UEFI SETUP UTILITY

1 简介

本节介绍如何使用 UEFI SETUP UTILITY 配置您的系统。打开计算机电源后按 <F2> 或 <Del> ，您可以运行 UEFI SETUP UTILITY，否则，开机自检 (POST) 将继续其测试例程。如果您想要在 POST 后进入 UEFI SETUP UTILITY，可按 <Ctl> + <Alt> + <Delete> 或按系统机箱上的重置按钮重新启动系统。也可以通过关闭系统后再开启来重新启动它。

由于 UEFI 软件在不断更新，因此以下 UEFI 设置屏幕和说明仅供参考，并且可能与您在自己屏幕上看到的内容不同。

1.1 UEFI 菜单栏

屏幕上部有一个菜单栏包含以下选项：

主画面	设置系统时间 / 日期信息
高级	高级系统配置
工具	有用的工具
硬件监视器	显示当前硬件状态
引导	配置引导设置和引导优先级
安全	安全设置
退出	退出当前屏幕或 UEFI Setup Utility

1.2 导航键

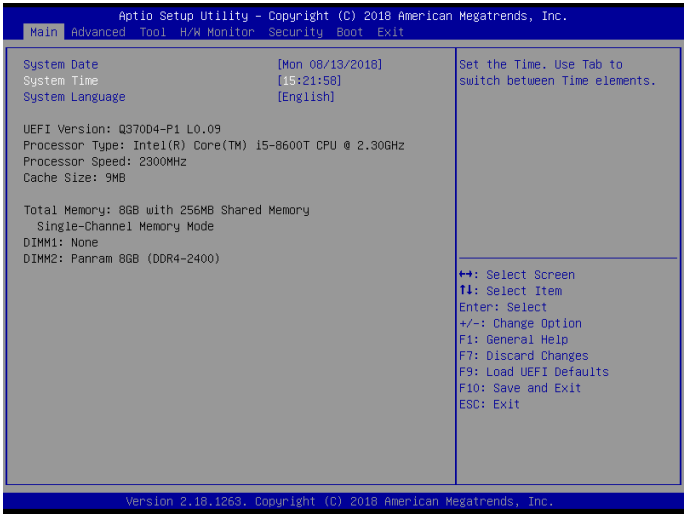
使用 < ← > 键或 < → > 键选择菜单栏上的选项，并使用 < ↑ > 键或 < ↓ > 键上下移动光标以选择项目，然后按 <Enter> 进入子屏幕。您也可以使用鼠标单击需要的项目。

请检查下表了解每个导航键的说明。

导航键	说明
+ / -	更改所选项目的选项
<Tab>	切换到下一个功能
<PGUP>	转到上一页
<PGDN>	转到下一页
<HOME>	转到屏幕顶部
<END>	转到屏幕底部
<F1>	显示一般帮助屏幕
<F7>	放弃更改并退出 SETUP UTILITY
<F9>	加载所有设置的最佳默认值
<F10>	保存更改并退出 SETUP UTILITY
<F12>	打印屏幕
<ESC>	跳到退出屏幕或退出当前屏幕

