



Zigbee EmberZNet SDK 7.2.0.0 GA

Gecko SDK Suite 4.2

December 14, 2022

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):

7.2.0.0 released December 14, 2022



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 Items3
 - 1.1 New Features.....3
 - 1.2 New Applications.....3
 - 1.3 New Components.....3
 - 1.4 New APIs.....4
 - 1.5 New CLI Commands4
 - 1.6 New Platform Support5
 - 1.7 New Documentation.....5
- 2 Improvements.....6
- 3 Fixed Issues7
- 4 Known Issues in the Current Release9
- 5 Deprecated Items12
- 6 Removed Items13
- 7 Multiprotocol Gateway and RCP.....14
 - 7.1 New Items.....14
 - 7.2 Improvements14
 - 7.3 Fixed Issues.....14
 - 7.4 Known Issues in the Current Release15
 - 7.5 Deprecated Items.....15
 - 7.6 Removed Items.....15
- 8 Using This Release.....16
 - 8.1 Installation and Use.....16
 - 8.2 Security Information16
 - 8.3 Support.....17

1 New Items

1.1 New Features

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 EMO 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 7.2.0.0

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 7.2.0.0

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 7.2.0.0

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 subgigahertz 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 7.2.0.0

ID #	Description
498094	Fixed an issue in function <code>checkForReportingConfig()</code> in <code>metering-server.c</code> where the second input parameter of the invoked function <code>emberAfContainsServer()</code> had incorrectly referenced the cluster ID instead of the attribute ID.
657626	OTA update with page request can now handle up to <code>EMBER_AF_PLUGIN_EEPROM_PARTIAL_WORD_STORAGE_COUNT</code> 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 <code>emberPacketHandoffIncoming</code> to receive bad index for <code>EMBER_ZIGBEE_PACKET_TYPE_NWK_DATA/EMBER_ZIGBEE_PACKET_TYPE_NWK_COMMAND</code> 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 <code>DynamicMultiprotocolLight</code> . 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 "ncc-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 <code>DynamicMultiprotocolLight</code> and <code>DynamicMultiprotocolLightSed</code> 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 <code>wwah-server-silabs</code> component.
1024651	Fixed an issue where <code>emberAfMessageSentCallback()</code> was not called if child had been removed during the transmission.
1026622	Fixed an issue that caused missing last byte with packet-handoff when <code>EMBER_MANGLE_PACKET</code> is used.
1027200	Fixed an issue where the Key Establishment component sent <code>NO_RESOURCES</code> instead of the required <code>BAD_MESSAGE</code> 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.
1042022	Fixed issue where the Key Establishment component didn't check for minimum command request and command response length.
1058984	The templated callback for <code>message_sent</code> 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.

ID #	Description
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.silabs.com/developers/zigbee-emberznet> in the Tech Docs tab.

ID #	Description	Workaround
N/A	The following apps/components are not supported in this release <ul style="list-style-type: none"> NCP Sleepy EM4 support 	Features will be enabled in subsequent releases.
135649	Multi-networking can cause APS frame counter confusion between networks.	Use <code>emberAfSecurityInitCallback</code> to add <code>EMBER_NO_FRAME_COUNTER_RESET</code> to <code>EmberInitialSecurityBitmask</code> .
193492	<code>emberAfFillCommandGlobalServerToClientConfigureReporting</code> 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.
266341	Z3 Light sample app has two endpoints that support similar cluster commands, so duplicate responses may be generated for certain commands.	No known workaround
271644	A device that performs a classic join to a legacy ZLL gateway may eventually leave the network on its own initiative.	No known workaround
278063	Smart Energy Tunneling plugins have conflicting treatment/usage of address table index.	No known workaround
281832	Green Power Common plugin incorrectly formats <code>groupList</code> and <code>groupListCount</code> parameters of GP Pairing Configuration frame.	No known workaround
289569	Network-creator component power level picklist doesn't offer full range of supported values for EFR32	Edit the range <code><-8..20></code> specified in the CMSIS comment for <code>EMBER_AF_PLUGIN_NETWORK_CREATOR_RADIO_POWER</code> in the <code><sdk>/protocol/zigbee/app/framework/plugin/network-creator/config/network-creator-config.h</code> file. For example, change to <code><-26..20></code> .
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 <code>halCommonGetIntxxMillisecondTick</code> functions on Linux hosts currently use the <code>gettimeofday</code> 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 <code>clock_gettime</code> with the <code>CLOCK_MONOTONIC</code> source instead.
331438	Service discovery may time out too quickly in busy networks.	Define <code>EMBER_AF_DISCOVERY_TIMEOUT_QS</code> to customize the timeout period.
338151	Initializing NCP with a low packet buffer count value may cause corrupt packets.	Use the <code>0xFF</code> reserved value for packet buffer count to avoid the too-low default value
356937	Read/write attribute CLI commands do not support manufacturer-specific ZCL attributes. Some implementations may allow local CLI debug access to display or modify these attributes.	Access the attributes from a remote device in the network via ZCL global <code>Read/WriteAttributes</code> commands.
363162	There is a bug in <code>emberAfAddAddressTableEntry</code> which could allow for duplicate entries in the address table	Under Investigation
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.

