AN710: Bringing up Custom Devices for the Ember ® EM35x SoC or NCP Platform

This application note describes how to initialize a piece of custom hardware (a “device”) based on the EM35x so that it interfaces correctly with the EmberZNet PRO or Silicon Labs Thread network stack. The same procedures can be used to restore Ember development kit devices whose settings have been corrupted or erased.

KEY POINTS

- Information required before board bring-up
- Setting manufacturing tokens
- Bootloading
- Performing functional testing using NodeTest
- Setting stack tokens

1. Introduction

Before an Ember EM35x-based product can be initialized and tested, SIMEE tokens within the EM35x Customer Information Block (CIB) must be configured. To do so, the product design team must know how the EM35x is to be used in the wireless system.

In particular, the design team must know the following:

- PCB Manufacturing-specific information (serial number, product numbers, EUI, and so on)
- Bootloader architecture (serial dataflash)
- EM35x transmit port (bidirectional or alternate transmit)
- External components in the RF Path (PA, LNA, and so on)
- 24 MHz crystal oscillator specification
- Application security tokens (Keys, certificates, and so on)

This application note describes how to initialize a piece of custom hardware (a “device”) based on the EM35x so that it interfaces correctly with the EmberZNet PRO or Silicon Labs Thread network stack. The same procedures can be used to restore development kit devices whose settings have been corrupted or erased.

Even though the EM35x flash is fully tested during production test, the flash contents in the main flash block (MFB) are not set to a known state before shipment. The CIB is left erased with read protection disabled (read protection is an option byte and part of the CIB manufacturing tokens).

2. EM35x Wireless System

Once the hardware design of a custom device has been completed, the assembled product is ready for test and functional validation. Before testing, developers must understand how the device will operate at both the device-level and system-level. The following table describes the different items that developers should know before board bring-up.

Table 2.1. Information Needed Before Board Bring-Up

Information	Required or Optional	Description
Device Level		
Product Information	Optional	Most products have unique serial numbers as well as generic product codes that might be stored in the EM35x. These might include where and when the device was assembled, a product serial number and product name.
Custom EUI	Optional	IEEE 64-bit unique number. Each EM35x comes with an EUI64 programmed into the FIB. Customers that have their own IEEE address block can use it in place of the provided EUI64.
RF Component Information	Required	Most products use external power amplifiers (PAs) or low noise amplifiers (LNAs) in order to maximize the range of the communication link. If the product uses PAs or LNAs, then developers must know the pin-connections between the off-chip components and the EM35x, as well as whether the RF front end is using the bidirectional or alternate transmit port. They should also understand the LNA Gain as it will be used to offset the clear channel assessment (CCA) threshold.
Protocol-Specific Information	Optional	If developing a product using the ZigBee networking protocol, obtain a ZigBee-assigned manufacturer code before testing the application.
System Level		
Bootloader Option	Required	Silicon Labs offers two bootloading options: application bootloader and a stand-alone bootloader.
System Security	Optional	If device-level security is required for the product, determine necessary security settings and keys before setting up the device.

As detailed in the above table, Silicon Labs offers its customers an opportunity to guarantee a device's uniqueness on the network. In addition, it allows customers a way to store product descriptions, manufacturer-specific information and device information.

3. Setting CIB Manufacturing Tokens

Ember EM35x chips are delivered to customers with only the fixed information block (FIB) programmed. The FIB contains a serial-link-only monitor, chip identifiers, a pre-programmed EUI64, and calibration values. The FIB cannot be modified. Before the EM35x chips can be used to run network stack applications, the customer or a contract manufacturer/test house must prepare them. Preparation includes programming the proper application and bootloader, if necessary, into the Main Flash Block (MFB), as well as programming customer manufacturing tokens in the Customer Information Block (CIB).

