

机械革命S1强刷微星BIOS后修改BIOS解锁高级设置

浏览 42477 | 评论 49 | 字数 5587



卖女孩的小火柴 - 春招结束

2019年08月14日

折腾那么久，刷上了MSI的BIOS，除了开机logo帅了一点外，好像没啥改变？

这怎么行？于是就动上了修改BIOS的心思。

当然，其他机型也可以参考此教程。

和前文一样，干这个就得做好去售后的准备！

废话不多说，我们直接开始！

注意：此文已被废弃，BIOS选项可以直接通过快捷键开启，无风险，请移步最新文章！

注意：此文已被废弃，BIOS选项可以直接通过快捷键开启，无风险，请移步最新文章！

注意：此文已被废弃，BIOS选项可以直接通过快捷键开启，无风险，请移步最新文章！

最新文章： <https://www.shinenet.cn/archives/61.html>

注意：MX250版本必须使用
<https://www.shinenet.cn/archives/61.html> 的方法！

准备工具/文件

1. U盘一个，好歹整个大点的

2. 所需的文件需要的文件.7z
蓝奏云 <https://www.lanzous.com/i5kprxa>
3. U盘所需的 grup引导 BOOTX64.7z
蓝奏云 <https://www.lanzous.com/i5kqxwb>

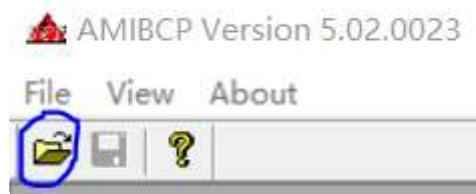


准备环境

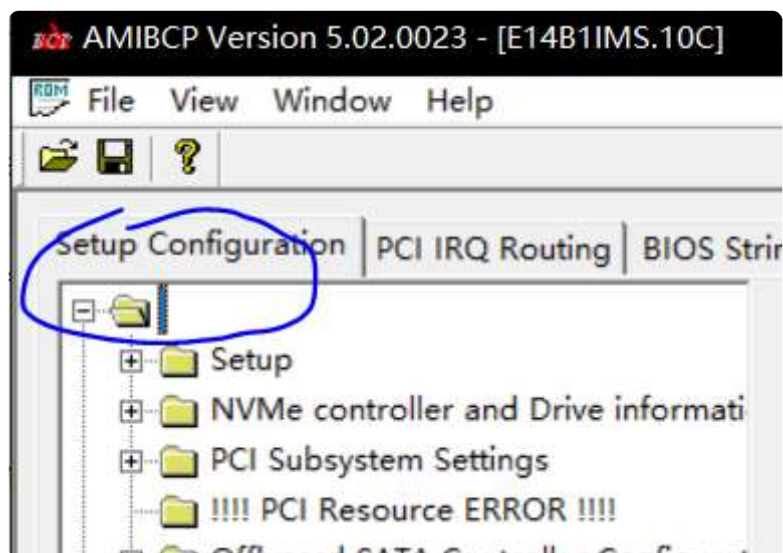
这次将会在两个环境中操作 一个是EFI的grup环境，一个是熟悉的WINDOWS环境
同样，关闭所有软件尤其是杀毒软件。

修改BIOS

1. 打开AMIBCP502里面的AMIBCP.exe(当然你们要是能找到更新版最好，可以在评论区分享一下，官网也下载不到这个软件，实在是找不到最新版)
2. 选择右上角的 open 按钮图标



1. 修改 文件类型 为 All Files(*), 并选中MSI的BIOS (最好提前复制一个文件夹，便于区分修改版和原版区别) 打开
2. 标签栏 Setup Configuration - 第一个空白名字的文件夹 - 打开



