American Megatrends

AMI Software Utility User Guide

Aptio 5.x AFU for Aarch64 User Guide

Document Revision 1.0

June 16, 2017

NDA Required
(NDA)

American Megatrends, Inc.
5555 Oakbrook Parkway
Suite 200
Norcross, GA 30093 (USA)

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

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 for updating system BIOS.

Audience

Generic BIOS Engineers, OEM Engineers, and Aptio Customers.

Change History

Date	Revision	Description
2017-06-16	1.00	Initial document created and update content to the latest released of Afu.

Introduction

Overview

AFU (AMI Firmware Update) is a package of utilities used to update the system BIOS under various operating systems. AFU for Aarch64 needs RuntimeFlash module to serve in system BIOS.

AFU Features

This list of features is supported by command line under EFI Shell and Linux shell.

- Read system ROM image
- Flash ROM image
- Command line operating

Requirements

Supported Operating System

AFU is supported by the following operating systems:

- EFI Shell Environment
- Linux(*1)(*2)
  - ✓ *Ubuntu*
  - ✓ *Red Hat*
  - ✓ *Fedora*
  - ✓ *openSUSE*

Note:

1. On Linux Xen environment, AFULNX must be executed in host desktop (Domain 0) of the virtual machine.

2. Enable UEFI Runtime Services support in the kernel configuration.

Firmware Requirements

- Compatible with AptioV.
- Requires that the currently installed firmware has RuntimeFlash support enabled.

- - ***RuntimeFlash(RuntimeFlash_0.8 or above)***
- For supporting UEFI Capsule, the following eModule is required:
  - ***AfriCapsule (AfriCapsule_0.1 or above)***
- For supporting Custom Firmware (EC, MAC… etc), the following eModule are required:
  - ***On Flash Block Description (APTIO) (OFBD_11 or above)***
  - ***Embedded Controller Flash (OFBD_11 or above)***
- For supporting Supervisor password check (the password to enter BIOS setup screen, customized password check mechanism… etc), the following eModule are required:
  - ***On Flash Block Description (APTIO) (OFBD_11 or above)***
  - ***Oem Password Checking (OFBD_11 or above)***
- For supporting preservation of specific data (NVRAM variables, customized preservation… etc), the following eModule are required:
  - ***On Flash Block Description (APTIO) (OFBD_11 or above)***
  - ***Oem NvRam/Setup Variable Preserve (OFBD_11 or above)***

Getting Started

Installation

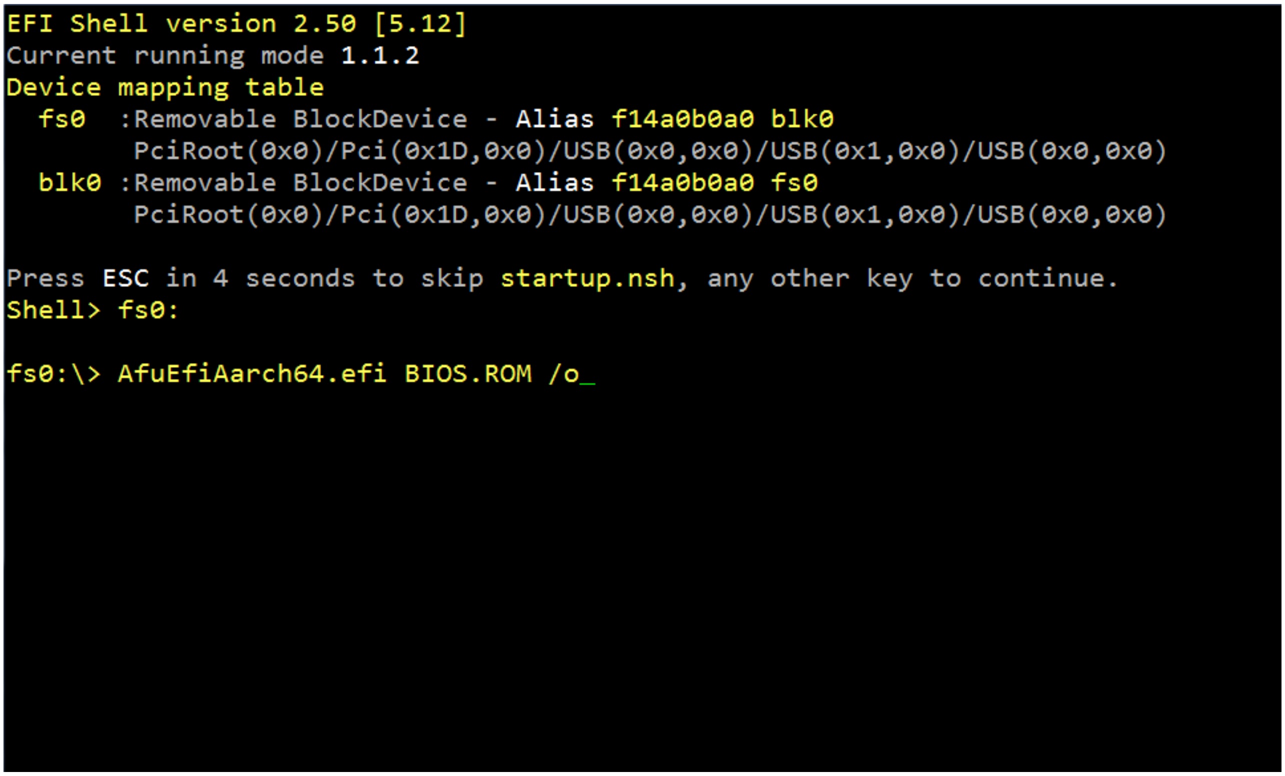
To run, extract all of the files from the folder with the name corresponding to the desired operating system.

