



# Zigbee EmberZNet SDK 8.1 GA

## Simplicity SDK Suite 2024.12.0

### December 16, 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):

8.1 released December 16, 2024



#### KEY FEATURES

##### Zigbee

- -250+ entries in APS link key table
- ZigbeeD support on Android 12 (v21.0.6113669) and Tizen (v0.1-13.1)
- xG26 Module support

##### Multiprotocol

- ZigbeeD and OTBR support on OpenWRT – GA
- DMP BLE + CMP ZB & Matter/OT with Concurrent Listening on MG26 for SoC – GA
- 802.15.4 Unified radio scheduler priority component
- Debian packaging support for MP host applications - Alpha

## Compatibility and Use Notices

For information about security updates and notices, see the Security chapter of the 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 9.40.1.

- Using wine to build with the larBuild.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 0x10.

**Contents**

- 1 New Items ..... 3
  - 1.1 Important Changes ..... 3
  - 1.2 New Components ..... 3
  - 1.3 New APIs ..... 3
  - 1.4 New Platform Support ..... 3
  - 1.5 New Documentation ..... 4
  - 1.6 New Application ..... 4
  - 1.7 Intended Behavior ..... 4
- 2 Improvements ..... 5
- 3 Fixed Issues ..... 6
- 4 Known Issues in the Current Release ..... 10
- 5 Deprecated Items ..... 14
- 6 Removed Items ..... 15
- 7 Network Limitations and Considerations ..... 16
- 8 Multiprotocol Gateway and RCP ..... 17
  - 8.1 New Items ..... 17
  - 8.2 Improvements ..... 17
  - 8.3 Fixed Issues ..... 17
  - 8.4 Known Issues in the Current Release ..... 18
  - 8.5 Deprecated Items ..... 18
  - 8.6 Removed Items ..... 18
- 9 Using This Release ..... 19
  - 9.1 Installation and Use ..... 19
  - 9.2 Security Information ..... 19
  - 9.3 Support ..... 20
  - 9.4 SDK Release and Maintenance Policy ..... 20
  - 9.5 Zigbee Certification ..... 20

# 1 New Items

## 1.1 Important Changes

The APS link key table size (configured using `SL_ZIGBEE_KEY_TABLE_SIZE`) is expanded from 127 to 254 entries.

- R23 support is added for ZDD Network commissioning functionality. Tunneling functionality is available without support for Legacy Network use cases.
- The Network Steering and Network Creator components have been updated to include support for R23 joining. These include the following related changes.
  - The default Trust Center Link Key (TCLK) request policy has been updated to generate new keys for each requesting device. A new key is generated each time the requesting devices attempt to update their Trust Center Link Key.
  - Due to the previous TCLK policy change, the Network Creator Security component now requires the Security Link Keys component. Applications upgrading will be updated to conform to this new requirement.
  - A new configuration, `SL_ZIGBEE_AF_PLUGIN_NETWORK_CREATOR_SECURITY_ALLOW_TC_USING_HASHED_LINK_KEY`, is added to allow joining using a core, hashed key. This configuration is found under the Network Creator Security component. Use of this policy allows each joining device to receive a unique TCLK post-join, but repeated attempts to update the TCLK will not result in a new key for the requesting device. This using of hashed link keys was the default policy before this release, and use of this policy allows the Trust Center to avoid bringing in the Security Link Keys component, which saves keys in flash. Note: Silicon Labs does not recommend use of this policy, as this prevents joining devices from rolling, or updating, their TCLKs.
- A new configuration set is added to the component `zigbee_ezsp_spi` to allow configuration of host SPI device and its pin interfaces.
- The example projects, including the project files (.slcps) and project folder, are renamed to Silicon labs naming guidelines and moved under “projects” directory.

## 1.2 New Components

None.

## 1.3 New APIs

None.

## 1.4 New Platform Support

- New modules
  - MGM260PD32VNA2
  - MGM260PD32VNN2
  - MGM260PD22VNA2
  - MGM260PB32VNA5
  - MGM260PB32VNN5
  - MGM260PB22VNA5
  - BGM260PB22VNA2
  - BGM260PB32VNA2
- New radio boards
  - MGM260P-RB4350A
  - MGM260P-RB4351A
- New part
  - efr32xg27
- Explorer Kit
  - BRD2709A
  - MGM260P-EK2713A

## 1.5 New Documentation

- A new EZSP user guide UG600 for releases 8.1 and above.

