Zigbee EmberZNet SDK 7.2.5.0 GA
Gecko SDK Suite 4.2
January 24, 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):

7.2.5.0 released January 24, 2024
7.2.4.0 released August 16, 2023
7.2.3.0 released May 3, 2023
7.2.2.0 released March 8, 2023
7.2.1.0 released February 1, 2023
7.2.0.0 released December 14, 2022

Zigbee

KEY FEATURES

Zigbee

- Secure key storage support for MG2x parts that support Secure Vault-High
- MG24+Si4468 Dual-PHY Zigbee Smart Energy support
- MG12 Dual-Band 2.4GHz + SubGHz Zigbee Smart Energy support
- MGM240S SiP Module Support
- Zigbee on Host (ZigbeeD) support for 32 bit and 64 bit x86 architecture - experimental

Multiprotocol

- Dynamic Multiprotocol Bluetooth and multi-PAN 802.15.4 in RCP mode
- Dynamic Multiprotocol Bluetooth and Zigbee NCP - experimental
- Manufacturing Library (MfgLib) support for Concurrent Multiprotocol RCP
- Zigbee + OpenThread Concurrent Listening on MG24 parts - experimental

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, see Using This Release.

Compatible Compilers:

IAR Embedded Workbench for ARM (IAR-EWARM) version 9.20.4.

- 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 10.3-2021.10, provided with Simplicity Studio.

Contents

1 New Items 3
1.1 New Features 3
1.2 New Applications 3
1.3 New Components 3
1.4 New APIs 4
1.5 New CLI Commands 5
1.6 New Platform Support 5
1.7 New Documentation 5
2 Improvements 6
3 Fixed Issues 8
4 Known Issues in the Current Release 12
5 Deprecated Items 15
6 Removed Items 16
7 Multiprotocol Gateway and RCP 17
7.1 New Items 17
7.2 Improvements 17
7.3 Fixed Issues 17
7.4 Known Issues in the Current Release 19
7.5 Deprecated Items 19
7.6 Removed Items 19
8 Using This Release 20
8.1 Installation and Use 20
8.2 Security Information 20
8.3 Support 21

1 New Items

1.1 New Features

New in release 7.2.0.0

Zigbee Security

Support is available for storing encryption keys securely on EFR32MG2x parts that support the Secure Vault-High feature. Refer to *AN1271: Secure Key Storage* for information about securely storing security keys. Applications that wish to store security keys in secure storage must be used for new deployments, as OTA upgrade for existing devices is currently unsupported in this release.

Smart Energy

Simultaneous Dual-PHY Smart Energy support is now available on EFR32xG24+Si4468 parts.

Zigbee Smart Energy Dual-Band 2.4GHz and Sub-GHz support for end-devices is now available on EFR32xG12 parts.

DMP NCP

Dynamic Multiprotocol Zigbee-NCP + Bluetooth-NCP support is now available.

1.2 New Applications

None

1.3 New Components

New in release 7.2.0.0

Zigbee Security Manager Components

Zigbee Security Manager

The Zigbee Security Manager component is a common component that provides an interface for the user to manage security keys and crypto routines. This component is tailored to Zigbee-specific keys and crypto routines.

Security Manager

The Security Manager component is a stack-agnostic component that provides an interface to manage keys in PSA storage. These may be wrapped keys if the device supports the Secure Vault-High feature. The Security Manager component also provides an interface to certain crypto routines. The Zigbee Secure Key Storage component utilizes the Security Manager component.

Classic Key Storage

The Zigbee Classic Key Storage component handles the storing and fetching of security keys in NVM3 tokens. NVM3-stored keys are saved in-the-clear in flash, which means that keys can be read when flash is read from the device. This storage method is the way Zigbee applications have previously stored keys on the device.

Secure Key Storage

The Zigbee Secure Key Storage component handles storing keys using PSA APIs. For devices that support the Secure Vault-High feature, keys are wrapped in secure storage and cannot be gleaned by reading flash from the device.

The Security Manager component is used by the Zigbee Secure Key Storage component to execute certain crypto routines, like AES encryption and decryption.

