congatec Application Note #8

Affected Products	All congatec x86 Products with BIOS
Subject	Create and Add an OEM CMOS Default Map Module
Confidential/Public	Public
Author	CJR

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2006-07-31	OAL	Initial release
1.1	2006-08-30	RCH	Added guideline for the DOS version in section 3.
1.2	2006-11-09	OAL	Updated for congatec System Utility Tool version 1.3.0
1.3	2007-10-19	RCH	Updated DOS commands in section 3
1.4	2013-03-28	HOM	Added a Note for Section 2 and 3
1.5	2014-07-23	CJR	Major rework. Added chapter 4. Removed all references to saving a BIOS from flash to file and using this file to update other modules.
1.6	2017-03-21	CJR	Updated template and major rework.
1.7	2020-05-08	CJR	Added chapter 5 Updated for congatec System Utility Tool version 1.5.8
1.8	2021-03-01	CJR	Added note on page 6.
1.9	2024-04-24	MAN	Updated template and preface section. Added note in section 3, page 16.

Preface

This application note describes with examples, how to create an OEM Default Settings Map module using the congatec System Utility.

The names "CMOS Default Map" and "CMOS Backup Map" refer to the old legacy BIOS. With the new UEFI firmware, these names are not used anymore because UEFI does not use the CMOS RAM in the RTC to store the system configuration. Therefore, congatec System Utility revision 1.5.7 and later refer to "Current Settings Map" instead of "CMOS Backup Map" and "Default Settings Map" instead of "CMOS Default Map".

Software Licenses

Notice regarding Open Source software

The congatec products contain Open Source software that has been released by programmers under specific licensing requirements such as the "General Public License" (GPL) Version 2 or 3, the "Lesser General Public License" (LGPL), the "ApacheLicense" or similar licenses.

You can find the specific details at https://www.congatec.com/en/licenses/. Search for the revision of the BIOS/UEFI or Board Controller Software (as shown in the POST screen or BIOS setup) to get the complete product related license information. To the extent that any accompanying material such as instruction manuals, handbooks etc. contain copyright notices, conditions of use or licensing requirements that contradict any applicable Open Source license, these conditions are inapplicable.

The use and distribution of any Open Source software contained in the product is exclusively governed by the respective Open Source license. The Open Source software is provided by its programmers without ANY WARRANTY, whether implied or expressed, of any fitness for a particular purpose, and the programmers DECLINE ALL LIABILITY for damages, direct or indirect, that result from the use of this software.

OEM/ CGUTL BIOS

BIOS/UEFI modified by customer via the congatec System Utility (CGUTL) is subject to the same license as the BIOS/UEFI it is based on. You can find the specific details at https://www.congatec.com/en/licenses/.

Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec GmbH provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec GmbH assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec GmbH be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

Electrostatic Sensitive Device

All congatec GmbH products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec GmbH product except at an electrostatic-free workstation. Additionally, do not ship or store congatec GmbH products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec GmbH Limited Warranty.

Technical Support

congatec GmbH technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Symbols

The following are symbols used in this application note.

Note

Notes call attention to important information that should be observed.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Warning

Warnings indicate that personal injury can occur if the information is not observed.

Copyright Notice

Trademarks

Terminology

Term	Description
BIOS	BIOS: Basic Input Output System. BIOS is actually firmware, the software that is programmed into a ROM (Read-Only Memory) chip built onto the motherboard of a computer
UEFI	Unified Extensible Firmware Interface is a specification that defines a software interface between an operating system and platform firmware. UEFI is meant as a replacement for the Basic Input/Output System (BIOS) firmware interface.
Flash	A special type of EEPROM (Electrically Erasable Read Only Memory) that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can easily be updated if necessary.
POST	Power-on Self Test - a diagnostic testing sequence run by a computer's BIOS as the computer's power is initially turned on. The POST will determine if the computer's RAM, disk drives, peripheral devices and other hardware components are properly working.
CGUTIL	congatec System Utility – universal tool for BIOS updates and BIOS modifications.
CGOS	congatec Operating System API – software driver for the congatec Embedded Features
ME	Management Engine (Intel specific controller and firmware offering additional features)
COM	Computer-on-module
dTPM	Discrete TPM chip
fTPM	Firmware TPM
PTT	Platform Trust Technology (Intel firmware TPM solution in the Intel ME)

1 Introduction

The following sections describe how to create an OEM Default Settings Map module within the BIOS module using the congatec System Utility. It is compatible to all congatec x86 products and available as a Windows (CGUTIL GUI) application and a command line (CGUTLCMD) application.

The second chapter is based on the Windows GUI version. The third chapter is based on the command line version. The fourth chapter explains the most commonly used procedure to create a new OEM BIOS file. Chapter 5 explains some limitations and exceptions of the OEM Default Settings Map.

The target system consists of conga-TS170 COM and BIOS ROM file "BHSLR123.BIN". The initial production BIOS is identified as BHSLR1xx:

- BHSL is the congatec internal project name.
- R is the identifier for a BIOS ROM file.
- 1 is the type descriptor for a production BIOS.
- xx is the revision number.

The congatec Embedded BIOS employs a security feature that prevents a password protected BIOS from being overwritten.

To understand which settings are required in the congatec Embedded BIOS to enable the security feature and how the congatec System Utility (CGUTIL) can be used with a protected BIOS, see application note AN5_BIOS_Update_And_Write_Protection.pdf. It can be downloaded from the congatec website at www.congatec.com. For detailed information about the congatec System Utility, refer to the user's guide. It can be downloaded from the congatec website as well.

Note

Generate the "Current Settings Map" via the BIOS setup menu -before- starting an external boot loader or the UEFI shell. Press the DEL key during power on self-test to enter the BIOS setup menu. If the BIOS setup menu is entered after starting an external boot loader or the UEFI shell, it is not possible to generate the "Current Settings Map".