## 1.6 New Application

None.

## 1.7 Intended Behavior

None.

## 2 Improvements

- SL\_ZIGBEE\_KEY\_TABLE\_SIZE limits expanded up to 254 entries.
- Added zigbee\_security\_link\_keys to Z3Light.
- Added zigbee\_security\_link\_keys to zigbee\_mp\_z3\_tc\_z3\_tc. Updated its key table size as well.
- Increased the Z3 Gateway key table size (that will be set to ncp) to 20.

### 3 Fixed Issues

ID #	Description
1043514	Fixed a potential issue when the neighbor table size on an end device is configured greater than 1 by flagging an error at the generation step.
1105979	Renamed component zigbee_app_framework_common to zigbee_system_common. Renamed source files, header files zigbee_app_framework_common to sl_zigbee_system_common. Added priority to function sli_zigbee_ncp_tick_callback in order to reorder autogen function.
1240421	Added all R23 pro-compliance CLIs to ZUTH.
1254397	Added mutex protection for App Framework event queue so App Framework event APIs can be called from multiple tasks.
1259298	Fixed an issue with the label of the pro leaf stack.
1265831	Fixed an issue on NCP where source route overhead should always present for incoming message callback.
1275779	Added a global processing that sends a success default response when the ZCL command was handled successfully but no response was sent, and removed the manually triggered success default responses in cluster command handler.
1277857	Fixed an issue that caused GPD Commissioning Reply to be filtered at the test harness. Also, added support for quick response for GPDF with App ID 0x02.
1294341	Fixed an issue that caused zigbee AF debug prints to add an extra line.
1296881	After a new end device joined on the sub-GHz band, the duty cycle aging data was mistakenly cleared for all end device children.
1298015	Removed the indirection through sli_zigbee_common_wakeup_isr which was only being used for an internal component and was made redundant by preceding calls in the same call chain.
1297976	<p>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.</p> <p>Note the following information on GPIOs that maps to the SPI NCP interface. On kernel 6.6, running</p> <pre>sudo cat /sys/kernel/debug/gpio</pre> <p>That will display following</p> <pre>gpio-520 (GPIO8 ) gpio-534 (GPIO22 ) gpio-535 (GPIO23 ) gpio-536 (GPIO24 )</pre> <p>redefine the GPIO for SPI NCP interface from above sysfs in spi-protocol-linux-config.h as</p> <pre>#define NCP_CHIP_SELECT_GPIO "520" #define NCP_HOST_INT_GPIO "534" #define NCP_RESET_GPIO "535" #define NCP_WAKE_GPIO "536"</pre>
1300935	Fixed excess default response from Z3Gateway for OTA cluster.
1305214	sl_zigbee_mac_filter_match_list has been fixed to work properly in RTOS builds. The API now relies fully on list_length to parse the length of the passed-in filter list, and the length of a MAC filter match list has a limit of 32 (SL_802154MAC_FILTER_MATCH_LIST_MAX_LENGTH).
1306512	Introduced new APIs to allow customers Set/Get CTUNE value via mfglib mode with command plugin mfglib ctune set/get. Changing CTUNE only in mfglib normal mode, it can't be set in tone/stream operations.
1307470	Tizen-13.1 specific 32 bit and 64 bit libraries with soft floating point support have been added to the list of Zigbee library variants. Zigbeed could be generated and built with these libraries using zigbee_aarch64_tizen_13_1_gcc_9_2 or zigbee_arm7l_tizen_13_1_gcc_9_2 components.
1309915	Zigbeed libraries for Android ndk-r25c have been added to our list of supported variants. To use these libraries, Zigbeed needs to be generated with the newly added zigbee_aarch64_android_ndk_r25c component, and built with adnroid-ndk-r25c or compatible compilers.
1310485	Reworked internal stack buffer initialization to acquire memory for buffer heap via library code callback.

