congatec Application Note#5

Affected Products	Products featuring UEFI Firmware
Subject	BIOS Update and Write Protection
Confidential/Public	public
Author	CJR

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2006-10-31	HCH	Initial Release
1.1	2010-12-13	CJR	EOL products removed, new products added
1.2	2017-02-24	CJR	Complete rework and update to new template

Preface

Application Note explains the benefits and describes the security feature called 'BIOS Update and Write Protection' incorporated in the congatec Embedded BIOS. This Application Note also describes how this feature can be used with the congatec System Utility Tool (CGUTIL).

Disclaimer

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

congatec AG 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 AG 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 AG 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 AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG 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 AG Limited Warranty.

Technical Support

congatec AG 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

congatec AG has made every attempt to ensure that the information in this document is accurate yet the information contained within is supplied "as-is".

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user's guide or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

Terminology

Term	Description
UEFI	Unified Extensible Firmware Interface
AMI	American Megatrends, Inc - congatec's BIOS partner
Aptio	AMIs UEFI Firmware product
POST	Power On Self Test
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.

CGOS API	congatec operating system application programming interface
CGUTIL	congatec System Utility
COM	Computer on Module
SBC	Single board computer
GUI	Graphical user interface

1 Introduction

Some applications require security features that must protect the BIOS against undesired manipulations. Most common BIOS support password protected BIOS setup programs to avoid unauthorized access to the BIOS settings. This security feature can be easily bypassed by flashing over the secured BIOS using an adequate non secured BIOS. Common BIOS flash tools have no mechanism to recognize if the BIOS that is to be overwritten is secured or not.

The congatec Embedded BIOS employs a security feature which prohibits flashing over a secured BIOS (see note below).

The following sections will explain the necessary settings in the congatec Embedded BIOS to enable the security feature and how the congatec System Utility (CGUTIL) can be used with a password protected BIOS.

For detailed information about the congatec System Utility please consult the user's guide. This can be found on the congatec homepage (www.congatec.com).

Note

congatec has removed the support for other BIOS flash tools except for the congatec System Utility. With such flash tools the BIOS update is not possible regardless of the protection mechanism described in the AN.

Requirements

The feature described in this Application Note is supported by the congatec System Utility starting from Revision 1.3.0. It is recommended to always use the latest revision of the congatec System Utility. Check the congatec website regularly to ensure that you have the latest version of the utility.

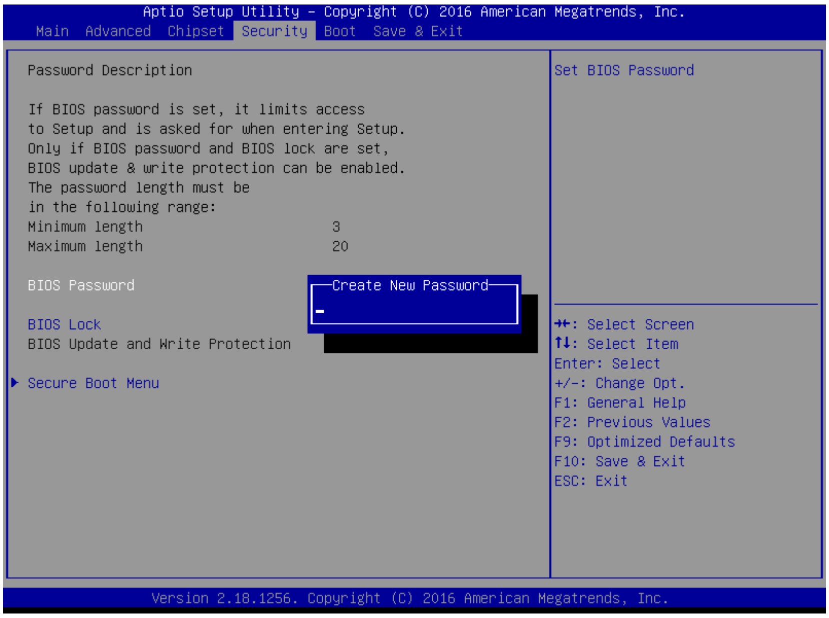
The congatec System Utility requires a cgos driver version equal to or higher than 1.02.014. The driver can be downloaded from the congatec homepage (www.congatec.com).

