# WinFlash 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; Phoenix Technologies; the Phoenix Technologies Logo; AwardCore; Embedded BIOS; Embedded Simplicity; Firmbase; Microcore; Phoenix SecureGuard; Phoenix ServiceMeter; Phoenix WorkBench; SecureCore Tiano; StrongFrame; StrongRom; Tool Development Kit; Trusted Core; WinFlash; and WinPhlash.

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-WINFLASH-1.5.59.0

**Revision Date:** August 30, 2011

# TABLE OF CONTENTS

# CHAPTER 1

## *INTRODUCTION*

## 1.1. About WinFlash

The Phoenix SecureCore Tiano™ WinFlash utility is a 32-bit Windows application that allows you to update, backup, and restore the BIOS on a flash device.

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

| File Name | Operating System | User Interface | Default Settings* |
|---|---|---|---|
| Winflash.exe | WinXP x86, Win7 x86/x64, and WinPE 2.0/2.1/3.0 on Win7 & Vista (SP1) x86 | Both Graphical & Command Line | `WINFLASH.INI` `PFLASH.RSP` |

* WinFlash initializes based on the settings within the `WINFLASH.INI` file. Command options can be added to a response file; `PFLASH.RSP` is the default filename. (For more information about command options, see Chapter 3 WinFlash Commands.)

## 1.2. Features

The following lists each feature and its available options:

- Phoenix SecureCore Tiano™ BIOS support
- 32-bit UEFI emulation and Windows Flash Application
- Supports Windows XP (x86) and Windows 7 (x86/x64 legacy/UEFI)
- Use SMI handler to update BIOS (Erase/Write/Verify)
- Based on FD spec. version 0.96 or above
- Default to preserve the variables of ROM
- Default to skip Recovery volume (like Boot block)
- Support flash command line extension (PFLASH.RSP)

- DMI string update support
- Supports SLP2.0/2.1
- BIOS capsule support

## 1.3. Required Software

The following software is required in order to use the WinFlash utility.

Microsoft Visual Studio® 2005 or later

## 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 WINFLASH*

## 2.1. Before Using WinFlash

### 2.1.1. Installing WinFlash

Perform the following steps to install WinFlash.

1. Within the Tools Subscription Program (TSP) release package, locate the correct archive, and extract the setup package (e.g. **UEFIWinFlash.msi**) to your computer.

   **Note**: You can choose to install the English, Japanese or Korean versions of this tool.

2. Open the setup package to launch the Phoenix UEFI Winflash Setup Wizard.

3. Select the radio button to accept the License Agreement.

4. Click **Install** to install the tool to the default folder (e.g. %ProgramFiles%\UEFI Winflash). To select a different destination folder click the **Advanced** button and select another file path.

5. Wait until the installation is complete and then click **Finish** to exit the Setup Wizard. Upon successful installation, the WinFlash tool will be available in the Start menu.

### 2.1.2. Removing WinFlash

Perform one of the following steps to uninstall WinFlash.

- Go to Start > Control Panel > Add or Remove Programs > Phoenix UEFI Winflash and then click Remove.
- Run the original setup package (e.g. **UEFIWinFlash.msi**). If the tool is present on your computer, you will be prompted to either repair or remove it. Click **Remove** to remove the tool.

### 2.1.3. Prerequisites

Prepare the following to flash a new BIOS.

- A new BIOS image or capsule file
- SMI interface with FD support

**Note**: You can inherit the SETUP variable from the system ROM and add a new variable image file.

## 2.2. Running WinFlash

You can choose to run WinFlash in either command-line or GUI mode. The procedure for capsule files is slightly different so they have separate instructions. For more information about flashing capsule files see Section 2.2.3 BIOS Capsule Flashing.

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 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 are displayed 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).

### 2.2.1. Command Line Mode

Perform the following steps to run WinFlash in command line mode.

1. Close all other programs.
2. From the *Start* menu, select **Run**.
3. Enter the path for the WinFlash program when the Run message box displays, for example, …`\WinFlash [options]`
4. Press **OK**.