AFU Operation

Overview

This chapter explains the operation of AFU.

An example of AfuEfiAarch64 that backup current system BIOS to a specific file “BIOS.ROM”, the command looks like this



```
EFI Shell version 2.50 [5.12]
Current running mode 1.1.2
Device mapping table
  fs0  :Removable BlockDevice - Alias f14a0b0a0 blk0
        PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x1,0x0)/USB(0x0,0x0)
  blk0 :Removable BlockDevice - Alias f14a0b0a0 fs0
        PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x1,0x0)/USB(0x0,0x0)

Press ESC in 4 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> AfuEfiAarch64.efi BIOS.ROM /o_
```

Commands and Options

The following list is to offer you an overview of the commands and options provided by AFUAPTIO. The content can also be found in AFUAPTIO's help information.

Usage

AfuEfiAarch64 <BIOS ROM File Name> [Option 1] [Option 2] …

Or

AfuEfiAarch64 < Input or Output File Name > <Command>

Or

AfuEfiAarch64 <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.

- /O	Save current ROM image to file
- /ROMINFO	Dump system BIOS information
- /ECINFO	Display OEM firmware information
- /CAPSULE	Update firmware via Runtime Capsule service

Options

The optional field is used to supply more information for flashing BIOS ROM. Following lists the supported optional parameters and format:

- /P	Program DXE region of given ROM file
- /K[N]	Program n-th NCB region of given ROM file
- /N	Program NVRAM region of given ROM file
- /B	Program PEI region of given ROM file
- /EC	Update EC Firmware by specified file

- /Q	Suppress progress output
- /SP	Force BIOS to preserve specific data

Rules

- Any parameter enclosed by < > is a mandatory field.

- Any parameter enclosed by [ ] is an optional field.

- <Commands> should not use with [Options].

- If [/B] present alone, there is only the Boot Block area to be updated.

- If [/N] present alone, there is only the NVRAM area to be updated.

Usage

Overview

The AFUAPTIO offers the following basic command and option usages:

- AfuEfiAarch64 <Input or Output File Name> [Option 1] [Option 2] …
- AfuEfiAarch64 <Input or Output File Name> <Command>
- AfuEfiAarch64 <Command>

AfuEfiAarch64 <Input/Output File Name> [Option 1] [Option 2] …

Users could put no option or combine multiple options in one command line. Commands cannot be combined in command line like options unless the command is categorized as both a command and an option, such as /ROMINFO.

For option combination case, AFUAPTIO will check its option priority list and execute the options according to the priority order. An example of this usage is provided below.

AfuEfiAarch64 <Input BIOS ROM File Name> /P /B /N /K

Where the BIOS ROM File Name, the mandatory field is used to specify path/filename of the BIOS ROM file with extension. In this case, AFUAPTIO will update the regions of PEI, DXE, NVRAM and all NCBs in the system BIOS with the specified input ROM file.

AfuEfiAarch64 <Input/Output File Name> <Command>

AFUAPTIO can only execute one command at a time and it does not accept combinations of command and option in one command line except those can be both command and option. An example of this usage is provided below.

AfuEfiAarch64 <Output BIOS ROM File Name> /O

Where the BIOS ROM File Name, the mandatory field is used to specify path/filename of the BIOS ROM file with extension. This command line saves the current system BIOS to the specified file.

AfuEfiAarch64 <Command>

This command usage is for some commands which do not require inputting any file to complete the execution. Usually, this type of commands accesses the current BIOS only. An example of this usage is provided:

AfuEfiAarch64 /ROMINFO

This command line gets and displays the information of the current BIOS in the system.