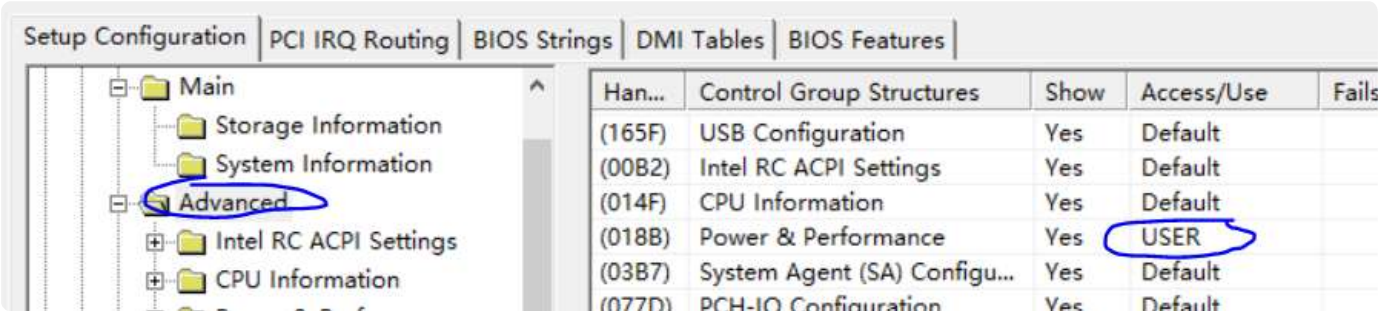
1. 打开 Setup，出现了熟悉的菜单
2. 按需修改需要显示的项目，当然，大部分都在Advance里面
3. **千万不能修改Failsafe或者Optimal的值！还有空白选项卡的任何选项！如果你不认识这个选项，请不要修改！！**除非你有足够的把握。这个值代表着默认采用的BIOS设置和故障时启动的BIOS设置（猜测），也就是说，如果修改了默认值而导致笔记本无法开机，那么重置

≡ 卖女孩的小火柴的博客

CMOS 拔掉电池恢复BIOS默认设置都是无效的，因为恢复的默认设置后那个值并没有发生变化，仍会导致不开机。相反，我们解锁了高级设置的选项后，如果因为瞎设置导致的不开机，我们只需要重置CMOS拔掉电池之后就可以继续开浪了这点切记。

4. 如果我们想要让一个设置显示在BIOS中，那应该怎么做呢？虽然Show是Yes的状态，但由于后面的Access/Use设置的全都是默认，而用户打开BIOS后只拥有最低的USER权限，所以我们只需要双击将其修改为USER即可

5. 比如我想要显示 Power & Performance 选项，我们应该打开Advance(这是它的上级菜单，我们修改的是它在上级菜单中的权限/可见性)，找到Power & Performance，修改为USER，如图



1. 确认好我们的设置不会导致BIOS挂掉或者无法开机后，ctrl+s快捷键保存，耐心等待程序运行结束，关闭程序会再次提醒是否保存，是否随意。保存的新BIOS为打开的原文件

2019.08.15 20:51更新：首发版本提供一个我已经修改好的BIOS，下载E14B1IMS.7z

主要修改内容：

- 解锁Advanced里面的大部分有用的选项卡
- 默认开启 VT-D
- 默认开启 Intel(R) Speed Shift Technology
- 默认开启 超频设置 并且开放XTU接口
- 默认关闭 BIOS LOCK
- 默认关闭 CFG LOCK

刷入修改好的BIOS

由于我们已经修改好了BIOS，下面只要按之前的操作刷入就可以了。

Emmmm，其实是不行的。

BIOS中有区段是BIOS厂商给BIOS的签名，很明显这个签名方法和签名KEY不可能泄露出来，也就断绝了你自己签名的可能性。由于我们修改了BIOS，会导致签名的自校验被破坏，无论是BIOS中刷入，还是AFU刷入都会弹出校验错误阻止我们刷入修改后的BIOS。

有人问，我们可以用AFU 3.7以前的版本呀，那些版本带有 /GAN参数，可以强制忽略签名校验

答：使用3.7版本无法识别S1的平台，事实上，AFU的版本必须在5.9以上才能识别S1的平台和BIOS芯片

那就没有解决的办法了吗？

还是有点，这个方法由intel提供。intel提供了一个直接由CPU刷入主板上储存ROM芯片的方法，不

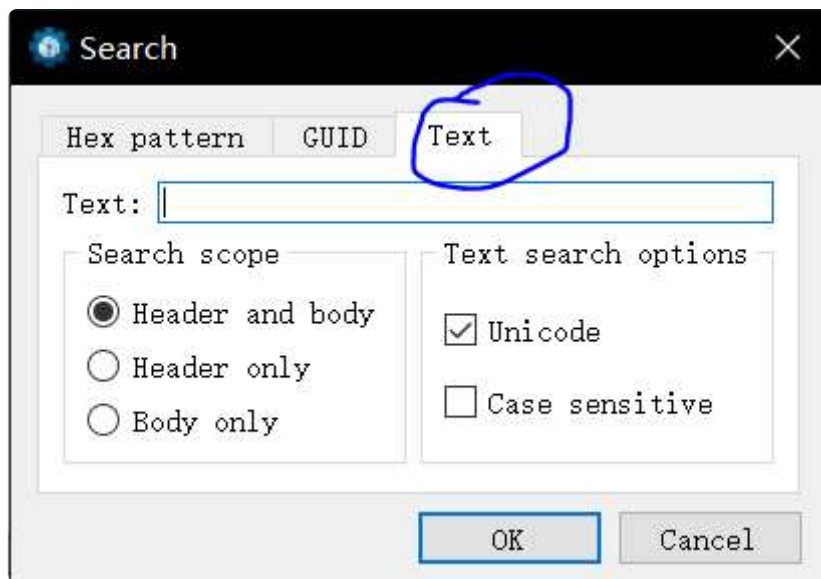
仅仅可以用来刷BIOS，需要BIOS的ME支持。但这个方法需要BIOS自己主动关闭BIOS LOCK，但大部分BIOS都会隐藏这个选项，我们无法关闭这个锁，那怎么办呢？