Users wishing to have the application store keys securely must do so on fresh deployments only. There is currently no support for deployed devices to upgrade their key storage and move security keys from tokens into secure key storage. This upgrade functionality is planned for a future release.

Devices that include the Secure Vault High feature may still store security keys classically (for example in tokens) by including the Classic Key Storage component instead. SDK 7.2.0.0-based applications that include OTA upgrade functionality for these Secure Vault-High devices running pre-SDK 7.2.0.0 code are currently limited to using the Classic Key Storage component.

Secure Vault-High devices may not downgrade from an image that stored keys in secure storage to an image that stores keys back into tokens.

Other Components

Watchdog Refresh

The watchdog refresh component resets the watchdog timer periodically (value is configurable and holds a default of 1 second). Note that in order to accomplish this, the part needs to get into EM0 energy mode. This component is included by default when there is an RTOS and watchdog is used in the code. Refreshing of the watchdog timer can be disabled using the configuration option in the component.

Green Power Adapter

The zigbee_green_power_adapter component supports use of green power server or client component in a custom framework. This component includes a set of minimum required source files from the application framework and it provides a number of subroutines to be used to integrate the custom framework.

1.4 New APIs

New in release 7.2.1.0

Renamed sl_set_passive_ack_config() to sl_zigbee_set_passive_ack_config()

Renamed emAfOverrideAppendSourceRouteCallback() to emberAfOverrideAppendSourceRouteCallback()

Reinstated emberChildId() after removal in 7.2.0.0

Reinstated emberChildIndex() after removal in 7.2.0.0

New in release 7.2.0.0

Zigbee Security Manager Component

The Zigbee Security Manager component provides several APIs, which are implemented by either the Zigbee Classic Key Storage or Zigbee Secure Key Storage component. They provide functionality that includes importing and exporting keys stored by the component, retrieving key metadata, loading keys to use in an operation, and performing cryptographic operations with a loaded key. A full list of these new APIs is available in Zigbee Stack API documentation at https://docs.silabs.com. A subset of those APIs are listed here.

- `void sl_zb_sec_man_init_context(sl_zb_sec_man_context_t* context)`
- `sl_status_t sl_zb_sec_man_import_key(sl_zb_sec_man_context_t* context, sl_zb_sec_man_key_t* plaintext_key)`
- `sl_status_t sl_zb_sec_man_export_key(sl_zb_sec_man_context_t* context, sl_zb_sec_man_key_t* plaintext_key)`
- `sl_status_t sl_zb_sec_man_load_key_context(sl_zb_sec_man_context_t* context)`
- `sl_status_t sl_zb_sec_man_hmac_aes_mmo(const uint8_t* input, const uint8_t data_length, uint8_t* output)`
- `sl_status_t sl_zb_sec_man_aes_ccm(uint8_t* nonce, bool encrypt, const uint8_t* input, uint8_t encryption_start_index, uint8_t length, uint8_t* output)`

Miscellaneous

`bool emberAfClusterEnableDisable(uint8_t endpoint, EmberAfClusterId clusterId, EmberAfClusterMask mask, bool enable)` allows enabling and disabling clusters at runtime, with `bool emberAfIsClusterEnabled(uint8_t endpoint, EmberAfClusterId clusterId, EmberAfClusterMask mask)` to check whether a cluster is enabled. These APIs require setting EMBER_AF_PLUGIN_ZCL_CLUSTER_ENABLE_DISABLE_RUN_TIME in the ZCL framework core plugin to true in order to be compiled.

1.5 New CLI Commands

New in release 7.2.0.0

Added new CLI command for "bluetooth_on_demand_start" component, 'plugin ble start' and 'plugin ble stop' to request starting and stopping the Bluetooth stack when needed.

1.6 New Platform Support

New in release 7.2.4.0

BRD4195B and BRD4196B radio board support is now available.

New in release 7.2.0.0

MGM240S SiP Module support is now available.

1.7 New Documentation

All components have documentation available. If you have an issue seeing the documentation when you select the component in Project Configurator, you can find it on https://docs.silabs.com/.

