Zigbee EmberZNet SDK 7.3.1.0 GA
Gecko SDK Suite 4.3
July 26, 2023

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):

7.3.1.0 released July 26, 2023
7.3.0.0 released June 7, 2023

Zigbee

KEY FEATURES

Zigbee

- Zigbee R23 compliance, with these Security enhancements among others:
  - Dynamic link key negotiation
  - Device interview to query devices before they are allowed to join
  - Trust Center Swap Out to replace an existing Trust Center with a new one
  - Frame Counter Synchronization
- Zigbee Direct Device (ZDD) support for:
  - Onboarding/commissioning
  - Communication to all Zigbee devices without a hub (Alpha), using Bluetooth LE
- Zigbee Smart Energy 1.4a compliance (Alpha)
- Enhancements to Zigbee GP APIs
- New Zigbee Security upgrade component for moving encryption keys from cleartext NVM3 tokens into secure storage

Multiprotocol

- Zigbee/OpenThread Concurrent Multiprotocol SoC sample app
- CPC GPIO expander module
- Zigbeed enhancements

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

1.1 New Features

New in release 7.3.1.0

Zigbee R23 Feature

- **Enable fragmentation for R23.** Zigbee R23 incorporates APS datagram fragmentation at the stack level. This means that R23 stacks will always enable fragmentation, as well as performing fragmentation on certain ZDO clusters.
- **Introduce new capabilities to join combining Network Commissioning command frames with Dynamic Link Key Negotiation and APS Relay frames.** This allows for a joining device to establish a unique APS link key with the Trust Center before being authorized on a centralized network. This unique link key can then be used to encrypt the Network Key when joining the network, which eliminates a potential vulnerability to passive listening attacks. Additionally, when performing "Dynamic Commissioning" this way, the TC application is permitted to perform transactions with the joining device before issuing the Network Key, to authenticate capabilities or query device data.
- **Introduce new APS Relay frames**. These facilitate communication between Joining Devices, the Trust Center, and the joiner's immediate parent node. Messages sent "Downstream" from the TC to the Joiner and "Upstream" in the reverse direction, are routed via the parent node, which handles the network layer framing on behalf of the terminal nodes.

New in release 7.3.0.0

Zigbee Direct Device (ZDD)

ZDD is a full Zigbee device running an additional Bluetooth LE (BLE) stack that enables BLE communications with the Zigbee Virtual Device (ZVD). This supports the following features:

- Onboarding/commissioning: (Set up or add devices to the Zigbee network)
- Control: Send/receive Zigbee data and communicate to all Zigbee devices without a hub (Alpha), using Bluetooth Low Energy.

Secure Vault

Added the Zigbee Secure Key Storage Upgrade component to support migration of key data from classic key storage into secure key storage, allowing for secure key storage to be added to existing deployments of Secure Vault High devices.

SE 1.4 CCB Spec Updates

This release updates the Smart Energy 1.4a Specification CCBs (alpha).

Green power endpoint support on NCP

This release updates green power cluster and framework components to enable the green power endpoint, cluster configuration and command processing to be added on an NCP application.

Zigbee R23 Feature

Added support for Zigbee Revision 23 (available through zigbee_r23_support and zigbee_zdo_dlk_negotiation components and their corresponding libraries). The main library contains functionality including variable length TLV payloads, support for new ZDO clusters, and network updates to joining and link cost measurements. Additional enhancements to joining and overall security features can be added with the Dynamic Commissioning feature, enabling establishment of Trust Center Link Keys during joining via Dynamic Link Key Negotiation.

Added new security primitives to facilitate negotiating Dynamic APS Link Keys.

Dynamic Commissioning enables devices on a Centralized Network to establish new symmetric encryption keys utilizing Secure Pass-phrase Ephemeral Key Exchange, powered by contemporary Elliptic Curve Cryptography technique.

R23 stacks will automatically detect potential parents that support R23 features, and join via Network Commissioning frames (for both Join and Rejoin). If no suitable beacons are observed during joining, the stack will fall back to use existing frames (MAC Association for Join, NWK Rejoin).

Added a Zigbee TLV processing modules for handling new serial data format introduced in Revision 23.

R23 Support adds a new mechanism for Device Authentication. Once established on a Centralized network a device can establish a security token that can be used to authenticate and re-negotiate security credentials across rejoins.

1.2 New Applications

A new sample application for ZDD is added in this release.

- Zigbee - SoC ZigbeeDirectDeviceLight

1.3 New Components

New in release 7.3.1.0

The "zigbee_direct_security_p256" and "zigbee_direct_security_curve25519" components are added so that users can configure a specific Zigbee Direct Security option.