办法还是有的，就是有点麻烦。在group中我们可以直接修改BIOS设置项目的值，所以接下来我们就是准备找到这个值并且在group中修改它。这个方法还可以修改一些不能修改BIOS的笔记本的一些设置，比如HP，HP的BIOS有自校验，如果你修改了它并且成功刷入了它，在启动的时候，BIOS还会自己检验自己，如果错误会拒绝启动。对于这种笔记本只能在group中挨个修改值，很是麻烦。

如果你是初代S1，即8250U/8550U+MX150+无OFFICE的版本，下面你可以跳过直接到group的操作，如果不是，那么我们开始吧。

寻找BIOS LOCK

1. 打开UEFITool软件，菜单栏选择File>Open image file... 切换成All Files(*) 选择原版BIOS
2. 在Name框中出现Intel image
3. CTRL+F 快捷键 或者 Action-Search 打开搜索框，点击Text切换到文本搜索模式，如图所示



1. 输入 BIOS LOCK 然后回车，如果操作无误会在下方出现"Unicode text "BIOS LOCK" found in PE32 image section at header-offset 6D926h"类似字样，双击它
2. 在Name窗口右击刚刚弹出的 PE32 image(不同的选项搜索会出现不一样的对应区块)，右键-Extract-body，保存到合适的位置，最好修改一下文件名让它更短些，下面会需要输入这个文件名
3. 保存下来的仍然是二进制文件，我们看不懂，这时候就需要ifreextract 来将其翻译成txt文件以供阅读
4. 将刚刚的文件复制到和ifreextract同目录，在空白处按住shift并右键，在此处打开PowerShell/Cmd窗口
5. 输入 `./ifreextract.exe Section_PE32_image_Setup_Setup_body.efi output.txt`，当然需要更换Section_PE32_image_Setup_Setup_body.efi 为你们自己保存的文件名，如果目录中出现output.txt就成功了，然后关闭窗口

6. 记事本/notepad++/sublime 等等任何可以打开txt并且搜索的软件，打开output.txt文件，
CTRL+F搜索 BIOS LOCK，会出现

```
0x3E293 One Of: BIOS Lock, VarStoreInfo (VarOffset/VarName): 0x929, VarStore: 0x1,
QuestionId: 0x77F, Size: 1, Min: 0x0, Max 0x1, Step: 0x0 {05 91 17 08 18 08 7F 07 01 00 29
09 10 10 00 01 00}
0x3E2A4 Default: DefaultId: 0x0, Value (8 bit): 0x1 {5B 06 00 00 00 01}
0x3E2AA One Of Option: Disabled, Value (8 bit): 0x0 (default MFG) {09 07 04 00 20 00 00}
0x3E2B1 One Of Option: Enabled, Value (8 bit): 0x1 {09 07 03 00 00 00 01}
0x3E2B8 End One Of {29 02}
```

类似的文本，我们来分析它。VarStoreInfo (VarOffset/VarName): 0x929 为变量储存的地址，需要记下来，VarStore: 0x1 为BIOS不设置的情况下默认的变量值（不修改Failsafe或者Optimal的情况下），One Of Option: Disabled 为可以设置的选项，Value (8 bit): 0x0 (default MFG) {09 07 04 00 20 00 00}，0x0为Disabled对应的值，同理，0x1为Enabled对应的值

1. 很明显，我们这里需要修改0x929地址的值为0x0，也就是Disabled

进入grup修改BIOS LOCK的值

1. 格式化U盘为FAT32格式，在U盘分区里新建一个EFI文件夹，EFI文件夹里新建一个BOOT文件夹，把BOOTX64.efi，放入BOOT文件夹里面。文件看起来像是 U盘:/EFI/BOOT/BOOTX64.efi
2. 关闭BIOS中的安全引导，快速引导（MSI的BIOS是按住F11键），选择U盘，直到界面显示 grup>
3. 介绍两句命令 setup_var_3 地址，会显示当前地址的值 setup_var_3 地址 值 会修改当前地址的值
4. 对于首发版本的S1来讲，输入 setup_var_3 0x929 0x0 修改BIOS LOCK，其他机型按上一个修改地址和值，然后再进行查询查看修改正不正确。
5. 输入 reboot 重启进入WIN