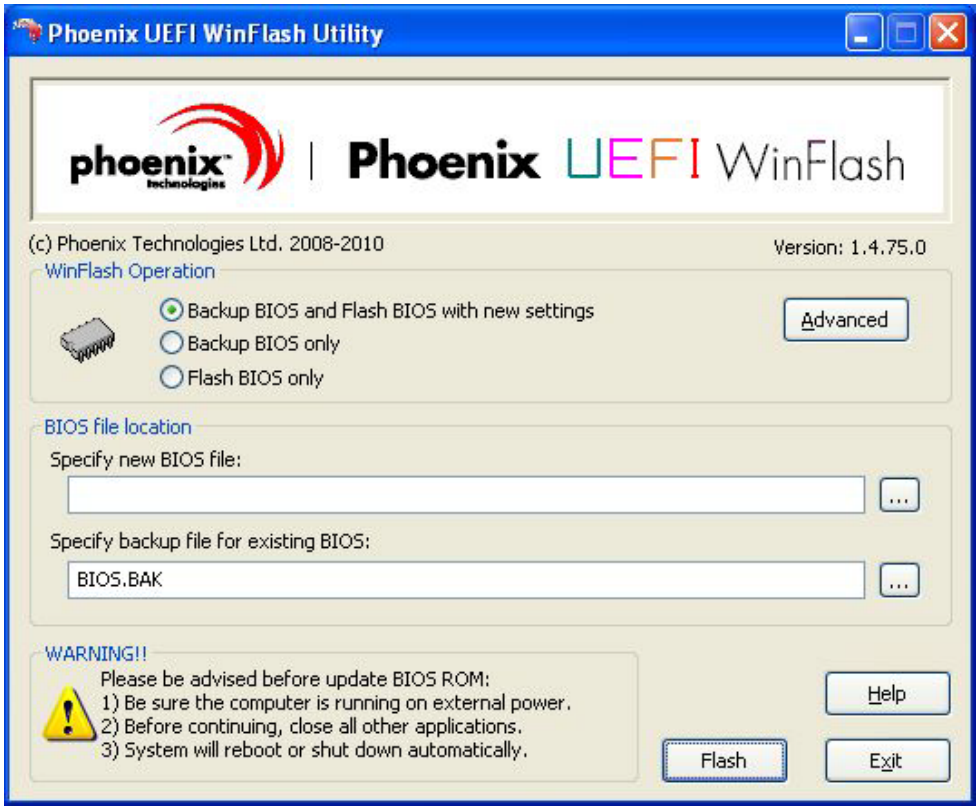
**Note**: You can also run WinFlash from the MS-DOS prompt within Windows.

### 2.2.2. Windows GUI Mode

Perform the following steps to run the WinFlash Windows utility.

1. Close all other programs and applications.
2. Double-click on **WinFlash.exe** to start the program.

   The following Graphical User Interface (GUI) displays.




**Note**: The GUI will not display when WinFlash is launched from the command line with the `/p` or `/remote2` options.

3. Select one of the following radio buttons in the *WinFlash Operation* box:

   - Backup BIOS and Flash BIOS with new settings
   - Backup BIOS only
   - Flash BIOS only

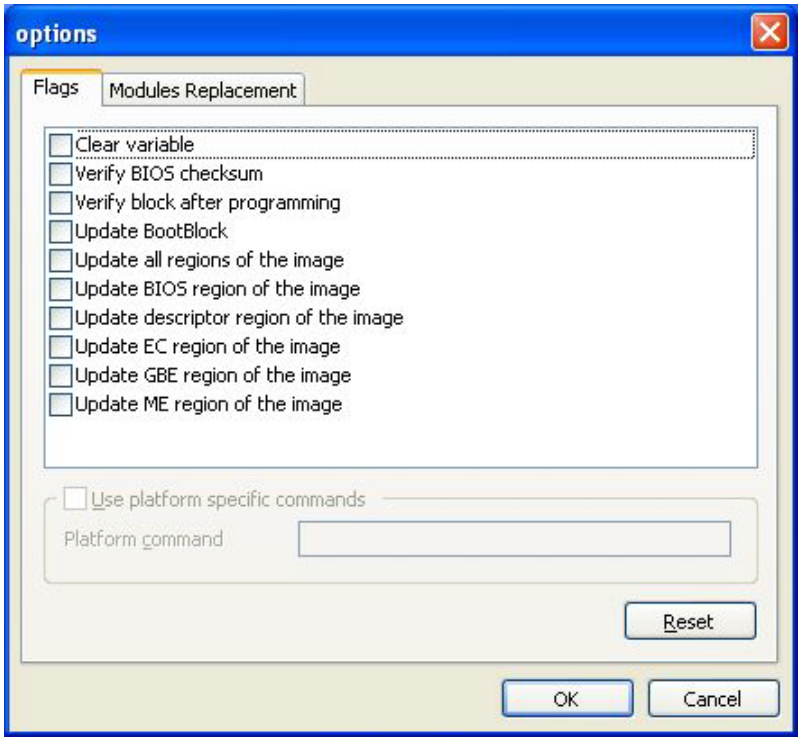
4. If you are flashing a new BIOS, enter the file path and name of the new BIOS file in the **Specify new BIOS file:** box or use the ... button to browse for the file.

