PFlash 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-PFLASH-1.5.29.0

Revision Date: June 2, 2011

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1. About PFlash

The Phoenix SecureCore Tiano™ PFlash utility is a 16-bit MS-DOS application that allows you to update, backup, and restore the BIOS on a flash device.

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

File Name	Operating System	User Interface	Default Settings*
Pflash.exe	16-bit MS-DOS	Command Line	`PFLASH.INI`

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

1.2. Features

The following lists each feature and its available options:

- Phoenix SecureCore Tiano™ support
- 32 bit UEFI emulation (DUET)
- A user interface similar to Legacy Phlash16 tool
- Based on FD specification version 0.96 or above
- Use SMI handler to update BIOS (Erase/Write/Verify)
- Support flash command line extension (PFLASH.INI)
- Default to preserve ROM variables
- Default to skip Recovery volume (like Boot block)
- Support to return DOS (16-bit environment)
- DMI string update support
- Support SLP2.0 and SLP2.1 replacement

1.3. 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 PFLASH

2.1. Before Using PFlash

The following tasks must be completed before using PFlash:

- Prepare the soft SMI to call the FD protocol (erase/program/verify).
- Prepare Efildr16 and a new BIOS image.

2.2. Building PFlash

1. Open A20.
2. Enter big real mode.
3. Read Efildr16 to memory.
4. Switch to 32-bit protected mode.
5. Load Efildr16 and start each module to generate the basic UEFI boot/runtime service.
6. Search FADT and RSDT to get the SMI I/O port address, the flash soft SMI value (written to soft SMI port), and the Phoenix Flash Shared Memory address. The flash tool will return to the DOS command line if these are not found.
7. Execute the PFAE function.
8. Get Phoenix FD information using the SMI method. You will return to DOS prompt if this fails.
9. Enable flash ROM write.
10. Open the whole BIOS gated region.
11. Erase/write/verify each block of flash ROM.
12. Close the whole BIOS gated region.
13. Disable the flash ROM write.
14. Reboot or shutdown or return to DOS.

2.3. Running PFlash

Perform the following steps to flash a new BIOS.

1. Quit all programs.
2. Access the command prompt.
3. Enter `pflash [options]` to display

When PFlash 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.

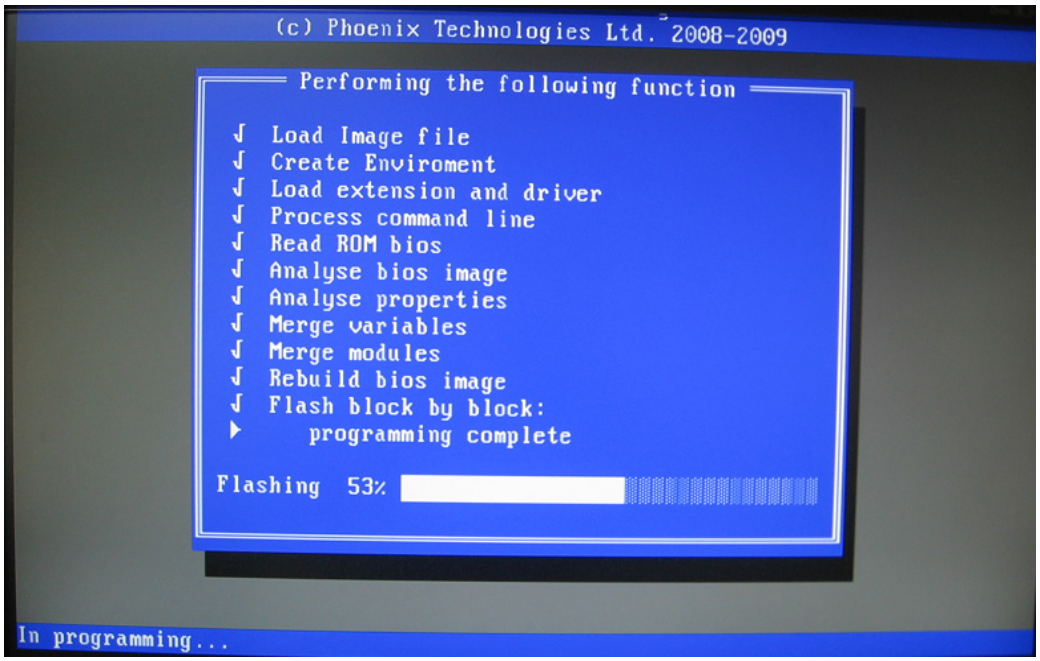

Figure 2.1: Flash Checklist

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)

2.4. Using the Command Prompt

When you run PFlash from the command prompt, you can perform any of the following options:

- Flashing a new BIOS to your system
- Backing up an existing BIOS before flashing

- Verifying the new BIOS checksum before flashing

You must run PFlash under MS-DOS, not from Windows.