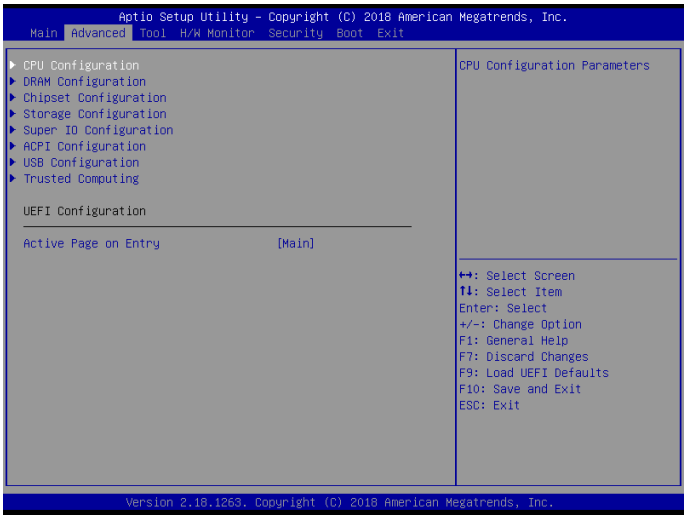
2 主画面

在您进入 UEFI SETUP UTILITY 时，主画面会出现并显示系统概览。



3 高级

在此部分中，您可以配置以下项目 : CPU 配置、DRAM 配置、芯片组配置、存储配置、超级 IO 配置、ACPI 配置、USB 配置和可信赖运算。



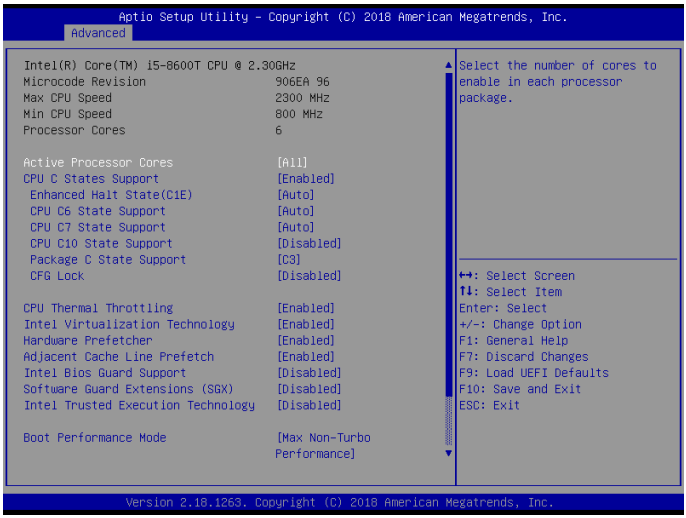
在此部分中设置错误的值可能会造成系统故障。

UEFI 设置

初始页面

选择进入 UEFI 设置实用程序时的默认页面。

3.1 CPU 配置



Intel 超线程技术

Intel 超线程技术允许在每个内核上运行多个线程，从而提升线程软件的整体性能。

激活处理器内核

选择在每个处理器封装中启用的内核数。

CPU C 状态支持

启用 CPU C 状态支持以节能。建议将 C3、C6 和 C7 全都启用以达到更好节能目的。

增强暂停状态 (C1E)

启用增强暂停状态 (C1E) 以降低能耗。

CPU C6 状态支持

启用 C6 深度睡眠状态以降低能耗。

CPU C7 状态支持

启用 C7 深度睡眠状态以降低能耗。

CPU C10 状态支持

启用 C10 深度睡眠状态以降低能耗。

软件包 C 状态支持

启用 CPU、PCIe、内存、图形 C 状态支持以节能。

CFG 锁定

此项目可用来关闭或开启 CFG 锁定。

CPU 过热降频保护

启用 CPU 内部温度控制以防 CPU 过热。

不执行内存保护

采用不执行内存保护技术的处理器可以防止某类恶意缓冲区溢出攻击。

Intel 虚拟化技术

Intel 虚拟化技术允许一个平台在独立分区中运行多个操作系统和应用程序，以便一个计算机系统可以用作多个虚拟系统。

硬件预取器

自动预取处理器的数据和代码。启用可取得更多性能。

相邻缓存行预取

在检索当前请求缓存行的同时预取后面缓存行。启用可取得更多性能。

软件防护扩展（SGX）

使用此项目来开启或关闭软件控制的软件防护扩展指令（SGX）。

启动性能模式

默认为最大 Non-Turbo 性能模式。该设置将保持 CPU 灵活倍频直到操作系统接手。最大电池模式将 CPU 倍频设置为 x8 直到操作系统接手。BCLK 超频时建议设置此选项。

