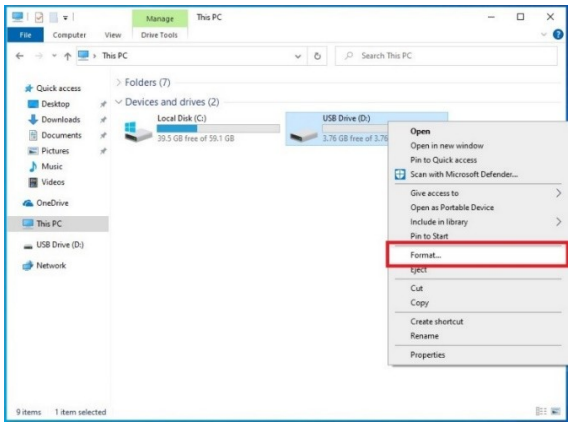
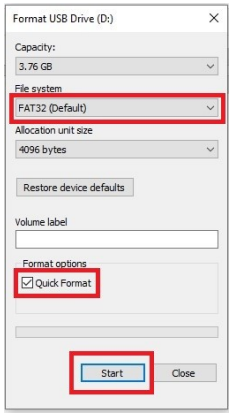
How to Flash BIOS in UEFI Shell? - English

Doc version 1.1

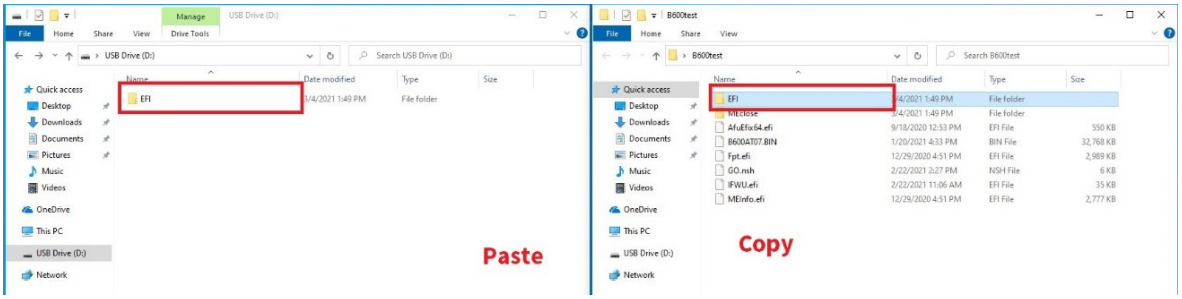
Step 1: Create UEFI Shell USB Disk

1. Find the USB disk in Windows Explorer. Right click USB disk and then click "Format" to format USB disk. (Note: Format USB disk will erase all your data on the USB disk, please backup the data if necessary.)
2. Select FAT32 file system.
3. Select Quick Format and Click Start button.
4. USB format is completed.

