studio ensures that most software and tool compatibilities are managed correctly. Install software and board firmware updates promptly when you are notified.

This version of the SDK is compatible with the following tool chains.

- IAR Embedded Workbench for ARM (IAR-EWARM) version 8.30.1. Follow instructions in QSG106: Getting Started with EmberZNet Pro, to download from the support portal, and obtain a 30 day trial license.
- GCC (The GNU Compiler Collection) version 7.2.1 is provided with Simplicity Studio.



IAR builds in Simplicity Studio are fully supported. However, an issue has been identified when using wine to build with the IarBuild.exe command line utility or IAR Embedded Workbench GUI on macOS or Linux. This could result in incorrect files being used due to collisions in wine's hashing algorithm for generating short file names.

It is not recommend for customers on macOS or Linux to build with IAR outside of Simplicity Studio. Customers who do should carefully verify that the correct files are being used.

2.2 Support

Development Kit customers are eligible for training and technical support. You can use the Silicon Laboratories web site <http://www.silabs.com> to obtain information about all Silicon Labs Zigbee products and services, and to sign up for product support.

You can contact Silicon Laboratories support at <http://www.silabs.com/support>

3 Added Items

3.1 Version 6.4.0 GA:

3.1.1 New Stack APIs:

- **emberGetBeaconClassificationParams**
emberSetBeaconClassificationParams
Get or set beacon/node prioritization parameters which are used during (re)join process. E.g. one can choose `PRIORITIZE_BEACONS_BASED_ON_TC_CONNECTIVITY` so that nodes with trust center connectivity get higher priority.
- **emberGetAvgParentRssi** Retrieves average rssi value between this device and its parent.
- **emberGetParentId** Retrieves the short id of this device's parent.

3.1.2 New Plugin Options:

- Network Creator Security Plugin
 - **Allow Trust Center rejoin with well known key** The TC will allow rejoining of a device using the well known key for the number of seconds mentioned in the timeout option below.
 - **Allow Trust Center rejoin with well known key timeout (seconds)** The TC will allow rejoining of a device using the well known key for the seconds mentioned here unless it has been set to 0 in which case trust center rejoin with well known key will be allowed forever.
- Network Find Plugin
 - **Enable scanning all channels** Enable scanning all channels when forming and joining if none of the preferred channels are found suitable. Use `emberAfPluginNetworkFindGetEnableScanningAllChannelsCallback()` to override this option.
 - **Cut-off value (dBm)** The maximum noise allowed on a channel to consider for forming a network. If the noise on all preferred channels is above this limit and "Enable scanning all channels" is ticked, the scan continues on all channels. Use `emberAfPluginNetworkFindGetEnergyThresholdForChannelCallback()` to override this value.
- OTA Bootload Cluster Server

- **Dynamic Block Period Download Timeout** This option's value dictates the amount of inactivity in seconds before the server purges a client from the dynamic block period downloads. This value must be greater than the 'Test Block Period Value' below, otherwise a client who resumes querying after a test delay will be immediately purged.
- **Test Block Period Value** The value a client is told to delay when determining whether it treats the Minimum Block Period as seconds or milliseconds. When a client begins an OTA download, it is sent a Minimum Block Period with this value. The amount of time that the client delays determines whether it treats this value as seconds or milliseconds (the client's delay time is judged against a threshold of this configured value). It is recommended that this value not be less than the longest expected delay time in the network, as sleepy end devices may delay longer than the Minimum Block Period amount, which tricks the OTA server into thinking that the client treats this value as seconds. Once the client is judged to be using seconds or milliseconds, the Minimum Block Period will revert to being the value contained in the `otaMinimumBlockPeriodMs` variable, which is settable with `"plugin ota-server policy image-req-min-period."`
- ZigBee Light Link Library
 - **Apply RSSI threshold to all interpan messages** True if the RSSI threshold is to be applied to all incoming touchlink interpan messages. This is not required by the Zigbee 3.0 specifications, but may be useful for testing in a busy environment.

3.1.3 New CLI commands:

- **plugin ota-server policy client-delay-units** For testing, force the server to treat the Minimum Block Period in a certain unit (see `ota-server-policy.h` for values).

