

英特尔® 台式机主板
BIOS 设置词典 – 按菜单

BIOS Setup 程序可用于查看和更改计算机的 BIOS 设置。在开机自检 (POST) 内存测试开始之后，操作系统开始启动之前，按 <F2> 键进入 BIOS Setup 程序。将显示以下菜单：

菜单标题	用途
Maintenance	清除密码并显示处理器信息。 仅当台式机主板处于配置模式 (Configure Mode) 时才会显示 Maintenance 菜单。
Main	显示处理器和内存配置。
Configuration	配置通过芯片组提供的高级功能。
Performance	用于对 CPU、内存和总线设置进行高级配置。
Security	设置密码和安全功能。
Power	配置电源管理功能和电源控制。
Boot	选择启动选项。
Intel® ME	配置英特尔® 管理引擎和英特尔® 主动（或标准）管理技术的选项。
Exit	保存或放弃对 Setup 程序选项的更改。

所显示的菜单和 BIOS 设置取决于您的主板型号、所安装的硬件组件以及 BIOS 版本。BIOS 菜单标题可能有所不同。

如果对 BIOS 设置作出更改后出现任何问题（性能较差、间歇性问题等），请将台式机主板重置为默认值：

1. 启动时，按 F2 进入 BIOS 设置程序。
2. 按 F9 设置默认值。
3. 按 F10 保存并退出。

如果在更改 BIOS 设置后系统锁住或无法启动，请按以下链接中的说明执行 BIOS 恢复：
<http://support.intel.com/support/cn/motherboards/desktop/sb/CS-023360.htm>。

Boot

BIOS 设置	选项	说明/用途
Boot Device Priority	<ul style="list-style-type: none"> • Removable Devices • Optical Drive • Hard Disk Drive • Ethernet 	指定从可用设备启动的顺序。根据具体的主板型号和硬件配置，选项列表可能有所不同。
Boot Drive Order	取决于已安装的可启动设备	<p>用于指定从可用启动设备类型启动的顺序。</p> <p>列表中将包含检测到的所有可启动设备。用户可以更改设备的顺序。BIOS 将尝试按照此列表中的顺序，依次从各个设备启动。</p>
Boot Menu Type	<ul style="list-style-type: none"> • Normal • Advanced 	<p>Normal: 用于根据设备的类型设置启动优先顺序。</p> <p>Advanced: 无论设备属于哪种类别，都可以设置各个设备的启动优先顺序</p>
Boot to Network	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用从网络 (PXE) 启动。
Boot to Optical Devices	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用从光盘设备 (CD/DVD) 启动。
Boot to Removable Devices	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用从可移除设备启动。
Boot USB Devices First	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: BIOS 将尝试按照此列表中的顺序，依次从各个设备启动。</p> <p>Disable: 将使用正常的启动顺序。</p>
Fast Boot	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用快速启动功能。</p> <p>要在不进入 BIOS 设置界面的情况下禁用“快速启动”，请关闭系统 5 秒钟，然后按住电源按钮 2 秒钟将其重新打开（系统将发出蜂鸣声）。</p>
General Optimization	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: BIOS 的启动将更快，不过下列功能将被禁用：Boot to Network（引导至网络）、Boot to Optical Devices（引导至光学设备）和 Boot to Removable Devices（引导至移动设备）</p> <p>RAID 设备仍可启动，但不可配置。</p> <p>启用 Fast Boot 时会显示这项 BIOS 设置。</p>
Hard Drive Order	Lists all installed hard drive devices	<p>允许设置从硬盘（Boot Menu type 设为 normal 时使用）启动的顺序</p> <p>列表中将包含检测到的所有硬盘。您可以更改设备的顺序。尝试启动至硬盘时，BIOS 将按照此列表的顺序尝试从各个设备启动。</p>