The BIOS Update and Write Protection feature is supported on most newer congatec COMs and SBCs. Some older products running UEFI firmware versus the legacy BIOS do not support the BIOS Update Write Protection feature.

Check the user’s guide of the product you are using for detailed information.

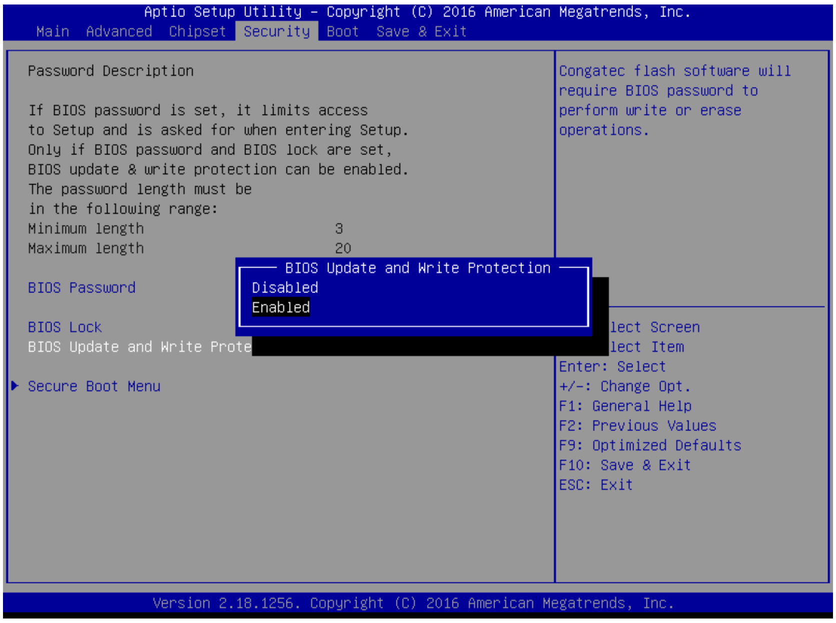
2 BIOS Settings

After a BIOS password has been set in the BIOS setup (see image 1) an additional 'BIOS Update and Write Protection' setup node will appear. If set to 'Enabled', the BIOS protection will be activated after the next reboot (see image 2).



```
Aptio Setup Utility – Copyright (C) 2016 American Megatrends, Inc.

Password Description                                     Set BIOS Password

If BIOS password is set, it limits access
to Setup and is asked for when entering Setup.
Only if BIOS password and BIOS lock are set,
BIOS update & write protection can be enabled.
The password length must be
in the following range:
Minimum length                    3
Maximum length                    20

BIOS Password           ┌Create New Password┐
                        │_                  │
BIOS Lock               └───────────────────┘
BIOS Update and Write Protection

► Secure Boot Menu

Version 2.18.1256. Copyright (C) 2016 American Megatrends, Inc.
```

Image 1: Entering the BIOS Password



```
Aptio Setup Utility – Copyright (C) 2016 American Megatrends, Inc.

Password Description                                     Congatec flash software will
                                                         require BIOS password to
If BIOS password is set, it limits access                perform write or erase
to Setup and is asked for when entering Setup.           operations.
Only if BIOS password and BIOS lock are set,
BIOS update & write protection can be enabled.
The password length must be
in the following range:
Minimum length                    3
Maximum length                    20
                       ┌── BIOS Update and Write Protection ──┐
BIOS Password          │Disabled                              │
                       │Enabled                               │
BIOS Lock              └──────────────────────────────────────┘
BIOS Update and Write Prote

► Secure Boot Menu

Version 2.18.1256. Copyright (C) 2016 American Megatrends, Inc.
```

Image 2: Enable BIOS Update and Write Protection

The BIOS Password cannot be changed or disabled as long as the BIOS Update and Write Protection feature is enabled.

3 congatec System Utility (Windows GUI)

Any write access to the BIOS Flash device (BIOS Update or BIOS Module Modification) with CGUTIL will fail when the BIOS Update and Write Protection is enabled (see images 3, 4, 5, 10 and 11).