   **Note**: BIOS files are normally supplied by system manufacturers.

5. If you are backing up the existing BIOS, enter the file path and name of the backup file in the **Specify backup file for existing BIOS:** box or use the ... button to browse for the file.

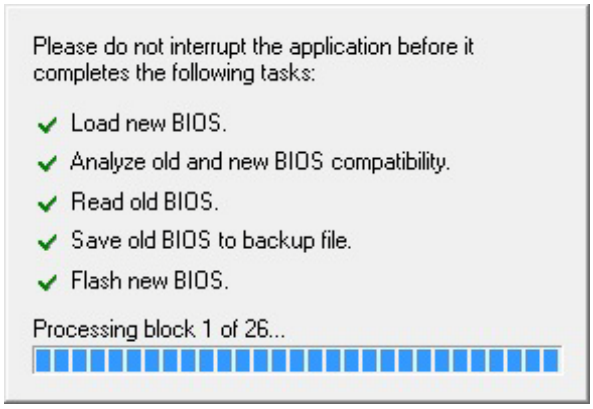
6. Click the **Advanced** button for additional options. Select the options you require and then click **OK**.

   **Note**: These settings become the new default as they are saved to the settings file (winflash.ini).




7. Click the **Flash** or **Backup** button and then press **OK** in the popup box to start the process. The following progress dialog displays.

   **Warning**: Do not interrupt the program under any condition.




8. If you are backing up your BIOS only, the utility will display a confirmation message upon successful completion. If you successfully backup and upgrade (flash) your BIOS, the utility displays the following message.


9. Press **Cancel** to terminate the restart dialog and return to the main window. Be aware that your system may not execute the features of the newly programmed BIOS until you reboot.

   Press **Restart**, or wait, to allow the program to reboot your computer. If your system does not shut down automatically, reboot the system by pressing the **Reset** button or by turning the power switch off and on.