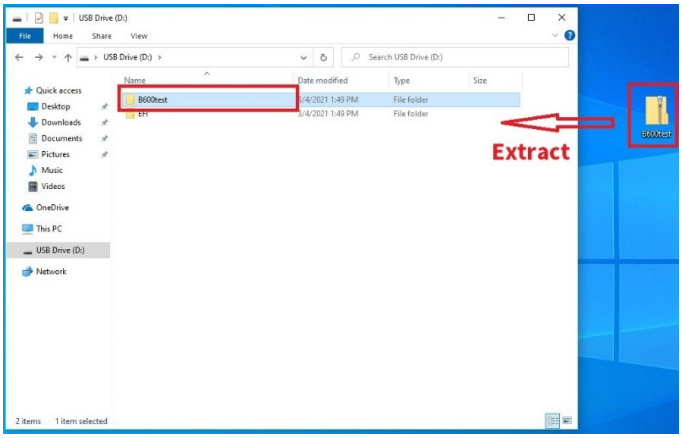




5. Copy the "EFI" folder from this folder of BIOS package to the root directory of the USB disk.

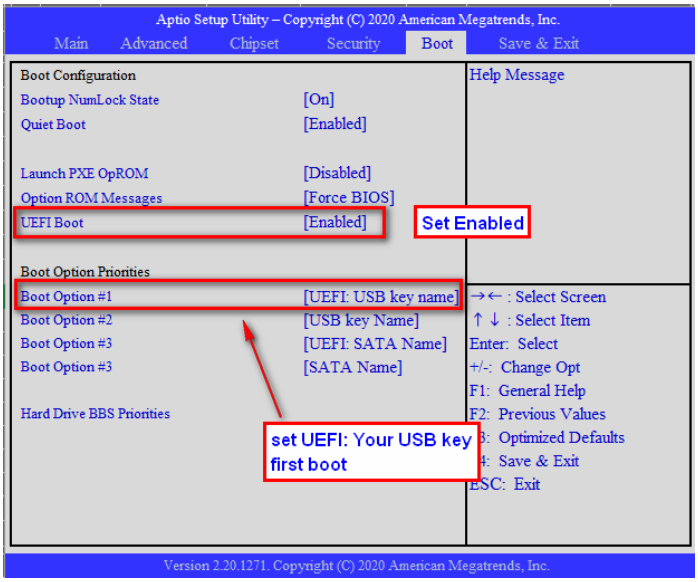


6. Extract BIOS package to the root directory of USB key.



Step 2: Prepare Update

1. Plug USB key to IEI Board or system.
2. Power on system and press "Delete" or "F2" key to enter BIOS setup.
3. Find Boot page.
4. If "UEFI boot" item value is [Disabled], please set [Enabled] and Press "F4" key to save settings and exit.
5. It will restart. And press "Delete" or "F2" key to enter BIOS setup again.
6. Find Boot page and Boot Option #1 items. Please set [UEFI: Your USB key] and Press "F4" key to save settings and exit (If "UEFI boot" item is exist, please Enable it first).



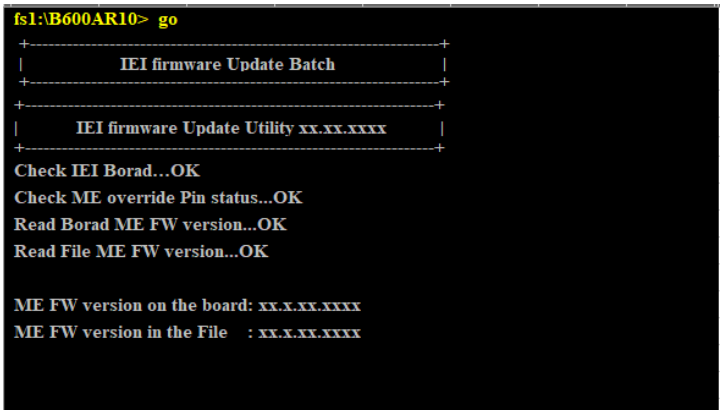
7. When system restarts, it will enter UEFI Shell from your USB key.
8. Check Removable HardDisk(your USB key) is assigned to which Device mapping Table. (Here is FS1: as an example)
9. Type "fs1:" and then press Enter key to go to USB key.
10. Type "cd (This folder of BIOS package)" and then press "Enter" key to go to folder.



■ Intel Platform

Step 3: Flash BIOS

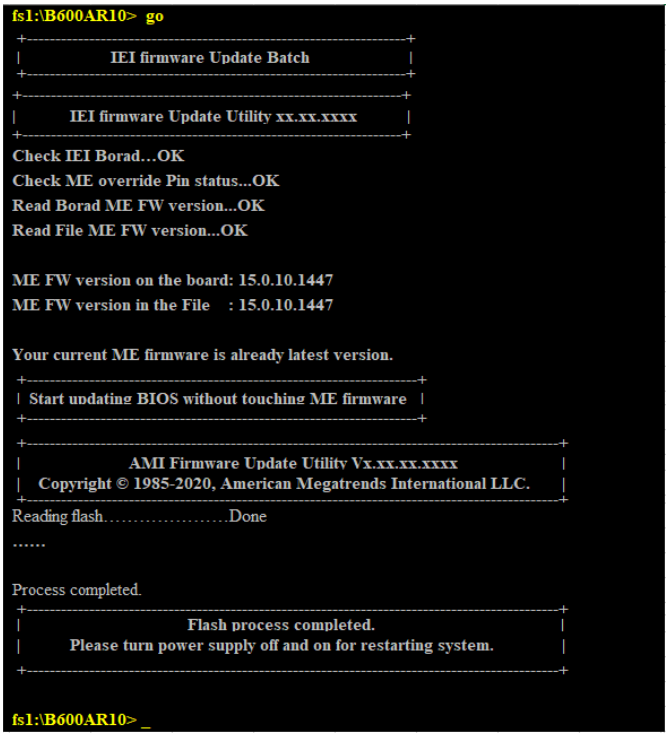
1. Type "go" then press Enter key to start flash BIOS update process.
2. It will check ME/TXE firmware version first.