2 Creating and adding a OEM Default Setting Map using CGUTIL GUI (Windows version)

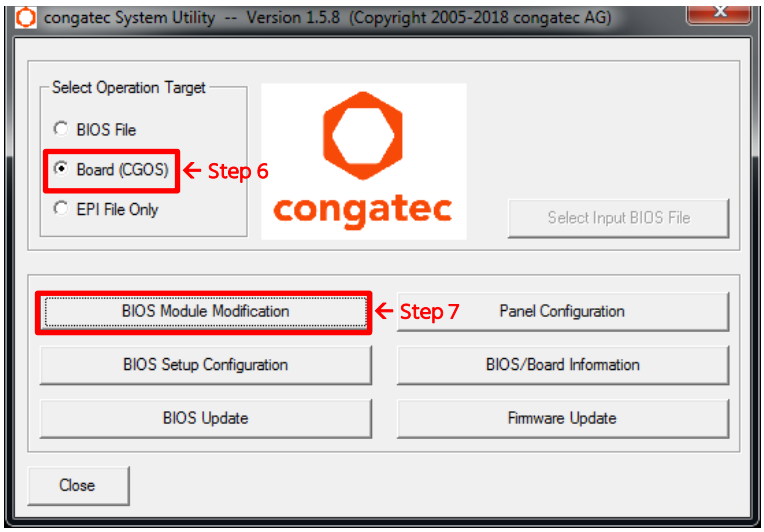
The method described below is useful for evaluating and testing the OEM customization feature offered by the congatec System Utility. On the target system, you can immediately check the BIOS setup changes.

1. Enter the BIOS Setup Program of your congatec CPU board.
2. Select the settings required for your OEM specific Default Settings Map. A Current Settings Map will be automatically generated and written to the BIOS flash chip when saving the BIOS setup configuration before exiting setup.

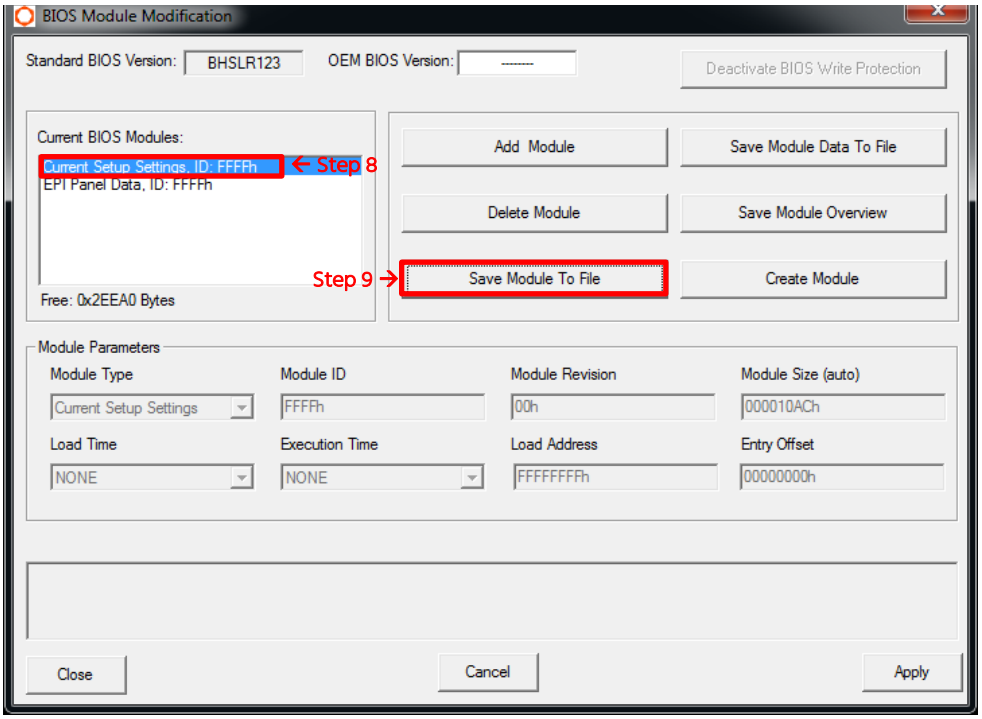
Note

The OEM maps are specific to BIOS revisions. A created OEM map can only be used on the BIOS revision it is derived from. It cannot be integrated into another BIOS revision.

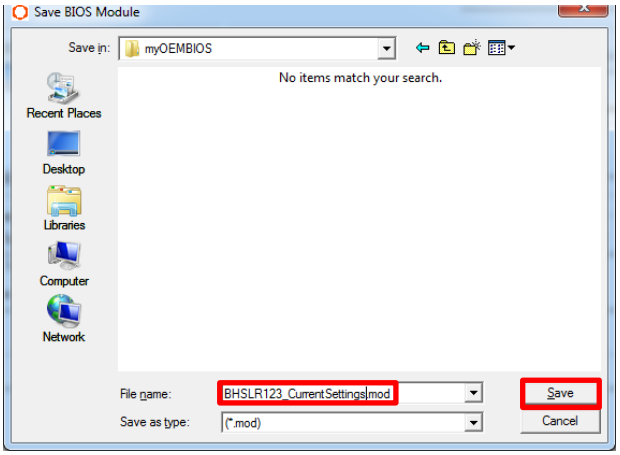
3. Boot Microsoft Windows.
4. To install the congatec System Utility, refer to the congatec System Utility user's guide.
5. Start the congatec System Utility.
6. Select "Board (CGOS)" to modify the onboard BIOS of your running system.
7. Click "BIOS Module Modification".