With older revisions of CGUTIL, it was only possible to write to the BIOS Flash device after the system supervisor disabled the BIOS Update & Write Protection in the BIOS setup.

Newer CGUTIL tools (from revision 1.3.0) can temporarily disable the BIOS Update and Write Protection so that the user can do the necessary changes in the BIOS flash (see images 6, 7 and 8). Although the BIOS Update and Write Protection is deactivated by the CGUTIL tool, it will still remain enabled in the BIOS setup and will be reactivated after the next reboot.

3.1 BIOS Update

Install the latest versions of the congatec system utility and CGOS driver. Then launch the CGUTIL GUI version and select Board (CGOS) as operation target.

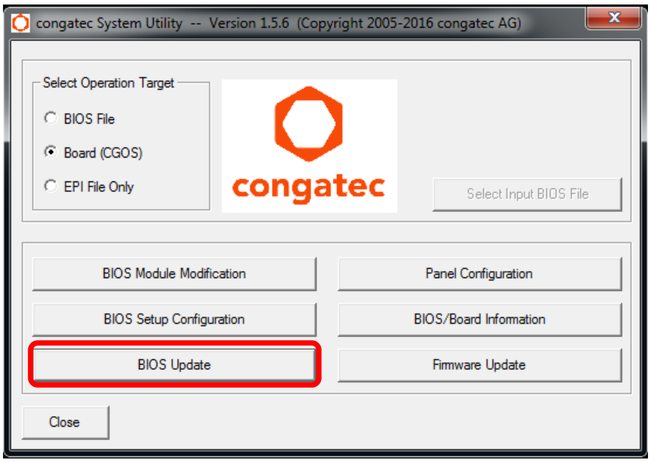
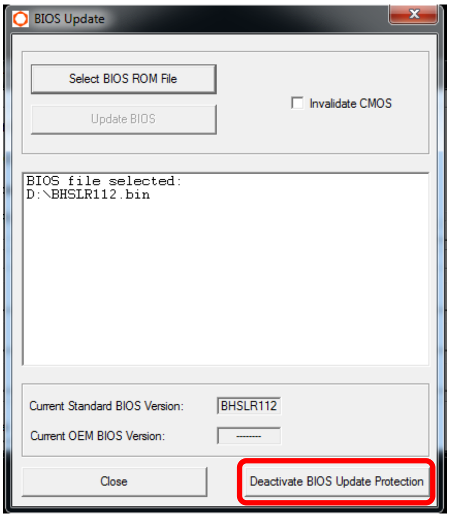


Image 3: CGUTIL Main window

Press the BIOS Update button and select the BIOS file to be updated.



BIOS file selected:
D:\BHSLR112.bin

Current Standard BIOS Version: BHSLR112
Current OEM BIOS Version: -------

Image 4: Deactivate BIOS Update Protection

The button 'Deactivate BIOS Update Protection' must be pressed to temporarily allow write accesses to the BIOS flash device and provides the ability to perform the BIOS update. The Update BIOS button is grayed out until the correct password has been entered (see image 5). The protection will remain disabled until the next reboot.

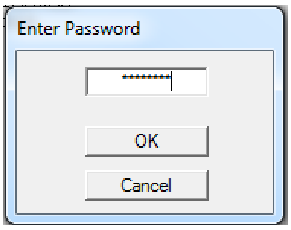
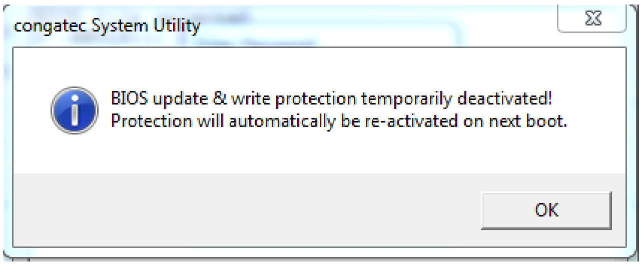


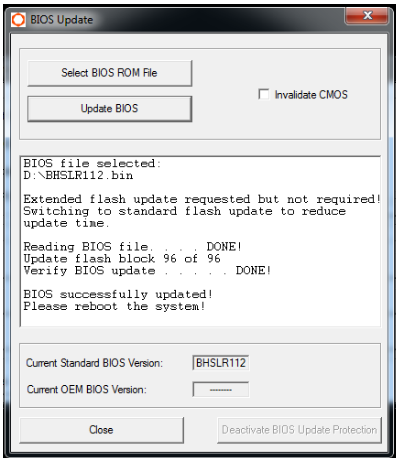
Image 5: Popup window to enter the BIOS password



BIOS update & write protection temporarily deactivated!
Protection will automatically be re-activated on next boot.