ID #	Description
1310501	The DMP Tuning component is now deprecated. Users may refer to the '802.15.4 Unified radio scheduler priority' (radio_priority_15_4) component in its place to alter stack radio priorities. This component allows configuration of radio priorities for transmits, background receive, and active receive states of the 802.15.4 radio in a single-stack and multiprotocol scenario.
1312065	Fixed an issue where the non-stub implementation of sl_zigbee_child_index() was incorrectly placed inside the Zigbee R22 Support library, causing it to return an invalid index for builds that do not use that library.
1312097	Fixed an issue that could pass an invalid mac layer packet to cause an assert.
1312099	Fixed an issue that could pass an APS malformed packet to cause a bus fault.
1312369	Made SL_LEGACY_HAL_WDOG_IRQHandler() weak function, that allows customers to provide their own implementation.
1314347	Adjusted "find_and_bind" CLI to "find-and-bind" to conform to CLI naming convention.
1315570	Token Manager shouldn't assert in cases when the NVM3 cache is too small. Instead, we print a warning on a debug firmware, and also introduce sl_token_manager_assert_on_cache_overflow_callback that determines whether we want to assert on the NVM3 cache overflow or not.
1316959	Fixed a compile issue when enabling multi-network on a standard app.
1318352	Reorganized all Zigbee and MP apps into a common app/projects folder.
1321780	Fixed an issue that cause the DUT dropping the GPDF commissioning from GPD which has IntraPAN set to 0, and source PAN ID presents.
1327706	The EZSP_MAX_FRAME_LENGTH is reverted back to 220. This allows the maximum length of XNCP message to be 220 as well.
1328991	Fixed an issue that caused some GP proxy tests to fail on RCP setup.
1330292	Added R23 support for network steering/network creator (initial join).
1330418	Fixed an issue where the beaconPayloadStartIndex was incorrect when parsing the beacon tlvs.
1331483	Updated the CPC host app usage text to bring it in line with currently supported functionality.
1331580	Fixed an issue in handling unsolicited rejoin response.
1331924	Introduced new APIs to allow customers a Set/Get CTUNE value via mfglib mode with command plugin mfglib ctune set/get. When changing CTUNE only in mfglib normal mode, it could not be set in tone/stream operations.
1332086	Fixed an issue that caused MAC Address Filtering component to be always dependent on the CLI component.
1332364	Upgraded host_token.nvm (zigbeed) on the host to use new file format.
1332932	Zigbee Direct: ZDD's Tunneling Service now supports receiving multiple NPDUs in a single connection interval. Zigbee Direct: ZDD will buffer outgoing NPDUs to the ZVD beyond what can be exchanged in a single connection interval
1334060	Fixed an issue on GP RCP interface that caused some GP proxy tests to fail.
1334549	Fixed an issue in some GPD apps's initialization that caused a RAIL crash.
1334581	Fixed an issue that caused the reported LQI and RSSI always zero on Z3Gateway.
1337956	Renamed alpha and internal apps according to UX/DX guidelines.
1339456	Added the new configuration, SL_ZIGBEE_AF_PLUGIN_NETWORK_STEERING_ENABLE_AUTOSTART, and a new function, sl_zigbee_af_network_steering_autostart, to network steering. sl_zigbee_af_network_steering_autostart will begin network steering if the configuration is enabled and will otherwise only print a message that the configuration is disabled. This can be used for testing purposes that require more predictable behavior for when network steering is to run.  Custom preconfigured keys (pre-configured-key-set command in network steering CLI) are now compatible with optimized scans.
1341928	Si4468 firmware patch added to phy-pro2plus-library to address race condition in sub-GHz Tx/Rx processing.