In Windows 95/98, you can also run MS-DOS from the Windows Startup Menu by:

1. Click **Start**, and then click **Shut Down**.
2. Click **Restart**, and then click **OK**.
3. After the system starts rebooting, repeatedly press **F8** until the Windows Startup Menu displays.
4. Use the arrow keys to highlight **Safe Mode with the Command Prompt**, and then press **Enter**.

PFlash does not run in any environment with memory management such an MS-DOS Window or Window Console. Do not run MS-DOS with CONFIG.SYS or AUTOEXEC.BAT. Do not open any memory manager such as HIMEM.SYS or EMM.386.

2.5. Using PFlash with Memory Managers

PFlash can fail if your system uses memory managers because the flash utility must switch to 32-bit mode for main parts of the application.

2.6. Disabling PFlash with Memory Manager

To avoid failure when flashing, you must disable the memory managers that load from **CONFIG.SYS** and **AUTOEXEC.BAT**. There are two recommended procedures for disabling these memory managers, depending on the operating system you use. Each method is described below.

2.6.1. MS-DOS 5.0 (or Later)

For MS-DOS 5.0 or later, follow the steps below to disable any memory managers on your system. If you are not using at least MS-DOS 5.0, then you must create a boot disk to bypass any memory managers.

1. Reboot your system.
2. When the MS-DOS displays the “Starting MS DOS” message, press **F5**.

Pressing **F5** causes MS-DOS to bypass the CONFIG.SYS and AUTOEXEC.BAT files. As a result, no memory managers are loaded.

2.6.2. MS-DOS Prior to 5.0

If your operating system is a version prior to MS-DOS 5.0, you must create a boot disk in order to bypass memory managers. Follow the steps below to bypass memory managers in MS-DOS versions prior to 5.0.

1. Insert a disk into your **A:** drive.
2. Enter the following command from the command line:
   ```
   Format A: /S
   ```
3. Reboot your system from the **A:** drive.

Upon successful completion, your system will reboot without loading the memory managers.

CHAPTER 3

PFLASH 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).
/endkey	Press a key to continue after flashing
/exit	Exit without rebooting. **Note**: This option should not be used with the /p option.
/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.

Option:Parameter(s)	Function
/gbe	Flash the GbE region
/ioset:`port,value`	Sets a specific IO port value. **Note**: Enter parameters in hexadecimal format.
/logo:`imagefile [:index]`	Replace a BIOS logo with an `imagefile` in JPG, BMP or GIF formats. **Note:** The file size of the new logo cannot be larger than the current logo and bitmap images should be in 24bit color mode. This option can be used in two ways: 1. If the BIOS image is not defined in the command line, this option will replace the logo of the current BIOS (i.e. `PFLASH /logo:imagefile`). 2. If the BIOS image is defined in the command line, this option will replace the logo of the new BIOS image (i.e. `PFLASH /logo:imagefile romfile`). Use the `index` parameter when you wish to replace one of multiple BIOS logos within an image. The "*Logo index must be 1 to %d (INVALID PARAMETER)*" error message (EFI error #152) will display if the value of `index` is out of range (i.e. greater than the number of logo images in the BIOS = %d).
/ls	Preserves logo images in the system BIOS when flashing. **Note**: Logo images must be stored in SystemSplashDxe.efi and the total size of images in this file cannot be larger than that in the new BIOS; if so, the flash process will abort.
/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.
/p	Production mode (minimize messages and delays). **Note**: This option will reboot the system after flashing. It should not be used with the /exit option.
/**pfaefv**:`PFAEIA32.fv`	In addition to handling PFAE modules packed into the flash BIOS image, now this flash tool can load and run PFAE modules in a separate volume file (e.g. PFAEIA32.fv). Only 32-bit mode PFAE modules are supported within a volume file. If both the volume file and the flash BIOS image contain PFAE modules, the modules in the flash BIOS image are loaded first. **Note**: The flash tool will abort if it cannot successfully load and run all the PFAE modules within a volume file.

