ShellFlash for SecureCore Tiano™

User Guide

For Phoenix SecureCore Tiano™

phoenix technologies

Innovation at the CORE ™

Notices

Confidential and Proprietary Information

The contents of this document are confidential and proprietary to Phoenix Technologies Ltd. Access to this information is restricted. This document is provided for Distributor's internal use only. This document should not be disclosed to any third party, including customers.

Copyright

Disclaimers

PHOENIX TECHNOLOGIES LTD. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION HEREIN DESCRIBED AND SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. FURTHER, PHOENIX TECHNOLOGIES LTD. RESERVES THE RIGHT TO REVISE THIS DOCUMENTATION AND TO MAKE CHANGES FROM TIME TO TIME IN THE CONTENT WITHOUT OBLIGATION OF PHOENIX TECHNOLOGIES LTD. TO NOTIFY ANY PERSON OF SUCH REVISIONS OR CHANGES.

Trademarks

The following list contains the trademarks and/or registered trademarks of Phoenix Technologies Ltd. Exclusion from this list does not imply loss of trademark or registered trademark rights by Phoenix Technologies Ltd: Phoenix; TrustedCore; FirstBIOS; PhoenixBIOS; StrongROM; CoreArchitect; Phoenix Technologies; WinPhlash; WinFlash; Phoenix Technologies Logo; AwardBIOS; Embedded Simplicity; Embedded BIOS; StrongFrame; Firmbase; Purpose-Driven Firmware; and SecureCore Tiano.

Any use of other companies or legal entities' copyrights, trademarks, or registered trademarks is unintentional and in no way implies any legal claim to those copyrights, trademarks, or registered trademarks.

Document

The contents of this document are subject to change at the discretion of Phoenix Technologies.

P/N: SCT-TOOLS-SHELLFLASH-1.5.29.0

Revision Date: June 2, 2011

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1. About ShellFlash

The Phoenix SecureCore Tiano™ ShellFlash utility is an EFI shell application that allows you to update, backup, and restore the BIOS on a flash device.

The following table describes the basic features of the ShellFlash program.

File Name	Operating System	User Interface	Default Settings*
PFlash.efi	UEFI Shell	Command Line	`PFLASH.INI`

* Command options can be added to `PFLASH.INI`. (For more information about command options, see Chapter 3 SHELLFLASH COMMANDS)

1.2. Features

The following lists each feature and its available options:

- Phoenix SecureCore Tiano™ support
- Use SMI handler to update BIOS (Erase/Write/Verify)
- Based on FD specification (version 0.96 or above)
- Default to preserve ROM variables
- Default to skip Recovery volume (like Boot block)
- Support flash command line extension (pflash.ini)

1.3. Requirements

The following is required in order to use the ShellFlash utility.

- UEFI compatible hardware
- EFI Shell

1.4. Conventions Used in this Manual

This table below shows typographic conventions used in this manual.

Bold	Indicates text the user must enter or select, such as menu items, buttons, and commands. Also indicates computer paths, such as **File** > **Save**.
Italics	Represents optional variables that a user can specify.
`Courier New`	Represents filename or code.

CHAPTER 2

USING SHELLFLASH

2.1. Before Using ShellFlash

Perform the following steps to flash a new BIOS.

1. Prepare the BIOS image (e.g. BIOS.FD) and copy it to the boot drive.
2. Set the boot drive (e.g. USB key) within system BIOS.
3. Do either step **A** or **B.**

   A : Copy EFI Shell boot loader (e.g. boot.efi) to //EFI/BOOT/ folder on boot drive.

   B : Activate the EFI Shell within the system BIOS then copy PFlash.efi, BIOS image, and pflash.ini(if required) to boot drive.

4. Power ON to launch EFI Shell at boot.
5. Run ShellFlash from the boot drive (see section 3.1.1 Command Option Syntax for details)

2.2. Running ShellFlash

When ShellFlash is running, the screen will display the flash checklist, as shown in Figure 2.1. The progress bar at the bottom of the checklist shows the current function and the percent completion. The status bar at the bottom of the screen provides supporting information.

Warning! Do not interrupt the program before it completes.