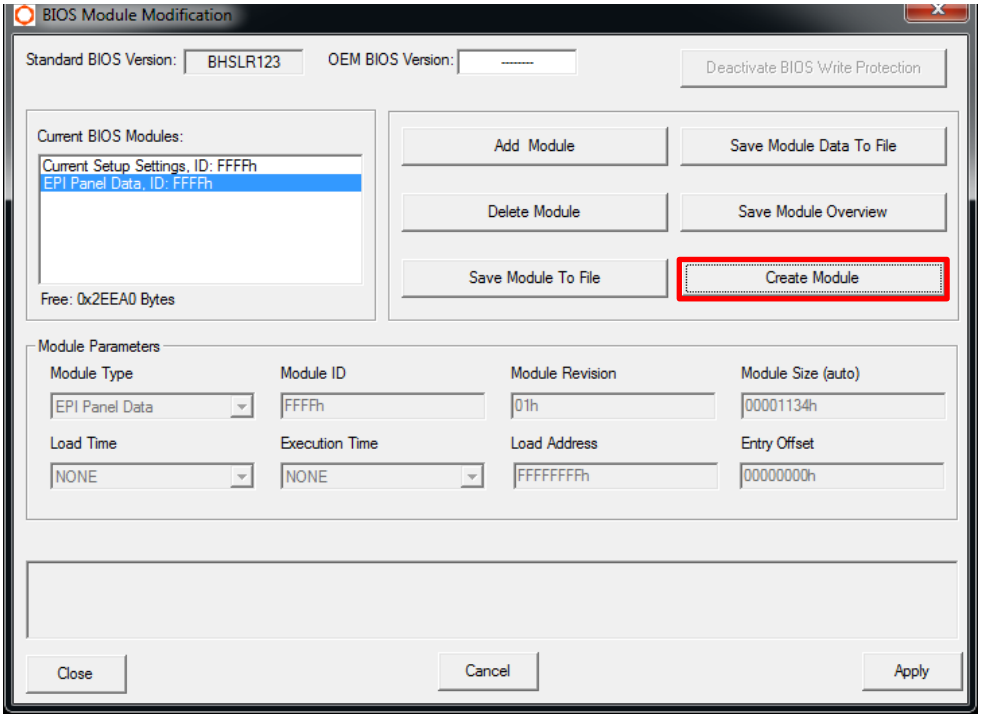
8. Click “Current Setup Settings” in the “Current BIOS Modules” section.
9. Click “Save Module To File” button.



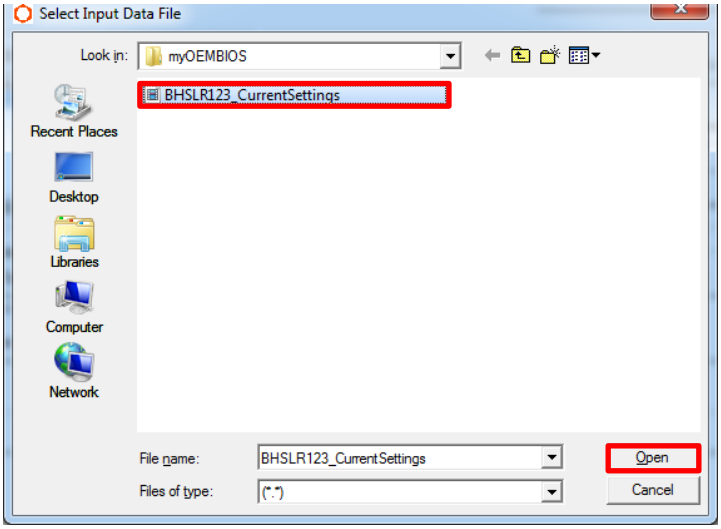
10. Enter a name for the Current Setup Settings Map (in this example “BHSLR123_CurrentSettings.mod”) and click “Save”. Later on, this map will also be implemented into your OEM BIOS binary file.



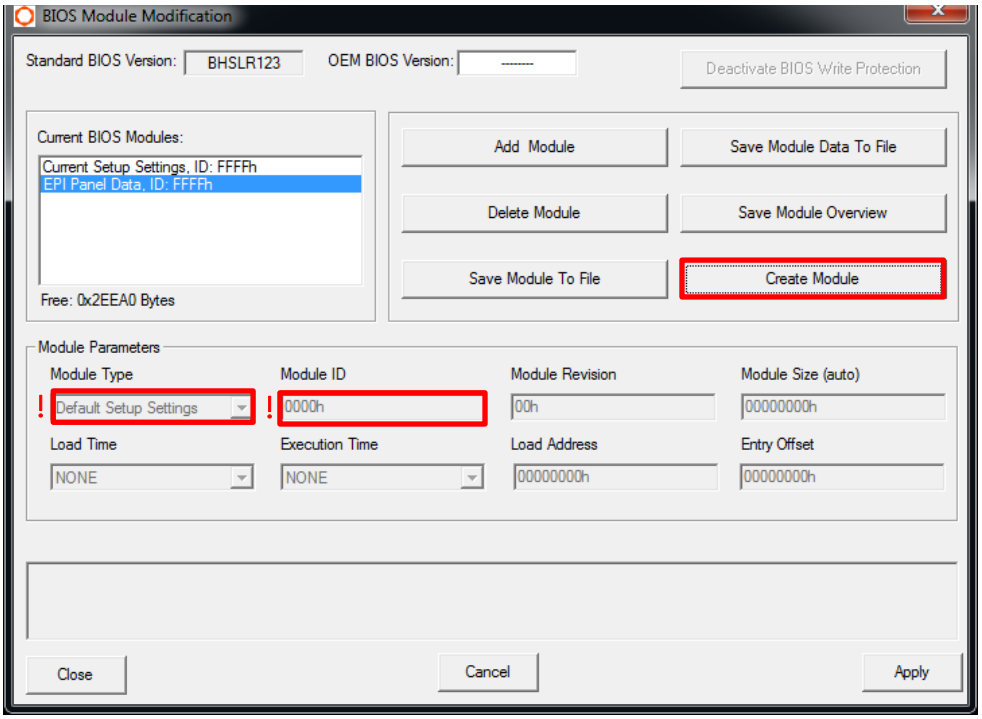
11. Click “Create Module” button to create an OEM Default Settings Map from your Current Settings Map.



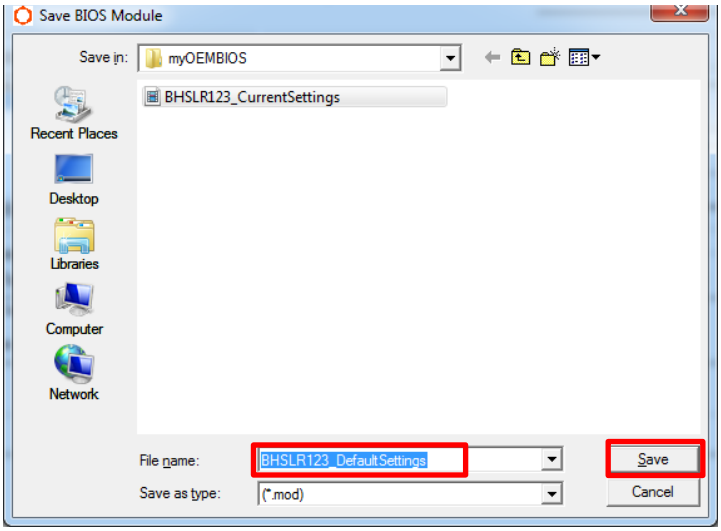
12. The “Select Input Data File” window appears. Click the previously saved backup file (in this example “BHSLR123_CurrentSettings.mod”) and then click “Open”.