2 Improvements

Changed in release 7.2.5.0

MAC TX Unicast Retry Counter

In previous versions, the Counter Handler callback for MAC and APS layer EmberCounterTypes 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 emberCounterHandler() has not changed, the way its parameters are populated have changed slightly. Changes around this API include the following:

- Comments around EmberCounterType enums in ember-types.h have been expanded for clarity.
- Node ID parameter to the Counter Handler for TX-related counters now check whether the destination address mode indicates 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.)
- Node ID parameter to the Counter Handler for RX-related counters now reflect 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, retry count for APS layer retries continues to be populated in the data parameter for EMBER_COUNTER_APS_TX_UNICAST_SUCCESS/FAILED counter types, 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 address (or EMBER_UNKNOWN_NODE_ID if a Node ID was expected but not able to be obtained from the packet), or data as described in revised ember-types.h documentation.
- 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.
- 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.

Intended Behavior Clarification for CSL

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.

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.

Changed in release 7.2.2.0

Miscellaneous

Improved the reportable change calculation in the Reporting component by supporting float datatype difference calculation. This is supported using the platform float libraries. If the reportable change calculation involves double or semi precision data types, a set of callbacks (emberAfGetDiffCallback and emberAfDetectReportChangedCallback) are introduced for the user to provide their arithmetic functions.

Updated application framework stack callback function signatures and added missing host framework callbacks. These updates are available at https://docs.silabs.com/.

Updated the ezspPollHandler function with updated input arguments, that required updating the EZSP_PROTOCOL_VERSION to 0x0B.

Changed in release 7.2.1.0

Miscellaneous

Improved error handling in sl_zigbee_set_passive_ack_config().

Changed in release 7.2.0.0

Watchdog

Re-enabled the watchdog timer on Zigbee sample applications. We now pet the watchdog once per second in the app.c file for the corresponding project.

Sub-GHz Network Find

Added the CMSIS configuration for channel pages and masks for the sub gigahertz network find component.

Network Steering

Added a validation script for the Zigbee Network Steering component to confirm that the optimized scans option is also enabled if the ‘try all keys’ option is enabled* .

NCP - CPC

Documentation was updated to indicate that the NCP applications need CPC included in RTOS-based applications and must be used with a host application that supports CPC.

Green Power Sink

The GP sink table now stores the group ID for the groupcast sink type (EMBER_GP_SINK_TYPE_GROUPCAST) in the respective token. The sink type enumeration was updated to remove the EMBER_GP_SINK_TYPE_SINK_GROUPLIST.

Miscellaneous

Documentation was updated to state that the last two bytes of the received packet in manufacturing mode is not to be interpreted as the FCS / CRC bytes.

Command structs with items of size greater than 4 bytes are now defined as integer arrays instead of integer pointers.

3 Fixed Issues

Fixed in release 7.2.5.0

ID #	Description
1147306	Fixed an issue for multi mac coordinator that prevented scanning on sub ghz interface during network formation because of the previous network leave.
1198598, 1196698	Fixed spurious frame pending bit set when there is no data pending
1215648	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.
1215649	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().
1215650	Destination and PHY Index provided in EmberExtraCounterInfo struct as part of emberCounterHandler() may be incorrect for MAC TX Unicast counter types.
1215652	Outgoing Beacon packets should trigger EMBER_COUNTER_MAC_TX_BROADCAST instead of EMBER_COUNTER_MAC_TX_UNICAST.
1215653	Sending data poll when packet buffers have been depleted to near zero can lead to a bus fault.
1221878	Rejoining an end device a with previous NWK key after a key change caused the end device to mistakenly be put into the neighbor table and treated like a router instead of an end device child, interfering with proper message delivery.
1240390	ZDO Bind/Unbind Requests refused for access/permission reasons should return EMBER_ZDP_NOT_AUTHORIZED status rather than EMBER_ZDP_NOT_PERMITTED status as per Zigbee specifications.
1240620	Fixed an issue that caused the end device move state machine to stop attempts to rejoin the network under heavy traffic conditions.

Fixed in release 7.2.4.0

ID #	Description
1174328	Fixed an issue that caused one of the steps in Touchlink test (DN-TLM-TC-02B) to fail.