Users are allowed to have multiple "zigbee_direct_security" components enabled on a ZDD application. In this case, the actual security option depends on the ZVD configuration.

New in release 7.3.0.0

Green power endpoint support on NCP Components

The following component consists of a set of necessary resources to allow the Green Power endpoint to function within the NCP framework:

- zigbee_af_support

The following new CLI components are introduced as part of separating the CLI commands from the plugin functionality for Green Power client, server and translation table components:

- Zigbee_green_power_client_cli
- Zigbee_green_power_server_cli
- Zigbee_green_power_translation_table_cli

Processing of the Green Power endpoint needs the Green Power endpoint zap configuration, provided by the following new components for either Green Power combo or proxy:

- Zigbee_green_power_combo_zap_config
- Zigbee_green_power_proxy_zap_config

Zigbee Direct Components

ZDD Command Line Interface component:

- zigbee_direct_cli

Zigbee Direct Device Functionality component that implements the ZDD security and session key negotiations:

- zigbee_direct_zdd

Zigbee Direct Tunneling Functionality component implements the tunneling of data from Zigbee to BLE and vice versa:

- zigbee_direct_tunneling

Smart Energy 1.4a CCB updates

The following new component introduces the new end device type as part of the SE 1.4a spec updates:

- zigbee_phy_2_4_subghz_joining_end_device

Zigbee R23

The following components are part of the R23 feature that is introduced in this release:

- zigbee_dynamic_commissioning
- zigbee_r23_support
- zigbee_security_manager_dlk_ecc
- zigbee_security_manager_host
- zigbee_enhanced_routing
- zigbee_stack_specific_tlv

In a future release more R23 features such as network commissioning with high security join that involves dynamic link key and device interview will be available.

Secure Vault

The following new component is introduced for secure key storage upgrade feature.

- zigbee_secure_key_storage_upgrade

1.4 New APIs

New in release 7.3.1.0

Added new API `sl_zigbee_token_factory_reset` to reset zigbee nvm3 tokens to default value.

New in release 7.3.0.0

Green Power

A new API, `emberAfGreenPowerServerRemoveSinkEntry`, is added for clearing all the entries of the Green Power device for addressing modes with application Id 0 or 2 with the supplied endpoint number 0xFF.

Secure Vault

Added `sl_zb_sec_man_aes_128_crypt_block (bool encrypt, const uint8_t* input, uint8_t* output)` to Zigbee Security Manager, for handling AES block encryption and decryption.

Zigbee Direct Device

The following new public APIs are introduced as part of the ZDD feature. Details are available in the respective component documentation on docs.silabs.com.

ZDD Security APIs

sl_zigbee_direct_handle_authenticate_write

sl_zigbee_direct_calculate_basic_key

sl_zigbee_direct_calculate_admin_key

sl_convert_16bit_uuid_to_128bit_uuid

sl_zigbee_direct_security_encrypt_packet

sl_zigbee_direct_security_decrypt_packet

ZDD Tunnelling APIs

sl_zigbee_direct_tunnel_indicate

sl_zigbee_direct_tunnel_write

Zigbee R23 APIs

The following new public APIs are introduced as part of the Zigbee R23 feature. Details are available in the respective component documentation on docs.silabs.com.

Zigbee R23 Dynamic Commissioning

sli_zigbee_dlk_context_bind

sli_zigbee_dlk_open_key_exchange

sli_zigbee_dlk_close_key_exchange

sli_zigbee_dlk_start_key_exchange

sli_zigbee_dlk_finish_key_exchange

- sl_zigbee_zdo_dlk_get_supported_negotiation_parameters
- sl_zigbee_zdo_dlk_select_negotiation_parameters
- sl_zigbee_zdo_dlk_start_key_update
- sl_zigbee_zdo_dlk_start_key_negotiation

Zigbee R23 TLV Core APIs

- sl_zigbee_tlv_value_byte_length
- sl_zigbee_tlv_get_tag
- sl_zigbee_tlv_set_tag
- sl_zigbee_tlv_get_length
- sl_zigbee_tlv_set_length
- sl_zigbee_tlv_get_value_ptr
- sl_zigbee_tlv_serial_length
- sl_zigbee_tlv_check_general_format_env
- sl_zigbee_tlv_check_general_format
- sl_zigbee_tlv_concat_to_buffer
- sl_zigbee_tlv_search_buffer_payload_for_id
- sl_zigbee_tlv_ptr_find_by_id
- sl_zigbee_encap_tlv_add_tlv
- sl_zigbee_encap_tlv_find_tag_id
- sl_zigbee_tlv_chain_contains_all_tags
- sl_zigbee_tlv_chain_contains_any_tag
- sl_zigbee_tlv_initialize_chain
- sl_zigbee_tlv_initialize_empty_chain
- sl_zigbee_tlv_initialize_full_chain
- sl_zigbee_tlv_chain_find_by_id
- sl_zigbee_tlv_chain_add_tlv
- sl_zigbee_tlv_chain_add_tlv_block
- sl_zigbee_tlv_chain_append_to_buffer
- sl_zigbee_tlv_chain_get_tlv_count