ID #	Description
1342410	Expanded link key table to accommodate 254 entries in the stack key table. Each entry represents a piece of security information mapped to a particular EUI64 address. Some devices, depending on the use case, may consume 2 entries in the key table - 1 for APS Link Key, 1 for ZDO Authentication Token (used for Dynamic Link Key). Link Key access APIs remain largely unchanged, although index 255 remains a special reserved value for some APIs.
1342412	SL_ZIGBEE_KEY_TABLE_SIZE limits expanded up to 254 entries.
1344155	Fixed an issue of enumeration mismatch for EmberLeaveRequestFlags.
1345981	Custom Basic tokens are non-indexed type, which should not be accessed by index, unlike indexed tokens. While using sl_token_get_data, the index 0x7F should be used.
1348659	Fixed an issue that caused starting find and bind target on two endpoints at the same time get stuck in an infinite loop in Z3Gateway host application and crash reboot on Z3Light SoC.
1348673	Fixed an issue that caused the end device joining failure through the router when R23 and DLK were enabled.
1349749	Extraneous ZCL Default Responses with ZCL Success status were sent in response to cluster-specific ZCL commands even when a specific ZCL response was already being sent for that command.
1350285	In rare cases, a packet was passed to the Outgoing Packet Handoff Callback with a payload index parameter that exceeded the stated length of the packet buffer, leading to an assert in legacy-packet-buffer.c if the Packet Handoff component was enabled.
1351489	Fixed an issue that caused LQI Response to be received with MAC address as All Zeros.
1351894	Added new library variant of Zigbee PRO Router Stack, which provides support for rail mux, separate from the already existing variant which combines it with high-datarate PHY support.
1352421	Added RX packet information to GP handlers at the application layer.
1354519	Fixed issue that caused the APS Verify Key Confirm message processing error.
1355430	Fixed warning on mismatched sli_mac_upper_mac_state declaration.
1356289	Stack functions that use Buffer Manager APIs to extend/append a packet buffer now perform additional sanity-checking to avoid conditions where insufficient heap space exists to extend the buffer length.
1357515	Fixed an issue that caused build errors when the secondary network has the SLI_ZIGBEE_NETWORK_SECURITY_TYPE_SE_FULL type since key-establishment.c expects this to be mapped to the EMBER_AF_HAS_SECURITY_PROFILE_SE_FULL define.
1358823	Fixed an issue with ZCP tests where the new link key sent by TC with policy sent a current key that was not hashed.
1360076	Zigbee Direct: Fixed handling of authentication of new ZVD to help pass Zigbee Direct Testcases ZDD-CONF-TC-02-CENTR-ZC-0 and ZDD-CONF-TC-02-DISTR.
1355154	Fixed an issue in the attribute metadata that caused the access of Electrical Measurement attributes to be read-only instead of read-write as per the ZCL Specification.
1363780	Fixed several warning in the framework code with IAR compiler.
1366437	Added ezsp.yaml, a machine-readable version of the EZSP specification.
1367530	Removed the usage of SL_ZIGBEE_KEY_TABLE_SIZE on the host. From now on, the link key table size will be stored where the stack is running, such as SoC, NCP, or zigbeed images.
1367899	Fixed an issue that prevented incoming GP message to the NCP (with GP plugin installed) passing to the host.
1368790	Fixed RAIL Mux did not forward packets to upper layer when application was running in mfglib mode.
1370016	Increased the GP_INCOMING_FC_TOKEN_TIMEOUT upper limit, so customers can adjust to avoid the flash from quickly wearing out.
1356760	A new configuration item, SL_ZIGBEE_AF_PLUGIN_ZCL_CLUSTER_DEFER_ATTRIBUTE_WRITES_TO_NVM_MS, has been added under the ZCL Framework Core component. This configuration item allows the user to defer updating NVM by a specified delay when a ZCL attribute's value is changed. This option is used where an attribute might be getting updated many times in a short time interval, flash access is slower, such as with external flash parts, or if the number of writes to flash is of concern.



ID #	Description
1379172	New Component: Radio Priority Configurator Added a new component named "radio_priority_configurator." This component allows Zigbee/multiprotocol projects to use the Radio Priority Configurator tool in Simplicity Studio to configure the radio priority levels of the 802.15.4 stack.
1383387	An issue has been fixed where a device was unable to join a network, with the message "Error: Scan complete handler returned 0x44" printed on the console during the scan process. This error stopped all transmits on the device and is now resolved.
1379187	Fixed race condition where CSL changed lower mac state in an interrupt context which caused an assertion in lower mac on zigbee_ble_sleepy_to_sleepy_shades app

## 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/component is not supported in this release: EM4 support.	Feature 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 <code>EMBER_AF_PLUGIN_NETWORK_CREATOR_RADIO_POWER</code> in the <code>&lt;sdk&gt;/protocol/zigbee/app/framework/plugin/network-creator/config/network-creator-config.h</code> 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 <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.
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
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 <code>ImageBlockResponses</code> to a size where the APS fragmentation is activated. This could lead to the OTA process failing.	No known workaround
486369	If a <code>DynamicMultiProtocolLightSoc</code> forming a new network has child nodes remaining from a network it has left, <code>emberAfGetChildTableSize</code> returns a non-zero value in <code>startIdentifyOnAllChildNodes</code> , 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 <code>emberRemoveChild</code> 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