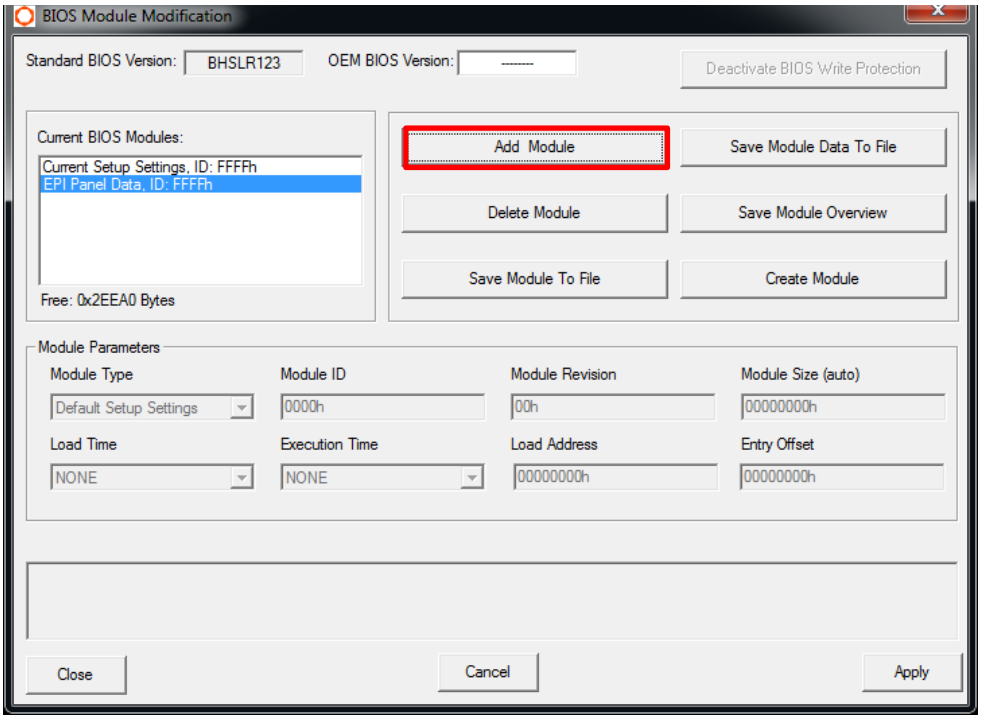
13. Make sure to change the "Module Type" to "Default Setup Settings" and keep the "Module ID" set at 0000h (default) before clicking the "Create Module" button again to generate the new module.



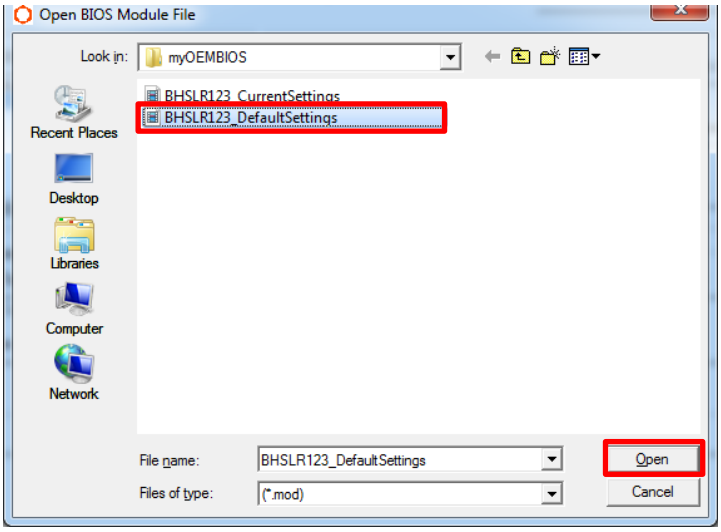
14. Save the created Default Settings Map (in this example "BHSLR123_DefaultSettings.mod"). Later on, this map will be implemented into your OEM BIOS binary file.



15. Click "Add Module" in the "BIOS Module Modification" window to add the Default Settings Map Module (in this example "BHSLR123_DefaultSettings.mod").

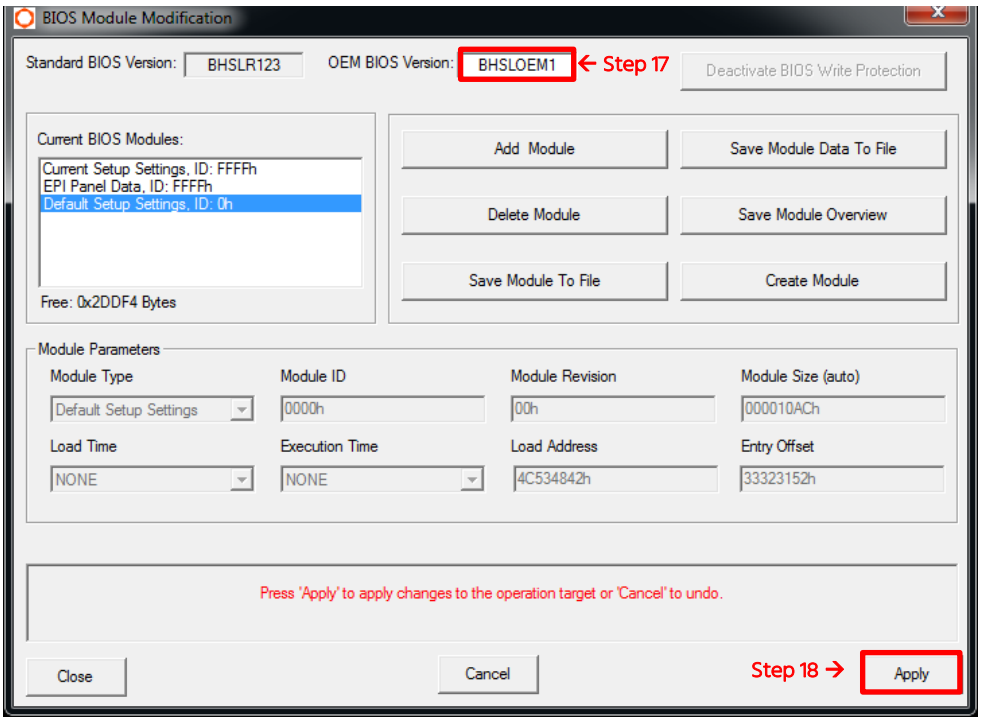


16. Click the previously saved Default Settings Map from step 14 (in this example "BHSLR123_DefaultSettings.mod") and then click "Open".