FCLK 频率

设置 FCLK 频率。

Intel SpeedStep 技术

Intel SpeedStep 技术允许处理器在多个频率和电压点之间切换以达到更好节能和散热目的。

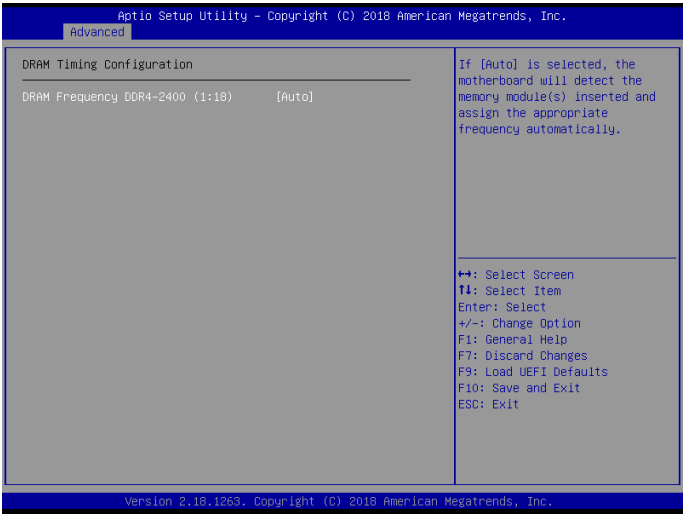
Intel Turbo Boost 技术

当操作系统要求最高状态时，Intel Turbo Boost 技术能够使处理器的运行速度高于其基本操作频率。

Intel Speed Shift 技术

开启 / 关闭 Intel Speed Shift 技术。开启此技术将暴露 CPPC v2 接口，允许硬件控制 P-state。

3.2 DRAM 配置



DRAM 时序配置

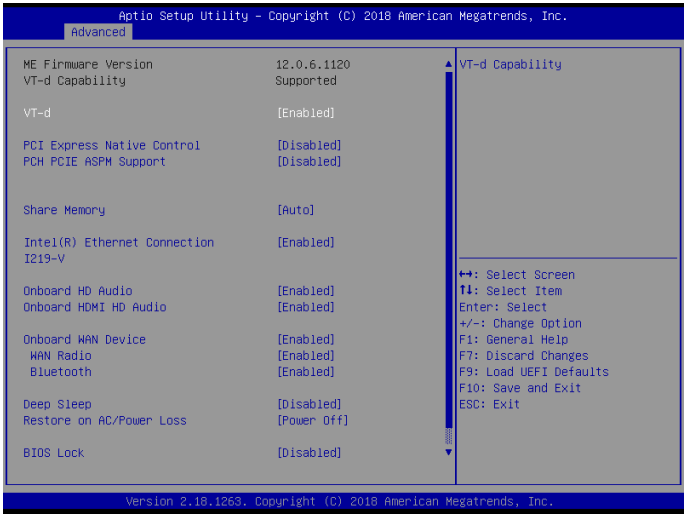
DRAM 基准时钟

选择 [自动] 可取得优化设置。

DRAM 频率

如果选择 [自动]，则主板将检测插入的内存模块，并自动分配相应的频率。

3.3 芯片组配置



VT-d

Intel® 虚拟化技术 Directed I/O 支持可帮助您的虚拟机监视器通过提高应用程序兼容性和可靠性，以及提供额外的可管理性、安全性、隔离和 I/O 性能，来更好地利用硬件。