Zigbee R23 Stack Specific TLV APIs

- sl_zigbee_global_tlv_add_configurations
- sl_zigbee_global_tlv_get_configurations
- sl_zigbee_global_tlv_pan_id_conflict
- sl_zigbee_global_tlv_next_pan_from_pan
- sl_zigbee_global_tlv_next_pan_get_pan
- sl_zigbee_global_tlv_next_channel_from_pg_ch
- sl_zigbee_global_tlv_next_channel_change_get_bitmask

sl_zigbee_global_tlv_symmetric_passphrase

Zigbee R23 ZDO Security APIs

sl_zigbee_get_authentication_level

sl_zigbee_zdo_generate_retrieve_authentication_token_req

sl_zigbee_get_symmetric_passphrase

Zigbee R23 ZDO Management APIs

sl_zigbee_request_beacon_survey

Zigbee R23 ZDO Configuration APIs

sl_zigbee_zdo_get_configuration_req

sl_zigbee_zdo_set_add_configuration

sl_zigbee_zdo_set_send_configuration_req

Zigbee R23 Security Manager Host APIs

sl_zb_sec_man_version

1.5 New CLI Commands

New in release 7.3.0.0

Zigbee Direct Device

The following new CLIs are introduced in ZDD:

- plugin zigbee-direct keysprint
- plugin zigbee-direct reset-out counter
- plugin zigbee-direct set-join-timeout

1.6 New Platform Support

New in release 7.3.1.0

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

New in release 7.3.0.0

Zigbee stack support for the following new modules and radio boards is added in this release.

- A new module MGM240L lighting module and respective new radio board BRD4337A are added.
- New EFR32MG27 parts are supported along with respective radio boards BRD4194A, BRD4110B, BRD4111B and BRD2602A

1.7 New Documentation

All the new 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/.

Zigbee Direct Device documentation: https://docs.silabs.com/zigbee/latest/zigbee-direct/

Zigbee R23 documentation: https://docs.silabs.com/zigbee/latest/zigbee-r23-introduction/

1.8 Intended Behavior

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

2 Improvements

Changed in release 7.3.1.0

APS Command frames will now request APS acks by default.

Add configuration of retry queue size (using ezsp config id EZSP_CONFIG_RETRY_QUEUE_SIZE) in the NCP initialization callback.

Changed in release 7.3.0.0

The EZSP protocol is updated to version 12 and associated changes are made to *UG100: EZSP Reference Guide*.

The emberAfPluginGreenPowerServerUpdateAliasCallback is added to call the user to provide an alias to the commissioning GPD.

The emberAfGreenPowerServerPairingStatusCallback is added to inform user the status of Green Power commissioning at various stages including failure cases.

The sl_zb_sec_man_network_key_info_t returned by sl_zb_sec_man_get_network_key_info now includes a new field (network_key_frame_counter).

The emberAfPluginGreenPowerServerPreSinkPairingCallback is introduced to allow user to inspect the gpd that gets paired to the sink. This callback gives a chance to user to update the pairing group. It is implemented as a weak callback in green-power-server.c with default setup, which can optionally be overridden by the user.

The emberAfGreenPowerClientGpdfSinkTableBasedForwardCallback is introduced in green-power-client.c before forwarding the notifications to sink table-based forwarding for proxy devices. This callback is consumed by the green-power-server.c in case of a combo device.

The device table component is updated so that it can be used with both host and SoC framework.

Printing functions for the Link Key Table will now display the type "A" to indicate that a printed key in the table is an authentication token, compared to "L" for a link key.

All APIs inside the Security Manager component that return a status now return psa_status_t instead of sl_sec_man_status_t.

