Manuals+ — User Manuals Simplified.

SILICON LABS 7.4.5.0
Zigbee Ember Z Net SDK

SILICON LABS 7.4.5.0 Zigbee Ember Z Net SDK User Guide

Contents

SILICON LABS 7.4.5.0 Zigbee Ember Z Net SDK

Specifications

- Zigbee EmberZNet SDK Version: 7.4.5.0 GA
- Gecko SDK Suite Version: 4.4
- Release Date: October 23, 2024
- Platform: Silicon Labs
- Supported Compilers: GCC (The GNU Compiler Collection) version 12.2.1
- EZSP Protocol Version: 0x0D

Product Usage Instructions

Key Features
The Zigbee EmberZNet SDK by Silicon Labs offers the following key features
Multiprotocol (CMP) Zigbee and OpenThread support on SoC.

Compatibility and Use Notices
For security updates and notices, refer to the Security chapter of the Gecko Platform Release notes or visit the TECH DOCS tab on Silicon Labs website. It is recommended to subscribe to Security Advisories for the latest information.

Compatible Compilers
Make sure to use the correct files with the supported compiler
GCC (The GNU Compiler Collection) version 12.2.1 provided with Simplicity Studio.

EZSP Protocol
The EZSP protocol version for this release is 0x0D.

FAQ

- **Q: What are the new components introduced in release 7.4.5.0?**
  - A: Users can now have multiple zigbee_direct_security components enabled on a Zigbee direct device (ZDD) application, with the actual security option depending on the Zigbee Virtual Device (ZVD) configuration.
- **Q: What are the new APIs added in release 7.4.4.0?**
  - A: New APIs include mfglibSetCtune and mfglibGetCtune.
- **Q: What is the new platform support introduced in release 7.4.5.0?**
  - A: EFR32MG24A020F768IM40 is now supported as a platform.
- **Q: Where can I find updated documentation for the Zigbee Secure Key Storage component?**

Zigbee EmberZNet SDK 7.4.5.0 GA

Gecko SDK Suite 4.4

October 23, 2024

Silicon Labs is the vendor of choice for OEMs developing Zigbee networking into their products. The Silicon Labs Zigbee platform is the most integrated, complete, and feature-rich Zigbee solution available.
Silicon Labs EmberZNet SDK contains Silicon Labs' implementation of the Zigbee stack specification.

These release notes cover SDK version(s)

- 7.4.5.0 released October 23, 2024
- 7.4.4.0 released August 14, 2024
- 7.4.3.0 released May 2, 2024
- 7.4.2.0 released April 10, 2024
- 7.4.1.0 released February 14, 2024
- 7.4.0.0 released December 13, 2023

Compatibility and Use Notices

For information about security updates and notices, see the Security chapter of the Gecko Platform Release notes installed with this SDK or on the TECH DOCS tab on **https://www.silabs.com/developers/zigbee-emberznet** . Silicon Labs also strongly recommends that you subscribe to Security Advisories for up-to-date information. For instructions, or if you are new to the Zigbee EmberZNet SDK, seeUsing This Release.

Compatible Compilers
IAR Embedded Workbench for ARM (IAR-EWARM) version 9.40.1.

- Using wine to build with the IarBuild.exe command line utility or IAR Embedded Workbench GUI on macOS or Linux could result in incorrect files being used due to collisions in wine's hashing algorithm for generating short file names.
- Customers on macOS or Linux are advised not to build with IAR outside of Simplicity Studio. Customers who do should carefully verify that the correct files are being used.

GCC (The GNU Compiler Collection) version 12.2.1, provided with Simplicity Studio.

The EZSP protocol version for this release is 0x0D.

New Items

New Components

New in release 7.4.0.0
The "zigbee_direct_security_p256" and "zigbee_direct_security_curve25519" components have been added so that users can con-figure a specific Zigbee Direct security option.
Users are allowed to have multiple "zigbee_direct_security" components enabled on a Zigbee direct device (ZDD) application. In this case, the actual security option depends on the Zigbee Virtual Device (ZVD) configuration.

New APIs

New in release 7.4.4.0
Introduced two dedicated manufacturing lib APIs to get and set CTUNE values.
In earlier patch releases the access to and setting of CTUNE value became part of the RAIL APIs. In this patch a set of manufacturing APIs that encapsulate the RAIL APIs are introduced as follows to set and get the value.
mfglibSetCtune
mfglibGetCtune

New in release 7.4.2.0

- Extended SPI NCP to support sleep modes in some Host-NCP use cases.

  In this use case the SPI NCP can be configured as a sleepy end device. The host Z3Gateway sample application is extended with additional custom CLI code responsible for commanding the NCP to enter one of the sleep modes through the custom CLI command sleepMode, and must wake up using the custom CLI command wakeup before further EZSP communication.

- Introduced a new API sl_zigbee_af_isr_event_init to initialize the application framework events that are intended to be activated inside an interrupt service routine(ISR). These events, which are scheduled from the ISR, must have a delay parameter of 0 milli-seconds. In other words, events from ISR must be activated as an immediate event. There is no event deactivation allowed inside ISR.

  The reason for the above is as follows: The event system manipulates the event queue during scheduling (activating with a non zero delay, or deactivating) an event. To minimize the latency, an ISR should activate an event with 0 delay, which gets scheduled in the next event queue processing. This allows the further delay, or deactivation, to be carried out after the ISR exits. To distinguish the events intended to be used inside ISR context, the event structure is marked with an sli_zigbee_isr_event_marker during initialization.