ID #	Description	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.
481618	The "Network Open Time" option of the Network Creator Security plugin may not work as expected when you open network if the time does not match the transient key timeout.	Set the Network Open time to the same value as the Transient Key Timeout.
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
521706	A duplicated attribute ID is assigned in the altConsumptionMonthAttrIds[] array of the gas-proxy-function plugins in gpf-structured-data.c.	Change the second ZCL_PREVIOUS_MONTH6_ALTERNATIVE_CONSUMPTION_DELIVERED_ATTRIBUTE_ID to ZCL_PREVIOUS_MONTH7_ALTERNATIVE_CONSUMPTION_DELIVERED_ATTRIBUTE_ID.
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.
621144	GP on/off switch example cannot be compiled for the BRD4183A board.	The sample has to be manually modified to use only one button.
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.

ID #	Description	Workaround
648906 659010	emberChildId and emberChildIndex APIs were accidentally removed in EmberZNet 6.8.0.2.	Call <code>sl_mac_child_short_id</code> and <code>sl_mac_child_index</code> instead.
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 <code>addEntryToGroupTable()</code> can create a spurious binding and cause groupcast reporting messages to be sent.	Add <code>"binding.clusterId = EMBER_AF_INVALID_CLUSTER_ID;"</code> after <code>"binding.type = EMBER_MULTICAST_BINDING;"</code>
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.
758966	Add "Enable command discovery" CMSIS option in <code>zcl_framework_core</code>	No known workaround
760811	In the CPCd configuration, if <code>STDOUT_TRACE</code> and <code>TRACE_TO_FILE</code> are both disabled, a timing issue with CPC causes the Zigbee endpoint to close on some setups.	For a short-term workaround, enable traces using either <code>STDOUT_TRACE</code> or <code>TRACE_TO_FILE</code> .
765735	The OTA update fails on Sleepy End Device with enabled Page Request.	Use Block Request instead of Page Request.
823617	The watchdog cannot be enabled on MG24 device for Zigbee applications in this release.	No known workaround
829647	<code>emberAfSendUnicastWithCallback()</code> never fires the callback for fragmented messages: When sending a message large enough to require fragmentation with <code>emberAfSendUnicastWithCallback()</code> , the callback is never called.	No known workaround
845649	Removing CLI:Core component does not eliminate EEPROM cli calls to <code>sl_cli.h</code>.	Delete the <code>eeprom-cli.c</code> file that calls the <code>sl_cli.h</code>. Additionally, calls to <code>sl_cli.h</code> as well as <code>sl_cli_command_arg_t</code> in the <code>ota-storage-simple-eeprom</code> can be commented out.
857200	<code>ias-zone-server.c</code> 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
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.

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 7.2.0.0

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 7.2.0.0

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

None

7.3 Fixed Issues

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 multipan 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.slcpc 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.
1032183	Zigbeed does not support EZSP coex commands.	Support is planned in a future release.
1036645	BGAPI host app cannot connect to multiprotocol NCP via CPC after a reset.	Reset CPCd or the NCP. This will be fixed in the next patch release.
1076235	ot-cli does not run in the multiprotocol docker container due to a library version mismatch.	The issue can be worked around using the following shell commands: '/run.sh -o; cd /lib/arm-linux-gnueabi; ln -s libreadline.so libreadline.so.7'
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.
1080517	Z3GatewayCPC does not currently automatically handle a reset of the NCP (CPC secondary).	Restart the Z3GatewayCPC process after the NCP has been reset.

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.

The screenshot shows the 'Update Preference' page in the Silicon Labs customer portal. The page is titled 'Update Preference' and has a search bar at the top. Below the search bar, there are navigation links for 'HOME', 'CASES', and 'SOFTWARE RELEASES'. The main content area is divided into two sections: 'WHAT EMAILS WOULD YOU LIKE TO RECEIVE?' and 'SELECT THE PRODUCTS TO RECEIVE UPDATES FOR'.

In the 'WHAT EMAILS WOULD YOU LIKE TO RECEIVE?' section, there are two sub-sections: 'Newsletters' and 'Product Specific Notifications'. The 'Product Specific Notifications' section has a red box around it, and the 'Software/Security Advisory Notices & Product Change Notices (PCNs)' checkbox is checked.

In the 'SELECT THE PRODUCTS TO RECEIVE UPDATES FOR' section, there are two red boxes. The first red box is around the 'Modems and DAAs' and 'Microcontrollers' categories, with the '32-bit MCUs' checkbox checked. The second red box is around the 'Voice' and 'Wireless' categories, with the 'Proprietary' checkbox checked.

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

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 implementers 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 information 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.

Note: This content may contain offensive terminology that is now obsolete. Silicon Labs is replacing these terms with inclusive language wherever possible. For more information, visit www.silabs.com/about-us/inclusive-lexicon-project

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, ThreadArch[®], 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