ZDO Beacon Survey provides a standard ZDO interface by which devices can monitor overall network health by issuing requests to perform scans and collect statistics about the observed beacons. This introduces following updates

- Updates to the existing emberSurveyBeacons API to include a channel mask, allowing for multiple channels to be scanned at once. Using 0 as an argument indicates to scan on the current channel.
- Updates to the EmberNetworkFoundCallback callback function signature. Combines the individual fields from before into the EmberBeaconData struct used in the stack. Updates to existing application code defining these callbacks can emulate the original arguments by restructuring the individual fields from the argument.

sl_sec_man_aes_ccm_crypt has a new argument, uint8_t mic_length to perform frame counter challenge exchange in R23. So the new function signature is:

```
sl_sec_man_aes_ccm_crypt(psa_key_id_t sl_psa_key_id, uint8_t* nonce, bool encrypt, const uint8_t* input, uint8_t encryption_start_index, uint8_t length, uint8_t mic_length, uint8_t* output)
```

Use a value of 4 for this new argument if replacing any calls to the old function signature.

sl_zb_sec_man_aes_ccm_extended is added, which also takes in uint8_t mic_length after the message length. The sl_zb_sec_man_aes_ccm API is unchanged (will always use a 4-byte MIC when called).

PAN ID Conflict Detection has changed. As of Revision 23 of the Zigbee Specification, PAN ID Conflicts will no longer cause unsolicited transmits from the application, and a PAN ID update will not be issued on receipt of a Network Report indicating PAN ID Conflict. Instead R23 stacks will maintain a counter of the number of PAN ID Conflicts encountered. Trust Centers may still issue PAN ID updates when initiated by the application.

The sample applications Z3Light, Z3LightGPCombo, Z3 Gateway and Z3GatewayGPCombo now include the optional attributes gpSharekey and gpSharedKeyTye in their default zap configuration. This makes the ZUTH PICs remain the same for all the applications.

3 Fixed Issues

Fixed in release 7.3.1.0

ID #	Description
829508	Additional validation added in emberSetLogicalAndRadioChannel to return unsuccessful if the lower layers are busy or not in a state to change the channel.
1024246	Update function description for emberHaveLinkKey() and sl_zb_sec_man_have_link_key().
1036503	Added description to specifically recommend Micrium Kernel for DMP sample apps.
1078136	Fixed an issue that causes intermittent crash when updating events in an interrupt context.
1079418	In Trust Center Swap Out case, if security processing fails with normal TC link key, a second security processing procedure will be done with the hashed link key.
1088788	Added new API to reset zigbee nvm3 tokens to default value.
1104056	Added support for network-steering to run on secondary network in case of multi-network.
1130590	Fixed a potential buffer overflow issue in the zigbee_throughput component.
1141109	Updated the dependent component and resource list for the zigbee_green_power_adapter component.
1144316	Updated missing descriptions for some green power data types in gp-types.h header file.
1144884	Fixed spurious frame pending bit set when there is no data pending.
1152229	Fixed an issue where the Zigbee Classic Key Storage component was not calling the intended implementation of AES encryption (using a pure software version instead of the PSA Crypto components). Note: If code size reductions are needed, the component can be modified to remove the requirement for PSA Crypto CCM.
1152512	Fixed potential crash in low-mac-rail when modifying the event in isr context.
1153819	Updated description for the Zigbee Secure Key Storage component to reflect the addition of Zigbee Secure Key Storage Upgrade (which added backwards compatibility with existing projects).
1154616	Add an exception for the condition to initialize network with the case "Switching role from Sleepy End device to Non-sleepy End device"
1157289	Fixed an issue that caused the ZLL BDB test DN-TLM-TC-02B failure.
1157891	The issue that users cannot make stack configurations on ZDD has been fixed.
1157932	Added a condition to check if the "transition time" field is missing and set a default value 0xFFFF for this missing field.
1161341	A Zigbee Direct connection issue regarding supported key negotiation global TLV has been fixed.
1167807	Fixed an issue where devices acting as Trust Centers in distributed networks would incorrectly clear their transient link keys each time a new device joined.
1167894	Fixed a syntax error in af-trust-center.c that occurred when NETWORK_CREATOR_SECURITY_BDB_JOIN_USES_INSTALL_CODE_KEY is defined.
1171477	Changed the output print message for mfglib start 1 to output the number of packet received in certain duration in milli-seconds.
1172778	Added the missing invocation of the emberAfPluginGreenPowerServerUpdateAliasCallback in green power server.

Fixed in release 7.3.0.0

ID #	Description
621144	Added support for GPD switch on single-button devices such as BRD4183A.
648906	Reimplemented emberChildId().
659010	Reimplemented emberChildIndex().
660031	Fixed all warnings/errors related to wrong print format.
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.
756459	Fixed the issue that prevented StandardizedRfTesting from receiving packets after rstream command.