  Refer to the zigbee_app_framework_event.h source file for details of this new function.

- Clarification on the use of the new function ember Update Multi Mac Rejoin Channel Mask For Selection Or Joining Device that is called inside the stack API ember Find And Rejoin Network With Reason to get a channel mask used for rejoining.

The SE1.4a specification restricts the change of interface (from 2.4GHz to sub-GHz or vice versa) during rejoining of a Multi-MAC Joining End device type device. Since the device type is an application framework configuration (that is, the joining end device type will be either a sub-GHz device or a 2.4 GHz device, not both, at configuration), this call provides the channel mask based on that configuration so that the rejoin mask is always same as the joining interface mask.

New in release 7.4.0.0

- Added a new API void sl_zigbee_token_factory_reset(bool exclude_outgoing_fc, bool exclude_boot_counter) to reset Zigbee NVM3 tokens to their default value.

- Added the API bool sl_zigbee_sec_man_link_key_slot_available(EmberEUI64 eui), which returns true if the link key table can add or update an entry with this address (table is not full).

Added a new API bool sl_zb_sec_man_compare_key_to_value (sl_zb_sec_man_context_t* context, sl_zb_sec_man_key_t* key), which returns true if the key being referenced by context has the same value as the key supplied in the argument.

New Platform Support

New in release 7.4.0.0
Zigbee stack support for the following new parts is added in this release: EFR32MG24A010F768IM40 and EFR32MG24A020F768IM40.

New Documentation

New in release 7.4.0.0
Updated the description for the Zigbee Secure Key Storage component to reflect the addition of Zigbee Secure Key Storage Upgrade (which adds backwards compatibility with existing projects).
Added a new application note for interacting with the Zigbee Security Manager group of components (AN1412: Zigbee Security Manager).

Intended Behavior
Users are reminded that Zigbee unsynchronized CSL transmissions are subject to protocol preemption at the radio scheduler. In the SleepyToSleepy applications, BLE can and will preempt a Zigbee CSL transmission, which will terminate the transmission. Scheduler preemption is more common for unsynchronized CSL, given that a potentially lengthy wake up frame sequence may be used. Users wishing to adjust transmission priorities may use the DMP Tuning and Testing component to do so. Users may also consult UG305: Dynamic Multiprotocol User's Guide for more information.

Improvements

Changed in release 7.4.0.0 ember Counter Handler API Doc Changes
In previous versions, the Counter Handler callback for MAC and APS layer Ember Counter Types concerning packet RX and TX was not being passed the passing proper target node ID or data arguments, and API documentation concerning behavior of certain counters that used these parameters was unclear or misleading.

While the signature of ember Counter Handler() has not changed, the way its parameters are populated have changed slightly.

- Comments around EmberCounterType enums in ember-types.h have been expanded for clarity.
- The Node ID parameter to the Counter Handler for TX-related counters now checks whether the destination address mode indi-cates a valid short ID before using it. (If not, no destination address is populated, and a placeholder value of
  EMBER_UNKNOWN_NODE_ID is used instead.)
- The Node ID parameter to the Counter Handler for RX-related counters now reflects the source node ID, not the destination node ID.
- Retry count is *not* passed as the data parameter for EMBER_COUNTER_MAC_TX_UNICAST_
  SUCCESS/FAILED counters as described in ember-types.h in previous versions, but this was never properly populated in previously released versions so its value in previous releases would always have been 0. This behavior has been clarified in the description of those EmberCounterTypes. However, the Retry count for APS

layer retries continues to be populated in the data parameter for EMBER_COUNTER_APS_TX_UNICAST_SUCCESS/FAILED counter types, to be consistent with prior releases.

- All counters that populate the Node ID or data parameter for the callback have been audited to ensure they pass the expected data, address, or EMBER_UNKNOWN_NODE_ID, if a Node ID was expected but could not be obtained from the packet, as described in the revised ember-types.h documentation.
- The Counter handler for EMBER_COUNTER_MAC_TX_UNICAST_RETRY now correctly reflects the MAC layer destination node ID and number of retries in its Destination Node ID and data parameters.
- The Counter handler for EMBER_COUNTER_PHY_CCA_FAIL_COUNT now provides destination node ID information through the Node ID parameter about the intended MAC layer target of the message that failed transmission.

Updated Green Power Code
Green power server code is updated with various improvements including

- Added more validation code for incoming commands with invalid endpoint when receiving on the GP server.
- Added code to handle the case when there is no more space to build Green Power messages.
- The sink now drops pairing configuration with action Remove Pairing in some cases per spec section A.3.5.2.4.1.
- The sink now saves the existing group list of an entry before removing when processing Pairing Configuration with action Extend.
- The Translation query command returns "NOT FOUND" as the error code when the translation table is empty or the index is bigger than number of entries in the table.
- Changed the version of GP endpoint in some apps from 1 to 0.

Using CSMA in the GPDF Send function is restricted because Green Power Devices are minimal energy devices and do not use CSMA in most of the designs. Instead, the preferred design is to send out multiple packets using the same energy budget.
Removed the use of a hidden endpoint in the Green Power Server plugin option. Use one of the application endpoints instead.

Network Key Update Plugin Code Improvements
Changed the periodic network key update period to be as long as 1 year.

Restructured Some APIs to Avoid Unnecessary Key Export
Made changes to favor the use of key contexts over plaintext key data.

- sl_zigbee_send_security_challenge_request now takes in an sl_zb_sec_man_context_t argument in place of EmberKeyData.
- The sl_zb_sec_man_derived_key_type enum's values are now a 16-bit bitmask to directly support certain key derivations that combine multiple derived types.