Fixed in release 7.2.3.0

ID #	Description
1130734	Fixed null pointer dereference when sending an association response if no buffers are available.

Fixed in release 7.2.2.0

ID #	Description
660624	Device table component updated to be used by both SoC and host architectures.
754110	The reportable change calculation is updated to support float calculation using platform-dependent float library.
1026022	Fixed an issue that was affecting the UART baud rate when setting the CTUNE value on NCP from host using set the EZSP_CONFIG_CTUNE_VALUE command.
1026760	Fixed an issue that was letting the dual PHY-capable end devices to rejoin on 2.4 GHz interface after associating on sub gigahertz interface.
1030357	Fixed an issue with "plugin mfglib set-options" command returning an error in manufacturing mode by registering the callbacks for setting configuration values.
1063627	Updated emberAfRemoteSetBindingCallback() and added missing callback for the host architecture.
1079388	Fixed an issue where the EMBER_AF_PLUGIN_NETWORK_CREATOR_SECURITY_BDB_JOIN_USES_INSTALL_CODE_KEY option in the Network Creator Security component is overwritten when the “plugin network-creator-security open-network” or “plugin network-creator-security open-with-key” CLI commands are invoked.
1087526	Fixed some Coverity issues.

ID #	Description
1096375	Fixed an issue where the emberHmacAesHash API had been unavailable for application builds since EmberZNet 7.2.0.
1097258	Fixed an issue that affected Green Power Server test cases 4.5.2.2, 4.5.2.3, 4.4.3.1 and 4.4.2.8.
1099131	Fixed an issue that was preventing the server to send a termination message to a client if it received a malformed certificate during key establishment.
1103117	Fixed an issue that was causing the Green Power Server to remain uninitialized after a network leave and re-association of the Green Power Combo application.
1104793	Fixed an issue that was causing an assert failure for the scenario of ongoing data transactions on both the interfaces of dual PHY stack.
1106002	Fixed an issue that affected Green Power server test case 4.4.1.7 steps 1-2.

Fixed in release 7.2.1.0

ID #	Description
289695	The range check for reserved and non-existent Green Power device source Id are added to the Green Power cluster command handlers.
651930	Removed legacy NCP callback emberAfPluginConcentratorBroadcastSentCallback().
621144	Added support for GPD switch on single-button devices such as BRD4183A.
648906	Reimplemented emberChildId().
659010	Reimplemented emberChildIndex().
727076	Fixed an issue that could result in diagnostics function to use incorrect Endpoint to update LQI, RSSI, and average MAC retry.
746260	Added support for Smart Energy KEEP-ALIVE cluster.
1026760	Fixed issue where End Device could rejoin using incorrect interface.
1031169	Fixed an issue where a paired GPD could be removed irrespective of presence in translation table.
1031241	Improved validation of reserved Green Power address.
1063525	Fixed an issue that could result in an invalid verify link key exchange to succeed even when Trust Center used an incorrect link key.
1067877	Fixed an issue whereby Scene information was incorrectly removed when adding a new Scene with the same GroupId and SceneId.
1068968	Improved handling of child table timeouts in emberGetChildData().
1069245	Improved device table plugin prototype emberAfTrustCenterJoinCallback() to fix compilation errors.
1074378	Fixed an issue that allowed dual-band End Devices to incorrectly join non-preferred channel yet not disallow re-joining PAN on channel.
1075748	Fixed an issue that caused an EEPROM compilation error when removing CLI.
1077176	Fixed an issue that could cause NCP to fail on startup due to inter-PAN MAC filter (0x36) as a result of an incorrect MAC filter table size.
1081511	Fixed an issue preventing the usage of correct type 4 (OOB) key for commissioning.
1082602	Fixed an issue that could cause packets that fail to decrypt during commissioning to be forwarded as commissioning notifications with authentication failed flag set.
1083200	Fixed an issue where Message Integrity Codes where not being copied back to host in emGpCalculateIncomingCommandMic().
1083835	Fixed sink table read command handling for the gpSharedKey type that fixed the GP Test Case failure 4.4.4.3.
1085137	Fixed an issue where the Sink could remove all entries for app mode 2 and matching EUI64s.
1087618	Fixed compilation issues due to missing Green Power Adaptor header files not being included in release.
1092779	Fixed issue that was preventing an End Device to process a ZDO Leave Request from a non-parent network node.
1091792	Improved error handling and return code of emberGetCurrentSecurityState().
1087567	The ncp sample application “ncp-uart-hw-dual-phy” is not supported by the development board BRD4155.