3. Depending on the version, there will be different processing methods.

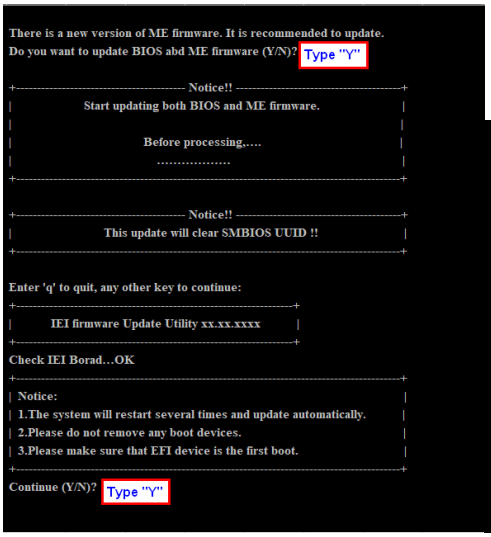
● No new ME/TXE FW version:

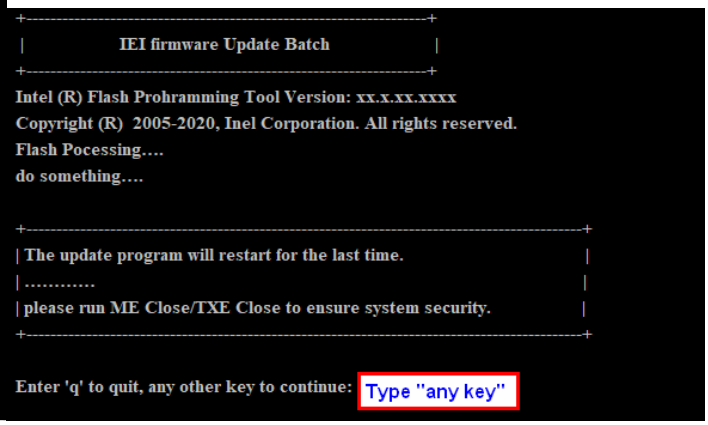
4. It will flash BIOS without ME/TXE firmware.
5. When the flash process is completed, please restart the system.
6. It done (No need to execute Step4: Execute ME/TXE Close).



● ME/TXE New/old FW version (If software security override is supported):

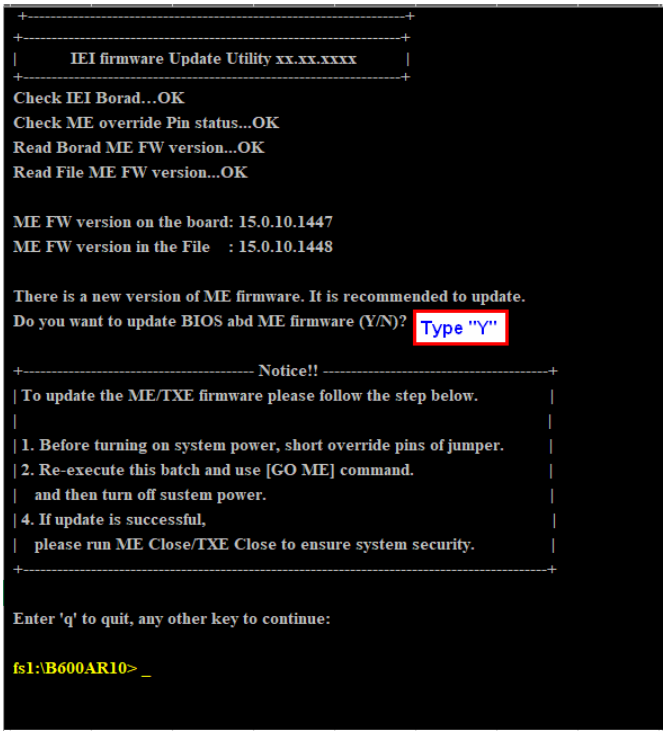
4. It will ask you if you want to update the BIOS and ME/TXE firmware.
   Type "N" and it will only update BIOS (Ref. “No new ME/TXE FW version” steps).
   Type "Y" and it will update BIOS with ME/TXE FW (Ref. 5.).
5. System will restart and start update process automatically, after you agreed and read notes.
6. System restarts the last time to complete the update, after typed any key.