Fixed Issues

Fixed in release 7.4.5.0

ID #	Description
1357860	Fixed an issue that caused a crash when multiple end points start to initialize identify feedback event. (Other ref: 1348659)
1357517	Fixed an issue that caused crash when a multi-network app tries steering on the secondary network.
1356285	In rare cases, a packet may be passed to the Outgoing Packet Handoff Callback with a payload index parameter that exceeds the stated length of the packet buffer, leading to an assert in legacy-packet-buffer.c if the Packet Handoff component is enabled. The component's Incoming and Outgoing handler functions now catch this condition and discard the invalid packet without further processing. (Other ref: 1350285)
1355289	Fixed an issue that caused LQI Response to be received with MAC address as all zeros. (Other ref: 1351489)
1349160	- The Z3Gateway built on Raspberry Pi with kernel 6.6 failed to connect to NCP over SPI by default. Solution is to redefine the GPIOs as described here. - Note the following information on GPIOs that maps to the SPI NCP interface. On kernel 6.6, running sudo cat /sys/kernel/debug/gpio - That will display following gpio-520 (GPIO8) - gpio-534 (GPIO22) gpio-535 (GPIO23) gpio-536 (GPIO24) - Then redefine the GPIO for SPI NCP interface from above sysfs in spi-protocol-linux-config.h as #define NCP_CHIP_SELECT_GPIO "520" #define NCP_HOST_INT_GPIO "534" #define NCP_RESET_GPIO "535" #define NCP_WAKE_GPIO "536" (Other ref: 1297976)
1343044	If Fragmentation plugin miscalculated available payload for a unicast fragment, it could send more data to the NCP than will fit in a single packet after all stack overhead was accounted for. This could lead to memory corruption in the NCP that triggered assert failures or other unexpected behavior. (Other ref: 1289413)
1343012	Si4468 firmware patch added to phy-pro2plus-library to address race condition in sub-GHz Tx/Rx processing. (Other ref: 1341928)
1311214	Fixed additional default response generated when the incoming OTA server command ZCL message has default response enabled. Only one response to an error is sent, and for successful block image requests, no default response is set. (Other ref: 1300935)

1296653	If a dual-PHY NCP device were performing an Energy Scan on the sub-GHz band while the 2.4GHz radio was active, large bursts of incoming Beacon traffic in response to incoming Beacon Requests on the 2.4GHz radio channel could occupy a large amount of the stack's buffer memory (allocated from the Heap segment) while the many sub-GHz channels were being scanned, which could lead to buffer shortages and EZSP Overflow conditions if the Heap size (which determines how many buffers are available to the system) was not sufficiently large. This Overflow condition could prevent the Scan Complete Handler from reaching the host application, causing the app's scan state machine to be stuck forever. The Energy Scanning code for dual PHY devices now discards any Beacon packets received on the 2.4GHz radio during the scanning of a sub-GHz channel, thus preventing a large influx of beacons from creating the aforementioned problem. Note this does not prevent normal operation of the network on 2.4GHz as Beacons are only used for potential PAN ID conflict detection when the device isn't performing an Active Scan, and PAN ID conflicts can still be detected by other routers in the network during this time or by the coordinator once the Energy Scan has completed. (Other ref: 1276049)

ID #	Description
1295250	Fixed compile issues when adding test harness zigbee 3.0 component to a standard application. (Other ref: 1280058)
1294848	Added checks for the ZCL data array to accommodate the longest string length unto 253. (Other ref: 1275092)
1294843	Fixed missing initialization of local variables before use. (Other ref: 1275104)
1271968	- The zigbee_watchdog_periodic_refresh component is no longer used in the zigbee application framework and is deprecated in this release. - The watchdog timer is disabled by default for all the sample applications. There will be an improved watchdog component added to the SDK in the future. **Note** : Please ensure to enable the watchdog timer with configuration item SL_LEGACY_HAL_DISABLE_WATCHDOG set to 0 in your application.
1270721	Fixed an issue to improve multi hop joining of the devices. Upon device announcement, the address pair is added to the address cache. (Other ref: 1266351)

Fixed in release 7.4.4.0

ID #	Description
1334454	Fixed an issue in handling rejoin response. (Other ref: 1331580)
1330732	Diagnostic functionality should disable the interrupt after calling Iostream to avoid an assert when acquiring the mutex.
1330720	The EZSP_MAX_FRAME_LENGTH is reverted back to 220, allowing the maximum length of XNCP message to be 220 as well. (Other ref: 1327706)
1330311	Fixed an issue that caused some GP proxy tests to fail on RCP Host setup. (Other ref: 1328991)
1312369	Made SL_LEGACY_HAL_WDOG_IRQHandler() weak function, allowing customers to provide their own implementation.
1310711	Added compile time error checking for SL_STACK_SIZE when RTOS component is used in zigbee project.
1309913	Added mutex protection for App Framework event queue so that App Framework event APIs can be called from multiple tasks. (Other ref: 1252940, 1254397)
1309333	After a new end device joins on the sub-GHz band, the duty cycle aging data was mistakenly cleared for all end device children. (Other ref: 1296881)
1296002	An issue that caused Multiple definitions of the halAppBootloader function is resolved.
1295756	Stack events not marked interrupt-safe should not be scheduled in ISR context as this could create a race condition resulting in the event being dropped from the event queue. An instance of this prevented sub-GHz devices from properly scheduling MAC backoffs when this race condition was triggered. (Other ref: 1269856)
1294660	Fixed an issue where the network steering plugin could act as if the device was already on a network when it was not, being stuck in this invalid state until reset. This could be triggered by calling the network leave CLI command with precise enough timing while network steering was in the middle of joining a network and with a MAC scan still pending. (Other ref: 1293923)
1290695	Fixed an issue that dropped a ZLL commissioning packet for the use case when one endpoint is disabled while other endpoints are still enabled. The fix is added to check all the enabled endpoints. (Other ref: 1275586)