ID #	Description
813340	Fixed failed SE test 15.57.
849183	Fixed an issue where vcom line used in Zigbee samples caused a conflict with SPI bootloader when using slot-manager plugin. By default, the default recommended vcom line (USART/EUSART) is used for each board. However, whenever customers install the zigbee_debug_basic component, they must manually install the iostream (USART/EUSART) to use vcom.
1026610	The range checks for reserved and non existent green power device source Id are added to the green power cluster command handlers.
1026760	Fixed an issue where End Device could rejoin using incorrect 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.
1031241	Improved validation of reserved Green Power address.
1031910	Fixed a MISRA error in SeSampleEsi, file app.c
1032366	Improved error handling in sl_zigbee_set_passive_ack_config(), renamed sl_set_passive_ack_config().
1036948	Fixed an issue where the NCP didn't de-assert nHOST_INT when all data were transferred to HOST and nSSEL was de-asserted
1040523	Implemented functionality relating to delayed polling used in MAC certification tests MAC-TEST.16
1063166	Fixed the issue that could cause a watchdog reset while traversing the source route indeci.
1063466	Fixed an issue when end device rejoining the ZLL network caused network address conflict. A Zigbee device will now clear its parent ID if it is leaving the network without rejoining.
1063525	Removed the transient link key earlier from the joiner device to prevent an invalid verify link key exchange from succeeding even when Trust Center uses an incorrect link key.
1063627	Updated emberAfRemoteSetBindingCallback() signature. Added more callbacks dispatcher on HOST.
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.
1074105	Fixed transient device timeout that got initialized with an incorrect value on a Router, which led to an issue where Coordinator couldn't send back Trust Center Key to the end device.
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.
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. The EMBER_AF_PLUGIN_NETWORK_CREATOR_SECURITY_BDB_JOIN_USES_INSTALL_CODE_KEY option enforces a device to join using a unique key instead of a global key. With the option overwritten, devices are able to join using a global key, which is what "plugin network-creator-security open-network" would allow. "plugin network-creator-security open-network" and “emberAfPluginNetworkCreatorSecurityOpenNetwork” now return EMBER_INVALID_CALL when the EMBER_AF_PLUGIN_NETWORK_CREATOR_SECURITY_BDB_JOIN_USES_INSTALL_CODE_KEY option is set in the Network Creator Security component. These routines are meant for global key joins, which is counter to what EMBER_AF_PLUGIN_NETWORK_CREATOR_SECURITY_BDB_JOIN_USES_INSTALL_CODE_KEY enforces.
1079680	Fixed an issue that caused Z3Gateway to consume 100% CP at steady state.
1081914	Fixed an incompatibility issue between the Secure Key Storage component and the token file-based Trust Center Backup feature that is described in *AN1387: Backing Up and Restoring a Z3 Green Power Combo Gateway*.
1082602	Fixed issue that could cause packets that failed to decrypt during commissioning to be forwarded as commissioning notifications with authentication failed flag set.
1082798	Corrected an issue where Throughput Plugin would limit the maximum test packet 5-bytes smaller than the actual maximum possible.
1083200	Fixed an issue where Message Integrity Codes where not being copied back to host in emGpCalculateIncomingCommandMic().