● ME/TXE New/old FW version (If hardware security override is supported):

4. It will ask you if you want to update the BIOS and ME/TXE firmware.
   Type "N" and it will only update BIOS (Ref. “No new ME/TXE FW version” steps).
   Type "Y" and it will update BIOS with ME/TXE FW (Ref. 5.).
5. The system will prompt you to do something to update.



6. According to the prompt, please turn off the power first.
7. Then, please find "J_FLASH1" or related words (please refer to the user manual [keyword: security override]) on the motherboard and short pins of the jumper.

4.7.3 Flash Descriptor Security Override Jumper

The Flash Descriptor Security Override jumper (J_FLASH1, p=2.00 mm) allows users to enable or disable the ME firmware update. Refer to **Figure 4-12** and **Table 4-2** for the jumper location and settings.

Setting	Description
Short 1-2	Disabled (default)
Short 2-3	Enabled

Table 4-2: Flash Descriptor Security Override Jumper Settings

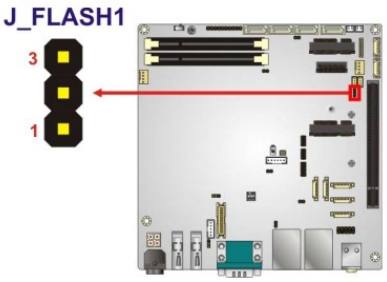


Figure 4-12: Flash Descriptor Security Override Jumper Location

8. Power on system and enter UEFI Shell from your USB key again.
   (Ref. Step 2: Prepare Update)
9. Type "go me" then press Enter key to start flash BIOS with ME/TXE FW update process.
10. If the update is complete, please power off the system and restart it.

Step 4: Execute ME/TXE Close

(If you have to update the BIOS with ME/TXE firmware, you need to do this step)

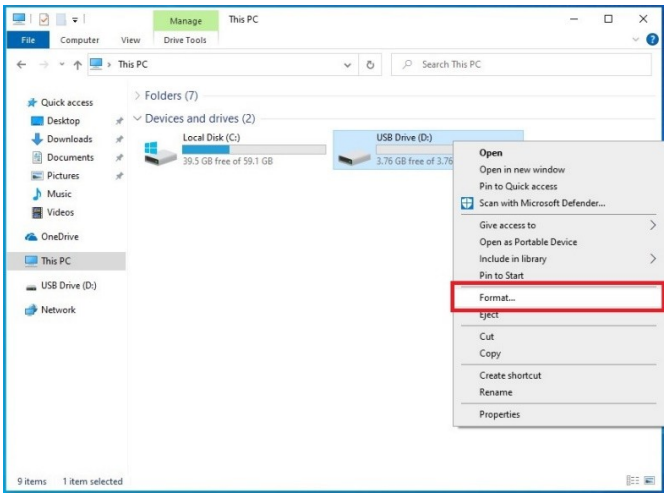
1. Power on system and enter UEFI Shell from your USB key again.
   (Ref. Step 2: Prepare Update)
2. Type "cd MEClose" (or "cd TXEClose") and then press "Enter" key to go to folder.
3. Type "MEclose.nsh" (TXEclose.nsh) then press "Enter" key to execute ME/TXE Close.
4. The system may reboot several times, please repeat (2.) - (3.) until the "MEClose Finished" (or TXEClose Finished) message is displayed.
5. It done.