Fixed in release 7.4.0.0

ID #	Description
1019348	Fixed the dependency requirements for the Zigbee ZCL Cli component so that it can be removed when not needed.
1024246	Updated the function description for emberHaveLinkKey() and sl_zb_sec_man_have_link_key().
1036503	Added a description to recommend use of the Micrium Kernel for DMP sample apps.
1037661	An issue that was preventing the application to install either pro stack or leaf stack has been fixed.
1078136	Fixed an intermittent crash when modifying events from interrupt context
1081548	An issue has been fixed in CSL where a new wake up frame sequence that is received immediately following a previous payload frame would not be recorded correctly. This would result in a missed payload frame.
1084111	Initial sleepy SPI-NCP support for MG24 based boards is updated as part of this release.
1104056	Added support for network-steering to run on secondary network in case of multi-network
1120515	Fixed an issue where the channel did not change when using the mfglib set-channel command.
1141109	Fixed an issue that caused the generated sample application ncp-uart-gp-multi-rail to miss some header files when using the Green Power adapter component with the -cp option.
1144316	Updated the description of some data structure types in gp-types.h documentation.
1144884	Fixed spurious frame pending bit set when there is no data pending.
1152512	Fixed a potential crash in low-mac-rail when modifying the event in ISR context.
1154616	Added an exception for the condition to initialize the network with the case "Switching role from Sleepy End device to Non-sleepy End device".
1157289	Fixed an issue that may cause BDB test failure DN-TLM-TC-02B.
1157426	Fixed a build issue when building zigbee_simple_app with green_power_adapter component.
1157932	Added a condition to check if the "transition time" field is missing and set a default value 0xFFFF for this missing field.
1166340	Fixed an issue that was preventing the emberAfGpdfSend from sending out the intended number of repeated transmissions.

ID #	Description
1167807	Fixed an issue where devices acting as Trust Centers in distributed networks would incorrectly clear their transient link keys each time a new device joined.
1169504	Fixed an issue that caused reset of a sleepy device upon force wake up.
1169966	Fixed missing return value validation in buffer allocation code.
1171477, 172270	With mfglib start 1 no messages are transmitted but received, so the displayed terminal message "mfglib send complete" is wrong and changed to "RXed %d packets in the last %d ms".
1171935	Changed the periodic network key update period to be as long as 1 year.

1172778	Added the missing invocation of the emberAfPluginGreenPowerServerUpdateAliasCallback to the Green Power server..
1174288	Fixed an issue that causes the network steering process to assert if a call to stop ongoing scan is called.
1178393	Updated a documentation error.
1180445	In Smart Energy, OTA now continues to download if the Coordinator reaches Limited Duty Cycle.
1185509	Fixed an issue in CSL where a new wake up frame sequence that is received immediately following a previous payload frame would not be recorded correctly. This would result in a missed payload frame.
1186107	Fixed an issue that caused the unsuccessful decryption of received GPDFs to replace the incoming GPDF in the gp commissioning notification.
1188397	Fixed an issue that caused a compilation error when enabling extended report table size.
1194090	Corrected the failure status in the default response for Sink Commissioning Mode command – following section 3.3.4.8.2
1194963	Fixed an issue with memset being done for the commissioningGpd structure before calling user callback emberAfGreenPowerServerPairingStatusCallback.
1194966	Fixed an issue where the endpoint and proxiesInvolved fields were not set with the Exit Commissioning action.
1196698	Fixed a spurious frame pending bit set when there was no data pending.
1199958	Added code to handle the case when there is no more space to build green power messages.
1202034	Fixed an issue where sl_zb_sec_man_context_t stack variable was not initialized correctly, causing joining with install code to fail.
1206040	Calling emberRemoveChild() during a secure rejoin attempt by an end device can potentially lead to an extra decrement of the Child Count, potentially leading to a Child Count of -1 (255), inhibiting end devices from joining/rejoining due to an indicated lack of capacity in the Beacon.
1207580	Child Table search functions within the stack are inconsistent in use of 0x0000 versus 0xFFFF for node ID return value representing invalid/empty entries, leading to problems checking for unused entries in APIs like emberRemoveChild().
1210706	Destination and PHY Index provided in EmberExtraCounterInfo struct as part of emberCounterHandler() may have been incorrect for MAC TX Unicast counter types.
1211610 1212525	Fixed an issue where Dynamic Multiprotocol applications crashed after enabling Secure Key Storage Upgrade component.
1211847	While the signature of emberCounterHandler() has not changed, the way its parameters are populated have changed slightly. Changes around this API is explained in section 2 above.
1212449	Outgoing Beacons were incorrectly categorized by the MAC layer, leading to emberCounterHandler() failing to catch these packets with the EMBER_COUNTER_MAC_TX_BROADCAST counter type and instead counting the Beacons with the EMBER_COUNTER_MAC_TX_UNICAST_SUCCESS counter type. That potentially resulted in unreliable values for the dest EmberNodeId parameter passed to the EmberCounterInfo struct
1214866	Sending data poll packet in certain high traffic configurations may result in a bus fault.