PCI Express 原生控制

选择开启可提升 PCI Express 在操作系统中的节能性能。

共享内存

配置系统引导时分配给集成图形处理器的内存大小。

Inte(R) 高速乙太网路控制 I219-V

启用或禁用板载网络接口控制器。

板载 HD 音频

启用 / 禁用板载高清音频。设为自动启用板载高清音频并在安装了声卡时自动禁用它。

板载 HDMI HD 音频

启用 / 禁用板载 HDMI HD 音频

WAN 无线通讯

启用 / 禁用 WiFi 模块的连接。

蓝牙控制

启用 / 停用 蓝牙 (Bluetooth) 的连接。

深度睡眠

在计算机关闭时，配置深度睡眠模式以节能。

交流 / 电源断电恢复

选择电源故障后的电源状态。如果选择 [关机]，则在电源恢复后电源将保持关闭。如果选择 [开机]，则在电源恢复后系统将开始启动。

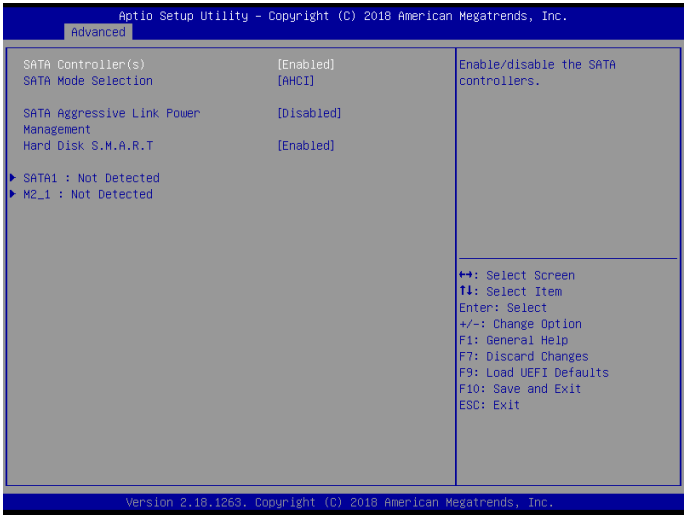
BIOS 锁定

开启 / 关闭 PCH BIOS 锁定功能。开启此项目可确保闪存的系统管理模式（SMM）保护。

性能模式

开启 / 关闭性能模式。

3.4 存储配置



SATA 控制器

启用 / 禁用 SATA 控制器。

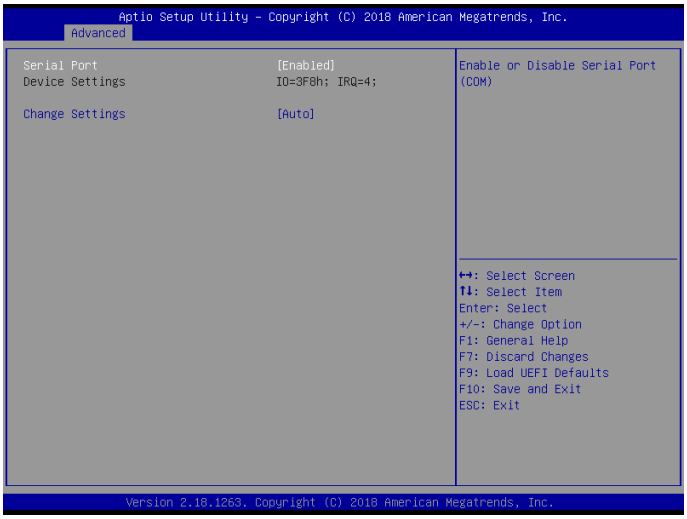
SATA 主动式链接电源管理

允许 SATA 设备在不活动期间进入低能耗以达到节能目的。仅 AHCI 模式支持。

硬盘 S.M.A.R.T.