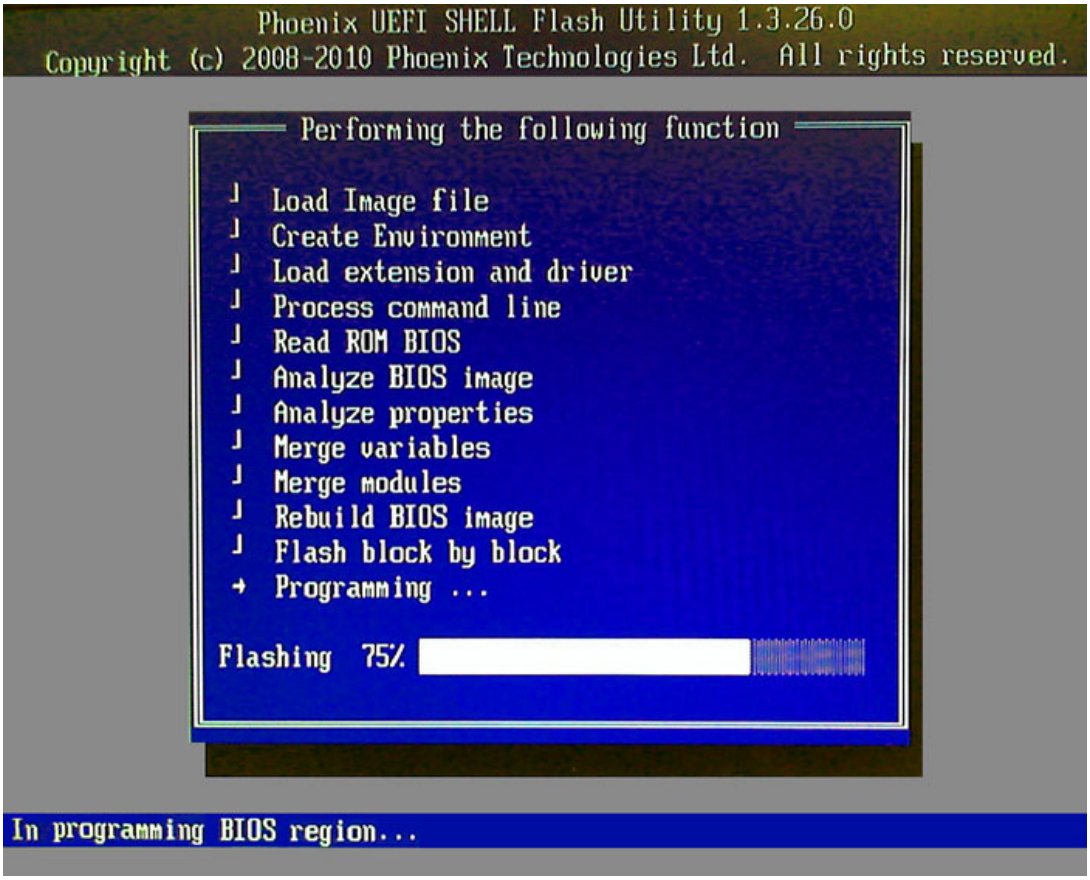

Figure 2.1: Flash Checklist

When flashing to BIOS, you may see warning messages if the flash tool detects an issue. For example, you will see a warning message if the flash BIOS has a different product ID or part number than the system BIOS. Warnings will also display if the flash BIOS is not new (i.e. same or older) when compared with the date or version number of the system BIOS. Other warnings may appear if the flash BIOS version string or FlashMap is not found or invalid. In all cases you must cancel the flash operation.

Note: If you wish to force flash a new BIOS under any of the conditions described above, use the /force command option or the matching skip BIOS check command options: /sa, /sd, /sn, /sp, or /sv (as described in Section 3.1.2 Command Options List)

.

CHAPTER 3

SHELLFLASH COMMANDS

3.1. Command Options

Command options can be used in the following ways:

- On the command line
- Within PFLASH.INI

3.1.1. Command Option Syntax

```
PFLASH [options] romfile
```

`[options]`

Entered on the command line or read from PFLASH.INI.

`romfile`

The new BIOS image name, e.g. BIOS.FD.

3.1.2. Command Options List

The following table lists all available command line options.