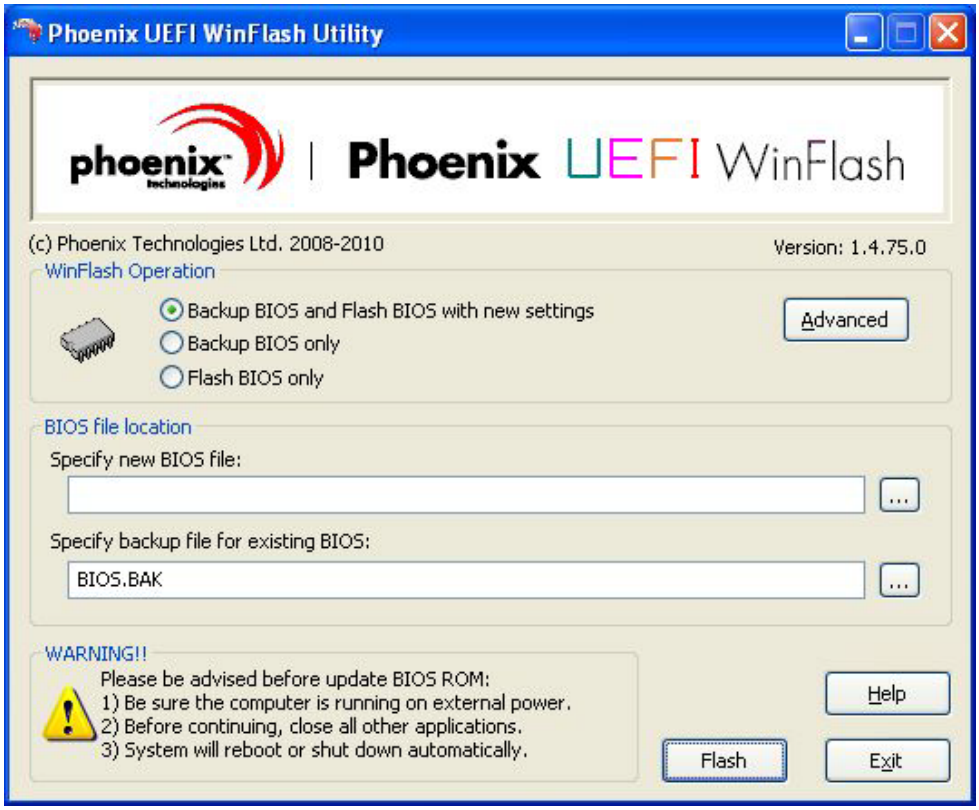
### 2.2.3. BIOS Capsule Flashing

SecureCore Tiano WinFlash (version 1.3.65.0 and later) can load and flash BIOS capsule files.

Perform the following steps to flash a BIOS capsule file.

1. Close all other programs and applications.
2. Double-click the **WinFlash.exe** icon to start the program.

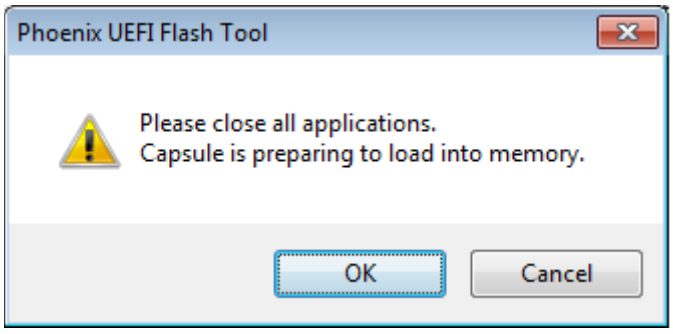
   The following Graphical User Interface (GUI) displays.



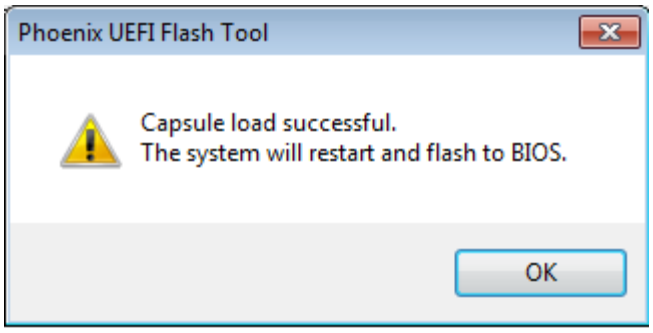

**Note**: The GUI will not display if WinFlash is launched from the command line with the `/p` or `/remote2` options. Also, only the flags tab is visible after clicking the **Advanced** button.

3. Select the **Flash BIOS only** radio button.
4. Enter the file path and name of the new BIOS capsule file in the **Specify new BIOS file:** box or use the ... button to browse for the file.