ID #	Description
1089841	An issue that caused the emberFindAndRejoinNetworkWithReason to return busy status for an end device move procedure on sub gigahertz interface is fixed.
1094643	The function prototype for emGpOutgoingCommandEncrypt is removed from the green-power-server.h because it is only internal to the green-power-security.c file.
1097536	Fixed an issue that caused multi-MAC coordinator to use an incorrect MAC interface to send unsolicited rejoin response to its child during address conflict resolution. This issue caused ZCP Test Case 10.12 to fail on sub-gigahertz.

Fixed in release 7.2.0.0

ID #	Description
498094	Fixed an issue in function `checkForReportingConfig()` in metering- server.c where the second input parameter of the invoked function `emberAfContainsServer()` had incorrectly referenced the cluster ID instead of the attribute ID.
657626	OTA update with page request can now handle up to EMBER_AF_PLUGIN_EEPROM_PARTIAL_WORD_STORAGE_COUNT number of out-of-order write operations without an assert.
684653	Fixed an issue that caused network-steering start to add TC task without checking network state and steering state.
688985	Fixed issue where the joining device joined the network with wrong Extended Pan ID, which would result in a Pan ID conflict.
742167	Fixed an issue that caused the discrepancy of Sequence Number field in ZLL message pairs (request - response).
755880	Changed GBCS event IDs to have correct values from the spec.
756571	Fixed the issue that caused emberPacketHandoffIncoming to receive bad index for EMBER_ZIGBEE_PACKET_TYPE_NWK_DATA/EMBER_ZIGBEE_PACKET_TYPE_NWK_COMMAND packets
760759	An issue has been fixed where certain modules, such as MGM210, can be used to generate and build an application that uses LEDs and buttons, such as DynamicMultiprotocolLight. Apps that use these peripherals are not supported for modules that lack dedicated lines for using both buttons and LEDs.
763728	Handled the insufficient space case when reading attributes.
819117	Fixed an issue that caused parent not to check RX on idle bit when responding to a rejoin request from an unknown device
824361	Fixed typedef warnings when building "ncp-uart-hw" sample app with IAR.
825902	Resolved an issue where association, rejoin, and node ID updates may end up with a node being assigned an invalid address.
829607	Fixed an issue of end device configuration overriding the user-provided network address alias value to its own node ID when multicast and broadcast messages were originated by the application.
841499	Fixed an issue where a newly joined device can sometimes not get added to the child table if its IEEE address is not known.
842361	Fixed a parsing issue caused by incorrect min length array of OTA cluster commands.
844016	Fixed an issue that caused compilation errors on BRD4183C by excluding this board for some apps. *
850747	Watchdog is now enabled by default on all Zigbee EmberZNet sample applications.
1017165	Fixed an issue that caused Force Sleep & Wake Up component to depend CLI component
1021877	Fixed issue in DynamicMultiprotocolLight and DynamicMultiprotocolLightSed projects where scheduler was not properly being locked from the CLI task context when the number of CLI command arguments was less than 2.
1021884	Fixed an incorrect alignment for an indexed token in wwah-server-silabs component.
1024651	Fixed an issue where `emberAfMessageSentCallback()` was not called if child had been removed during the transmission.
1026622	Fixed an issue that caused missing last byte with packet-handoff when EMBER_MANGLE_PACKET is used.
1027200	Fixed an issue where the Key Establishment component sent NO_RESOURCES instead of the required BAD_MESSAGE when an initiator with unknown EUI64 attempted key establishment.
1030940	Fixed issue in which really high APS message frequency towards SED devices could result in unprocessed (re)join requests.