4 Changed Items

4.1 Version 6.4.0 GA:

- The OTA dynamic block period feature on the OTA server has been improved to send a test delay to a client. The amount of time a client delays will be used to judge whether the client treats the Minimum Block Period field as seconds or milliseconds. The server no longer reads the client's OTA Cluster Revision attribute to determine delay units. Please see the OTA server plugin and its options for further information.
- When forming and joining the network, a new option now allows to search on all channels if no suitable channel has been found in the channel mask. The threshold can be set in App Builder and overridden by an application callback. The band selection scan mode applies if the sub-GHz support is included.
- The Zll Commissioning plugin will now allow a value of zero seconds for the `RxOnAtStartupPeriod`, which will have the effect of disabling the feature completely, for example, for a sleepy remote control which is never intended to be a touchlink target.
- The ZigBee PRO Leaf Library is now available for XNCP configuration.
- Micrium RTOS plugin - The system start task is removed from the plugin and its functionality is moved to the zigbee task, such as to configure and start other tasks. This saves the application up to 2 kB of RAM using NVM3 and up to 1 kB of RAM using SimEE1.
- Prepayment Alarm Status attribute changed to non-writable as per CCB 2314.
- Multi-network operation was disabled on 256kB EFR32 parts to save flash memory. If you need to re-enable it, please contact Silicon Labs Support.
- Pre-built NCP images no longer contain multi-network support. Support can still be added via XNCP configuration.

- The default setting for `EMBER_PAN_ID_CONFLICT_REPORT_THRESHOLD` has been changed from 1 to 2. This requires two PanID Conflict reports to be received within a minute to trigger a panID change. This dramatically reduces the chance panID thrashing due to corrupt beacons that pass the CRC check and trigger a false PAN id conflict, which can happen occasionally in large dense networks.
- Within the Network Creator plugin, the max value for the Radio Power field has been increased from 8 to 20 dBm.
- The info command has been updated to include the device's parent's nodeID and average rssi.
- **Z3 Test Harness**
 - Disallow insecure rejoins for a node on a distributed network - this is now enforced in 'emberFindAndRejoinNetworkWithReason' (an 'Invalid Operation' status will be returned) as well as in the End Device Support plugin.
 - Disable the delay on network leave (the delay which allows a leave announcement to propagate) if the Z3 Test Harness plugin is selected, for compatibility with the Zigbee Alliance test tool.
 - Change to the ZLL scan request processing such that the initiator bit is only set in the touchlink information field in a scan request if the initiator is address-assignment-capable, rather than unconditionally, as was previously the case.
 - Since the ZCL specification states that it is mandatory to write the current channel to the ZLL scan response, the ZLL library configuration option is not required, and has therefore been removed.
 - RSSI threshold for incoming scan requests has been changed, both as a default for the ZLL library option setting and in touchlink target sample applications. Previously, we used a value of -128 for the RSSI threshold for incoming scan requests, which would in practice allow all incoming requests. We have also added a ZLL stack library option to apply the threshold to all interpan messages (for example, scan responses), as an aid to testing in a busy environment.
 - Added additional validation to an incoming touchlink interpan command to check that the source address in the MAC header is the same for a scan response as for a network join/start response.

5 Deprecated Items

5.1 Version 6.4.0 GA:

- Prebuilt NCP images for all platforms (found in the `ncp-images/` directory) are targeted to be removed in the next release. Customers are recommended to utilize the XNCP framework to customize and build their own NCP images.

6 Removed Items

6.1 Version 6.4.0 GA:

- Support for the infrared-led plugin has now been removed. Any app using the infrared-led plugin will need to be updated to not use it.

7 Fixed Issues

7.1 Version 6.4.0 GA:

- 185603 An issue has been fixed where calling `ezspSendBootloadMessage` would cause a crash when called on newer NCPs that are supposed to include `bootloadMessage` functionality.
- 261038 A warning in `COM_Unused` has been fixed by changing the type of the port argument.