CIB manufacturing tokens are values programmed into a special, non-volatile storage area of flash known as the CIB. The CIB contains data that manufacturers of EM35x-based devices can program. The Fixed Information Block (FIB) also contains manufacturing tokens, but these tokens are fixed values that cannot be modified.

Note: Applications and the stack can read any manufacturing tokens at any time.

Use the em3xx_load.exe utility to set manufacturing tokens. em3xx_load.exe can be found in the Debug Adapter (ISA3) Utilities install directory, installed as part of Simplicity Studio. The default is under the Simplicity Studio installation in \Developer\adapter_packs \em3xx\utils. em3xx_load.exe has many commands, but four commands are specifically designed for manipulating CIB manufacturing tokens, as shown in the following table.

Table 3.1. em3xx_load.exe CIB Manufacturing Token Commands

Command line entry	Description
`--cibtokenspatch <file>`	Patch the CIB tokens with the token set defined in the specified file. See `--cibtokenspatch-help` for additional help on this command.
`--cibtokensprint`	Print the contents of the CIB tokens from the target in a very easy to read form.
`--cibtokensdump`	Print the contents of the CIB tokens from the target in a format that can easily be imported using `--cibtokenspatch`.
`--cibtokenspatch-help`	Print out additional help about how to set the tokens using `--cibtokenspatch`, including detailed file syntax and a list of all supported tokens.

Executing `em3xx_load.exe –-help` causes em3xx_load.exe to print its online help menu detailing all commands, modifiers, and arguments. In addition, document *UG107: EM35x Utilities Guide* provides many examples detailing how the em3xx_load.exe utility can be used. This document also includes examples showing how to print and patch CIB manufacturing tokens.

Silicon Labs recommends that CIB manufacturing tokens be written with an external utility such as em3xx_load.exe at the same time as programming the MFB. Using an external utility allows for patching and reprogramming the CIB as many times as necessary. Some situations, though, may require that a CIB manufacturing token be programmed at runtime from code running on the chip itself. The manufacturing token module of the HAL provides a token API to write CIB manufacturing tokens. However, this API only writes CIB tokens that are in a completely erased state. If a CIB token must be reprogrammed, you must use an external utility. The API on SoC platforms is `halCommonSetMfgToken(token, data)`. The parameters for this API are the same as the API `halCommonSetToken(token , data)`.

For EmberZNet PRO EZSP NCP platforms, the host API is `ezspSetMfgToken(tokenId, tokenDataLength, tokenData)`. (See *UG100: EZSP Reference Guide* for details.)

For Silicon Labs Thread, the API is `emberSetMfgToken(tokenId, tokenDataLength, tokenData)`.

Note: CIB manufacturing tokens written with `halCommonSetMfgToken()` or `ezspSetMfgToken()` must be located on a 16-bit address boundary and the byte length must be a multiple of 16 bits.

The following table identifies the CIB manufacturing tokens that OEMs and CMs may want to program at manufacturing time. Refer to \hal\micro\cortexm3\token-manufacturing.h for the token definition because, depending on the stack release version, it may differ from the information provided in this table. The location of each CIB manufacturing token is described as an offset to the starting address of the CIB. For the most accurate and specific information about where the CIB flash region begins in the address map of your chip, please consult your IC's Reference Manual or Data Sheet. However, as a general rule, EM35x chips with a 3-digit part number, such as "EM351" or "EM357", use a starting address of 0x08040800 for the CIB region, while EM35x chips with a 4-digit part number, such as "EM3581" or "EM3588", use a starting address of 0x08080800 for the CIB region.