Optical Drive Order	列出所有已安装的光盘设备 (CD/DVD)	选择从光盘设备启动的顺序。列表中将包含检测到的所有光盘设备。用户可以更改设备的顺序。尝试从光盘设备启动时，BIOS 将按照此列表的顺序尝试从各个设备启动。
Removable Drive Order	列出所有已安装的可移除设备	用于设置从可移除设备（软盘、USB 盘等）启动的顺序 - Boot Menu type 设置为 normal 时使用。 列表中将包含检测到的所有可移除设备。用户可以更改设备的顺序。尝试从可移除设备启动时，BIOS 将按照此列表的顺序尝试从各个设备启动。
UEFI boot	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用统一可扩展固件接口 (UEFI) 启动。必须启用 UEFI 启动，才能从容量大于 2 TB（兆兆字节）的驱动器启动。</p> <p>Enable: BIOS 在使用旧的启动顺序之前，将尝试通过 UEFI 启动。</p> <p>Disable: BIOS 将使用旧的启动顺序。</p> <p>有关 UEFI 的信息，请访问 http://www.uefi.org/home</p>
USB Boot	<ul style="list-style-type: none"> • Enable • Disable 	启用/禁用从 USB 启动设备进行启动。
USB Optimization	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 直到操作系统启动后，所有 USB 设备才可用，但 BIOS 的启动将更快。</p> <p>Disable: 在操作系统启动前，USB 设备将可用，但 BIOS 的启动较慢。</p> <p>安装了用户密码或硬盘密码时，无法启用此功能。</p> <p>这项 BIOS 设置在已启用 Fast Boot 时显示。</p>
Video Optimization	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: BIOS 将仅显示文本，但启动速度更快。</p> <p>Disable: BIOS 将显示标志，但启动较慢。</p> <p>在操作系统启动后，此功能并不影响视频功能。</p> <p>这项 BIOS 设置在已启用 Fast Boot 时显示。</p>

Boot > Boot Display Options

BIOS 设置	选项	说明/用途
Display F10 to Enter Boot Menu	<ul style="list-style-type: none"> • Enable • Disable 	如果启用，BIOS 将显示“F10 to Enter Boot Menu”提示。即使禁用此提示，仍将接受 F10 键输入。
Display F12 for Network Boot	<ul style="list-style-type: none"> • Enable • Disable 	如果启用，BIOS 将显示“F12 for Network Boot”提示。即使禁用此提示，仍将接受 F12 键输入。

Display F2 to Enter Setup	<ul style="list-style-type: none"> • Enable • Disable 	如果启用，BIOS 将显示“F2 to Enter Setup”提示。即使禁用此提示，仍将接受 F2 键输入。
Display F7 to Update BIOS	<ul style="list-style-type: none"> • Enable • Disable 	如果启用，BIOS 将显示“F7 to Update BIOS”提示。即使禁用此提示，仍将接受 F7 键输入。
Display F9 for Remote Assistance	<ul style="list-style-type: none"> • Enable • Disable 	如果设置为“Enable”，BIOS 将显示“F9 for Remote Assistance”提示。即使禁用此提示，仍将接受 F9 键输入。 <i>BIOS 设置仅在主板支持 Remote Assistance 时才显示。</i>
Expansion Card Text	<ul style="list-style-type: none"> • Disable • Enable • Hide all 	Disable: 在开机自检期间，BIOS 将仅从大容量存储 PCI 选项 ROM 显示文本。 Enable: 在开机自检期间，BIOS 将从任意 PCI 选项 ROM 显示文本。 Hide All: 在开机自检期间，BIOS 将不会从 PCI 选项 ROM 显示文本。
POST Code Routing	<ul style="list-style-type: none"> • Onboard • PCI 	端口 80h、84-86h、88h、8C-8Eh 的路由方式。 Onboard: 将 BIOS 开机自检代码发送到板载开机自检代码 LED 显示屏上 PCI: 将 BIOS 开机自检代码发送到 PCI 总线（PCI 插槽中的开机自检卡）
POST Function Hotkeys Displayed	<ul style="list-style-type: none"> • Enable • Disable 	如果启用，BIOS 将在开机自检期间显示功能键提示。即使禁用此提示，仍将接受功能键输入。