ID #	Description
1083835	Fixed sink table read command handling for the gpSharedKey type that fixed the GP Test Case failure 4.4.4.3.
1085652	Added C header guards to a number of Zigbee stack header files that lacked them. There were no known issues due to lack of these header guards, and this change just quiets MISRA warnings about possibility of multiple inclusion, with no functional change expected.
1087526	Fixed a few compiler warnings in the code.
1087618	Fixed compilation issues due to missing Green Power Adaptor header files not being included in release.
1089841	Fixed an issue that caused the emberFindAndRejoinNetworkWithReason to return busy status for an end device on sub gigahertz interface.
1090453	Fixed an issue that required increasing the size for emBufferToHostTagMapSize, which meant changing the data type associated with that variable from uint8_t to uint16_t to prevent overflow when EMBER_APS_UNICAST_MESSAGE_COUNT and EMBER_BROADCAST_TABLE_SIZE was set large enough.
1092779	Fixed an issue that was preventing an End Device from processing a ZDO Leave Request from a non-parent network node. This can be disabled by setting ZDO_LEAVE_FROM_NON_PARENT_NOT_ALLOWED in the security bit mask.
1096375	Fixed an issue where the emberHmacAesHash API had been unavailable for application builds since EmberZNet 7.2.0. It is in the process of being deprecated in favor of Zigbee Security Manager functionality, but should remain callable before it is removed.
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.
1097536	Fixed an issue that caused the multi-MAC coordinator to use 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-G.
1098896	Fixed a potential issue that can cause a sleepy child is removed (from stack tokens and child table) before the address conflict resolution is completed.
1099131	Fixed an issue where Server couldn't send Terminate message to Client if it received a malformed certificate.
1103117	The bug that was preventing the green power server from being left uninitialized after combo node leaving the network and joining back is fixed.
1103581	Fixed an issue that caused a new device to join the network with a random extended PAN Id instead of using the one from the received beacon. This difference in extended PAN Id was causing a PAN id conflict upon device join.
1104793	Fixed an issue for dual PHY operation that was causing an assert failure when data transactions are occurring on both the interfaces.
1105915	On a dual band selection device, emberGetRadioParameters now correctly returns the channel page.
1106002	Fixed an issue that affected green power server test case 4.4.1.7 steps 1-2.
1108592	Fixed an issue when running ZCP test on hardware, where the EUI did not change causing the test to fail.
1111460	Switched to use NVM storage for some ZCL attributes in sample apps.
1114376	Fixed wrong plugin mfglib send message command length when parsing on HOST.
1114634	Fixed an issue for multi mac coordinator that prevented scanning on sub gHz interface during network formation because of the previous network leave.
1120667, 1121005	Fixed an issue that caused the MG24-based Zigbee nodes to stop transmission or reception. The issue was rooted in the lower layer on EFR32xG24 when using the IEEE 802.15.4 PHY, where the radio could become stuck when doing an LBT transmit if a frame is received during the CCA check window.
1120886	Fixed an issue that caused the watchdog reset during the NCP operation under heavy traffic. It was a corner case in IOStream that would cause the read_rx_buffer function to never return when reading data after the buffer was completely filled up.
1126688	Fixed a linking error when building Z3Light without the Green Power client plugin.
1126968	Fixed ezsp error code 0x22 on the OTA server.
1129240	Fixed an assert in the stack when running out of buffers and a device tries to join.
1130245	Added code to check default move rate attribute when the rate is 0xff.
1130494	Fixed a key establish failure on a zcp test running on dual-PHY hardware.
1130734	Fixed null pointer de-reference when sending an association response if no buffers are available.
1131440	Fixed emberGetLastHopRssi() and emberGetLastHopLQi() return value when it's called inside packet handoff callback.
1133787	Fixed an issue that caused network steering to incorrectly use distributed test key instead of emberPluginNetworkSteeringDistributedKey.
1134053	Added back emberAfPluginIasZoneServerStackStatusCallback that was accidentally removed

ID #	Description
1142244	Fixed a null buffer dereference in the Zigbee source route code.
1145583	Fixed an issue that caused the permit join internal state of a router or coordinator to remain open after network leave command. This caused the node to carry forward the state while forming a new network after the leave and devices could join without the node opening up the permit join after the formation of the network.
1148111	Stop processing gp message after emberAfGreenPowerClusterGpNotificationCallback when security frame counter is incorrect.

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 .
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.**	**Workaround: Manually update the cluster revision attribute to their appropriate revision.**
1164768, 1171478, 1171479	**ERROR: ezspErrorHandler 0x34 reported repeatedly during mfglib receive mode**	**Workaround: Configuring EMBER_AF_PLUGIN_GATEWAY_MAX_WAIT_FOR_EVENT_TIMEOUT_MS on the host app to 100, so the callback queue is freed more quickly helps to reduce the error message printed.**

5 Deprecated Items

Deprecated in release 7.3.0.0

Deprecated emberGetKey alongside other legacy key access APIs.

Use sl_zb_sec_man_export_key to get the key itself, or sl_zb_sec_man_get_network_key_info / sl_zb_sec_man_get_aps_key_info to obtain the key's metadata.)

Deprecated the following legacy APIs regarding the link key table, in favor of using APIs provided by Zigbee Security Manager.

- * emberGetKeyTableEntry()
- * emberSetKeyTableEntry()
- * emberAddOrUpdateKeyTableEntry()
- * emberHaveLinkKey()
- * emberFindKeyTableEntry()

New APIs to use instead:

* sl_zb_sec_man_import_key, sl_zb_sec_man_import_link_key

(These now support adding by EUI64 only, like emberAddOrUpdateKeyTableEntry, if the passed-in index is 0xFF. On SoC, the placed index is returned by import_key inside the context.)

- * sl_zb_sec_man_export_link_key_by_index
- * sl_zb_sec_man_export_link_key_by_eui

(These are now modified to allow searching for the index without key export if a null pointer is passed in for the key.)

- * sl_zb_sec_man_have_link_key
- * sl_zb_sec_man_get_aps_key_info (if key metadata is requested but not the key data)

Deprecated the following legacy APIs for accessing transient keys:

- * emberAddTransientLinkKey(EmberEUI64 partnerEUI64, EmberKeyData*)
- * emberGetTransientKeyTableEntry(uint8_t index, EmberTransientKeyData* transientKeyData)
- * emberGetTransientLinkKey(const EmberEUI64 eui, EmberTransientKeyData* transientKeyData)

These will be removed in a future release.