Table 3.2. CIB Manufacturing Tokens for the EM35x

Offset from CIB starting address	Size (Bytes)	Name	Description
0x0000	16	TOKEN_MFG_CIB_OBS	Dedicated special flash storage called option bytes. Option bytes are special storage because they are directly linked to hardware functionality of the chip. There are 8 option bytes, each occupying 16 bits of flash as follows: Option Byte 0: Configures flash read protection Option Byte 1: Reserved Option Byte 2: Available for customer use Option Byte 3: Available for customer use Option Byte 4: Configures flash write protection Option Byte 5: Configures flash write protection Option Byte 6: Configures flash write protection Option Byte 7: Reserved Refer to the *EM35x Data Sheet* document for a detailed description of option byes, what they mean, how they work, and what values should be used. *Usage*: All option bytes must be set to a valid state.
0x0010	2	TOKEN_MFG_CUSTOM_VERSION	Version number to signify which revision of CIB manufacturing tokens you are using. This value should match CURRENT_MFG_CUSTOM_VERSION, defined in \hal\micro\cortexm3\token-manufacturing.h, and currently set to 0x01FE. *Usage*: Recommended for all devices using CIB manufacturing tokens.
0x0012	8	TOKEN_MFG_CUSTOM_EUI_64	IEEE 64-bit address, unique for each radio. Entered and stored in little-endian. Setting a value here overrides the pre-programmed EUI64 stored in the FIB (TOKEN_MFG_EMBER_EUI_64). This is for customers who have purchased their own address block from IEEE. **WARNING:** If this value is set "live," it may not propagate to all levels of the stack and some outgoing messages may continue to use the default value. Silicon Labs recommends forcing a reset after setting EUI64 and before starting the networking stack. *Usage:* Optionally set by device manufacturer if using custom EUI64 address block.
0x001A	16	TOKEN_MFG_STRING	Optional device-specific string, for example, the serial number. *Usage:* Optionally set by device manufacturer to identify device.
0x002A	16	TOKEN_MFG_BOARD_NAME	Optional string identifying the board name or hardware model. *Usage:* Optionally set by device manufacturer to identify device.

<table>
<tr><th>Offset from CIB starting address</th><th>Size (Bytes)</th><th>Name</th><th>Description</th></tr>
<tr><td>0x003A</td><td>2</td><td>TOKEN_MFG_MANUF_ID</td><td>16-bit ID denoting the manufacturer of this device. When you are programming with EmberZNet PRO, Silicon Labs recommends setting this value to match your ZigBee-assigned manufacturer code, such as in the stack's API call:

emberSetManufacturerCode()

Usage: Recommended for EmberZNet PRO devices utilizing the stand-alone bootloader. Not relevant for Silicon Labs Thread.</td></tr>
<tr><td>0x003C</td><td>2</td><td>TOKEN_MFG_PHY_CONFIG</td><td>Default configuration of the radio for power mode (boost/normal), transmit path selection (bi-directional/alternate), and boost transmit power level:

Bit 0 (lsb): Set to 0 for boost mode; set to 1 for non-boost (normal) mode. Boost mode mainly increases rx sensitivity but also increases tx output power by a small amount. Larger increases in tx output power are available in bits 3-7 of this token.

Bit 1: Set to 0 if an external PA is connected to the alternate TX path (RF_TX_ALT_P and RF_TX_ALT_N pins); set to 1 otherwise.

Bit 2: Set to 0 if an external PA is connected to the bi-directional RF path (RF_P and RF_N pins); set to 1 otherwise.

Bits 3-7: Set to the boost tx power offset from the first integer value above nominal maximum tx power (+3 dBm). This sets the default tx output power level when the radio is first started or whenever emberSetTxPowerMode() is called with EMBER_TX_POWER_MODE_USE_TOKEN. Note that other APIs executed during normal stack operation will typically override this value at runtime, so this value is most applicable to the RF-enabled versions of the Ember Stand-Alone Bootloader and the stack's treatment of the radio prior to entering a network (such as during Active Scans).

<table>
<tr><th>For tx power of…</th><th>Set this subfield to…</th></tr>
<tr><td>+4 dBm</td><td>0</td></tr>
<tr><td>+5 dBm</td><td>1</td></tr>
<tr><td>+6 dBm</td><td>2</td></tr>
<tr><td>+7 dBm</td><td>3</td></tr>
<tr><td>+8 dBm</td><td>4</td></tr>
</table>
Bit 7 is most significant; Bit 3 is least significant. All bits must be set to 1 if no tx boost power level is desired for the PHY default; in that case the bootloader PHY and the stack's initialization of the radio will use the default of +3 dBm.