- 277510 An issue with the EM35x SPI NCP nWAKE handshake has been resolved.
- 281833 An issue where the green power common plugin would malfom the Green Power Pairing Response frame has been resolved.
- 290265 Added minor changes to the code to alleviate the sleep cycle issue in sleepy end-devices with unreachable parents. The end-device should now go to sleep independently without requiring to disable EMBER_APS_OPTION_RETRY or to do extra polls during delivery process.
- 298029 A build failure has been fixed for SPI-based xNCPs when disabling nWAKE functionality.
- 298594 Fix a couple of race condition scenarios on an end device touchlink initiator, if a touchlink operation is performed at the same time as a rejoin.
- 300270 Fixes a bug where a leave announce, with the IEEE address field present in the NWK header, was incorrectly treated as a leave request.
- 300272 Fixes a problem where a unicast ZDO request from a router to one of its sleepy children would get incorrectly routed, and a ZDO response would get sent to the child instead.
- 303020 The attribute ID of ZCL R7 Color Control cluster's StartUpColorTemperatureMireds attribute had been corrected from 0x400E to 0x4010, and support for that attribute is implemented in the color-control-server plugin.
- 307886 When a Z3Gateway host application is launched using the -v flag to direct application output to a port, and a telnet connection is established on port 4901, disconnecting the telnet connection can cause CPU utilization to climb to 100%. The problem was reported for the host application running on Linux platforms, first observed on an Ubuntu 16.04 VM and subsequently replicated on a RaspberryPi.
- 313109 Reduced vector table alignments of dies such that they are now as minimum as required for IAR builds
- 313303 A bug in the gas-proxy-function plugin relating to an uninitialized variable is fixed, which was causing incorrect values of CurrentMonthAlternativeConsumptionDelivered to be calculated.
- 313989 MFGLIB may be used on Sub GHz channel regardless of the network setting.
- 315803 Several coverity failures have been repaired.
- 317234 Fixed an issue that could cause register corruption in very rare conditions due to a bus access race condition. The specific registers impacted were limited to those related to the radio and the corruption was most likely when running the coherent IEEE802.15.4 PHY on the EFR32xG12 and EFR32xG13 platforms. On other platforms and PHY configurations the issue is possible though very unlikely and never observed.
- 318018 EM3xx GCC applications now use the C startup routines found in platform/Device rather than those found in platform/base.
- 331623 Fixed an issue where the ZLL stack tokens were not being initialized by a touchlink Factory Reset command. In particular, the factory new bit was not being set.
- 331815 Fixed bug that caused NCP Applications compiled with GCC to not start correctly.
- 333590 Fixed a problem where the radio idle mode is getting reverted (i.e. potentially switched off) in the case of an aborted touchlink, even if 'Rx always on' mode is in operation. (In practice, this issue is only likely to affect router initiators which are also touchlink targets, i.e. it is very much a corner case)

- 333594 This is a fix to set the interoperability bit in the touchlink info field in the ZLL Scan Response according to the plugin setting - previously, it was set unconditionally. This means that the relevant plugin option needs to be set to 'true' for targets as well as for initiators, and it has therefore been changed accordingly for a number of sample applications.
- 334252 This fixes a problem where the Source Pan Id in both the Mac header and the Aps payload for touchlink interpan messages were set incorrectly. The two must match, and be in the valid range 0x0001 to 0xffff, but they were previously both set to 0xffff for a factory new device, which was both non-compliant according to the ZCL specification, and the cause of interoperability issues with legacy touchlink initiators.
- 334492 Stub versions of COM.InternalPowerUp/Down functions have been corrected to match the argument list of the non-stub versions.
- 334555 Added support for Occupancy Sensing Cluster's OccupancySensorTypeBitmap attribute (ID 0x0002) . The value of this attribute is set to a value consistent with the value of the existing OccupancySensorType enumeration attribute (ID 0x0001).
- 334816 This fixes a problem where the child status is not correctly set in its parent's child table following a network leave command with rejoin bit set. This means that a subsequent network leave or aps remove device command will cause the parent to remove the child directly, instead of sending a network leave command to the child, hence the child, unaware of the parent's action, will continue to poll, and the parent, on receiving the unexpected data request, will then send a network leave request to the child, this time with the rejoin bit set. The end result is that an aps or network leave after a network leave with rejoin will not succeed, since the child will always rejoin."
- 335841 Fixed a timer issue that prevent EM4 sleep from working properly.
- 336177 An issue was fixed where nodes failed to join a Z3.0 coordinator after entering "plugin network-creator-security open-network" multiple times without issuing a "plugin network-creator-security close-network." The joining nodes would be sent a Transport Key not encrypted with the well-known key, thus failing to obtain the network key and failing to join the network.
- 336755 An issue has been fixed where a multi-network device, acting as a trust center, failed to store a link key after performing Certificate Based Key Establishment (CBKE) with a joining device. The multi-network device would previously attempt to store the link key while not on the trust center network.
- 337207 An issue was corrected where a node would always send route records to a high ram concentrator when it was a one hop neighbor, rather than only on the initial packet following a many to one route request.
- 337431 A bug keeping a sleepy end device awake during the short poll interval has been resolved.
- 343247 Fixed a bug in the sim-eeeprom2-1to2-upgrade-library that could result in lost token data or an infinite reset loop due to incorrectly identifying a non-existent SimEEv1. The upgrade library could read out of bound addresses or incorrectly attempt an upgrade which was impossible. EmberZNet versions affected are 6.3.1.0 and earlier. Devices using these versions should either disable the SimEE v1 to v2 upgrade library and use the stub library instead, or update to EmberZNet 6.4.0.0 or later.
- 343807 A watchdog reset has been fixed in the SIMEE2 to NVM3 upgrade library when a large number of tokens are migrated.