17. The Default Settings Map appears in the "Current BIOS Modules" module window. Name your OEM BIOS Version (in this example "BHSLOEM1"). This name is shown in the BIOS Setup Program below the congatec BIOS version.

18. Click "Apply" to confirm your changes.



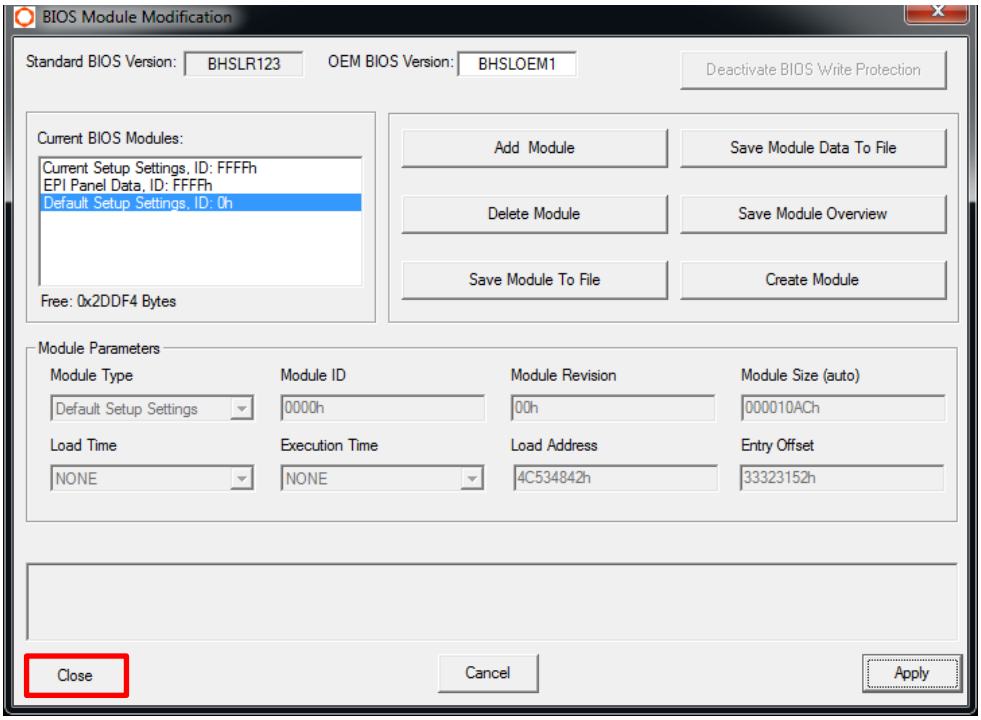
Caution

An incorrect setting may damage your onboard BIOS file which could lead to a problem. In worst case, the board may no longer be bootable. A safe alternative way would be to switch to a host PC system and do the necessary changes in a BIOS binary file separately.

Note

If the "Current Setup Settings" module is not visible in the "Current BIOS Modules" window (as in the picture above), add the module created in step 10 with your desired default settings. If a "Current Setup Settings" module is displayed with the wrong default settings, overwrite it with the correct module.

19. Click the "Close" button to close the "BIOS Module Modification" window.



Caution

Do not save the BIOS of the target module to a file to use for mass production of additional modules. For the purpose of generating a mass production BIOS, you should always work in file mode. UEFI based BIOS binaries might not work correctly following this procedure. Always work on a BIOS binary file as explained in chapter 4 when a new BIOS file must be created.

Note

For more information about how to update the BIOS file, see application note AN1_BIOS_Update.pdf. This application note can be downloaded from the congatec website.

3 Creating and adding an OEM Default Settings Map using CGUTIL command line version

The method described here is helpful for updating the congatec BIOS on the production line using the command lines from step 6 and 7 in a simple batch script. This example explains the procedure in DOS. The command line version of CGUTIL works the same way in Linux and the EFI shell. All example names used in the steps below may be changed. Only the DOS naming convention of an 8 character name and 3 character extension, separated by a dot, must be adhered to.

1. Enter the BIOS Setup of your congatec CPU board and select the settings required for your OEM specific Default Settings Map.
2. Press the <F10> key or "Save and Exit" to save the BIOS settings. A Current Settings Map will be automatically generated and written to the BIOS flash.
3. Reset your computer and start DOS.
4. Switch to the "congatec System Utility" folder.

   Enter the command below to save the Current Settings Map created in step 2. You may change the name "BHSLCSM.mod".

   ```
   cgutlcmd module /ot:board /save /of:BHSLCSM.mod /t:1
   ```
5. Enter the command below to create an OEM Default Settings Map. You may change the parameter "/of:" (in this example "BHSLDSM") with its default extension ".mod". Use the selected Current Settings Map name from the previous step (in this example "BHSLCSM.mod") after parameter '/if:'.

   ```
   cgutlcmd module /ot:board /create /if:BHSLCSM.mod /of:BHSLDSM.mod /t:2
   ```
6. Enter the command below to add the newly created OEM Default Settings Map to your BIOS. Use the name of the parameter '/if:' from the previous step (in this example "BHSLDSM.mod").