S.M.A.R.T 表示自我监控、分析和报告技术。它是计算机硬盘的监控系统，用来检测和报告不同的可行性指标。

3.5 超级 IO 配置



串行端口

启用或禁用串行端口。

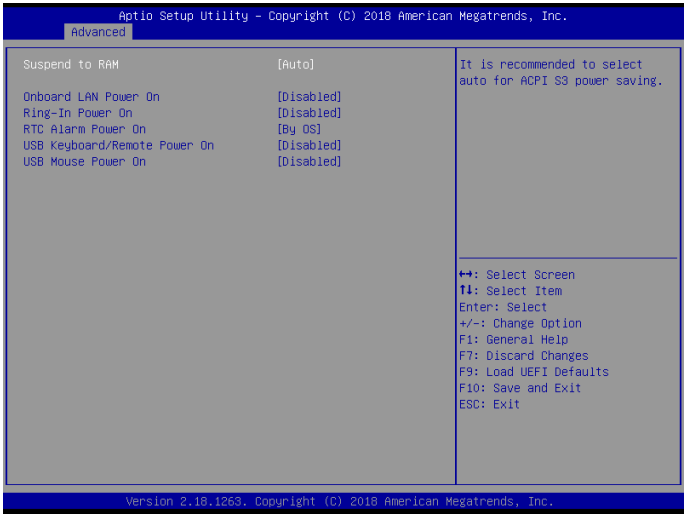
設備模式

根据所連接的設備選擇設備模式。

更改設置

選擇并行端口的地址。

3.6 ACPI 配置



挂起到內存

选择禁用执行 ACPI 挂起类型 S1。建议选择自动以实现 ACPI S3 节能。

通过板载网络唤醒

允许系统通过板载网络唤醒

振铃开机

允许通过板载 COM 端口调制解调器来电铃声信号唤醒系统。

定时开机

允许通过实时时钟开机。将其设置为 By OS（由操作系统）可以让您的操作系统处理它。

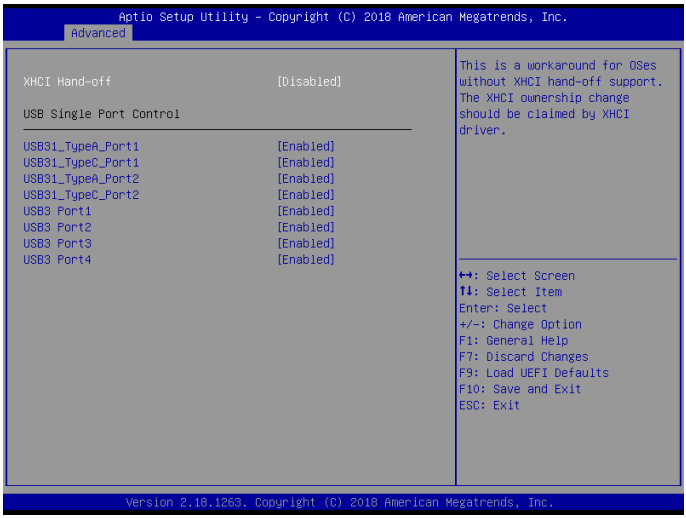
USB 键盘 / 远程开机

允许通过键盘或遥控器唤醒系统。

USB 鼠标开机

允许通过 USB 鼠标唤醒系统。

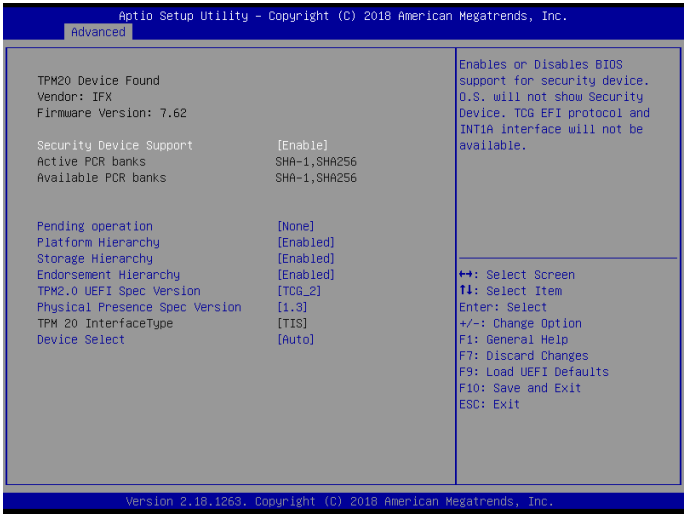
3.7 USB 配置



