



## AMI Software Utility User Guide

### Aptio 5.x AMIBGT User Guide

Document Revision 1.03

July 10, 2019



Confidential, NDA Required  
Copyright ©2019

American Megatrends International LLC  
5555 Oakbrook Parkway  
Suite 200  
Norcross, GA 30093 (USA)

All Rights Reserved  
Property of American Megatrends, Inc.

# Legal

## Disclaimer

This publication contains proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, American Megatrends, Inc. American Megatrends, Inc. retains the right to update, change, modify this publication at any time, without notice.

## For Additional Information

Call American Megatrends International LLC. at 1-800-828-9264 for additional information.

## Limitations of Liability

In no event shall American Megatrends be held liable for any loss, expenses, or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential, arising from the design or use of this product or the support materials provided with the product.

## Limited Warranty

No warranties are made, either expressed or implied, with regard to the contents of this work, its merchantability, or fitness for a particular use. American Megatrends assumes no responsibility for errors and omissions or for the uses made of the material contained herein or reader decisions based on such use.

## Trademark and Copyright Acknowledgments

Copyright © 2019 American Megatrends International LLC. All Rights Reserved.

American Megatrends International LLC  
5555 Oakbrook Parkway  
Suite 200  
Norcross, GA 30093 (USA)

All product names used in this publication are for identification purposes only and are trademarks of their respective companies.

# Table of Contents

|  |           |
|--|-----------|
| <b>Aptio 5.x AMIBGT User Guide .....</b>         | <b>1</b>  |
| <b>Legal .....</b>                               | <b>2</b>  |
| <b>Table of Contents.....</b>                    | <b>3</b>  |
| <b>Document Information .....</b>                | <b>4</b>  |
| Purpose .....                                    | 4         |
| Audience .....                                   | 4         |
| Change History.....                              | 4         |
| <b>Introduction.....</b>                         | <b>5</b>  |
| Overview .....                                   | 5         |
| AMIBGT Features .....                            | 5         |
| Requirements.....                                | 5         |
| Supported Operating System.....                  | 5         |
| Firmware Requirements .....                      | 6         |
| <b>AMIBGT Operation.....</b>                     | <b>7</b>  |
| Overview .....                                   | 7         |
| <b>Features and Functions .....</b>              | <b>8</b>  |
| Overview .....                                   | 8         |
| Program all regions with a BIOS ROM file.....    | 8         |
| Program Main BIOS with a BIOS ROM file .....     | 8         |
| Options.....                                     | 9         |
| Error Code Definition .....                      | 11        |
| <b>FAQ.....</b>                                  | <b>12</b> |
| Windows requires a digitally signed driver ..... | 12        |

## Document Information

### Purpose

This document provides information to use the AMIBGT to update the system BIOS.

### Audience

Generic BIOS Engineers, OEM Engineers, and Aptio Customers.

### Change History

| Date       | Revision | Description  |
|------------|----------|--|
| 2013-11-11 | 1.00     | Initial draft  |
| 2016-11-28 | 1.01     | Added /CAPSULE and /RECOVERY commands.                                     |
| 2017-04-27 | 1.02     | Added answer for Windows digitally signed driver.                          |
| 2018-07-10 | 1.03     | Update descriptions of commands and options.<br>Added options information. |

## Introduction

### Overview

**A**MIBGT (AMI BIOS Guard Firmware Update Tool) is a package of utilities used to update the system BIOS under various operating systems. AMIBGT only works for APTIO with BIOS GUARD support.

### AMIBGT Features

This list of features is supported from command line, command prompt, EFI Shell, or Linux shell.

Flash ROM image

Command line operating

### Requirements

#### Supported Operating System

AMIBGT is supported by the following operating systems:

- Microsoft® Windows® 7
- Microsoft® Windows® 8
- Microsoft® Windows® 8.1
- Microsoft® Windows® 10
- EFI Shell
- Linux

## Firmware Requirements

- Compatible with Aptio V.
- For supporting BIOS Guard Flash, the following eModules are required:
  - Intel Bios Guard Technology (5.008\_IntelBiosGuard\_003)
  - RomImage (5.008\_RomImage\_001)
  - Flash – Source(5.004\_Flash\_06)