ID #	Description	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-eeeprom 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
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. <a href="https://www.silabs.com/documents/public/application-notes/an1322-dynamic-multi-protocol-bluetooth-zigbee-sdk-7x.pdf">https://www.silabs.com/documents/public/application-notes/an1322-dynamic-multi-protocol-bluetooth-zigbee-sdk-7x.pdf</a> .
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.
1161063	Z3Light and potentially other applications report incorrect cluster revision values.	Manually update the cluster revision attribute to their appropriate revision.
1164768, 1171478, 1171479	ERROR: ezspErrorHandler 0x34 reported repeatedly during mfglib receive mode	To reduce the error messages printed, configure EMBER_AF_PLUGIN_GATEWAY_MAX_WAIT_FOR_EVENT_TIMEOUT_MS on the host app to 100, so the callback queue is freed more quickly.
1254368	Fragmentation of new Zigbee 2023 ZDO messages is not supported in this release	No known workaround. This will be supported in the next planned release.

ID #	Description	Workaround
1352533	sl_zigbee_token_factory_reset triggers watchdog when the link key table size is set to 120 or larger.	<p>Update the source code implementation of the function <code>sl_zigbee_token_factory_reset</code> in <code>zigbee_token_interface.c</code> to pet the watchdog in the inner most for loop as shown here.</p> <pre> void sl_zigbee_token_factory_reset(bool exclude_outgoing_fc, bool exclude_boot_counter) {     uint8_t num_of_tokens = sl_zigbee_get_token_count();     for (uint8_t token_idx = 0; token_idx &lt; num_of_tokens; token_idx++) {         sl_zigbee_token_info_t token_info;         sl_status_t status = sl_zigbee_get_token_info(token_idx, &amp;token_info);         if (status == SL_STATUS_OK) {             if (!is_token_excluded(exclude_outgoing_fc, exclude_boot_counter, token_info.nvm3Key)) {                 for (uint8_t arrayIndex = 0; arrayIndex &lt; token_info.arraySize; arrayIndex++) {                     sl_zigbee_token_data_t token_data;                     token_data.size = token_info.size;                     token_data.data = (void*) tokenDefaults[token_idx];                     // restore to default token value                     sl_zigbee_set_token_data(token_info.nvm3Key, arrayIndex, &amp;token_data);                      halResetWatchdog();                 }                 halResetWatchdog();             }         }     } } #endif SL_CATALOG_ZIGBEE_SECURE_KEY_STORAGE_PR ESENT // delete all zigbee managed psa keys zb_sec_man_delete_all_keys(); #endif // SL_CATALOG_ZIGBEE_SECURE_KEY_STORAGE_PR ESENT } </pre>

ID #	Description	Workaround
1340230	Network Steering calls network_found infinitely when too many beacons are present.	<p>Two possible workarounds:</p> <p>1. The first workaround was provided by a customer and is as follows:</p> <pre>EmberNetworkParameters parameters; parameters.radioChannel = BEACON_ITERATOR.beacon.channel; parameters.radioTxPower = radioTxPower; parameters.panId = BEACON_ITERATOR.beacon.panId; MEMCOPY(parameters.extendedPanId, BEACON_ITERATOR.beacon.extendedPanId, EXTENDED_PAN_ID_SIZE); status = emberJoinNetwork(nodeType, &amp;parameters);</pre> <p>2. The second workaround is to simply reset the device.</p>
1377518	NCP SPI - Z3GatewayCpc throwing EZSP 0x39 and 0x28 errors - frequent child table reads.	Perform child table read with minimum delay of 1 second from the last child table read.
1377221	Debug basic and extended is corrupting CLI.	No known workaround.
1369186	Address table size is not configurable for NCP.	<p>Address table size is now configurable on NCP using dynamic allocation based on the resource requirement. It does not have a configuration item like previous releases.</p> <p>But if it is needed to get configured from application or project scope, the workaround would be to define the SL_ZIGBEE_ADDRESS_TABLE_SIZE at the project level.</p>

## 5 Deprecated Items

- 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: Enable the watchdog timer with configuration item `SL_LEGACY_HAL_DISABLE_WATCHDOG` set to 0 in your application.

---

## 6 Removed Items

None.

## 7 Network Limitations and Considerations

The default Trust Center applications that come shipped with this EmberZNet release are capable of supporting a number of devices on the network. This number is determined based on several factors, including configured table sizes, NVM usage, and other generation-time and run-time values.