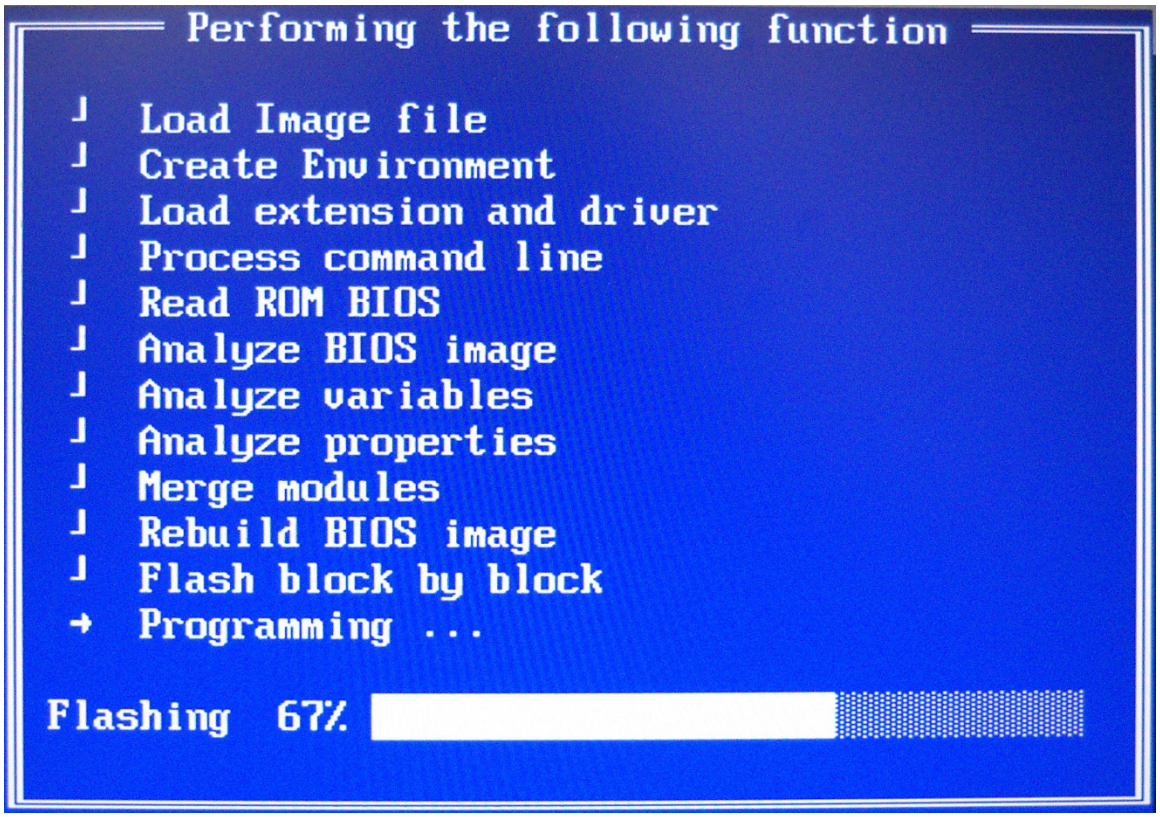
   **Note**: BIOS capsule files are normally supplied by system manufacturers.
5. Click the **Flash** button and then **OK** in the popup box to start the process or **Cancel** to terminate.




6. If the BIOS capsule file loads successfully, the following dialog box is displayed.




7. The system will restart and flash the capsule BIOS within an EFI shell environment. The following image displays the progress dialog for BIOS capsule flashing within an EFI shell.




8. Upon successful completion, the system will restart, and your OS will load as usual.

# CHAPTER 3

## *WINFLASH COMMANDS*

## 3.1. Command Options

Command options can be used in the following ways:

- On the command line
- Within PFLASH.RSP

### 3.1.1. Command Option Syntax

The command option syntax is as follows:

```
WINFLASH  [options] [romfile] [@rspfile]
```

[options]

Entered on the command line. For more information on the command options, see Section 3.1.2 Command Options List.

*romfile*

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

*@rspfile*

The response file (PFLASH.RSP by default) contains all command options in text format. Separate each command option with a carriage return and remove all preceding spaces or tabs.

### 3.1.2. Command Options List

The following table lists all available command line options.

| Option:Parameter(s) | Function |
|---|---|
| **/? /help /h** | Displays help screen |
| **/all** | Flash the entire image including the descriptor region |
| **/bak:**`filename` | Backup ROM to a file. |
| **/bbl** | Program the boot block. By default, bootblock is not updated. |
| **/bios** | Flash the BIOS region |
| **/cs** | Verify the checksum of a .FFS file. |
| **/console** | Console mode hides the GUI windows, but unlike the remote2 option, shows the progress dialog. Just as with **/remote2**, this option also stops the system from rebooting after BIOS flashing. |
| **/cvar** | Clear variables |
| **/desc** | Flash the descriptor the 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 |
| **/exit** | Exit without rebooting. **NOTE**: This option should not be used with the /p option. |
| **/force** | Flash without any modification of the BIOS image.<br>**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 |
| **/logo:**`imagefile [:index]` | Replace a BIOS logo with an `imagefile` in JPG, BMP or GIF formats.<br><br>**Note**: The file size of the new logo cannot be larger than the current logo and bitmap images should be in 24bit color mode.<br><br>This option can be used in two ways:<br><br>1. If the BIOS image is not defined in the command line, this option will replace the logo of the current BIOS (i.e. `WINFLASH /logo:imagefile`).<br><br>2. If the BIOS image is defined in the command line, this option will replace the logo of the new BIOS image (i.e. `WINFLASH /logo:imagefile romfile`).<br><br>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 |
| **/mfg** | Manufacturing mode. Automatically reboots without the need to press a key. |
| **/mod:**`filename` | Updates the module in the BIOS with the module contained in the file (such as /MOD:`vga.ffs`); the rest of the BIOS image remains unchanged. |
| **/mode**=n | Specify dmi mode n = {0, 1, 2, 3}<br><br>0: Just update BIOS with new file, don't update DMI variables.<br><br>1: Just update DMI variables, keep ROM BIOS as before.<br><br>2: Update BIOS, merge ROM DMI variables with command line (default).<br><br>3: Update BIOS, merge image variables with command line. |
| **/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. |