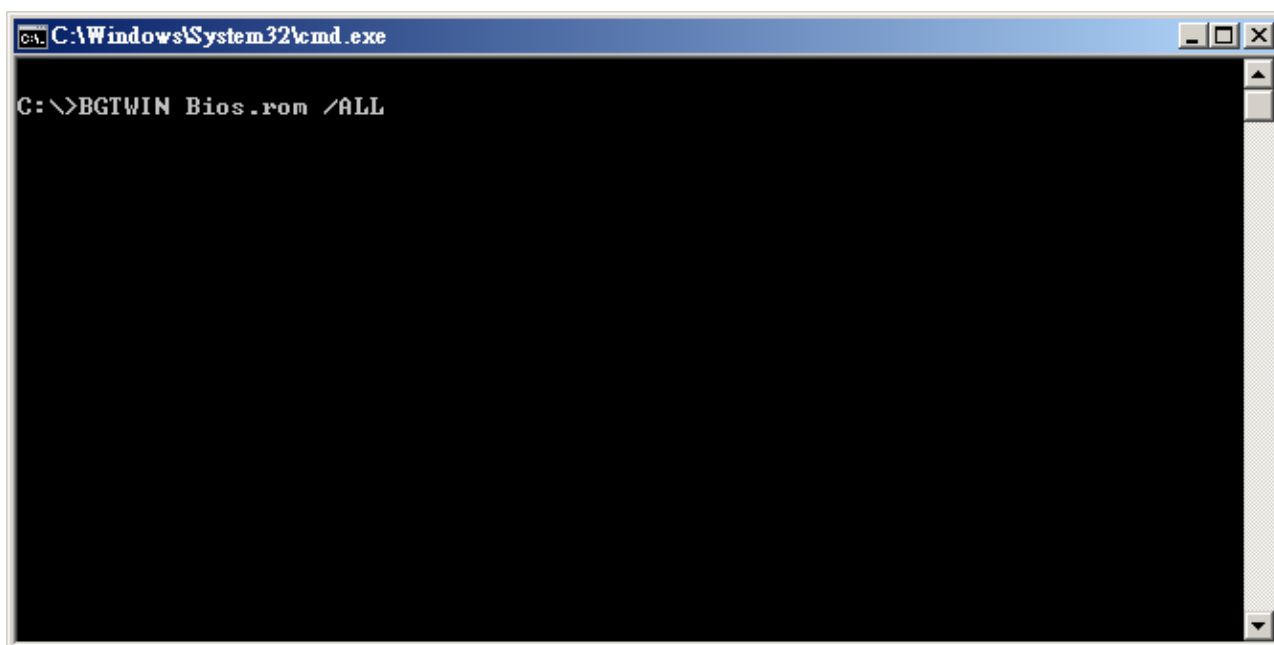
## AMIBGT Operation

### Overview

This chapter explains the operation of AMIBGT.

The AMIBGT operation mode includes all of the AMIBGT features such as programming all regions with a BIOS ROM file and programming Main BIOS with a BIOS ROM file.

An example of BGTWIN programming in all regions with a BIOS ROM file command screen is shown below:



```
C:\Windows\System32\cmd.exe  
C:\>BGTWIN Bios.rom /ALL
```

## Features and Functions

### Overview

The AMIBGT offers the following features:

- Program all regions with a BIOS ROM file
- Program Main BIOS with a BIOS ROM file

These features are explained in more detail in this chapter.

### Program all regions with a BIOS ROM file

The following command programs all regions with a BIOS ROM file:

***BGTEFI <Input BIOS ROM File Name> /ALL***

Where BIOS ROM File Name, the mandatory field is used to specify path/filename of the BIOS ROM file with extension.

### Program Main BIOS with a BIOS ROM file

The following command programs Main BIOS with a BIOS ROM file:

***BGTEFI <Input BIOS ROM File Name> /P***

Where BIOS ROM File Name, the mandatory field is used to specify path/filename of the BIOS ROM file with extension.

## Options

***BGTEFI <BIOS ROM File Name> [Option 1] [Option 2]***

Or

***BGTEFI <BIOS ROM File Name> <Command>***

### BIOS ROM File Name

The mandatory field is used to specify path/filename of the BIOS ROM file with extension.

### Commands

The mandatory field is used to select an operation mode.

- /BIOSALL      Flash all BIOS block
- /MEALL        Flash all ME region
- /ALL            Flash all (BIOS+ME)
- /CAPSULE      Override BIOS Guard Flash policy to Capsule.
- /RECOVERY    Override BIOS Guard Flash policy to Recovery. (\*1)

### Options

The optional field used to supply more information for flashing BIOS ROM. Following lists the supported optional parameters and format (\*2):

- /DESC          Flash descriptor region
- /EC            Flash EC region
- /GBE          Flash GBE region
- /ME            Flash ME region (Need to disable ME)
- /PAD          Flash Padding region (Gap between ME region and Bios region)
- /N             Flash NVRAM region
- /NB            Flash NVRAM backup region
- /OA            Flash OA3 region
- /P             Flash FV\_MAIN region

|                     |  |
|---------------------|--|
| -/DATA              | Flash FV_DATA region   |
| -/AB                | Flash FV_BB_AFTER_MEMORY region  |
| -/FSPS              | Flash FV_FSP_S region (If support FSP)   |
| -/FSPTM             | Flash FV_FSP_T_M region (If support FSP)   |
| -/B                 | Flash FV_BB region   |
| -/OEM               | Flash OEM region (Only support in CPASULE mode. /CAPSULE /OEM)                                       |
| -/P /B /N /CAPSULE  | Do capsule update and update FV_MAIN, all boot blocks and NVRAM (/p /b /n usage is same as AFU tool) |
| -/P /B /N /RECOVERY | Do recovery and update FV_MAIN, all boot blocks and NVRAM (/p /b /n usage is same as AFU tool)       |

\* 1: BGT only sends the recovery file name to BIOS. The action of flashing is handled by BIOS recovery module. The input file must be in root path and only supports 8+3 format.