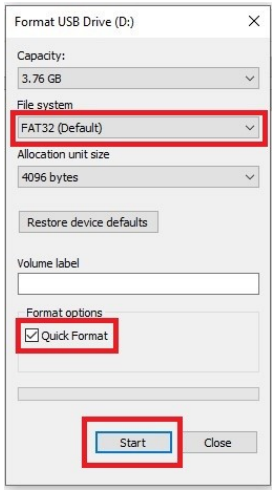
如何在 UEFI shell 下更新 BIOS? – 繁體中文

文件版本 1.0

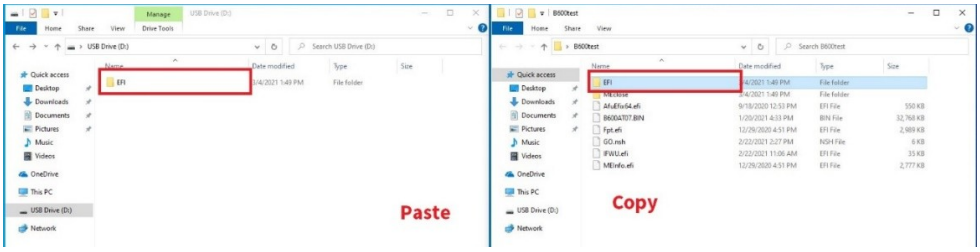
Step 1: 製作一個 UEFI Shell 隨身碟

1. 在 Windows 檔案總管中找到隨身碟。在隨身碟圖示上右鍵點擊選擇 "格式化" (Note: 格式化隨身碟接清除所有資料，如果有需要，請先備份資料。
2. 選擇 FAT32 檔案系統。
3. 選擇 快速格式化 後，點擊 開始 按鈕。
4. 隨身碟格式化完成。