8 Open Issues

8.1 EmberZNet Open Issues:

- 60757 Indirect Transaction Expiry route error not being sent when TX failure count is reached on parent router.

- 60774 MTORR reception by concentrator neighbor sometimes causes assert in route-discovery.c (emHandleRouteCommand).
- 60858 Sleepy broadcast payload is sometimes corrupted when relaying to child
- 60868 Extra retries seen on ZDO requests; ZDO response going out before APS ACK.
- 60944 EZSP-SPI NCP may become unresponsive if callbacks are received during ECC operations.
- 60970 TC link key should be used for Transport Key to rejoining devices even if decision is Send Key In Clear
- 60975 EZSP_VALUE_TOKEN_STACK_NODE_DATA, EZSP_VALUE_UART_SYNCH_CALLBACKS, EZSP_VALUE_MAXIMUM_INCOMING_TRANSFER_SIZE, and EZSP_VALUE_MAXIMUM_OUTGOING_TRANSFER_SIZE ValueIDs are writable but not readable.
- 61008 Scanning state machine (stack level or form-and-join util) can get stuck in "scanning" state indefinitely
- 66508 Framework should avoid sending unicast loopback messages with APS security since stack doesn't support this
- 66785 Messaging Client plugin should differentiate between Cancel Msg command and timed out / replaced message
- 66786 "zcl ota server reload" doesn't properly reload image info when using OTA Simple Storage plugin
- 66944 Duplicate Key Confirm Response message can lock up KE plugin state machine
- 70799 Overlay of RESETINFO on CSTACK causes IAR stack overflow warning
- 82600 Setting a non-zero MAC Filter Table Size but no MAC Filter Table Entries causes NCP resets when joining a network
- 86948 Fragmented messages can be passed to the application with old data from the rxFragmentedPacket buffer
- 92147 ZLL Scan Response Should Be Sent at Power 0 rather than last-used power level
- 103833 Second energy scan request caught in first energy scan request knocks node out of network.
- 106307 Nodetest calChannel command does not wake the radio to work properly.
- 119037 Packet-buffer.c Assert at line 352 occurs during rapid packet transmission and Partner-link-key-exchange.
- 119828 ota-client.c does not use the server EUI64 in Partner Link Key Exchange.
- 119939 ZDO IEEE Request's APS ACK proxied by parent incorrectly includes long source address.
- 121984 Turning off NCP concentrator support does not disable all stack concentrator logic.
- 126087 Sleepy end device would return NO_LOCAL_RESOURCES when a coordinator initiates key establishment with it in Multi-networking.
- 135649 Multi-networking can cause APS frame counter confusion between networks. Workaround: Use emberAfSecurityInitCallback to add EMBER_NO_FRAME_COUNTER_RESET to EmberInitialSecurityBitmask.
- 158598 OTA Client plugin's Bootloading Message Timeout doesn't account for Short Poll Interval being longer than the default and may spuriously time out messages before the sleepy client has had a chance to poll for the response.