AfuEfiAarch64 <BIOS ROM File Name> <Option><Number>

This command usage is for /K[N] command where N is indicating the numeric order of a certain non-critical block. For example, to program the 4th NCB, the command line could be:

AfuEfiAarch64 <BIOS ROM File Name> /K4

Where BIOS ROM File Name is used to specify path/filename of the BIOS ROM file with extension, and 4 is to specify that the 4th NCB is the one to perform /K operation.

However, if the number is not specified, AFUAPTIO will update all NCBs of the system BIOS.

Use case

Overview

This chapter is to describe commands/options which require extra attention and to explain cases which may occur in certain unique scenarios.

Preserving Setup Setting – /SP

/SP command is designed specifically for "OEM NVRAM/Setup Variable Preserve" module part of OFBD. If /SP is called, AFUAPTIO will inform BIOS before and after update operation. BIOS project owners can customize their OFBD module to preserve certain valuable data when AFUAPTIO tries to update specific areas. For example, to preserve Setup Password:

BIOS project owner can make use of the hook "PreserveSetupPassword" in OFBDSETUPStoreHandle and "RestoreSetupPassword" in OFBDSETUPRestoreHandle, and use /SP command to keep or not to keep the Setup Password while updating the NVRAM:

```
AfuEfiAarch64  xxx.ROM /N /SP       - keep Setup password
AfuEfiAarch64  xxx.ROM /N           - don't keep Setup password.
```

This feature needs BIOS' cooperation. To learn more about preserving function, please refer to OFBD Porting Guide.

Programming NVRAM Region – /N

Erasing NVRAM may cause important variables lose.

Programming Specific NCB Block – /Kn

/Kn command is designed to program a specific non-critical block, or NCB block. AFUAPTIO would search ROM and identify the first NCB Block found as K0, and the second one as K1, etc. Therefore, command /K2 would program the third NCB Block found by AFU.

Runtime Capsule Update – /CAPSULE

The system BIOS must have AfriCapsule eModule to update BIOS via Runtime Capsule service. If user select this method to update system BIOS, the update process will be rely on BIOS itself. What AFUAPTIO can do is transferring the payload to BIOS.

The command looks like this:

AfuEfiAarch64 <BIOS ROM File Name> /CAPSULE

Error Codes

Error Code Definition

CODE	Definition
0x01	Error: Unknown command.
0x02	Error: BIOS has no flash information available.
0x03	Error: ROM file size does not match existing BIOS size.
0x04	Error: ROM file ROMID is not compatible with existing BIOS ROMID.
0x05	Error: Bootblock error.
0x06	Error: This BIOS version has more Non-Critical blocks than supported.
0x07	Error: BIOS checksum error.
0x08	Error: Invalid option
0x09	Error: Size of ROM file does not match the size of system ROM
0x0A	Error: Unable to update ROM hole
0x0B	Error: ROMHOLE not exist
0x0C	Error: BIOS update cancelled by user.
0x0D	Error: BIOS Report Error.
0x0E	Error: Kernel source files cannot be found.
0X0F	Error: Size of PLDM file is more than the FV size.
0x10	Error: Unable to load driver.
0x11	Error: Unable to unload driver.
0x12	Error: No non-critical blocks found in ROM file.
0x13	Error: Requested non-critical block not available in ROM file.
0x14	Error: Non-critical blocks in ROM image file do not match those in the system.
0x15	Error: Secure Flash function is not supported on this platform.
0x16	Error: Unable to get Secure Flash policy from BIOS.
0x17	Error: Unsupported Secure Flash policy.
0x18	Error: Secure Flash Rom Verify fail.
0x19	Error: Failed to erase flash chip (at Runtime Secure Flash).
0x1A	Error: Failed to update flash chip (at Runtime Secure Flash).
0x1B	Error: Failed to read flash chip (at Runtime Secure Flash).
0x1C	Error: Failed to verify flash chip (at Runtime Secure Flash).
0x1D	Error: Failed to load image into memory.
0x1E	Error: Secure Flash function is not supported on this file.
0x1F	Error: Reserved for Secure Flash.
0x20	Error: Unable to initialize memory manager.
0x21	Error: Unable to close memory manager.

