American Megatrends

AMI Software Utility User Guide

AptioV AMIBGT User Guide

Document Revision 1.00

January 21, 2014

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, Inc. 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 © 2014 American Megatrends, Inc. All Rights Reserved.

American Megatrends, Inc.
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

Document Information

Purpose

This document provides information to use the AptioV AFU 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

Introduction

Overview

AMIBGT (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 (32 bit)
- Microsoft® Windows® 7 (64 bit)
- Microsoft® Windows® 8 (32 bit)
- Microsoft® Windows® 8 (64 bit)
- EFI Shell
- DOS
- 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)

Getting Started

Installation

To run, extract all of the files from the folder with the name corresponding to the desired operating
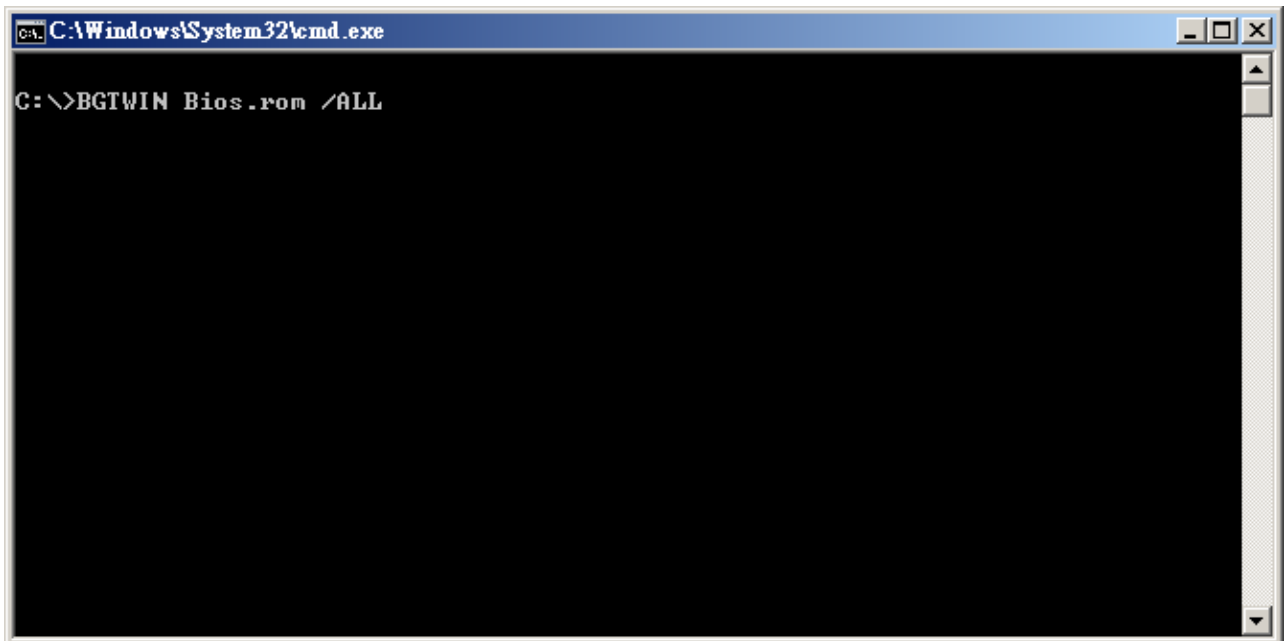
system.

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 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:

BGTDOS <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:

BGTDOS <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

BGTDOS <BIOS ROM File Name> [Option 1] [Option 2]

Or

BGTDOS <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   Program all BIOS block

- /MEALL   Program all ME region

- /ALL   Program all (BIOS+ME)

Options

The optional field used to supply more information for flashing BIOS ROM. Following lists the

supported optional parameters and format (*1):

- /DESC   Program Descriptor region

- /GBE   Program GBE region

- /ME   Program ME region

- /N   Program NVRAM

- /OA   Program OA region

- /DATA Program DATA region

- /P   Program Main BIOS

- /B   Program Boot Block

* 1: 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 bock 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