XHCI 接手

不支持 XHCI 接手的操作系统的工作区域。XHCI 驱动程序可更改 XHCI 所有权。

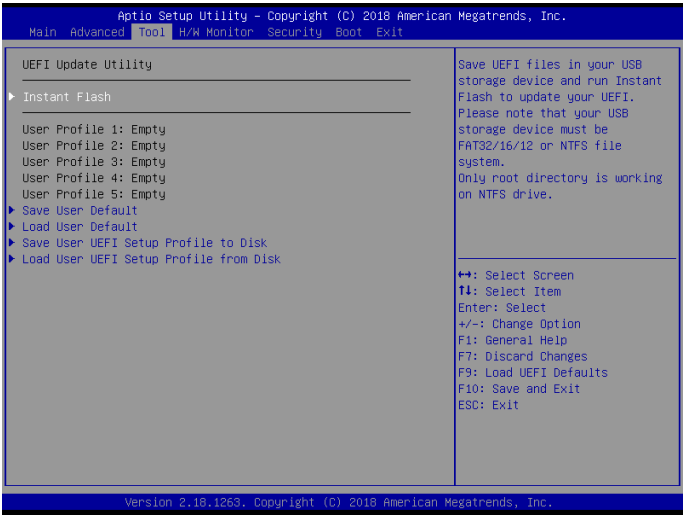
3.8 可信赖运算



安全设备支持

启用可为您的硬盘激活 Trusted Platform Module（信任平台模块，TPM）安全。

4 工具



Instant Flash

将 UEFI 文件保存在 USB 存储设备上，然后运行 Instant Flash 以更新您的 UEFI。

保存用户默认设置

输入一个配置文件名，然后按 enter 将您的设置保存为用户默认值。

加载用户默认设置

加载以前保存的用户默认值。

Save User UEFI Setup Prole to Disk (将用户 UEFI 设置配置文件保存到磁盘)

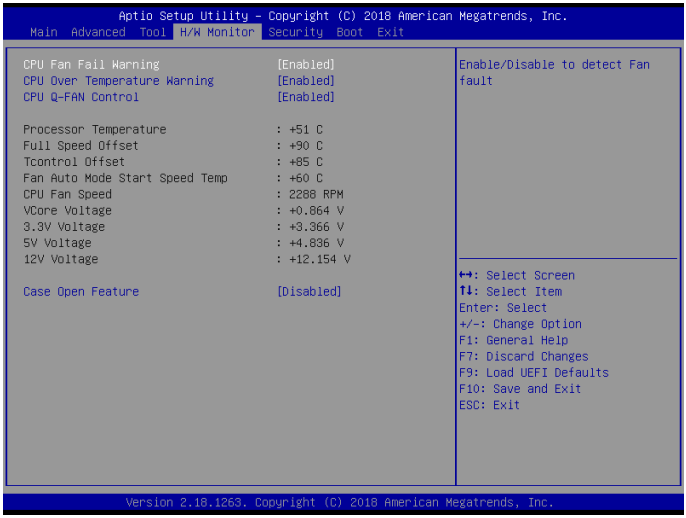
将当前 UEFI 设置作为用户默认配置文件保存到磁盘。

Load User UEFI Setup Prole from Disk (从磁盘加载用户 UEFI 设置配置文件)