ID #	Description
1042022	Fixed issue where the Key Establishment component didn't check for minimum command request and command response length.
1058984	The templated callback for message_sent would be called multiple times for fragmented packets, instead of once after all fragments get sent. This was a change in behavior starting in Zigbee EmberZNet SDK 7.0 and has been addressed in SDK 7.2.0 and later. The templated callback is now only invoked once per fragmented transmission.
1060156	Fixed an issue where TC did not send NWK Key when other devices were scanning.
1061948	The issue of a lower ZCL sequence number for initiate key establishment command that follows a read attribute is fixed.
1066234	Fixed an issue that caused the key establishment state machine to get stuck if ConfirmKeyDataResponse is lost over the air.
1066947	Fixed issue where scan procedure in form-and-join code could corrupt memory used by other buffers. This manifests as either a bus fault, usage fault or a packet buffer assert.
1068035	Fixed a potential issue that caused a linking error when customer wants to use green power client or server only for their NCP application.
1068055	The following ZCL Basic cluster optional attributes, which were missing from the XML definition file, have been added: 0x000C Manufacturer Version Details, 0x000D Serial Number, and 0x000E Product Label.
1069727	Fixed an uninitialized variable MISRA error in indirect-queue.c file.
1077662	Fixed issue where the upgrade rule did not fire correctly for the Zigbee RTOS task stack size configuration. It is now specified in bytes instead of words.

4 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/components are not supported in this release • NCP Sleepy • EM4 support	Features will be enabled in subsequent releases.
193492	emberAfFillCommandGlobalServerToClientConfigureReporting 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_POWER 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 (EFR32xGMG21) 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 .
1081914	An issue is present for applications that store keys securely, or those that include the Secure Key Storage component, and the token file-based Trust Center Backup feature, as described in AN1387: Backing Up and Restoring a Z3 Green Power Combo Gateway.	Either use Classic Key Storage or standard Trust Center Backup, which does not store token information to a text file.
1082798	Throughput plugin has 5 bytes less than maximum length of the packet.	In function getHeaderLen() located in zigbee/framework/plugin/app/framework/plugin/throughput/throughput.c , remove the subtraction of EMBER_AF_ZCL_MANUFACTURER_SPECIFIC_OVERHEAD macro during calculation of the maxPayloadLen variable.
1064370	The Z3Switch sample application only enabled one button (instance : btn1) by default that leads to mismatch in button description in the projectfile.	Workaround: Install the btn0 instance manually during Z3Switch project creation.
1105915	On a dual band selection device, emberGetRadioParameters always returns 0 for the channel page regardless of the current channel page.	As a workaround, the page can be retrieved with: emMacPgChanPg(emCurrentChannel) ? (emMacPgChanPg(emCurrentChannel) | 0x18).
1175771	**When running mfglib receive test mode for Host-NCP architecture with the sample application, Z3Gateway, reports a lot of ezspErrorHandler error 0x34 indicating the unavailability of message buffers.**	**Configure EMBER_AF_PLUGIN_GATEWAY_MAX_WAIT_FOR_EVENT_TIMEOUT_MS on the host app to 100, this reduces the error.**
1152898	**NCP with hardware flow control watchdog repeatedly gets triggered while host is not up.**	**Ensure the NCP is connected to the host before the NCP is powered.**

5 Deprecated Items

Deprecated in release 7.2.0.0

The Secure EZSP feature will be removed in a future release.

6 Removed Items

Removed in release 7.2.1.0

Removed unused, legacy NCP callback API emberAfPluginConcentratorBroadcastSentCallback().

Removed unused RESERVED_AVAILABLE_MEMORY and EXTRA_MEMORY defines in many Zigbee Sample Application project templates. Note the removal of these legacy defines has no effect on the Sample Applications.

Removed in release 7.2.0.0

The Zigbee AES (PSA) and Zigbee CCM (PSA) components have been removed. For EFR-based applications, hardware support for these crypto routines is now brought in with the Zigbee Security Manager component, which is brought into projects via component dependencies. Host applications do not use the Zigbee Security Manager component. Host applications may still consume the AES (Software) and CCM (Software) components if desired.