Bits 8–15: Reserved. Must be set to 1 (the erased state).

Usage: Bits 0-2 required for devices that utilize boost mode or an external PA circuit. Bits 3-7 only required for devices utilizing an RF-enabled variant of Ember Stand-alone Bootloader and desiring output power above +3 dBm.</td></tr>
</table>

Offset from CIB starting address	Size (Bytes)	Name	Description
0x003E	16	TOKEN_MFG_BOOTLOAD_AES_KEY	Sets the AES key used by the bootloader utility to authenticate bootloader launch requests of the Stand-alone bootloader. *Usage:* Required for devices that utilize the Stand-alone bootloader. This is not used by the application bootloader.
0x004E	8	TOKEN_MFG_EZSP_STORAGE	An 8-byte, general-purpose token that can be set at manufacturing time and read by the host microcontroller via EZSP's getMfgToken command frame. Can also be accessed by Thread host applications using emberGetMfgToken. *Usage:* Not required. EmbetZNet PRO device manufacturer may populate or leave empty as desired.
0x007E	92	TOKEN_MFG_CBKE_DATA	Defines the security data necessary for Smart Energy devices. It is used for Certificate Based Key Exchange to authenticate a device on a Smart Energy network. The first 48 bytes are the device's implicit certificate, the next 22 bytes are the Root Certificate Authority's Public Key, the next 21 bytes are the device's private key (the other half of the public/private key pair stored in the certificate), and the last byte is a flags field. The flags field should be set to 0x00 to indicate that the security data is initialized. *Usage:* Required by Smart Energy Profile-certified devices.
0x00DA	20	TOKEN_MFG_INSTALLATION_CODE	Defines the installation code for Smart Energy devices. The installation code is used to create a pre-configured link key for initially joining a Smart Energy network. The first 2 bytes are a flags field, the next 16 bytes are the installation code, and the last 2 bytes are a CRC. Valid installation code sizes are 6, 8, 12, or 16 bytes in length. All unused bytes should be 0xFF. The flags field should be set as follows depending on the size of the install code: 6 bytes = 0x0000 8 bytes = 0x0002 12 bytes = 0x0004 16 bytes = 0x0006 *Usage:* Required by Smart Energy Profile-certified devices. Optional for Zigbee 3.0 devices wishing to employ a pre-programmed installation code.
0x00EE	2	TOKEN_MFG_OSC24M_BIAS_TRIM	A relative amount (between 0x0000 and 0x000F) that trims the 24 MHz crystal bias drive. A lower value reduces drive and current consumption, but increases instability. Although a value can be set here manually, Silicon Labs recommends leaving this value unpopulated (0xFFFF) so that the stack can perform auto-calibration at runtime to determine the optimal value for lowest current consumption while maintaining stability. *Usage:* Not recommended (leave erased, 0xFFFF).