User seeking to create large networks may face resource issues when growing the network larger than the application can support. For example, a device requesting a Trust Center Link Key from the Trust Center may trigger a `sl_zigbee_af_zigbee_key_establishment_cb` callback on the Trust Center with status set to `SL_ZIGBEE_KEY_TABLE_FULL`, indicating that the key table does not have room to add a new key for the requesting device or that NVM3 has no available space.

Silicon Labs provides the following recommendations for users seeking to create large networks. For Trust Center applications, the following configurations are recommended. These recommendations are not exhaustive, and they serve as a baseline for applications intending to grow large networks.

- Inclusion of the Address Table component (`zigbee_address_table`), with
  - the `SL_ZIGBEE_AF_PLUGIN_ADDRESS_TABLE_SIZE` configuration item set to the size of the desired network
  - the `SL_ZIGBEE_AF_PLUGIN_ADDRESS_TABLE_TRUST_CENTER_CACHE_SIZE` value set to the maximum (4)
- Inclusion of the Security Link Keys component (`zigbee_security_link_keys`), with
  - The `SL_ZIGBEE_KEY_TABLE_SIZE` value set to the size of the network
- The following configuration items set to the size of the desired network
  - `SL_ZIGBEE_BROADCAST_TABLE_SIZE`, as found in the Zigbee Pro Stack component
  - `SL_ZIGBEE_SOURCE_ROUTE_TABLE_SIZE`, as found in the Source routing component, if source routing is used
- Adjustment of `NVM3_DEFAULT_NVM_SIZE` and `NVM3_DEFAULT_CACHE_SIZE` according to NVM3 usage
  - E.g. network sizes greater than 65 nodes likely require an NVM3 size of 64K. The default NVM3 size in Silicon Labs Zigbee sample applications is 32K. Applications that use NVM more heavily may require adjusting this value even higher.
  - Large networks up to 65 nodes may need a NVM3 cache size of 1200 bytes; growing networks larger than that may require doubling this value to 2400 bytes.

These adjustments apply to the Trust Center only.



## 8 Multiprotocol Gateway and RCP

### 8.1 New Items

Enabled GA SoC support for BLE DMP with Zigbee + Openthread CMP with concurrent listening on xG26 parts.

Debian alpha support has been added for zigbeed, OTBR and Z3Gateway applications. Zigbeed and OTBR are provided in DEB package format for the chosen reference platform (Raspberry PI 4) as well. See *Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol Co-Processor*, found at [docs.silabs.com](https://docs.silabs.com), for details.

Added Zigbeed support for Tizen-0.1-13.1 for arm32 and aarch64 as well as Android 12 for aarch64. More information on Zigbeed can be found at [docs.silabs.com](https://docs.silabs.com).

Added the new “802.15.4 Unified radio scheduler priority” component. This component is used to configure the radio priorities of a 15.4 stack. The component also requires the new “radio\_priority\_configurator” component. This component allows projects to use the Radio Priority Configurator tool in Simplicity Studio to configure the radio priority levels of the stacks that require it.

### 8.2 Improvements

Application note *Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol Co-Processor* (AN1333) has been moved to [docs.silabs.com](https://docs.silabs.com).

OpenWRT support is now GA quality. OpenWRT support has been added for zigbeed, OTBR and Z3Gateway applications. Zigbeed and OTBR are provided in IPK package format for the reference platform (Raspberry PI 4) as well. See *Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol Co-Processor*, found at [docs.silabs.com](https://docs.silabs.com), for details.

### 8.3 Fixed Issues

ID #	Description
1275378	Fixed an issue where calling <code>sl_802154_radio_set_scheduler_priorities()</code> prior to <code>sl_mac_lower_mac_init()</code> could result in a crash.
1300848	Fixed an issue where Z3Gateway in OpenWRT environment couldn't start EZSP communication caused by mismatching termios control characters running on OpenWRT and other environments.
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.
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).
1337228	In Zigbeed the <code>halCommonGetInt32uMillisecondTick()</code> tick API is now updated to use MONOTONIC clock, so that it does not get affected by the NTP in a host system.
1337295	The DMP CLI command “plugin ble gap print-connections” will now print “No BLE connections” if the connection table is empty, instead of providing no response.
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.
1346849	Adding the <code>rail_mux</code> components to a project will now cause it to automatically build with the associated stack library variants.
1365665	Fixed an issue where the host would report receiving a packet with an invalid checksum on end-point 12.