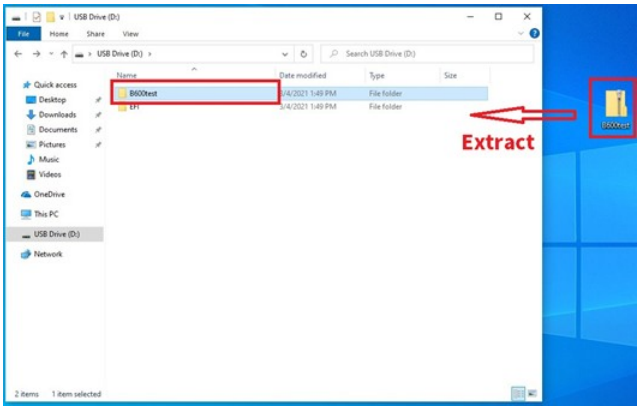




5. 從 BIOS 壓縮包中複製 "EFI" 資料夾到隨身碟的根目錄中。

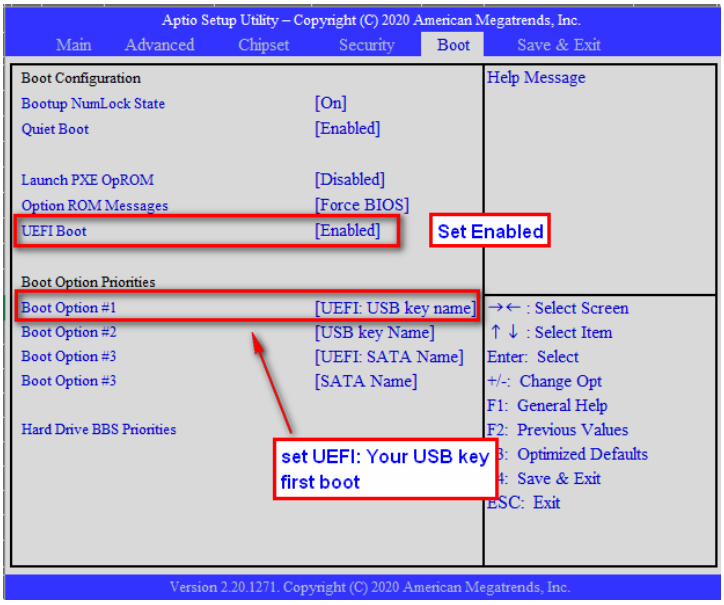


6. 解壓縮 BIOS 包到隨身碟的根目錄中。

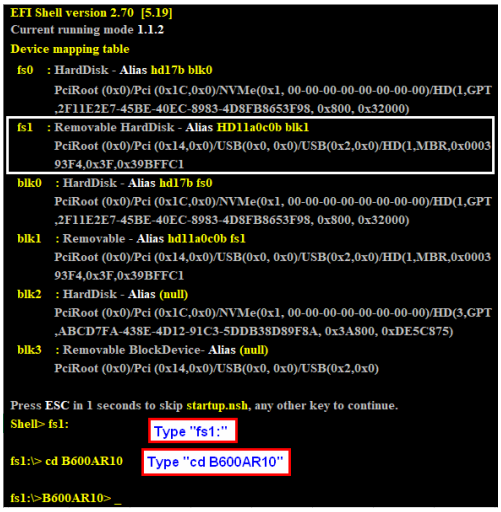


Step 2: 準備更新

1. 在 IEI 產品中插入隨身碟。
2. 開機後，在鍵盤中按 "Delete" 或 "F2" 鍵進入 BIOS 選單。
3. 找到 Boot 頁面。
4. 如果 "UEFI boot" 項目值為 [Disabled], 請設定為 [Enabled] 後按 "F4" 鍵選擇儲存並離開。
5. 系統將重新開機. 再次在鍵盤中按 "Delete" 或 "F2" 鍵進入 BIOS 選單。.
6. 找到 Boot 頁面並將 Boot Option #1 項目設為 [UEFI: 你的隨身碟]後按 "F4" 鍵選擇儲存並離開 (如果 "UEFI Boot" 項目存在，請先啟用它)。



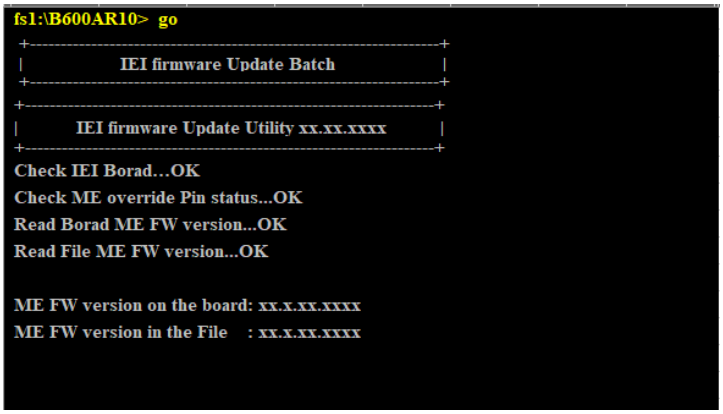
7. 當系統重新啟動後，它將進入 UEFI Shell。
8. 檢查 Device mapping Table 中 Removable HardDisk(你的隨身碟) 的分配。(這裡以 FS1: 當例子)
9. 輸入 "fs1:"後按 Enter 鍵進入隨身碟根目錄。
10. 輸入 "cd (BIOS 包的名稱)" 後，按 "Enter" 鍵進入資料夾。