Option:Parameter(s)	Function
/? /h /help	Displays help screen
/all	Flash the entire image including the descriptor region

Option:Parameter(s)	Function
/bak:`filename`	Backup ROM to a file.
/bbl	Update the boot block. By default, bootblock is not updated.
/bios	Flash the BIOS region
/cs	Verify the checksum of a .FFS file.
/cvar	Clear the variable storage in ROM
/desc	Flash the Descriptor region
/dmc:string	Specify chassis manufacturer DMI string
/dmm:string	Specify motherboard manufacturer DMI string
/dms:string	Specify system manufacturer DMI string
/dpc:string	Specify chassis asset tag number
/dpm:string	Specify motherboard product ID DMI string
/dps:string	Specify system product ID DMI string
/dsc:string	Specify chassis serial number DMI string
/dsm:string	Specify motherboard serial number DMI string
/dss:string	Specify system serial number DMI string
/dus:string	Specify UUID DMI string
/dvc:string	Specify chassis version DMI string
/dvm:string	Specify motherboard version DMI string
/dvs:string	Specify system version DMI string
/ec	Flash the EC region
/efivarmode=[0, 1, 3]	0: Preserve the variables of ROM 1: Replace variables of ROM with new BIOS image. 3: Merge variables from ROM and new BIOS image (default).
/exit	Exit without rebooting.
/force	Flash without any modification of the BIOS image. **Note:** Only the part numbers of the system and flash BIOS will be compared before flashing; all other BIOS metadata (e.g. product ID) will be ignored.
/gbe	Flash the GbE region
/ioset:`port,value`	Sets a specific IO port value. **Note**: Enter parameters in hexadecimal format.

Option:Parameter(s)	Function
/me	Flash the ME region
/mod:`filename`	Replace a FFS module. Updates the module in the BIOS with the module contained in the file. The rest of the BIOS image remains unchanged.
/mode=n	Specify DMI mode n = {0, 1, 2, 3} 0: Just update BIOS with new file, don't update DMI variables. 1: Just update DMI variables, keep ROM BIOS as before. 2: Update BIOS, merge ROM DMI variables with command line (default). 3: Update BIOS, merge image variables with command line.
/noflash	Perform all steps that do not update the flash part.
/prog: `Hex_physical_address:Hex_length`	Flash BIOS of `[Hex_length]` from `[Hex_physical_address]`. **Example:** To flash an EVSA subregion with a physical address of `0xfff73000` and a region size of `0xe000`: `PFlash /prog:fff73000:e000 BIOS.bin`
/raw:`GUID:filename`	Replace a RAW module. Updates the module in the BIOS with the module contained in the file. The rest of the BIOS image remains unchanged.
/rsbr:GUID,…	Preserve sub-regions with specified GUIDs (Global Unique Identifiers) during BIOS Update. Individual GUIDs are separated by commas and represented as 32-digit hexadecimal numbers without dashes (e.g. 8CB71915531F4AF582BFA09140AABBCC). Up to ten (10) GUIDs can be added using `PFLASH.INI`; while only three (3) can be added on the command line. The system and new BIOS images must share GUIDs and corresponding sub-regions must be the same size.
/sa	Skip all BIOS checks.
/sd	Skip BIOS date check.
/sn	Skip BIOS part number check
/sp	Skip BIOS product ID check
/ss	Keep current SLP keys. This option is useful when the SLP keys are not included with BIOS source files and you wish to flash without changing the SLP key areas.
/sv	Skip BIOS version check
/svs	Bypass the BIOS version check warning when flashing same version of BIOS. **Note:** Older BIOS versions will still display a warning message.
/silent	Silent operation (no beeps).
/v	Verify each block after updating it

Option:Parameter(s)	**Function**
/write:`file.bin: rom_address`	Flash an arbitrary binary (file.bin) to a specific ROM area (rom_address). **Example:** To flash `region15.bin` to physical address 0xFFF90000. `PFlash /write: region15.bin:FFF90000` **Note 1**: You can use the /exit option to avoid a system reboot after flashing. No other command options can be used with /write. **Note 2**: Users must know which physical address they want to flash. This is a very low level functionality so it should be used carefully.