Offset from CIB starting address	Size (Bytes)	Name	Description
0x00F0	2	TOKEN_MFG_SYNTH_FREQ_OFFSET	An offset applied to the radio synthesizer frequency. This offset can be used to compensate for variations in 24 MHz crystals to accurately center IEEE-802.15.4 channels. Note that this does not offset the 24 MHz system clock frequency derived directly from the crystal, but instead is applying an offset to the transmit frequency derived from the synthesizer. Bits 0-7: Set to the signed offset to be applied to the synthesizer frequency. Each step provides approximately 11 kHz of adjustment. Bit 8: Set to 0 if the offset is valid and should be used. Set to 1 (the erased state) if the token is invalid or has not been set. Bits 9-15: Reserved. Must be set to 1 (the erased state). *Usage:* Deprecated. Not recommended for use in new designs.
0x00F2	2	TOKEN_MFG_OSC24M_SETTLE_DELAY	The delay in microseconds to allow the 24 MHz crystal to settle after a bias change when waking up from deep sleep. Silicon Labs recommends leaving this value unpopulated (0xFFFF) so that the stack uses its default conservative delay value.
0x00F4	2	TOKEN_MFG_SECURITY_CONFIG	(EmberZNet PRO only) Defines the security policy for application calls into the stack to retrieve key values. The API calls `emberGetKey()` and `emberGetKeyTableEntry()` are affected by this setting. This prevents a running application from reading the actual encryption key values from the stack. This token may also be set at runtime with `emberSetMfgSecurityConfig()` (see that API for more information). The stack utilizes the `emberGetMfgSecurityConfig()` to determine the current security policy for encryption keys. The token values are mapped to the EmberKeySettings stack data type (defined in ember-types.h). See the following table for the mapping of token values to the stack values. *Usage:* Optional for EmberZNet NCP devices wishing to limit access to security data over the serial interface.

Offset from CIB starting address	Size (Bytes)	Name	Description
0x00F6	2	TOKEN_MFG_CCA_THRESHOLD	Threshold used for energy detection clear channel assessment (CCA). Bits 0-7: Set to the two's complement representation of the CCA threshold in dBm below which the channel will be considered clear. Valid values are -128 through +126, inclusive. +127 is NOT valid and must not be used. Bit 8: Set to 0 if the threshold is valid and should be used. Set to 1 (the erased state) if the token is invalid or has not been set; in this case the default threshold will be used. Bits 9-15: Reserved. Must be set to 1 (the erased state). The default CCA threshold for EM35x chips is -75 dBm. If bit 8 of this token is 1 then -75 dBm will be used. You may want to override the default CCA threshold by setting this token if your design uses an LNA. An LNA changes the gain on the radio input, which results in the radio "seeing" a different energy level than if no LNA was used. Example: A design uses an LNA that provides gain of +12 dBm. Add the default -75 dBm gain to the LNA's gain to get the dBm value for the token: -75 + 12 = -63 dBm. The two's complement signed representation of -63 dBm is 0xC1, and so the complete token value to be programmed is 0xFEC1.
0x00F8	16	TOKEN_MFG_SECURE_BOOTLOADER_KEY	This token holds the 128 bit key used by the secure bootloader to decrypt encrypted EBL files. A value of all F's is considered an invalid key and will not be used by the secure bootloader. *Usage:* Required only if using one of the bootloaders with the "secure" prefix.
0x010E	148	TOKEN_MFG_CBKE_283K1_DATA	Defines the security data necessary for Smart Energy 1.2 devices using the ECC 283k1 curve. It is used for Certificate Based Key Exchange to authenticate a device on a Smart Energy network. The first 74 bytes are the device's implicit certificate, the next 37 bytes are the Root Certificate Authority's Public Key, the next 36 bytes are the device's private key (the other half of the public/private key pair stored in the certificate), and the last byte is a flags field. The flags field should be set to 0x00 to indicate that the security data is initialized. *Usage:* Required for ZigBee Smart Energy 1.2 devices.
0x01A4	34	TOKEN_MFG_THREAD_JOIN_KEY	This token holds the random join key used to join a Thread Network. This token is for use with the Silicon Labs Thread stack only. This token contains 32 bytes of space for a random join key which needs to be null-terminated and two bytes that contain the length of the join key. The programmed length includes the null terminator (0x00) and any bytes beyond the programmed length are ignored (no special padding values required). *Usage:* Optional for a Thread Network

Table 3.3. Mapping of EmberKeySettings to `TOKEN_MFG_SECURITY_CONFIG`

EmberKeySettings Value	TOKEN_MFG_SECURITY_CONFIG Value
EMBER_KEY_PERMISSIONS_NONE	0x0000
EMBER_KEY_PERMISSIONS_READING_ALLOWED	0x00FF
EMBER_KEY_PERMISSIONS_HASHING_ALLOWED	0xFF00

For more information on the Smart Energy tokens, see document *AN708: Setting Manufacturing Certificates and Installation Codes*.