1216552	An issue that causes an assertion under busy traffic conditions is fixed.
1216613	Fixed an issue which led to an incorrect value of groupcast radius in the proxy table.
1222509	Router/coordinator sends a leave & rejoin request to a non-child polling end device, but the MAC destination is 0xFFFF instead of matching the NWK destination address.
1223842	Fixed an issue with generation of the sl_component_catalog.h that was leaving unwanted code in it causing compilation failure.

ID #	Description
756628	Changed the invocation of application callback emberAfMacFilterMatchMessageCallback to only be called for the ZLL messages that are validated by the stack.
816088	Moved EMBER configuration from zigbeed_configuration.h to zigbeed.slcp.
829508	To avoid a race condition, additional validation was added in emberSetLogicalAndRadioChannel to return unsuccessful if the lower layers are busy or not in a state to change the channel.

Known Issues in the Current Release

Issues in bold were added since the previous release. If you have missed a release, recent release notes are available on **https://www.si-labs.com/developers/zigbee-emberznet** in the Tech Docs tab.

ID #	Description	Workaround
N/A	The following apps/component is not supported in this release: EM4 support.	Feature will be enabled in subsequent releases.
193492	emberAfFillCommandGlobalServerToClientConfigureRe porting macro is broken. The filling of buffer creates incorrect command packet.	Use the "zcl global send-me-a-report" CLI command instead of the API.
278063	Smart Energy Tunneling plugins have conflicting treatment/usage of address table index.	No known workaround
289569	Network-creator component power level picklist doesn't offer full range of supported values for EFR32	Edit the range <-8..20> specified in the CMSIS comment for EMBER_AF_PLUGIN_NETWORK_CREATOR_RADIO_P OWER in the <sdk>/protocol/zigbee/app/framework/plugin/network- creator/config/network-creator-config.h file. For example, change to <-26..20>.
295498	UART reception sometimes drops bytes under heavy load in Zigbee+BLE dynamic multiprotocol use case.	Use hardware flow control or lower the baud rate.
312291	EMHAL: 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.	Modify these functions to use clock_gettime with the CLOCK_MONOTONIC source instead.

338151	Initializing NCP with a low packet buffer count value may cause corrupt packets.	Use the 0xFF reserved value for packet buffer count to avoid the too-low default value
387750	Issue with Route Table Request formats on end device.	Under Investigation
400418	A touchlink initiator cannot link to a non-factory-new end- device target.	No known workaround.
424355	A non-factory-new sleepy end device touchlink target- capable initiator is not able to receive a device information response in certain circumstances.	Under Investigation
465180	The Coexistence Radio Blocker Optimization item "Enable Runtime Control" may block proper Zigbee operation.	Optional 'Wi-Fi Select' Control of Blocker Optimization should be left "Disabled".
480550	The OTA cluster has its own built-in fragmentation method, hence it should not use APS fragmentation. Although, in case APS encryption is enabled it grows the payload of the ImageBlockResponses to a size where the APS fragmentation is activated. This could lead to the OTA process failing.	No known workaround
481128	Detailed Reset Cause and crash details should be available by default via the Virtual UART (Serial 0) on NCP platforms when Diagnostics plugin and Virtual UART peripheral are enabled.	Since Serial 0 is already initialized in the NCP, customers can enable the emberAfNcpInitCallback in the Zigbee NCP Framework and call the appropriate diagnostic functions (halGetExtendedResetInfo, halGetExtendedResetString, halPrintCrashSummary, halPrintCrashDetails, and halPrintCrashData) in this callback to print this data to Serial 0 for viewing in the Network Analyzer capture log. For an example of how to use these functions, refer to the code included in af-main-soc.c's emberAfMainInit() when EXTENDED_RESET_INFO is defined.

ID #	Description	Workaround
486369	If a DynamicMultiProtocolLightSoc forming a new network has child nodes remaining from a network it has left, emberAfGetChildTableSize returns a non-zero value in startIdentifyOnAllChildNodes, causing Tx 66 error messages when addressing the "ghost" children.	Mass-erase the part if possible before creating a new network or programmatically check the child table after leaving the network and delete all children using emberRemoveChild prior to forming a new network.
495563	Joining SPI NCP Sleepy End Device Sample App doesn't short poll, therefore the joining attempt fails at the state of Update TC Link Key.	The device that wishes to join should be in Short Poll mode before attempting to join. This mode can be forced by the End Device Support plugin.
497832	In Network Analyzer the Zigbee Application Support Command Breakdown for the Verify Key Request Frame mistakenly references the part of the payload that indicates the frame Source Address as the Destination Address.	No known workaround