7 Multiprotocol Gateway and RCP

7.1 New Items

Added in release 7.2.2.0

Zigbeed now loads the CREATOR_STACK_RESTORED_EUI64, if present, from the host tokens file, and uses it as the EUI64, overriding the EUI64 stored on the EFR32.

Added in release 7.2.1.0

Zigbeed now supports coex EZSP commands.

Added in release 7.2.0.0

Added Dynamic Multiprotocol BLE and Zigbee NCP project (zigbee_ncp-ble_ncp-xxx.slcp). Released as experimental quality.

Added 802.15.4 concurrent listening for EFR32MG24 CMP RCP. This is the ability to run Zigbee and OpenThread simultaneously on different channels using a single RCP (rcp-802154-xxx.slcp and rcp-802154-blehci-xxx.slcp). Released as experimental quality.

Added Zigbeed support for 32-bit x86 architecture.

Added support for BLE to de-init in multiprotocol use cases, freeing up memory resources for use by other protocol stacks.

The Stack API Trace now can be enabled for Zigbeed by setting the debug-level to 4 or 5 in the zigbeed.conf file.

Zigbeed stack version as well as build date and time are now printed in the logs.

7.2 Improvements

Changed in release 7.2.2.0

Reduced CPC Tx and Rx queue sizes to fit the Zigbee BLE DMP NCP onto the MG13 family.

Changed zigbee_ble_event_handler to print scan responses from legacy advertisements in DMPLight app.

The rcp-xxx-802154 and rcp-xxx-802154-blehci apps now use 192 µsec turnaround time for non-enhanced acks while still using 256 µsec turnaround time for enhanced acks required by CSL.

7.3 Fixed Issues

Fixed in release 7.2.5.0

ID #	Description
1188521	Fixed an RCP hang issue when running BLE Scan on with notification and OpenThread ping traffic.

Fixed in release 7.2.4.0

ID #	Description
1118077	In the CMP RCP, Spinel messages were being dropped under heavy traffic load due to CPC not keeping up with the incoming packets. Fixed this by bundling all Spinel messages ready to be sent over CPC into one payload on the RCP, and unbundling them on the host. This dramatically improves the efficiency of CPC so that it can keep up with the incoming radio traffic.

ID #	Description
1113498, 1135805, 1139990, 1143344	Fixed multiple intermittent Zigbeed crashes and asserts that could be triggered when joining many Zigbee devices simultaneously to the CMP RCP.

Fixed in release 7.2.3.0

ID #	Description
1130226	Fixed issue in which the RCP would not recover if CPC became temporarily busy.
1129821	Fixed null pointer dereference in Zigbeed when receiving a packet if no buffers are available.

Fixed in release 7.2.1.0

ID #	Description
1036645	Solved a bug in BLE CPC NCP which prevented a client app from reconnecting after the first disconnection.
1068435	Fixed Green Power bidirectional commissioning timing issue. Certification test case GPP 5.4.1.23 passes.
1074593	Fixed issue in which Just-in-time (JIT) messages to sleepy end devices were not sent correctly by Zigbeed + RCP.
1076235	Fixed issue where ot-cli failed to run in the multiprotocol docker container.
1080517	Z3GatewayCPC now automatically handles a reset of the NCP (CPC secondary).
1085498	Fixed an issue where Zigbeed was not sending rejoin responses to sleepy end devices indirectly.
1090915	Fixed issue where multiple 0x38 errors appeared when attempting to either open a Zigbee endpoint on the Z3GatewayCPC OR to set EZSP parameters without resetting the CPC NCP.