   ```
   cgutlcmd module /ot:board /add /if:BHSLDSM.mod
   ```

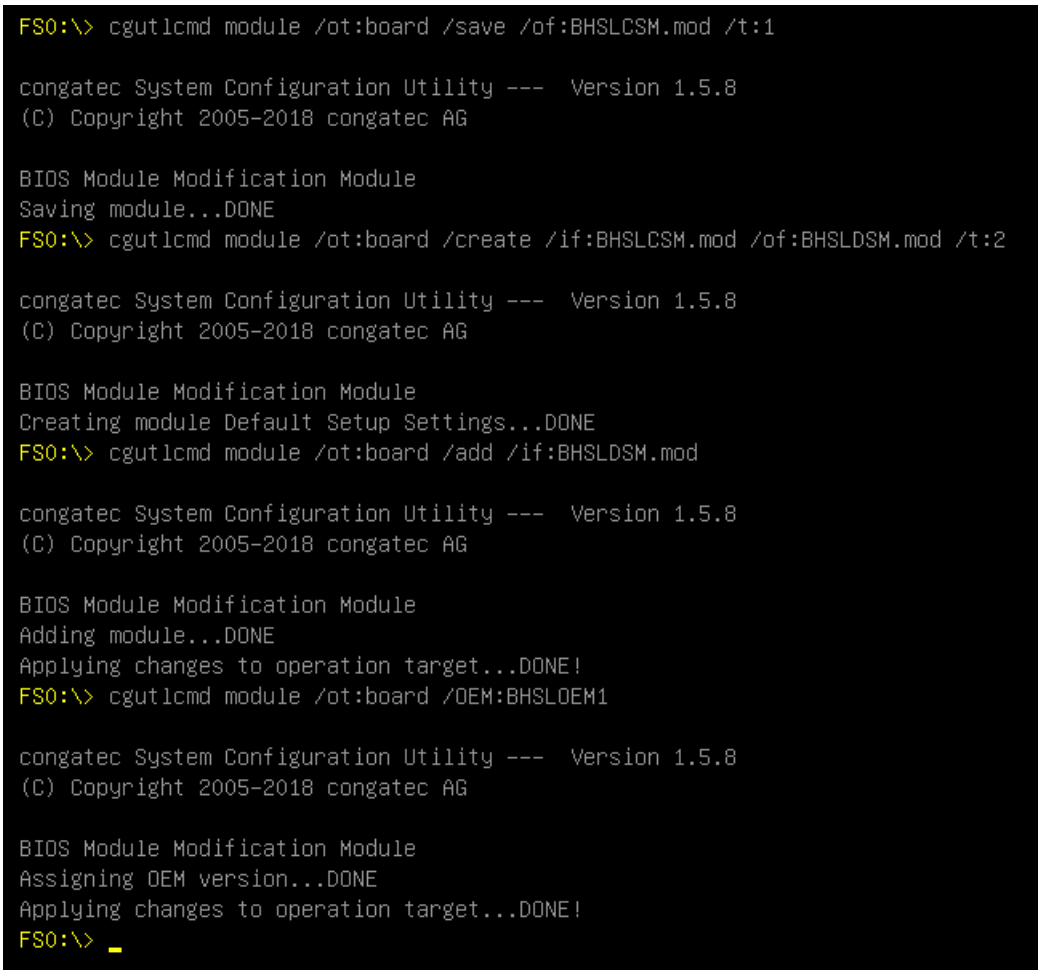
Note

The default settings maps are specific to BIOS revisions. A created map can only be used on the BIOS revision it is derived from. It can not be used to flash another BIOS revision. For further information about your system BIOS, please refer to the appropriate user's guide, which can be found on the congatec website.

7. Use the command below to assign a customized OEM BIOS name to the modified BIOS. This OEM name will be shown in the main page of the BIOS setup below the congatec standard BIOS name. You may change the name "BHSLOEM1".

   ```
   cgutlcmd module /ot:board /OEM:BHSLOEM1
   ```

The screenshot below shows how the commands above are executed in the EFI shell:



Note

The same method (steps 1-7) can also be applied to a BIOS file, which may later be used to program other modules.

In the commands of steps 6 and 7, replace 'board' with the specific BIOS file.

Example:

```
cgutlcmd module /ot:board /save /of:BHSLCSM.mod /t:1
cgutlcmd module /ot:board /create /if:BHSLCSM.mod /of:BHSLDSM.mod /t:2

cgutlcmd module /ot:BHSLR123.bin /add /if:BHSLDSM.mod
cgutlcmd module /ot:BHSLR123.bin /OEM:BHSLOEM1

mv BHSLR123.bin BHSLTEST.bin
```

The last command renames the modified BIOS file for easier identification later.

4 Creating and adding a OEM Default Settings Map using CGUTIL CMD and GUI

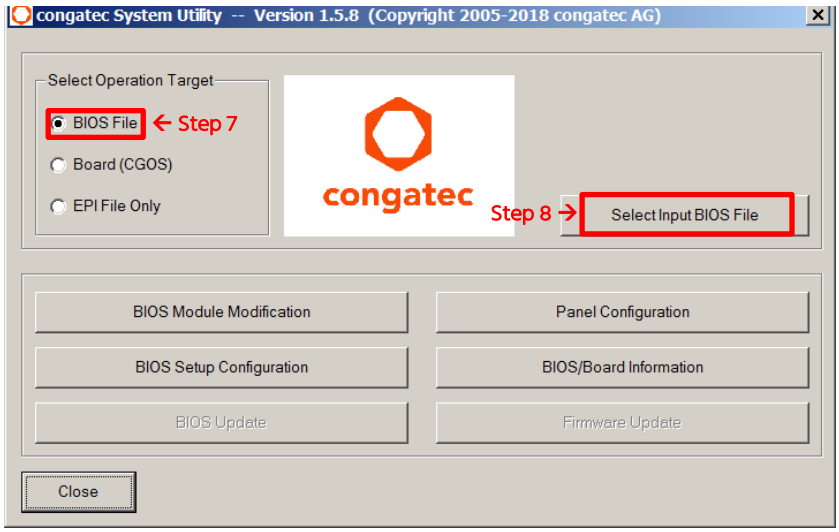
The easiest way to customize a BIOS with an OEM Default Settings Map is to use the command line version CGUTLCMD on the target system first and then switch to a development PC running the Windows GUI version of CGUTIL in 'File Mode'.

The method described here is typically used to build a customized OEM BIOS binary file that can then be flashed on additional congatec CPU boards.