- 162190 Fixed issue in packet reception that could cause misprocessing of non-ACK-requesting packets after an ACK with frame-pending bit set was sent.
- 180028 OTA Client Plugin should send ZCL Default Response to messages with wrong Mfg Code
- 192041 End devices may initiate route discoveries unexpectedly
- 201417 Adding GPIO Sensor Interface plugin to an EM358x project results in error: "identifier "GPIO_SENSOR_IRQ" is undefined".
- 213424 Problem with ZLL Devices responding to a multicast addScene when they should not.
- 229938 ZLL devices are sending ZLL device information frames with the 0x0104 HA/Z3 common profile ID instead of 0xC05E ZLL profile ID.
- 235222 Virtual UART (VUART) works on Ethernet but does not work over USB on WSTK.
- 251287 To achieve the lowest current during sleep on EFR32xG12, EFR32xG13, and EFR32xG14 parts, you must turn on voltage scaling. However, the radio will not operate with voltage scaling turned on, so to turn it on you must also make sure to disable it after each wake-up. Furthermore, some resets will not turn off voltage scaling, so please ensure that it is disabled before attempting to turn on the radio. Note that there is a ramp when turning voltage scaling on or off, so enabling this feature may increase the time it takes to go to sleep or wake up.
- 261670 Harden the ZLL touchlink process to mitigate malicious attacks
- 266341 Z3 Light sample app has two endpoints that support similar cluster commands, so duplicate responses may be generated for certain commands.
- 267722 Centralized Trust Center in Zigbee 3.0 security mode doesn't allow more than 10 devices to join during the Network Creator Open Network period
- 271644 A device that performs a classic join to a legacy ZLL gateway may eventually leave the network on its own initiative.
- 274414 AFv2 blank app project template for SOC and Host should use Z3 defaults, not ZHA defaults
- 278063 Smart Energy Tunneling plugins have conflicting treatment/usage of address table index
- 281231 Enabling Serial 3 or USB functionality on EM358x and EM359x may cause memory management faults and other errors. As EM358x and EM359x USB support has been deprecated, please ensure that Serial 3 and USB functionality are disabled.
- 281832 Green Power Common plugin incorrectly formats groupList and groupListCount parameters of GP Pairing Configuration frame.
- 289569 network-creator plugin power level picklist doesn't offer full range of supported values for EFR32
- 295498 UART reception sometimes drops bytes under heavy load in Zigbee+BLE DMP use case
- 301024 Currently the Dynamic Multi-Protocol Sample applications do not build with GCC, they require the IAR compiler due to dependencies on both the BLE and Micrium stacks.
- 303943 ezspGetStandaloneBootloaderVersionPlatMicroPhy only reports the major and minor version, excluding the build number, when used with the Gecko Bootloader
- 305621 Sleepy end devices staying awake for extended periods of time. After a failed APS_RETRY procedure, an application should attempt to repair the broken link or freeze outgoing aps-retried unicasts until the link is fixed in order to preserve battery life.

- 312291 The `halCommonGetIntxxMillisecondTick` functions on linux hosts currently use the `gettimeofday` function, which is not guaranteed to be monotonic. If the system time changes, it can cause issues with stack timing. The workaround is to modify these functions to use `clock_gettime` with the `CLOCK_MONOTONIC` source instead.
- 315661 Seeding of the random number generator on EM3xx can take ~400 milliseconds.
- 316212 The UART XMODEM standalone gecko bootloader with the legacy ebl parser can fail to return to the bootloader menu if the XMODEM transfer is interrupted unexpectedly (such as due to a power cycle). If the ebl file format is a requirement, then a recovery pin must be implemented to mitigate the risk.
- 331438 Service discovery may time out too quickly in busy networks. Define `EMBER_AF_DISCOVERY_TIMEOUT_QS` to customize the timeout period.
- 333146 The coexistence plugin behavior has changed to be required for all applications. By default coexistence functionality should be stubbed out when not configured via board header (EM35x) or not enabled via `HWCONF` (EFR32). Appbuilder may automatically enable the `HWCONF` coexistence module without warning which can trigger an error for dynamic multiprotocol applications, which do not yet support coexistence.
- 336103 Device reset will cause the network status of a sleepy end device to toggle if parent info is persisted in token.
- 336696 Idle-sleep minimum wake-time plugin option can cause sleepy-end device to stay awake longer than expected. This behavior does not occur when using the default value of 0 for minimum wake-time
- 338151 Initializing NCP with a low packet buffer count value may cause corrupt packets.
- 340003 The issue will cause watchdog reset after the joining device adds the transient link key which is different from the TC.
- 342334 Outstanding Coverity issues.
- 342464 An issue has been identified that can cause the EFR32 serial driver state to get out of sync with the actual contents of the buffer. This can result in partial or old data being returned.

9 Intended Behavior

10 Documentation Changes

11 History