\* 2: This option list demonstrates the default setting. The list is determined by the design of the BIOS ROM in use. The option items, the item order and the item description can be customized during the BIOS implementation.

## Rules:

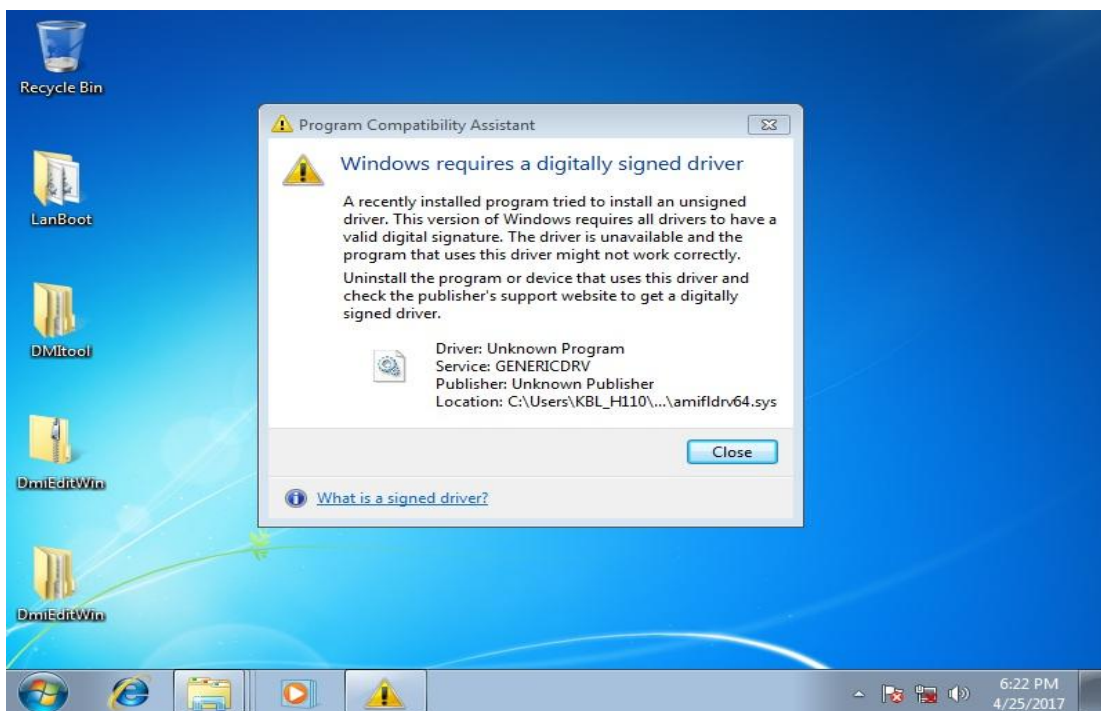
- Any parameter enclosed by < > is a mandatory field.
- Any parameter enclosed by [ ] is an optional field.
- <Commands> cannot co-exist with any [Options].

## Error Code Definition

| CODE   | Definition   |
|--------|--|
| 0x0001 | BIOS Guard module detected an incompatibility with the installed CPU   |
| 0x0002 | BIOS Guard Directory check failed  |
| 0x0003 | A pre-execution check of the PPDT failed   |
| 0x0004 | An inconsistency was found in the update package   |
| 0x0005 | Unknown operator or name, or invalid syntax found in script  |
| 0x0006 | An unimplemented flash object was referenced   |
| 0x0007 | A JMP, JE, JNE, JG, JGE, JL, or JLE operator has a target that is not within the script buffer (between BEGIN and END inclusive) |
| 0x0008 | BGUPC inconsistency found  |
| 0x0009 | SVN is lower than required by the BGPDT  |
| 0x000A | An EC related opcode found in a script when the PPDT indicates there is no EC in the system                                      |
| 0x000B | An implementation specific memory or IO configuration check failed   |
| 0x000C | An implementation specific general configuration check failed  |
| 0x000D | An EC related opcode was found in the script, but the EC hardware was not ready or is behaving in an unexpected way              |
| 0x000E | An attempt to modify B0 contents occurred in an unsigned script  |
| 0x8001 | Buffer or flash operation exceeded object bounds   |
| 0x8002 | An unsigned script attempted to write or erase a block of flash that overlaps with the SFAM                                      |
| 0x8003 | An integer overflow occurred   |
| 0x8004 | Total number of script opcodes retired exceeds either platform limit, or global limit  |
| 0x8005 | An internal consistency check failed within the BIOS Guard module  |
| 0xFFFF | CPU detected an error and did not execute the BIOS Guard module  |

## FAQ

### Windows requires a digitally signed driver



*This issue is resolved by a security fix provided by [MS. KB3033929](#) resolves this issue. The certificate used to sign the driver is higher security and older versions of Win7 don't support it.*