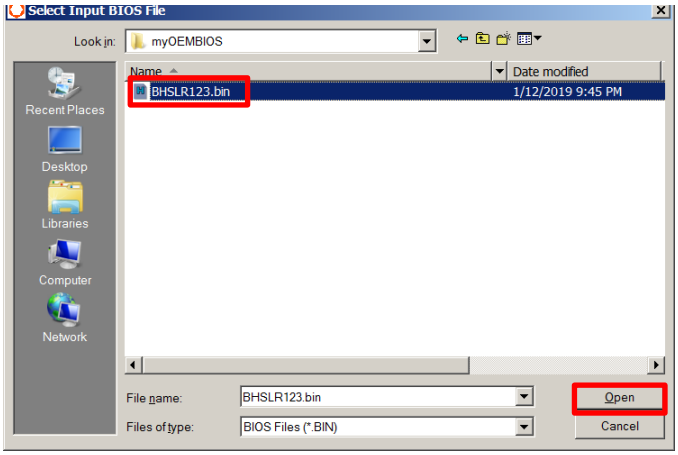
The first five steps are almost identical to the method described in chapter 3.

1. Enter the BIOS Setup of your congatec CPU board and select the settings required for your OEM specific Default Settings Map. For further information about your system BIOS, please refer to the appropriate user's guide, which can be found on the congatec website.
2. Press the <F10> key or "Save and Exit" to save the BIOS settings. A Current Settings Map will be automatically generated and written to the BIOS flash.
3. Reset your computer and start DOS or the EFI shell (typically from a USB stick).
4. Switch to "congatec System Utility" folder.
5. Enter the command below to save the Current Settings Map created in step 2. You may change the name "BHSLCSM.mod".

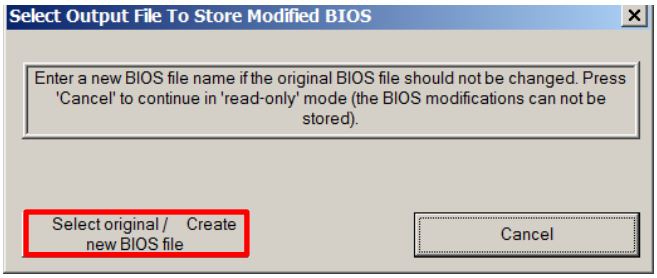
   ```
   cgutlcmd module /ot:board /save /of:BHSLCSM.mod /t:1
   ```
6. Switch to your Windows based development PC and start the congatec System Utility "CGUTIL.exe".
7. Select "BIOS File" to modify the original congatec BIOS binary file.
8. Click "Select Input BIOS ROM File".



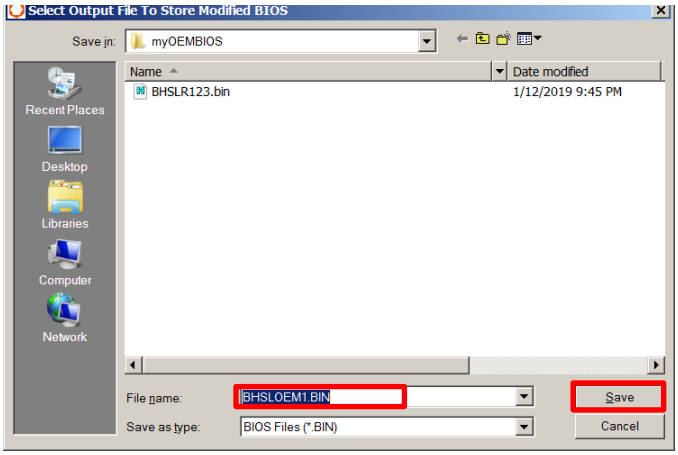
9. Load the BIOS binary you want to modify (in this example "BHSLR123.bin").



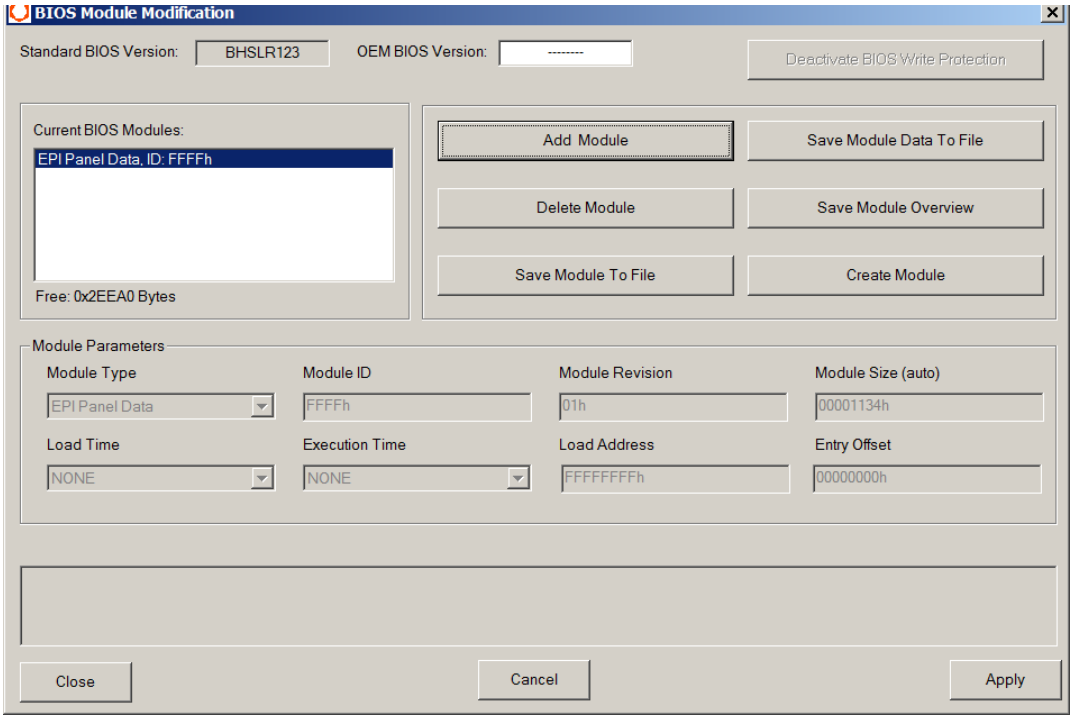
10. Click "Select original / Create new BIOS file" in order to create your new OEM BIOS binary file as shown in the pop-up menu below.