519905 521782	SPI NCP may very rarely fail to start up bootloader communication using the 'bootload' CLI command of the ota-client plugin.	Restart the bootload process
620596	NCP SPI Example for BRD4181A (EFR32xGMG 21) nWake default pin defined cannot be used as a wake-up pin.	Change the default pin for nWake from PD03 to a EM2/3 wake-up-enabled pin in the NCP-SPI Plugin.
631713	A Zigbee End Device will report address conflicts repeatedly if the plugin "Zigbee PRO Stack Library" is used instead of "Zigbee PRO Leaf Library".	Use the"Zigbee PRO Leaf Library" instead of the "Zigbee PRO Stack Library" plugin.
670702	Inefficiencies within the Reporting plugin can lead to significant latency based on data write frequency and table size, which may interfere with customer application code, including event timing.	If doing frequent writes, consider checking reporting conditions and sending reports manually rather than using the plugin.
708258	Uninitialized value in groups-server.c via addEntryToGroupTable() can create a spurious binding and cause groupcast reporting messages to be sent.	Add "binding.clusterId = EMBER_AF_INVALID_CLUSTER_ID;" after "binding.type = EMBER_MULTICAST_BINDING;"
757775	All EFR32 parts have a unique RSSI offset. In addition, board design, antennas and enclosure can impact RSSI.	When creating a new project, install the RAIL Utility, RSSI component. This feature includes the default RSSI Offset SiLabs has measured for each part. This offset can be modified if necessary after RF testing of your complete product.
758965	ZCL cluster components and ZCL command discovery table are not synchronized. Therefore, when enabling or disabling a ZCL cluster component, implemented commands will not be enabled/disabled in the corresponding ZCL Advanced Configurator command tab.	Manually enable/disable discovery for the desired ZCL commands in the ZCL Advanced Configurator.
765735	The OTA update fails on Sleepy End Device with enabled Page Request.	Use Block Request instead of Page Request.
845649	Removing CLI:Core component does not eliminate EEPROM cli calls to sl_cli.h.	Delete the eeprom-cli.c file that calls the sl_cli.h. Additionally, calls to sl_cli.h as well as sl_cli_command_arg_t in the ota-storage-simple-eeprom can be commented out.
857200	ias-zone-server.c allows for a binding to be created with a "0000000000000000" CIE address and posteriorly does not allow further bindings.	No known workaround
1019961	Generated Z3Gateway makefile hardcodes "gcc" as CC	No known workaround

ID #	Description	Workaround
1039767	Zigbee router network retry queue overflow issue in multi thread RTOS use case.	Zigbee Stack is not thread-safe. As a result, calling Zigbee stack APIs from another task is not supported in OS environment and may put the stack into "non-working" state. Refer to the following App note for more information and workaround using event handler. https://www.silabs.com/documents/public/application- notes/an1322-dynamic-multiprotocol-bluetooth-zigbee-sdk-7x.pdf .
1064370	The Z3Switch sample application only enabled one button (instance : btn1) by default that leads to mismatch in but- ton description in the project file.	Workaround: Install the btn0 instance manually during Z3Switch project creation.
1161063	Z3Light and potentially other applications report incorrect cluster revision values.	Manually update the cluster revision attribute to their appro- priate revision.
1164768, 1171478, 1171479	ERROR: ezspErrorHandler 0x34 reported repeatedly dur- ing mfglib receive mode	To reduce the error messages printed, configure EMBER_AF_PLUGIN_GATEWAY_MAX_WAIT_FOR_EV ENT_TIMEOUT_MS on the host app to 100, so the callback queue is freed more quickly.

Deprecated Items

Deprecated in release 7.4.5.0
In GSDK 7.4.5.0 zigbee_watchdog_periodic_refresh is deprecated. The alternative recommended way to refresh the watchdog timer is to use the legacy watchdog timer APIs in an application specific periodic event.

Deprecated in release 7.4.1.0
In GSDK 7.4.0.0 onwards, including this patch, the "-v" option in a Z3Gateway for a Linux host application to create a telnet interface with port 4900 or 4901 is deprecated. The alternative recommended way to create a telnet interface is to use Linux utilities such as "socat".

Deprecated in release 7.4.0.0
Removed the following deprecated security APIs

- emberGetKey()
- emberGetKeyTableEntry()
- emberSetKeyTableEntry()
- emberHaveLinkKey()
- emberAddOrUpdateKeyTableEntry()
- emberAddTransientLinkKey()
- emberGetTransientKeyTableEntry()
- emberGetTransientLinkKey()
- emberHmacAesHash()

Use the APIs provided by Zigbee Security Manager for access to key storage and HMAC hashing.

Removed Items

Removed in release 7.4.0.0

- Removed duplicate public APIs in public header file gp-types.h.
- The zigbee_end_device_bind component has been removed. This component was used for the coordinator to broker binding re-quests for end devices. This optional functionality was removed from R22 of the Zigbee core spec.
- Removed set Packet BufferCount() in af-host.c and useless check case EZSP_CONFIG_PACKET_BUFFER_COUNT: in command-handlers.c.
- Removed memory Allocation argument because there is no need to divide into two phases when initializing NCP.
- Removed emberAfNcpInitCallback() in se14-comms-hub, se14-ihd, and se14-meter-gas 's app.c.
- Removed setting EZSP_CONFIG_RETRY_QUEUE_SIZE value during ncp initialization in ncp-configuration.c.

Multiprotocol Gateway and RCP

New Items

Added in release 7.4.0.0
Concurrent listening, the ability for the Zigbee and OpenThread stacks to operate on independent 802.15.4 channels when using an EFR32xG24 or xG21 RCP, is released. Concurrent listening is not available for the 802.15.4 RCP/Bluetooth RCP combination, the Zigbee NCP/OpenThread RCP combination, or for the Zigbee/OpenThread system-on-chip (SoC). It will be added to those products in a future release.
The OpenThread CLI vendor extension has been added to the OpenThread host apps of multiprotocol containers. This includes the coex cli commands.

Improvements

Changed in release 7.4.0.0
The Zigbee NCP/OpenThread RCP multiprotocol combination is now production quality. This sample application is not supported on Series-1 EFR devices.