Call these functions instead:

```
* sl_zb_sec_man_import_transient_key(EmberEUI64, sl_zb_sec_man_key_t*)
* sl_zb_sec_man_export_transient_key_by_eui(EmberEUI64 eui64,
                                            sl_zb_sec_man_context_t* context,
                                            sl_zb_sec_man_key_t* plaintext_key,
                                            sl_zb_sec_man_aps_key_metadata_t* key_data)
* sl_zb_sec_man_export_transient_key_by_index(uint8_t index,
                                            sl_zb_sec_man_context_t* context,
                                            sl_zb_sec_man_key_t* plaintext_key,
                                            sl_zb_sec_man_aps_key_metadata_t* key_data)
```

emberAfMsToNextEventExtended has been marked as deprecated.

Call emberAfMsToNextEvent instead. emberAfMsToNextEventExtended will be removed in a future release.

Since GSDK 4.0.0.0/EmberZNet 7.0.0.0, events are maintained in a next-to-fire order, thus the second argument to emberAfMsToNextEventExtended, which returns the index of the next event to fire, is always implicitly 0.

6 Removed Items

Removed in release 7.3.1.0

Removed setPacketBufferCount() in af-host.c and redundant check in switch case EZSP_CONFIG_PACKET_BUFFER_COUNT in the command-handlers.c file.

Removed input argument to internal function memoryAllocation as part of merging the buffer queue size allocation during the ncp initialization and also removed explicit calls to emberAfNcpInitCallback() in sample applications app.c.

Removed in release 7.3.0.0

Removed legacy NCP callback emberAfPluginConcentratorBroadcastSentCallback().

Adjustments were made to APS Ack processing to better accommodate interop situations with other vendor stacks. During this process the uncertifiable feature of attaching data payloads to APS Acks when sending responses was removed.

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 APIs for the legacy event control system.

7 Multiprotocol Gateway and RCP

7.1 New Items

Added in release 7.3.0.0

Added a new application z3-light_ot-ftd_soc that demonstrates Zigbee and OpenThread Concurrent Multiprotocol functionality. It features a router on the Zigbee side and a Full Thread Device (FTD) on the OpenThread side. See the project description or app/framework/scenarios/z3/z3-light_ot-ftd_soc/readme.html for details.

First GA-quality release of CPC GPIO Expander module. The Co-Processor Communication (CPC) General Purpose Input/Output (GPIO) Expander is a software component designed to enable a Host device to utilize a Secondary device's GPIOs as if they were its own. With the CPC GPIO Expander, the Host device can seamlessly integrate with the Secondary device and make use of its GPIO capabilities. See https://github.com/SiliconLabs/cpc-gpio-expander/README.md for documentation.

Added antenna diversity and coex EZSP command support to Zigbeed.

Added better assert reporting to Zigbeed.

Added bt_host_empty application (option: -B for the run.sh script) to the multiprotocol docker container.

Zigbeed now includes an implementation of emberGetRestoredEui64() which loads the CREATOR_STACK_RESTORED_EUI64 token from the host_token.nvm file.

The multiprotocol container now sets the size of syslog to 100 MB by default. Users are able to change the size by modifying the "/etc/logrotate.d/rsyslog" and "/etc/rsyslog.d/50-default.conf" files and restarting the rsyslog service inside the container.

7.2 Improvements

Changed in release 7.3.1.0

Radio_url can now take a list of IIDs. This is to control IIDs a host can accept spinel frames from other than its own IID. RCP uses IID zero for the received broadcast packet to deliver a spinel frame to all the connected hosts/endpoints. An example of the new radio_url is ‘spinel+cpc://cpcd_0?iid=1&iid-list=0’.

CLI commands used by z3-light_ot-ftd_soc sample application have been moved from the project into a new component called ot_up_cli.

Changed in release 7.3.0.0

Reduced CPC Tx and Rx queue sizes to fit the DMP NCP on the MG13 family.

Configured options on the multiprotocol RCP projects to provide ~3.3k in RAM savings, particularly for the MG1 part. This was accomplished by

- Reducing
  - The number of user CPC endpoints to 0
  - Tx CPC queue size to 15 from 20
  - Rx buffer count to 15
- Disabling OpenThread RTT logs

For further savings, customers can look into reducing the Tx and Rx queue sizes further. Note that the downside to this change would be a reduction in message throughput due to added retries. Also, customers can look into reducing the NVM cache size based on need. As a last resort, customers may also choose to disable CPC security on both the RCP and the host. We do not recommend the last option.