使用FPT强行刷入BIOS

对于ME版本为11的可以直接使用提供的FPTW文件，其他版本的请爬微软论坛
S1的版本是11.7所以可以使用。

2019.8.24更新：

MX250版本的都是ME12，请使用这个工具：[FPT-WIN64-ME12.7z](#)

1. 右键win徽标，windows PowerShell(管理员)，打开有管理员权限的powershell
2. CD FPTW64.exe所在的目录，就像这样：CD C:\Users\XXX\Desktop\BIOS\需要的文件\FPW
3. 将修改好的BIOS文件放在目录中（我里面已经有一份我自己修改的，你们替换就好），命令：
./FPTW64.exe -bios -f E14B1IMS.10C

4. 如果出现刷入的进度条并且刷入完成，那么你可以重启了;如果出现Error 366则是没有用管理员权限运行,出现其他错误大多是BIOS LOCK没解锁，也可以尝试重启后再试试

卖女孩的小火柴的博客

1. 按捺住激动的心情，重启吧！如果重启成功且在BIOS内看到了解锁的选项，那么恭喜你，你成功了！

S1推荐的解锁项目和修改项目

待完成，目前还在摸索

本文作者：卖女孩的小火柴 - 春招结束
本文链接：<https://www.shinenet.cn/archives/26.html>
最后修改时间：2020-04-08 02:14:29
本站未注明转载的文章均为原创，并采用 [CC BY-NC-SA 4.0](#) 授权协议，转载请注明来源，谢谢！
如果文章对您有帮助，不妨打赏杯可乐？



评论

如果可能，请填写真实邮箱，有回复会送至邮箱。请不要水评论，谢谢。

...

卖女孩的小火柴的博客

留下你成为大佬的想法吧

支持 Markdown 语法

🔍

😊

😊

昵称

✉

邮箱（必填，将保密）

🔗

➤

- 评论列表

已有 49 条评论
- ZZZ

2021-02-26 01:19

关ME之后的提示有办法关闭吗，大佬

回复

卖女孩的小火柴

2021-02-26 11:34

@ZZZ 现在不是已经不需要强刷BIOS了吗...

回复

ZZZ

2021-02-26 13:34

@卖女孩的小火柴 上笔记本魔改cpu或志强徐要禁用me，禁用会显示ME异常 重刷BIOS，几秒后开机并且没有开机画面。我功力不够，请求大佬逆向去除

回复

卖女孩的小火柴

2021-02-26 13:37

@ZZZ 捣鼓这些个干嘛...是Ryzen不香了，还是小新提不动刀了，亦或者红米Book抢不到?

回复

ZZZ

2021-02-26 13:38

@卖女孩的小火柴 便宜啊 z170板子 130 z370 200左右 cpu i7 9850hk才650

回复
- https://www.shinenet.cn/archives/26.html?ivk_sa=1024320u

7/9

≡  卖女孩的小火柴的博客

@ZZZ 时间成本不算吗...

回复



ZZZ

2021-02-26 13:40

回复

@卖女孩的小火柴 算上时间也香啊 就是微星bios这个提示不会搞



87zrjojo

2019-11-25 21:53

回复

谢谢大神的教程，现在我可以直接刷修改后的BIOSb。但我想知道BIOS Lock 在Bios的什么位置呢，我想以后通过一次性修改BIOS刷机，而不再用GRUB引导去更改了，但找了半天，没有找到BIOS Lock在什么地方



June

2019-11-15 22:56

回复

请问老哥“开放XTU接口”的擦做是怎么实现的呢？我在修改其他主板的BIOS，希望大佬能指条路

admin

2019-11-18 14:39

回复



@June XTU只能用在3代和3代以上的U上，那个时候对XTU支持还不是很好，且主板需要支持超频。

如果是不支持超频的芯片组，自然也没有XTU接口。

XTU接口位于OverClock选项中，如果没有找到超频选项，那XTU也无法打开。



湾仔

2019-11-08 00:00

回复

求一个bios最优配置详解，8250u调来调去r15只能到550



admin

2019-11-18 14:40

回复

@湾仔 已经更新



jumpY

2019-10-14 18:34

回复

首先，感谢一波大佬们的努力给我们带来的幸福，其次，催更那个隔一段时间就撞电流墙的东西，我太菜了一个都看不懂，只能来祈求大佬



Copyright © 2022 卖女孩的小火柴的博客

苏ICP备2021007870号-1

Theme Castle By ohmyga | Powered By Typecho