从磁盘加载以前保存的用户默认值。

5 硬件监视器

此部分可以让您系统中监控硬件的状态，包括 CPU 温度、主板温度、风扇速度和电压等参数。



CPU 风扇失败警告

开启或关闭风扇失败警告功能。

CPU 过热警告

开启或关闭 CPU 过热警告功能。

CPU Q-Fan 控制

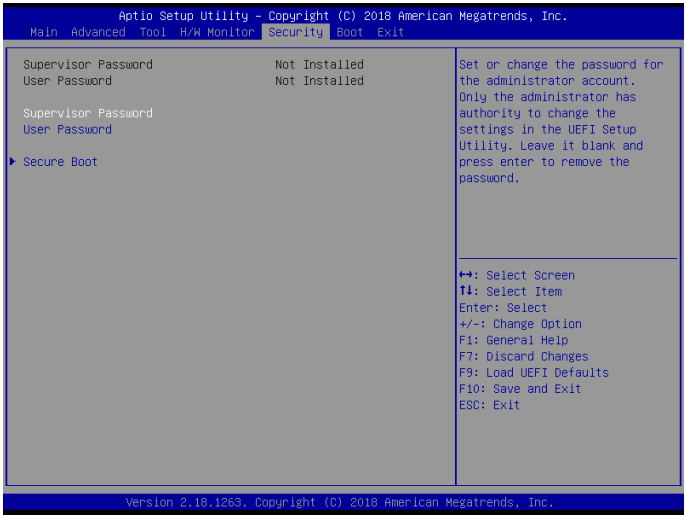
开启或关闭 CPU Q-Fan 控制功能。

机箱打开功能

启用或禁用 Case Open Feature (机箱打开功能) 以检测机箱盖是否已卸下。

6 安全

在此部分中，您可以设置或更改系统的监督人 / 用户密码。您也可以清除用户密码。



超级用户密码

设置或更改管理员帐户的密码。只有管理员有权更改 UEFI Setup Utility 中的设置。将其留白并按 enter 删除密码。

用户密码

设置或更改用户帐户的密码。用户不能更改 UEFI Setup Utility 中的设置。将其留白并按 enter 删除密码。

安全引导

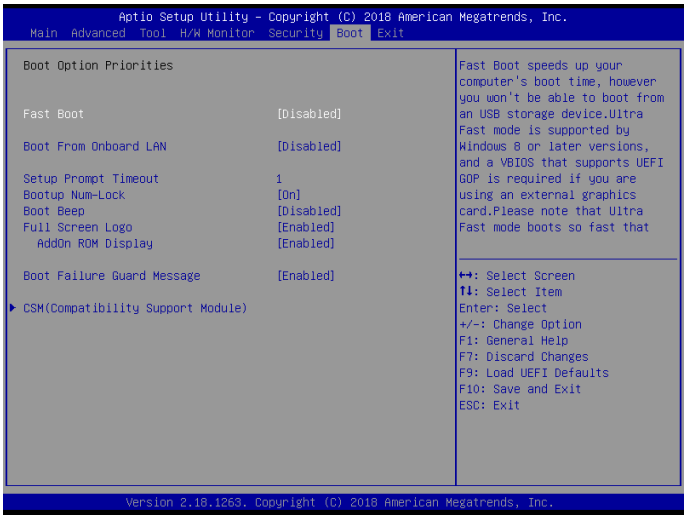
启用可支持 Windows 8.1 安全引导。

TPM 设备选择

开启 / 关闭 ME 中的 Intel PTT。关闭此项目来使用独立 TPM 模块。

7 引导

此部分显示系统上可用的设备，以供您配置引导设置和引导优先级。



闪速启动

闪速启动可使计算机引导时间最小化。在快速引导模式中，您不能从 USB 存储设备中引导。超快模式只有 Windows 8.1 支持，并且如果您使用外部图形卡，VBIOS 还必须支持 UEFI GOP。请注意，超快模式的引导非常快，您进入此 UEFI Setup Utility 的唯一方式是清除 CMOS 或在 Windows 中重新启动 UEFI 实用程序。