4. Bootloaders

For the EM35x, Silicon Labs provides two bootloader options:

- Application bootloader: Supports multi-hop bootloading from a gateway device. Enables an application to continue running and sending normal application packets while the new firmware image is being received.
- Stand-alone bootloader: Supports only one-hop bootloading from a gateway device. If some nodes are multiple hops away from a gateway, they must either be brought closer to the gateway for bootloading or you must create a portable device that is taken around the installation to bootload all of the nodes.

For a discussion on what the bootloaders are, their differences, their uses, and how to use the bootloaders, refer to document *UG103.6: Application Development Fundamentals: Bootloading*.

For a discussion on how to program applications and bootloaders to chips as well as convert applications to the bootloader compatible .ebl file format, refer to document *UG107: ISA3 Utilities Guide*.

5. Testing

At this point, you may want to use the NodeTest application to perform a simple send/receive test on the new device to determine its range and generally test its radio functionality. NodeTest is a pre-built application supplied by Silicon Labs for the purpose of performing RF functional testing and hardware validation on development boards or custom-designed hardware. *AN1019: Using the NodeTest Application* provides instructions for uploading NodeTest, and using NodeTest on a known good device and the new device to perform basic testing.

For customers who are using mature applications with the EmberZNet PRO or Silicon Labs Thread SDKs, Silicon Labs recommends using the manufacturing test library (also known as “mfglib”), a set of APIs or NCP serial commands provided for IEEE 802.15.4-based functional testing of the radio from within a normal EmberZNet PRO or Silicon Labs Thread application for an SoC or host platform. This library is typically used in the low-volume and high-volume phases of testing and manufacturing, where additional programming steps for a dedicated RF test application add unnecessary test time. For SoC applications based on EmberZNet PRO or Silicon Labs Thread, as well as for custom zigbee NCP builds through the NCP Framework, a “Manufacturing Library” plugin is provided as part of the corresponding application framework to enable this functionality in the build. The user must then add code to the application to invoke these functions (described in stack/include/mfglib.has well as *UG100: EZSP Reference Guide*) in the desired context. A serial command line-driven interface to these functions is available in EmberZNet PRO SoC and Host applications via the Manufacturing Library CLI plugin, and an over-the-air (OTA)-driven interface is available in EmberZNet PRO SoC applications via the Manufacturing Library OTA plugin.

If the new device fails to successfully transmit or receive packets with the known good device, you may want to attach the new device to a signal generator or network analyzer to verify that generated packets on the target frequency can be received and that the new device can transmit accurately at the center frequency of the selected channel. Other tests may be required for FCC or CE compliance testing.