■ Intel 平台

Step 3: 更新 BIOS

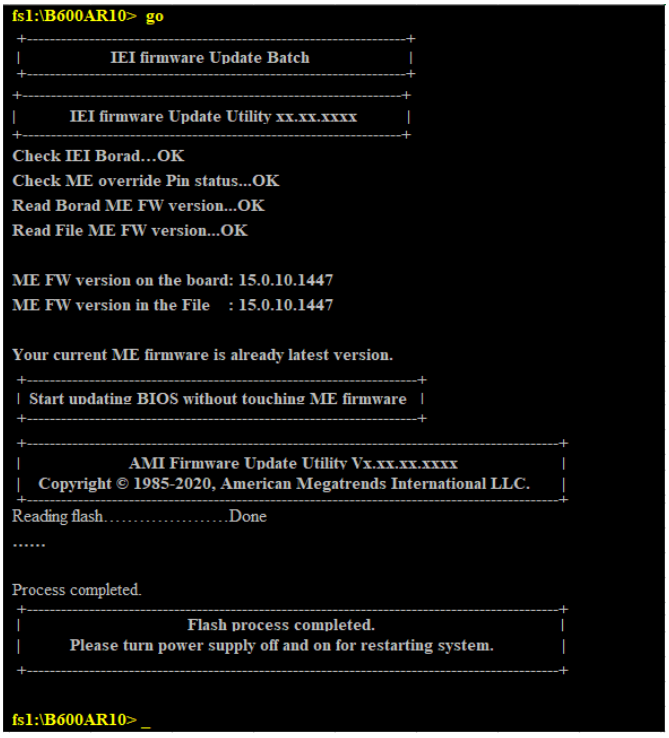
1. 輸入 "go" 後按 Enter 鍵開啟 BIOS 更新程式。
2. 程式將先檢查 ME/TXE 韌體版本。



3. 根據結果，將會有不同的處理方式。

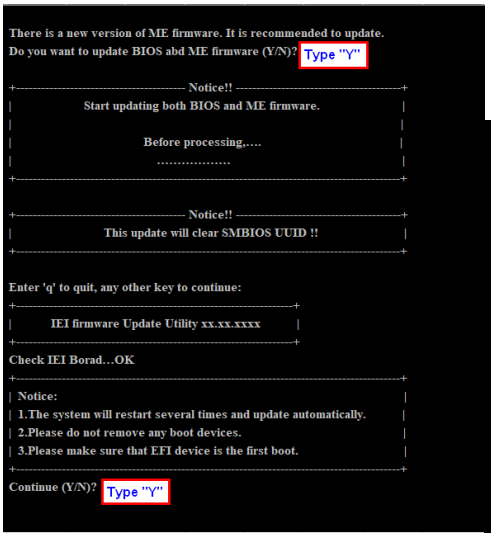
● 沒有新的 ME/TXE 韌體版本:

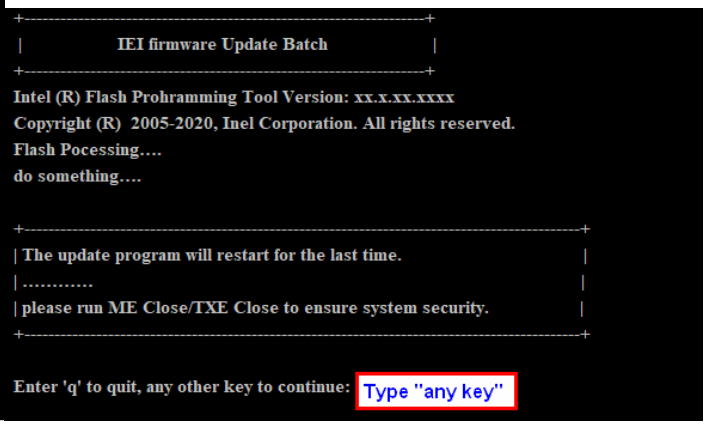
4. 系統將只更新 BIOS 的部分。
5. 當更新完成後，請將系統重新啟動。
6. 更新完成 (不需要執行 Step4: 執行 ME/TXE Close)。



● ME/TXE 韌體有 新/舊版本 (如果支援 軟體 安全性覆寫):