## 8.4 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/simplicity-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.
1209958	The ZB/OT/BLE RCP using concurrent listening on MG24 and MG21 may stop working in endurance test (lasts ~2 hours) with constant and concurrent traffic on all 3 stacks.	Disable concurrent listening in use cases involving constant and concurrent traffic across all 3 protocols.
1221299	Mfglib RSSI readings differ between RCP and NCP.	Will be addressed in a future release.
1385197	<b>The Gecko Bootloader application interface API for DMA-based operations of the Internal Storage Bootloader cannot be used with Concurrent Listening (enabled via the rail_util_ieee802154_fast_channel_switching component). This affects all Bootloader API calls made by the application, such as the OTA update logic. The issue is present on MG21, MG24, and MG26 parts.</b>	<b>If the application enables Concurrent Listening and uses the internal storage bootloader, this workaround must be applied for OTA updates to work on MG26. The Internal Storage Bootloader must be built with BOOTLOADER_MSC_DMA_WRITE set to false. In Simplicity Studio, this configuration is found in the Internal Storage component under Platform→Bootloader→Storage. For MG21 and MG24, contact support for additional details.</b>

## 8.5 Deprecated Items

The "Multiprotocol Container" which is currently available on DockerHub (siliconlabsinc/multiprotocol) will be deprecated in an upcoming release. The container will no longer be updated and able to be pulled from DockerHub. The Debian-based packages for cpdc, zigbeed, and ot-br-posix, along with natively generated and compiled projects, will replace the functionality lost with the removal of the container.

## 8.6 Removed Items

None.

## 9 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.

### 9.1 Installation and Use

The Zigbee EmberZNet SDK is provided as part of the Simplicity SDK, the suite of Silicon Labs SDKs. To quickly get started with the Simplicity SDK, install [Simplicity Studio 5](#), which will set up your development environment and walk you through Simplicity SDK 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, Simplicity SDK may be installed manually by downloading or cloning the latest from GitHub. See [https://github.com/SiliconLabs/simplicity\\_sdk](https://github.com/SiliconLabs/simplicity_sdk) for more information.

Simplicity Studio installs the Simplicity SDK by default in:

- (Windows): C:\Users\- (MacOS): /Users/<NAME>/SimplicityStudio/SDKs/simplicity\_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/>.

### 9.2 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 first section, the 'Software/Security Advisory Notices & Product Change Notices (PCNs)' checkbox is checked and highlighted with a red box. In the second section, the '32-bit MCUs' checkbox is checked and highlighted with a red box, and the 'Proprietary' checkbox is also checked and highlighted with a red box.

## 9.3 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>.

## 9.4 SDK Release and Maintenance Policy

For details, see [SDK Release and Maintenance Policy](#).

## 9.5 Zigbee Certification

The **Ember ZNet 8.1** release has been qualified for Zigbee Compliant Platform for SoC, NCP and RCP architectures. For ZCP certification ID tied to this release, please check the CSA website here: [https://csa-iot.org/csa-iot\\_products/](https://csa-iot.org/csa-iot_products/).

Please note that the ZCP certification is filed post the release, and takes a few weeks before getting reflected on the CSA website. For any further queries, please 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](http://www.silabs.com/IoT)



**SW/HW**  
[www.silabs.com/simplicity](http://www.silabs.com/simplicity)



**Quality**  
[www.silabs.com/quality](http://www.silabs.com/quality)



**Support & Community**  
[www.silabs.com/community](http://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.

## Trademark Information

Silicon Laboratories Inc.<sup>®</sup>, Silicon Laboratories<sup>®</sup>, Silicon Labs<sup>®</sup>, SiLabs<sup>®</sup> and the Silicon Labs logo<sup>®</sup>, Bluegiga<sup>®</sup>, Bluegiga Logo<sup>®</sup>, EFM<sup>®</sup>, EFM32<sup>®</sup>, EFR, Ember<sup>®</sup>, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Redpine Signals<sup>®</sup>, WiSeConnect, n-Link, EZLink<sup>®</sup>, EZRadio<sup>®</sup>, EZRadioPRO<sup>®</sup>, Gecko<sup>®</sup>, Gecko OS, Gecko OS Studio, Precision32<sup>®</sup>, Simplicity Studio<sup>®</sup>, Telegesis, the Telegesis Logo<sup>®</sup>, USBXpress<sup>®</sup>, Zentri, the Zentri logo and Zentri DMS, Z-Wave<sup>®</sup>, 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](http://www.silabs.com)