11. Name your OEM BIOS file (in this example "BHSLOEM1.BIN") and click "Save".

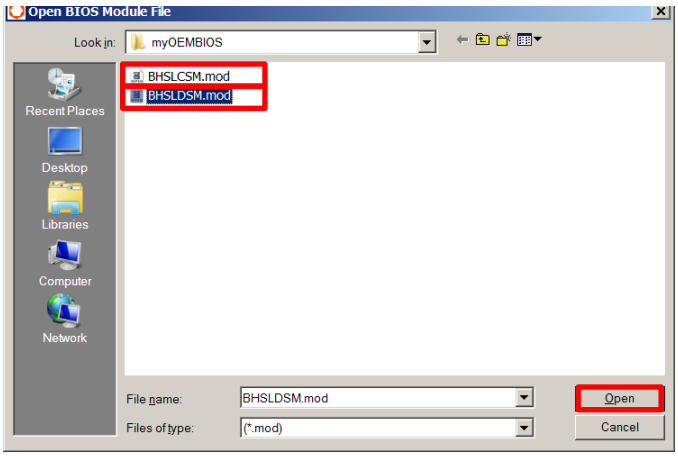


12. Click the "BIOS Module Modification" button to open the window pictured below. You will see that neither a Current Settings map nor a Default Settings map is present in the congatec standard BIOS binary.

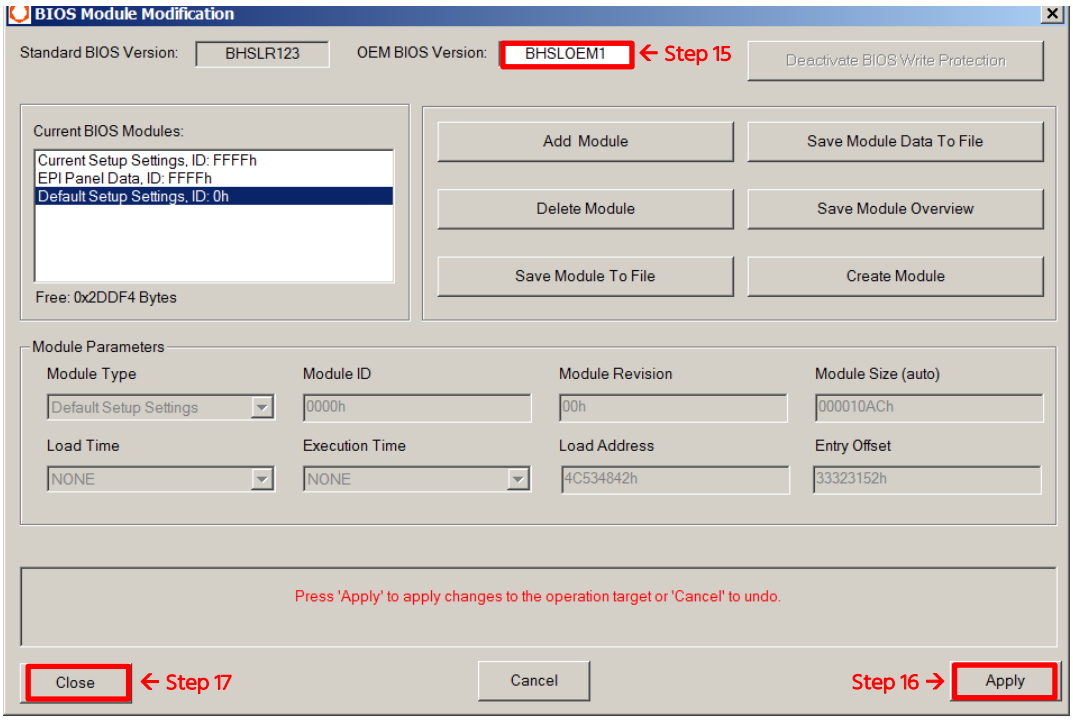


13. Create the OEM Default Settings Map as described in steps 11 to 14 in chapter 2. In this example, the file name of the Current Settings Map is "BHSLCSM.mod" and for the Default Settings Map "BHSLDSM.mod". You must copy the Current Settings Map file from your USB stick beforehand.

14. Click the "Add Module" button in the "BIOS Module Modification" window to add the Default Settings Map Module (in this example "BHSLDSM.mod"). Then, also add the Current Settings Map Module (in this example "BHSLCSM.mod") created earlier in DOS or the EFI shell to the new BIOS.



15. Assign your OEM name to the BIOS.
16. Save the new BIOS file by clicking the "Apply" button.
17. Click "Close" to close CGUTIL.



18. The new "BHSLOEM1.BIN" BIOS binary file can now be flashed on additional congatec products.

Note

It is assumed that a new OEM BIOS should not only load the OEM default settings when the Load Default command is executed in BIOS Setup (F9), it should also start with these settings on the first boot after the OEM BIOS has been flashed. That is why the same settings are also added as Current Settings Map.

5 Limitations / Exceptions

The setup settings described in this section cannot be modified with an OEM default map. These settings are handled differently by the UEFI firmware for security reasons.

5.1 BIOS Password

It is not possible to assign a default password in an OEM default map. To assign a default password, use the OEM backup map or set the password manually in the BIOS setup menu. After a password is assigned, you cannot revert or set it back to default by pressing F9 key to load default settings. The password can only be changed manually in the BIOS setup menu.

Note

Only a customized source code BIOS with a defined default password can restore the password when loading defaults (F9) in BIOS setup.

5.2 Secure Boot

The most important variables for Secure Boot are the Platform Key (PK), the Key Exchange Key (KEK) and the database of authorized boot loaders (DB). For security reasons, these variables cannot be handled by CGUTIL OEM default and backup maps. That is why Secure Boot always requires source code OEM BIOS development.

Note

Refer to the application note "AN39_Secure_Boot_BIOS_Customizations.pdf" on the congatec website or contact your local congatec FAE.

5.3 Trusted Computing (TPM Support)

The setup option to enable TPM support can also not be assigned a default with an OEM default map. Like the BIOS password, it can be customized using an OEM backup map. All other TPM settings in the Trusted Computing submenu are fully supported by OEM default and backup maps.

On Intel platforms that support PTT (fTPM), the initial power-on setting for the TPM Device Selection (PTT vs. dTPM) is hard coded in the Intel ME firmware. An OEM backup map cannot change this setting. However, it is possible to customized the default setting for TPM Device Selection in an OEM Default map.

Note

For PTT support, an Intel ME enabled BIOS (R7xy) is required.