Option:Parameter(s)	Function
/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.

/slp	Replace the SLP marker key in current or new BIOS image.
	1) To replace the SLP marker key within the current BIOS:
	`pflash /slp:filename`
	2) To replace the SLP marker key and flash a new BIOS image
	`pflash /slp:filename newbios.bin`
	Note: /slp and /spu can be used in combination.

/sn	Skip BIOS part number check
/sp	Skip BIOS product ID check

/spu:`filename:index`	Replace the SLP public key in current or new BIOS image. The SLP public key version is set using the `index` parameter.
	1) To replace a SLP2.0 public key within the current BIOS:
	`pflash /spu:filename:20`
	2) To replace a SLP2.1 public key and flash a new BIOS image:
	`pflash /spu:filename:21 newbios.bin`
	Note: /slp and /spu can be used in combination.

/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

Option:Parameter(s)	Function
/svs	Bypass the BIOS version check warning when flashing same version of BIOS. **Note:** Older BIOS versions will still display a warning message.
/shutdown	Shutdown without rebooting.
/silent	Silent operation (no beeps).
/v	Verify each block after updating it
/vbl	Show warning for Microsoft Bitlocker
/vcpu:`MCUfile`	Update variable size CPU microcode. The ROM, BIOS image, and `MCUfile` (if defined) will be compared. The most recent MCU will be flashed to ROM.
/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**:Binary files cannot exceed 400 kB. **Note 2**: You can use the /exit option to avoid a system reboot after flashing. No other command options can be used with /write. **Note 3**: Users must know which physical address they want to flash. This is a very low level functionality so it should be used carefully.

CHAPTER 4

PFLASH ERROR MESSAGES

4.1. Error Messages

The following table lists PFlash error messages in numerical order.

Error Code	Error Name
151	EFI_ERROR_LOAD_ERROR
152	EFI_ERROR_INVALID_PARAMETER
153	EFI_ERROR_UNSUPPORTED
154	EFI_ERROR_BAD_BUFFER_SIZE
155	EFI_ERROR_BUFFER_TOO_SMALL
156	EFI_ERROR_NOT_READY
157	EFI_ERROR_DEVICE_ERROR
158	EFI_ERROR_WRITE_PROTECTED
159	EFI_ERROR_OUT_OF_RESOURCES
160	EFI_ERROR_VOLUME_CORRUPTED
161	EFI_ERROR_VOLUME_FULL
162	EFI_ERROR_NO_MEDIA
163	EFI_ERROR_MEDIA_CHANGED

Error Code	Error Name
164	EFI_ERROR_NOT_FOUND
165	EFI_ERROR_ACCESS_DENIED
166	EFI_ERROR_NO_RESPONSE
167	EFI_ERROR_NO_MAPPING
168	EFI_ERROR_TIMEOUT
169	EFI_ERROR_NOT_STARTED
170	EFI_ERROR_ALREADY_STARTED
171	EFI_ERROR_ABORTED
172	EFI_ERROR_ICMP_ERROR
173	EFI_ERROR_TFTP_ERROR
174	EFI_ERROR_PROTOCOL_ERROR
175	EFI_ERROR_INCOMPATIBLE_VERSION
176	EFI_ERROR_SECURITY_VIOLATION
177	EFI_ERROR_CRC_ERROR
178	PFLASH_ID_CHK_FAIL
179	EFI_ERROR_BITLOCKER
180	PFLASH_PART_NUM_CHK_FAIL
181	PFLASH_VER_CHK_FAIL
182	PFLASH_DATE_CHK_FAIL
194	FLASH_ERROR_BIOS_PASSWORD_FAIL
195	FLASH_ERROR_EXCEED_PASSWORD_RETRY
241	DOS_ERROR_PARAMETERS_INPUT_ERROR
242	DOS_ERROR_FILE_NOT_FOUND
243	DOS_ERROR_PATH_NOT_EXIST
244	DOS_ERROR_NO_HANDLE_AVAILABLE
245	DOS_ERROR_EFILDR16_FILE_NOT_FOUND
246	DOS_ERROR_FLASHSUP_FILE_NOT_FOUND