Fixed Issues

Fixed in release 7.4.5.0

ID #	Description
1328799	The soft reset triggered by the Spinel RESET command now clears the buffers of the 15.4 RCP.
1337101	Incomplete 15.4 transmit operations (Tx waiting for an ack, Tx an ack in response to a message, etc) are no longer prematurely considered as failed upon radio interruption due to DMP. This allows said operation to be given a chance to be rescheduled after the interruption or permanently failed by RAIL (scheduler status error events). (Other ref: 1339032)
1337228	In Zigbeed the halCommonGetInt32uMillisecondTick() tick API is now updated to use MONOTONIC clock, so that it does not get affected by the NTP in a host system. (Other ref: 1339032)
1346785	Fixed a race condition which could cause concurrent listening to be disabled on the 802.15.4 RCP when both protocols were transmitting simultaneously. (Other ref: 1349176)
1346849	Adding the rail_mux component to a project will now cause it to automatically build with the associated stack library variants. (Other ref: 1349102)

Fixed in release 7.4.4.0

ID #	Description
1184065	Reduced RAM footprint for zigbee_ncp-ot_rcp-spi and zigbee_ncp-ot_rcp_uart on MG13 and MG21.
1282264	Fixed an issue that could have interrupted radio transmit operations by clearing the transmit fifo prematurely causing underflow.
1292537	DMP Zigbee-BLE NCP application now properly showing up in Simplicity Studio UI. (Other ref: 1292540)

1230193	Fixed incorrect node type issue when joining network on end device. (Other ref: 1298347)
1332330	Fixed an issue where a 15.4+BLE RCP operating in an environment with heavy network traffic could occasionally encounter a race condition that would leave it unable to send messages up to CPCd until rebooting the device. (Other ref: 1333156)

Fixed in release 7.4.2.0

ID #	Description
1022972	Added coexistence plugin back to Zigbee-OpenThread NCP/RCP sample application.
1231021	Avoid an assert in OTBR that has been observed when joining 80+ zigbee devices by recovering the RCP rather than by passing unhandled transmit errors to the sub mac.
1249346	Addressed an issue where the RCP could incorrectly dequeue packets destined for the host, resulting in a parse error in the OTBR and unexpected termination.

Fixed in release 7.4.1.0

ID #	Description
1213701	zigbeed didn't allow a source match table entry to be created for a child if MAC indirect queue has data already pending for that child. This behavior could lead to application layer transactions between the child and some other device failing due to lack of APS Ack or app-layer response, most notably the disruption and unexpected termination of ZCL OTA Upgrades targeting the child device.
1244461	Source match table entry for child being could be removed despite messages pending.

Fixed in release 7.4.0.0

ID #	Description
1081828	Throughput issue with FreeRTOS-based Zigbee/BLE DMP sample applications.
1090921	Z3GatewayCpc had trouble forming a network in a noisy environment.
1153055	An assert on the host was caused when there was a communication failure when reading the NCP version from the zigbee_ncp-ble_ncp-uart sample app.
1155676	The 802.15.4 RCP discarded all received unicast packets (after MAC acking) if multiple 15.4 interfaces shared the same 16-bit node ID.
1173178	The host falsely reported hundreds of packets received with mfglib in the Host-RCP setup.
1190859	EZSP error when sending mfglib random packets in the Host-RCP setup.
1199706	Data polls from forgotten end device children were not properly setting a pending frame on the RCP to queue a Leave & Rejoin command to the former child.
1207967	The "mfglib send random" command was sending out extra packets on Zigbeed.
1208012	The mfglib rx mode did not update packet info correctly when receiving on the RCP.
1214359	The coordinator node crashed when 80 or more routers tried to join simultaneously in the Host-RCP setup.
1216470	After relaying a broadcast for address mask 0xFFFF, a Zigbee RCP acting as a parent device would leave the pending data flag set for each child. This resulted in each child staying awake expecting data after each poll, and required some other pending data transaction to each end device to eventually clear this state.

Known Issues in the Current Release

Issues in bold were added since the previous release. If you have missed a release, recent release notes are available on **https://www.si-labs.com/developers/gecko-software-development-kit** .

ID #	Description	Workaround
937562	Bluetoothctl 'advertise on' command fails with rcp-uart- 802154-blehci app on Raspberry Pi OS 11.	Use btmgmt app instead of bluetoothctl.
1074205	The CMP RCP does not support two networks on the same PAN id.	Use different PAN ids for each network. Support is planned in a future release.
1122723	In a busy environment the CLI may become unresponsive in the z3-light_ot-ftd_soc app.	No known workaround.
1124140	z3-light_ot-ftd_soc sample app is not able to form the Zigbee network if the OT network is up already.	Start the Zigbee network first and the OT network after.
1170052	CMP Zigbee NCP + OT RCP and DMP Zigbee NCP + BLE NCP may not fit on 64KB and lower RAM parts in this current release.	64KB parts not currently supported for these apps.
1209958	The ZB/OT/BLE RCP on Bobcat and Bobcat Lite can stop working after a few minutes when running all three protocols.	Will be addressed in a future release
1221299	Mfglib RSSI readings differ between RCP and NCP.	Will be addressed in a future release.
1334477	Starting and stopping the BLE stack several times might result in the BLE stack not able to restart advertisement again on Series 1 EFR devices in the DMP Zigbee-BLE sample application.	N/A

Deprecated Items None

Removed Items

Removed in release 7.4.0.0
The "NONCOMPLIANT_ACK_TIMING_WORKAROUND" macro has been removed. All RCP apps now by default support 192 μsec turnaround time for non-enhanced acks while still using 256 μsec turnaround time for enhanced acks required by CSL.