0x22	Error: Problem allocating memory.
0x23	Error: Problem freeing memory.
0x24	Error: Problem allocating BIOS buffer.
0x25	Error: Problem freeing BIOS buffer.
0x26	Error: Problem freeing mapping BIOS.
0x27	Error: Problem freeing unmapping BIOS.
0x28	Error: Problem mapping BIOS data.
0x29	Error: Problem unmapping BIOS data.
0x30	Error: Problem opening file for reading.
0x31	Error: Problem reading file.
0x32	Error: Problem opening file to write.
0x33	Error: Problem writing file.
0x34	Error: Using the wrong AFU version, Please use Aptio 4 AFU.
0x35	Error: Using the wrong AFU version, Please use Aptio 5 AFU.
0x36	Error: Fail with problem of ESP Driver init.
0x37	Error: Fail with problem of copy ROM file to ESP driver.
0x40	Error: BIOS is write-protected.
0x41	Error: Can not close flash interface.
0x42	Error: Problem reading flash.
0x43	Error: Problem erasing flash.
0x44	Error: Problem writing flash.
0x45	Error: Problem verifying flash.
0x46	Error: Problem getting flash information.
0x47	Error: No firmware id.
0x48	Error: Power cord not connected. Plug in power cord to flash.
0x49	Error: A platform condition has prevented flashing.
0x4A	Error: Platform data is not empty, And data address is not Alignment Block Address.
0x4B	Error: SLP key is not empty at all.
0x4C	Error: Rom file ROM layout is changed.
0x50	Error: This program must be run in MS-DOS mode.
0x60	Error: Accessing registry.
0x61	Error: Program already running.
0x70	Error: BSD access IO.
0x71	Error: Linux does not support Auto Build Driver when Secure Boot Enable.
0x80	Error: Size of system ROM mismatches size of ROM file
0x81	Error: ROM ID mismatch
0x82	Error: Bootblock checksum error
0x90	Error: Error to shutdown
0x91	Error: Error to restart...
0x92	Error: Can't open ROM ID file
0x93	Error: ROM ID file is not a ROM file.
0x94	Error: Invalid MAC address
0x95	Error: Invalid load current CMOS option
0x96	Error: Invalid retry count
0x97	Error: Invalid defined ROM ID length
0x98	Error: Invalid SMI

0x99	Error: ROM File ID don't exist
0x9A	Error: System ROM ID don't exist
0x9B	Error: Password Retry count exceeded.
0x9C	Error: BIOS don't support NVRAM/SETUP preserve function
0x9D	Error: Store SETUP setting error
0x9E	Error: Restore SETUP setting error
0x9F	Error: Cannot analyze ROM file. ROM file may be corrupted
0xA0	Error: Cannot analyze the ME Data. ROM file may be corrupted
0xA1	Error: BIOS does not support ME Entire Firmware update
0xA2	Error: BIOS does not support ME Ignition Firmware update
0xA3	Error: Invalid EC ROM file
0xA4	Error: EC ROM file checksum error
0xA5	Error: Can't enter EC flash mode
0xA6	Error: Erasing EC flash memory fail
0xA7	Error: Initial EC programming fail
0xA8	Error: EC flash data transmit error
0xA9	Error: Writing EC flash memory fail
0xAA	Error: Exit EC programming mode fail
0xAB	Error: ROM Chip ID mismatch
0xAC	Error: Invalid EC Header Table
0xAD	Error: EC does not permit BIOS update
0xAE	Error: BIOS doesn’t support OEMCMD function
0xAF	Error: Store DMI Data error
0xB0	Error: Restore DMI Data error
0xB1	Error: Invalid Activation Key file.
0xB2	Error: File Size is greater than image activation key length.
0xB3	Error: Image activation key larger than BIOS activation key.
0xB4	Error: Activation Key checksum error.
0xB5	Error: No Support Activation Key error.
0xB6	Error: OA key is available, and OA Key is not the same as BIN file in the system.
0xB7	Error: OA key is empty.
0xB8	Error: OA key region incorrect.
0xB9	Error: BIOS doesn’t support Clear event log function.
0xBA	Error: Clear event log error.
0xBB	Error: Rom image layout detected RomHole is redesigned.
0xBC	Error: BIOS have more than one RomHole’s GUID is the same.
0xBD	Error: Requested Rom Hole not available in ROM file.
0xBE	Error: RomHoles in ROM image file do not match those in the system.
0xBF	Error: OA key is available, and OA Key is the same as BIN file in the system.
0xC0	Error: BIOS doesn’t support process ME information
0xC1	Error: BIOS return error, when trying to re-flash ME Firmware data.
0xC2	Error: Region is write-protected
0xC6	Error: No EC blocks found in system ROM.
0xC7	Error: BIOS doesn’t support all ROM flashing function.
0xD0	Error: OA key data is invalid.
0xD1	Error: BIOS has already updated OA.

0xD2	Error: BIOS does not allow updating OA.
0xD3	Error: BIOS doesn’t support updating OA.
0xD4	Error: The DMI data size of system is greater than File's DMI data length.
0xD5	Error: BIOS doesn't support EC Battery Check function.