Changed zigbee_ble_event_handler to print scan responses from legacy advertisements in the DMPLight(Sed) app.

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

7.3 Fixed Issues

Fixed in release 7.3.1.0

ID #	Description
1113498 1135805	Resolved several issues that caused intermittent failures in zigbeed when attempting to join 100 or more Zigbee devices to the network.
1153055	An issue has been fixed that caused failure on the host if a communication error occurred when reading the NCP version.
1171451	An argument parsing issue has been fixed in the CLI command ping_ipaddr of the ot_up_cli component.

Fixed in release 7.3.0.0

ID #	Description
1078323	Resolved issue where Z3GatewayCPC asserts when there is a communication failure with the NCP during address table initialization. We will now try to reconnect to the NCP upon failure.
1080517	Z3GatewayCPC now automatically handles a reset of the NCP (CPC secondary).
1117789	Fixed an issue where modifying OPENTHREAD_CONFIG_PLATFORM_RADIO_SPINEL_RX_FRAME_BUFFER_SIZE caused a linker error when building Zigbeed.
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.
1129821	Fixed null pointer dereference in Zigbeed in an out-of-buffer scenario while receiving packets.
1139990	Fixed an assert in the OpenThread Spinel code that could be triggered when joining many Zigbee devices simultaneously.
1144268	Fixed an issue where excessive radio traffic can cause the Zigbee-BLE NCP to get into a state where it continually executes the NCP and CPC initialization.
1147517	Fixed an issue with Z3GatewayCPC on startup that could cause the reset handling of the secondary to not work correctly.

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.si-labs.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.
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 can become unresponsive in the z3-light_ot-ftd_soc app.	This app is released as experimental quality and the issue will be fixed in a future release.
1124140	z3-light_ot-ftd_soc sample app is not able to form the Zigbee network if the OT network is up already.	Start the Zigbee network first and the OT network after.
1129032	Experimental concurrent listening feature on xG24 devices is disabled in this release.	Support is planned in a future release.
1143857	Antenna Diversity is not available on the CMP RCP for xG21 and xG24 parts, since the antenna diversity hardware is used for concurrent listening.	Intended behavior.

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.

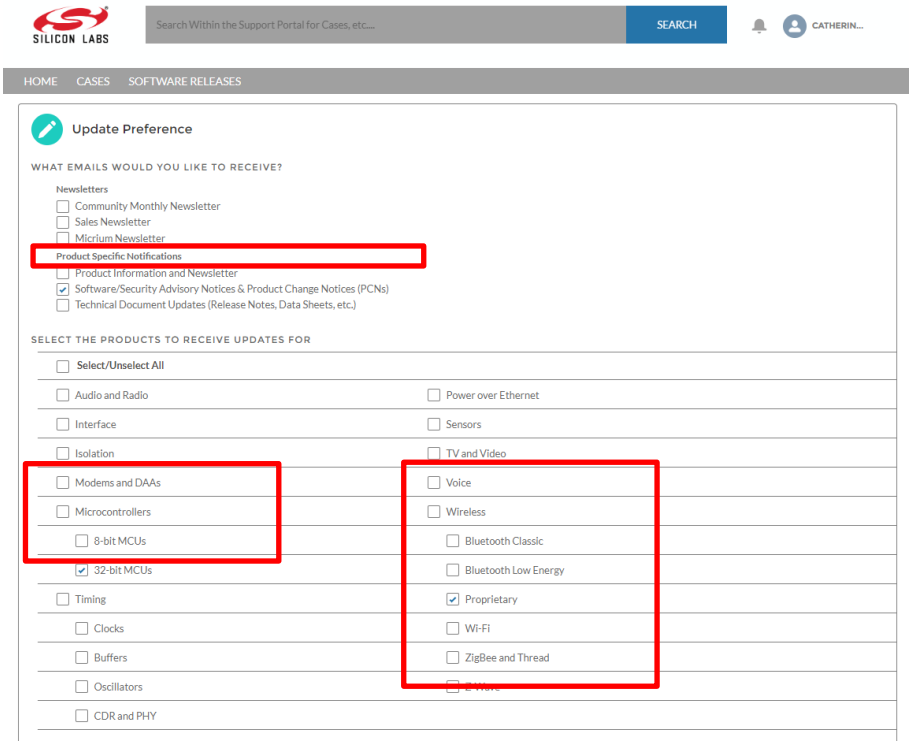
User applications never need to interact with the majority of these keys. Existing APIs to manage Link Key Table keys or Transient Keys are still available to the user application and now route through the Zigbee Security Manager component.

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