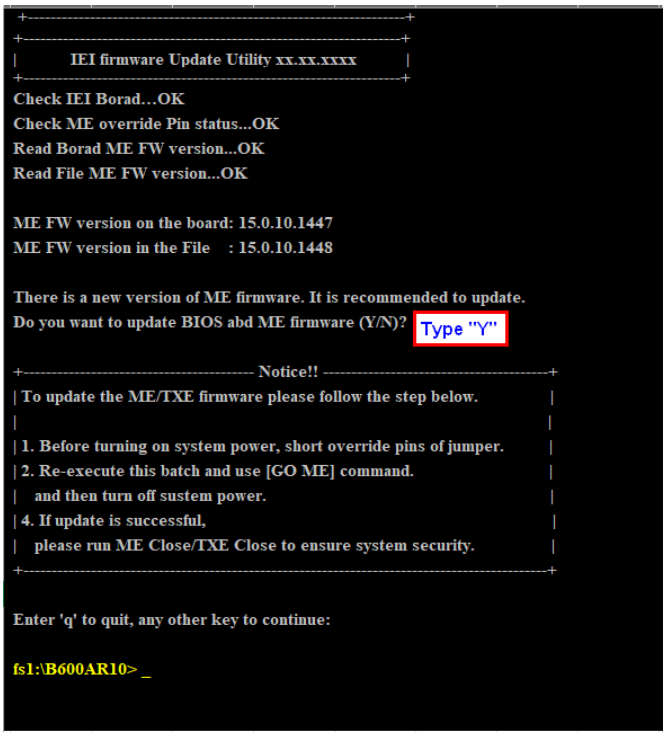
4. 它將詢問是否更新 BIOS 與 ME/TXE 韌體。
   輸入 "N" 後只更新 BIOS 的部分 (參考. "沒有新的 ME/TXE 韌體版本" 步驟)。
   輸入 "Y" 後將會更新 BIOS 與 ME/TXE 韌體 (參考 5.).
5. 在你同意且閱讀注意事項後，系統將重新啟動並自動開始更新程式。
6. 輸入任何鍵後，系統會重新開機以完成更新。





● ME/TXE 韌體有 新/舊版本 (如果支援 硬體 安全性覆寫)::

4. 它將詢問是否更新 BIOS 與 ME/TXE 韌體。
   輸入 "N" 後只更新 BIOS 的部分 (參考. "沒有新的 ME/TXE 韌體版本" 步驟)。
   輸入 "Y" 後將會更新 BIOS 與 ME/TXE 韌體 (參考 5.).
5. 系統將會提醒更新前的注意事項。



6. 根據注意事項, 請先將系統關機斷電。
7. 然後, 在主機板找到 "J_FLASH1" 或是相關文字(可以參考使用者手冊 [關鍵字: security override]) 後使用跳帽使其成短路狀態。

4.7.3 Flash Descriptor Security Override Jumper

The Flash Descriptor Security Override jumper (J_FLASH1, p=2.00 mm) allows users to enable or disable the ME firmware update. Refer to **Figure 4-12** and **Table 4-2** for the jumper location and settings.

Setting	Description
Short 1-2	Disabled (default)
Short 2-3	Enabled

Table 4-2: Flash Descriptor Security Override Jumper Settings

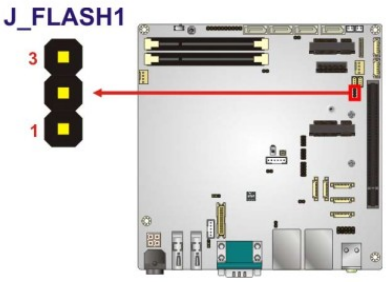


Figure 4-12: Flash Descriptor Security Override Jumper Location

8. 復電並將系統開機再次進入 UEFI Shell。
   (參考. Step 2: 準備更新)
9. 輸入 "go me"後按 Enter 鍵開始更新 BIOS 與 ME/TXE 韌體程式。
10. 如果更新完成，請斷電後重新開機。

Step 4: 執行 ME/TXE Close

(如果有更新 BIOS 與 ME/TXE 韌體, 必須執行此步驟)

1. 將系統開機再次進入 UEFI Shell。
   (參考. Step 2: 準備更新)
2. 輸入 "cd MEClose" (或 "cd TXEClose") 後按 "Enter" 鍵進入資料夾。
3. 輸入 "MEclose.nsh" (TXEclose.nsh) 按 "Enter" 鍵執行 ME/TXE Close.
4. 系統也許會重新啟動數次, 但請重複執行 (2.) 到 (3.) 直到出現 "MEClose Finished" (or TXEClose Finished) 訊息。
5. 完成更新。