Image 6: Confirmation that the BIOS Update Protection has been temporarily disabled

Only with the correct BIOS password entered, the BIOS Update command button will be activated.



```
BIOS file selected:
D:\BHSLR112.bin

Extended flash update requested but not required!
Switching to standard flash update to reduce
update time.

Reading BIOS file. . . . DONE!
Update flash block 96 of 96
Verify BIOS update . . . . . DONE!

BIOS successfully updated!
Please reboot the system!
```

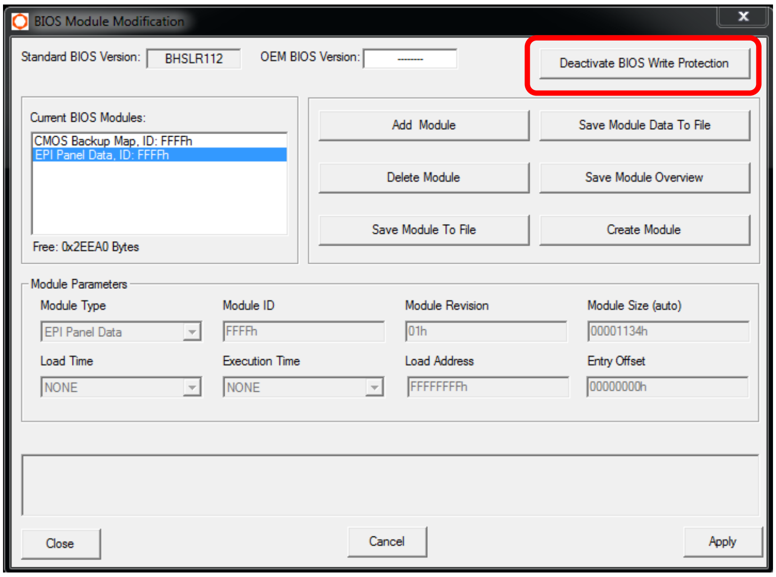
Current Standard BIOS Version: BHSLR112

Current OEM BIOS Version: -------

Image 7: After the BIOS Update Protection has been disabled, a BIOS update can be performed

3.2 BIOS Module Modification

What is true for a BIOS update is also true for BIOS module updates. A BIOS Module modification is also not possible when the BIOS Write Protection is active. The button 'Deactivate BIOS Write Protection' (see picture 8) will temporarily allow write accesses to the BIOS flash device. The protection will remain disabled until the next reboot.



Standard BIOS Version: BHSLR112

OEM BIOS Version: -------

Current BIOS Modules:

CMOS Backup Map, ID: FFFFh

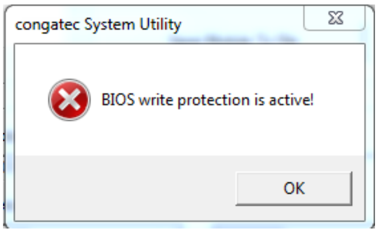
EPI Panel Data, ID: FFFFh

Free: 0x2EEA0 Bytes

Module Parameters

Module Type	Module ID	Module Revision	Module Size (auto)
EPI Panel Data	FFFFh	01h	00001134h
Load Time	**Execution Time**	**Load Address**	**Entry Offset**
NONE	NONE	FFFFFFFFh	00000000h

Image 8: BIOS Module Modification' window.



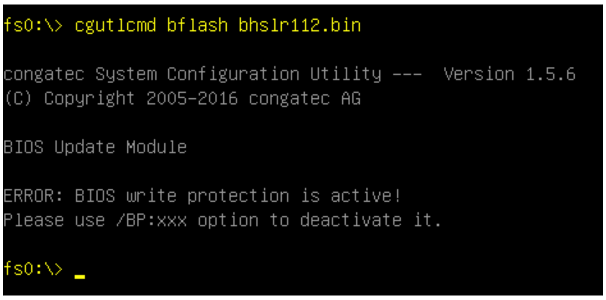
BIOS write protection is active!