Using This Release

This release contains the following

- Zigbee stack
- Zigbee Application Framework
- Zigbee Sample Applications

For more information about Zigbee and the EmberZNet SDK see UG103.02: Zigbee Fundamentals.

If you are a first-time user, see QSG180: Zigbee EmberZNet Quick-Start Guide for SDK 7.0 and Higher, for instructions on configuring your development environment, building and flashing a sample application, and documentation references pointing to next steps.

Installation and Use

The Zigbee EmberZNet SDK is provided as part of the Gecko SDK (GSDK), the suite of Silicon Labs SDKs. To quickly get started with the GSDK, install Simplicity Studio 5, which will set up your development environment and walk you through GSDK installation. Simplicity Studio 5 includes everything needed for IoT product development with Silicon Labs devices, including a resource and project launcher, software configuration tools, full IDE with GNU toolchain, and analysis tools. Installation instructions are provided in the online Simplicity Studio 5 User's Guide.

Alternatively, Gecko SDK may be installed manually by downloading or cloning the latest from GitHub. See **https://github.com/Sili-conLabs/gecko_sdk** for more information .

Simplicity Studio installs the GSDK by default in

- **(Windows):** C:\Users\<NAME>\SimplicityStudio\SDKs\gecko_sdk

- **(MacOS):** /Users/<NAME>/SimplicityStudio/SDKs/gecko_sdk

Documentation specific to the SDK version is installed with the SDK. Additional information can often be found in the knowledge base articles (KBAs). API references and other information about this and earlier releases is available on **https://docs.silabs.com/** .

Security Information

Secure Vault Integration
For applications that choose to store keys securely using the Secure Key Storage component on Secure Vault-High parts, the following table shows the protected keys and their storage protection characteristics that the Zigbee Security Manager component manages.

Wrapped Key	Exportable / Non-Exportable	Notes
Network Key	Exportable	
Trust Center Link Key	Exportable	
Transient Link Key	Exportable	Indexed key table, stored as volatile key
Application Link Key	Exportable	Indexed key table
Secure EZSP Key	Exportable	
ZLL Encryption Key	Exportable	
ZLL Preconfigured Key	Exportable	
GPD Proxy Key	Exportable	Indexed key table
GPD Sink Key	Exportable	Indexed key table
Internal/Placeholder Key	Exportable	Internal key for use by Zigbee Security Manager

- Wrapped keys that are marked as "Non-Exportable" can be used but cannot be viewed or shared at runtime.
- Wrapped keys that are marked as "Exportable" can be used or shared at runtime but remain encrypted while stored in flash.
- User applications never need to interact with the majority of these keys. Existing APIs to manage Link Key Table keys or Transient Keys are still available to the user application and now route through the Zigbee

Security Manager component.

- Some of these keys may become non-exportable to the user application in the future. User applications are encouraged to not rely on the exporting of keys unless absolutely necessary.

  For more information on Secure Vault Key Management functionality, see AN1271: Secure Key Storage.

Security Advisories
To subscribe to Security Advisories, log in to the Silicon Labs customer portal, then select Account Home. Click HOME to go to the portal home page and then click the Manage Notifications tile. Make sure that 'Software/Security Advisory Notices & Product Change Notices (PCNs)' is checked, and that you are subscribed at minimum for your platform and protocol. Click Save to save any changes.

The following figure is an example

Support
Development Kit customers are eligible for training and technical support. Use the Silicon Laboratories Zigbee web page to obtain infor-mation 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** .

Simplicity Studio
One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

- **IoT Portfolio**

  www.silabs.com/IoT
- **SW/HW**

  www.silabs.com/simplicity
- **Quality**

  www.silabs.com/quality
- **Support & Community**

  www.silabs.com/community

Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software imple-menters using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice to the product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Without prior notification, Silicon Labs may update product firmware during the manufacturing process for security or reliability reasons. Such changes will not alter the specifications or the performance of the product. Silicon Labs shall have no liability for the consequences of use of the infor-mation supplied in this document. This document does not imply or expressly grant any license to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any FDA Class III devices, applications for which FDA premarket approval is required or Life Support Systems without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons. Silicon Labs disclaims all express and implied warranties and shall not be responsible or liable for any injuries or damages related to use of a Silicon Labs product in such unauthorized applications.

Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Redpine Signals®, WiSeConnect , n-Link, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, Gecko OS, Gecko OS Studio, Precision32®, Simplicity Studio®, Telegesis, the Telegesis Logo®, USBXpress® , Zentri, the Zentri logo and Zentri DMS, Z-Wave®, and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. Wi-Fi is a registered trademark of the Wi-Fi Alliance. All other products or brand names mentioned herein are trademarks of their respective holders.

- Silicon Laboratories Inc.
- 400 West Cesar Chavez Austin, TX 78701
- USA
- **www.silabs.com**

Documents / Resources

SILICON LABS 7.4.5.0 Zigbee Ember Z Net SDK [pdf] User Guide
7.4.5.0, 7.4.4.0, 7.4.3.0, 7.4.2.0, 7.4.1.0, 7.4.0.0, 7.4.5.0 Zigbee Ember Z Net SDK, 7.4.5.0, Zigbee Ember Z Net SDK, Ember Z Net SDK, Z Net SDK, Net SDK, SDK

References

- **Silicon Labs**
- **Silicon Labs**
- **IoT – Internet of Things - Silicon Labs**
- **Simplicity Studio - Silicon Labs**
- **Technical Support - Silicon Labs**
- **User Manual**