6. Setting Stack Tokens

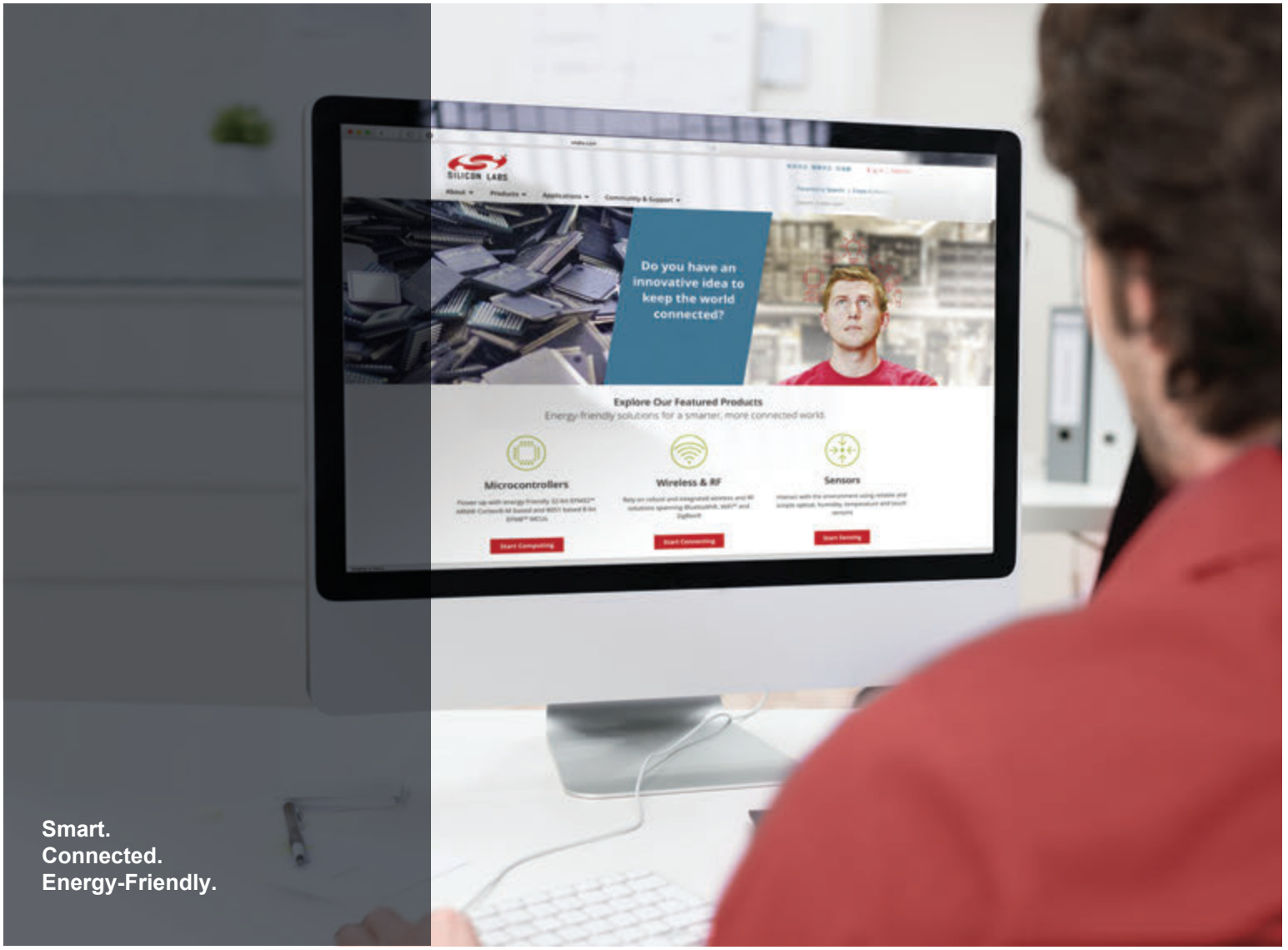
The stacks maintain several non-volatile settings (tokens) used for network operation. Additionally, certain applications may require the use of their own tokens for non-volatile data storage.

Note: NodeTest cannot be rebuilt with application tokens.

To use the NodeTest application for programming stack token values:

1. Install the NodeTest application on the device.
2. Using a serial or telnet connection with port speed set to 115200 bps, press **Enter** to initiate the NodeTest application.
3. Use the `tokmap` command to output the map of the token storage area.
4. Use the `loadtoks` command to initialize all stack tokens to their default values.
5. Use the `tokdump` command to confirm the values the tokens.
6. Use the `tokread` and `tokwrite` commands to view and manipulate individual tokens.

Note: For more information about tokens and the Simulated EEPROM, refer to the token.h File Reference in the stack API Reference for your Ember chip and document *AN703: Using the Simulated EEPROM*.



Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

SILICON LABS®

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

http://www.silabs.com