从板载 LAN 引导

允许通过板载 LAN 唤醒系统。

设置提示超时

配置等待设置热键的秒数。

引导时数字锁定键

选择在系统启动时数字锁定键关闭还是打开。

引导蜂鸣声

选择在系统启动时引导蜂鸣声关闭还是打开。请注意，需要蜂鸣器。

全屏徽标

启用可显示引导徽标，禁用可显示正常 POST 信息。

附加 ROM 显示

启用附加 ROM 显示可看到附加 ROM 信息，或配置附加 ROM（如果您已启用了全屏徽标）。禁用可取得更快引导速度。

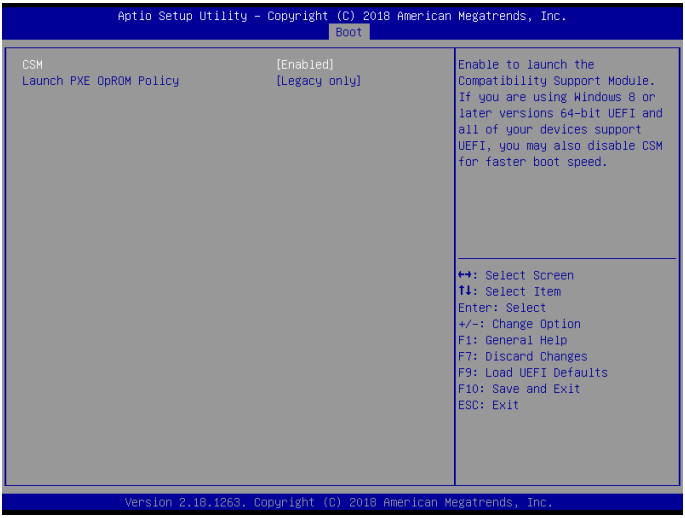
引导故障保护

如果计算机多次引导失败，则系统会自动恢复默认设置。

引导故障保护计数

配置系统自动恢复默认设置之前的引导尝试次数。

CSM（兼容性支持模块）



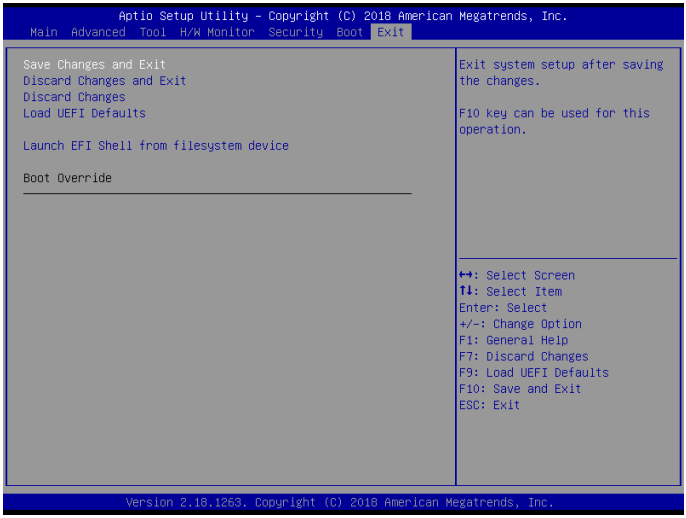
CSM

启用可启动兼容性支持模块。请勿禁用它，除非您正在运行 WHCK 测试。如果您使用 Windows 8.1 64-bit 并且所有您的设备支持 UEFI，则您也可以禁用 CSM 以取得更快引导速度。

启动 PXE OpROM 策略

选择仅 UEFI 可运行只支持 UEFI 选件 ROM 的项目。选择仅传统可运行只支持传统选件 ROM 的项目。选择 “不要开启” 以放弃执行 legacy 与 UEFI 选配 ROM。

8 退出



保存更改并退出

选择此选项时以下信息“保存配置更改并退出设置？”会弹出。选择 [确定] 可更改并退出 UEFI SETUP UTILITY。

放弃更改并退出

选择此选项时以下信息“放弃更改并退出设置？”会弹出。选择 [确定] 可退出 UEFI SETUP UTILITY 而不保存任何更改。

放弃更改

选择此选项时以下信息“放弃更改？”会弹出。选择 [确定] 放弃所有更改。

加载 UEFI 默认值

加载所有选项的 UEFI 默认值。可以使用 F9 键执行此操作。

从文件系统设备中启动 EFI Shell

将 shellx64.efi 复制到 root（根）目标以启动 EFI Shell。