Fixed in release 7.2.0.0

ID #	Description
828785	Fixed a bug in cpc-hci-bridge that caused an HCI packet to be dropped if BlueZ sent two at once.
834191	Improved the CPU utilization of the cpc-hci-bridge helper application.
1025713	Increased max length of Zigbeed device path to 4096.
1036622	Fixed a problem using cmake to build ot-cli using the multi-PAN RCP.
1040127	CPC security was failing to initialize for the rcp-uart-802154 and rcp-spi-802154 projects on MG13 and MG14 series parts. To work around this issue, mbedtls_entropy_adc has been added as entropy source for these parts. That might prevent the ADC from being used in combination with CPC security.
1066422	Fixed an intermittent buffer leak in Zigbeed.
1068429	Fixed a race condition that could cause the CMP RCP to assert.
1068435	Added capability on the RCP node to check and buffer a single bidirectional Green Power data frame and send it out upon rx offset timeout.
1068942	Fixed a leak in the RCP source match table that could prevent Zigbee devices from joining.
1074172	Fixed sending leave request from Zigbeed when receiving a poll from a non-child.
1074290	Stopped Zigbeed from processing un-acked polls.
1079903	Fixed a bug in the CMP RCP that could cause SPINEL messages to be dispatched incorrectly, resulting in Zigbeed and OTBR crashing or exiting.

7.4 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.silabs.com/developers/gecko-software-development-kit.

ID #	Description	Workaround
811732	Custom token support is not available when using Zigbeed.	Support is planned in a future release.
937562	Bluetoothctl 'advertise on' command fails with rcp-uart-802154-blehci app on Raspberry Pi OS 11.	Use btmgmt app instead of bluetoothctl.
1031607	The rcp-uart-802154.slcp project is running low on RAM on an MG1 part. Adding components may reduce the heap size below what is needed to support ECDH binding in CPC.	A workaround is to disable CPC security via the SL_CPC_SECURITY_ENABLED configuration.
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.

7.5 Deprecated Items

None

7.6 Removed Items

None

8 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: Z 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.

8.1 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/SiliconLabs/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/.

8.2 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.

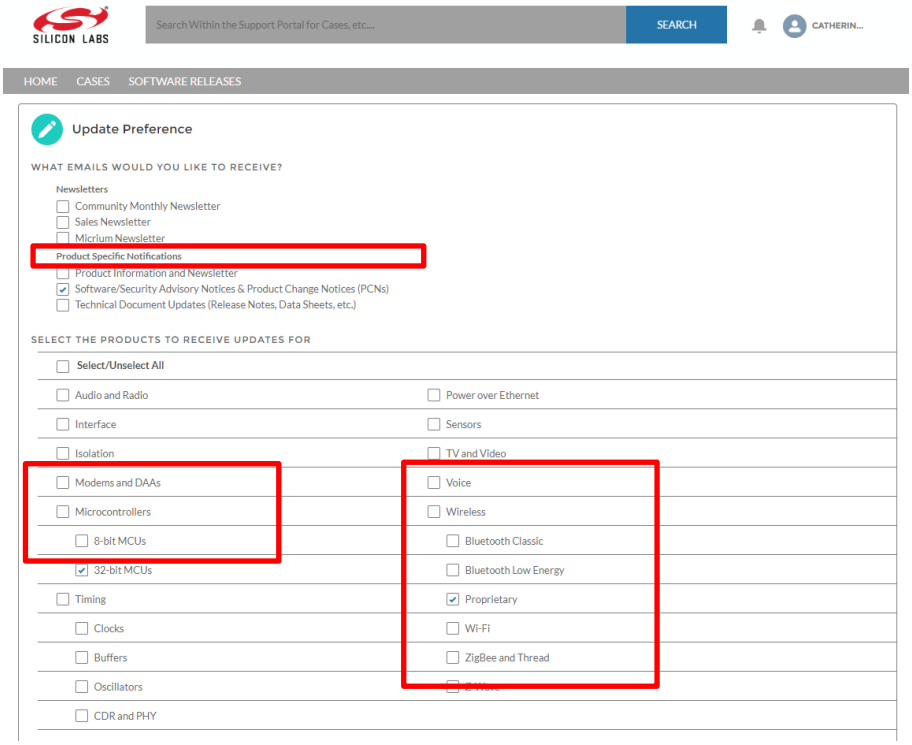
User applications never need to interact with the majority of these keys. Existing APIs to manage Link Key Table keys or Transient Keys are still available to the user application and now route through the Zigbee Security Manager component.

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.



8.3 Support

Development Kit customers are eligible for training and technical support. Use the Silicon Laboratories Zigbee web page 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.

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

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

www.silabs.com