| Option:Parameter(s) | Function |
|---|---|
| **/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.<br><br>**Note**: The flash tool will abort if it cannot successfully load and run all the PFAE modules within a volume file. |
| **/raw:**`GUID:filename` | Replace the RAW module. Updates the module in the BIOS with the module contained in the file. The rest of the BIOS image remains unchanged. |
| **/remote2** | Execute without GUI (allows other applications or computers to call WinFlash). Just as with **/console**, this option also stops the system from rebooting after BIOS flashing. |
| **/ro[**`=filename`**]** | In backup ROM only mode, the tool reads the contents of the flash part and saves them to `filename` without flashing. If `filename` is not specified, the flash part will be saved to `BIOSROM.BAK`. |
| **/sa** | Skip all BIOS checks. |
| **/sd** | Skip BIOS date check. |
| **/slp** | Replace SLP marker key in current or new BIOS image.<br><br>1) To replace the SLP marker key within the current BIOS:<br>`winflash /slp:filename`<br>2) To replace the SLP marker key and flash a new BIOS image<br>`winflash /slp:filename newbios.bin`<br><br>**Note**: /slp and /spu can be used in combination. |
| **/sm** | Skips all dialog boxes. |
| **/sn** | Skip BIOS part number check. |
| **/sp** | Skip BIOS product ID check. |
| **/spu:**`filename:index` | Replace SLP public key in current or new BIOS image. The SLP public key version is set using the `index` parameter.<br><br>1) To replace a SLP2.0 public key within the current BIOS:<br>`winflash /spu:filename:20`<br>2) To replace a SLP2.1 public key and flash a new BIOS image<br>`winflash /spu:filename:21 newbios.bin`<br><br>**Note**: /slp and /spu can be used in combination. |

| Option:Parameter(s) | Function |
|---|---|
| **/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.<br><br>**Note**: Older BIOS versions will still display a warning message. |
| **/swm** | Skips all dialog boxes with warnings. |
| **/v** | Verify each block after programming 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. |

# CHAPTER 4

## *WINFLASH ERROR MESSAGES*

### 4.1. Error Messages

The following table lists WinFlash error messages in numerical order.

| Error Code | Error Name |
|---|---|
| 6 | PFLASH_ERROR_IMAGE_SIZE |
| 30 | PFLASH_ERROR_DRV_MEM_ALLOC |
| 81 | PFLASH_ERROR_IMAGE_FILE |
| 82 | PFLASH_ERROR_BACKUP_FILE |
| 83 | PFLASH_ERROR_SAME_FILE |
| 85 | PFLASH_ERROR_NOT_ENOUGH_SPACE |
| 97 | PFLASH_ERROR_DRIVERLOADFAIL |
| 98 | PFLASH_ERROR_DRIVERSERVICEFAIL |
| 99 | PFLASH_ERROR_ENVDLLLOADFAIL |
| 100 | PFLASH_ERROR_INVALID_BIOS_IMAGE |
| 101 | PFLASH_ERROR_UNSUPPORT_BIOS_ROM |
| 102 | PFLASH_ERROR_ON_FLASHERROR |
| 103 | PFLASH_ERROR_CANNOT_LAUNCH_UEFI |

| Error Code | Error Name |
|---|---|
| 104 | PFLASH_ERROR_INPUT_FILE_FAILED |
| 105 | PFLASH_ERROR_COMMAND_LINE_ERROR |
| 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 |
| 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 |

| Error Code | Error Name |
|---|---|
| 177 | EFI_ERROR_CRC_ERROR |
| 178 | PFLASH_ID_CHK_FAIL |
| 179 | PFLASH_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 |