Image 9: The BIOS cannot be modified as long as the BIOS Write Protection is enabled.

After entering the BIOS password as in image 5 above, the BIOS module can be written to the flash device.

4 congatec System Utility (command line)

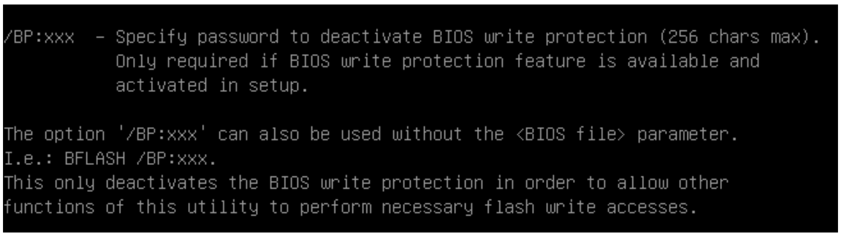
The same protection features mentioned in the previous sections are also applicable when using the command line version of the congatec System Utility (CGUTLCMD). BIOS update and write accesses will not be possible when the BIOS Update and Write Protection is active (image 10).



```
fs0:\> cgutlcmd bflash bhslr112.bin

congatec System Configuration Utility ---  Version 1.5.6
(C) Copyright 2005-2016 congatec AG

BIOS Update Module

ERROR: BIOS write protection is active!
Please use /BP:xxx option to deactivate it.

fs0:\> _
```

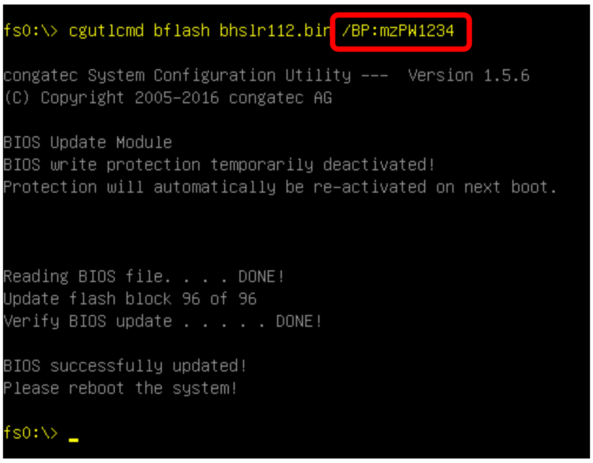
Image 10: Error message when a BIOS update is performed and the BIOS Update and Write Protection is activated

With the command line version of the congatec System Utility the BIOS Update and Write Protection can be disabled with the help of the /BP parameter.



```
/BP:xxx  - Specify password to deactivate BIOS write protection (256 chars max).
           Only required if BIOS write protection feature is available and
           activated in setup.

The option '/BP:xxx' can also be used without the <BIOS file> parameter.
I.e.: BFLASH /BP:xxx.
This only deactivates the BIOS write protection in order to allow other
functions of this utility to perform necessary flash write accesses.
```

Image 11: CGUTLCMD help text describing the /BP: parameter



```
fs0:\> cgutlcmd bflash bhslr112.bin /BP:mzPW1234

congatec System Configuration Utility ---  Version 1.5.6
(C) Copyright 2005-2016 congatec AG

BIOS Update Module
BIOS write protection temporarily deactivated!
Protection will automatically be re-activated on next boot.



Reading BIOS file. . . . DONE!
Update flash block 96 of 96
Verify BIOS update . . . . . DONE!

BIOS successfully updated!
Please reboot the system!

fs0:\> _
```

Image 12: /BP: parameter in the command line

/BP:[password] deactivates the BIOS write protection to allow BIOS updates.

The use of the command line version of the congatec system utility is shown here in the UEFI shell environment. The same procedure applies to DOS and Linux. Refer to the congatec application note AN1_BIOS_Update.pdf for more details about updating the congatec Embedded BIOS.