Configuration > Event Log

BIOS 设置	选项	说明/用途
Clear Event Log	<ul style="list-style-type: none"> • Disable • Enable <p>或</p> <ul style="list-style-type: none"> • Yes • No 	Enable (Yes) 放弃事件日志中的所有事件并在退出 BIOS 时将选项重置为 Disable (No) 。
Event Logging	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用事件日志记录。如果启用，BIOS 将在 NVRAM 中记录开机自检错误。

Configuration > Fan Control & Real-Time Monitoring

BIOS 设置	选项	说明/用途
All-On Temperature	数值	定义风扇控制子系统使风扇全速运转时的温度。
Control Mode	<ul style="list-style-type: none"> • Minimum • Off • Manual 	选择风扇的控制方式。 Minimum: 设置风扇的最小占空比。 Off: 将占空比设置为 0。 Manual: 指定准确的占空比。

Control Temperature	数值	定义风扇控制子系统尝试为此设备保持的温度。
Current Duty Cycle	仅供参考	显示风扇的当前占空比。
Current Fan Speed	仅供参考	显示风扇的当前速度。
Current Reading	仅供参考	对于温度传感器： 显示当前温度。 对于电压传感器： 显示当前电压。
Damping	<ul style="list-style-type: none"> • Low • Normal • High 	帮助减小风扇高速响应所产生的振动。 设定值越高，产生的振动就越小，但可能会使温度响应变慢。
Fan Type	仅供参考	显示检测到的风扇类型。
Fan Usage	<ul style="list-style-type: none"> • Unknown • CPU • System • MCH • VREG • Chassis • Inlet • Outlet • PSU • PSU In • PSU Out • HDD • Video • Aux • IOH • PCH • Memory 	选择风扇的使用方式。
Maximum Duty Cycle	数值	设置风扇正常使用时的最大占空比。
Minimum Duty Cycle	数值	选择风扇的最小占空比。
Over-Temperature Threshold	数值	将温度定义为运行时应用程序发出警报时的温度或高于此温度。
Over-Voltage Threshold	用户自定义	将电压定义为运行时应用程序发出警报时的电压或高于此电压。
Responsiveness	<ul style="list-style-type: none"> • Slow • Normal • Aggressive 	定义风扇速度根据温度变化而改变的速度。
Restore Default Configuration	Continue? (Y/N)	如果选择此问题，将删除 BIOS 风扇控制配置并加载默认值。 这并不影响任何其他 BIOS Setup 设置。
Under-Speed Threshold	数值	设置一个阈值，如果 RPM 中的速度小于该设定值，则发出警报。 需要使用监控实用程序来查看此警报。
Under-Voltage Threshold	用户自定义	将电压定义为运行时应用程序发出警报时的电压或低于此电压。

Configuration > On-Board Devices

BIOS 设置	选项	说明/用途
1394	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用 IEEE 1394 支持 <i>此 BIOS 设置仅适用于包含 IEEE1394 的英特尔® 台式机主板。</i> 有关 IEEE 1394 的信息, 请访问 http://en.wikipedia.org/wiki/IEEE_1394
Audio	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用板载音频。
Bluetooth Wireless	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用板载蓝牙无线控制器。 <i>此 BIOS 设置仅适用于包含蓝牙功能的英特尔® 台式机主板。</i>
Enhanced Consumer IR	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用消费者红外通信功能。
Floppy Controller	<ul style="list-style-type: none"> • Automatic • Enable • Disable 	配置软盘控制器。 仅支持 1.44 MB 软盘。 Automatic: 如果已连接软盘, 则启用板载软盘控制器。
Internal LED Brightness Level	<ul style="list-style-type: none"> • Off • Low • Med • High 	设置主板电源开关的亮度级别。 <i>此 BIOS 设置仅适用于英特尔® 台式机主板的某些至尊版系列。</i>
Internal SPDIF/DMIC Header	<ul style="list-style-type: none"> • SPDIF Out • DMIC Mic 	设置 SPDIF 或 DMIC 的内部数字音频接口。
LAN	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用板载 LAN 控制器。
Numlock	<ul style="list-style-type: none"> • Off • On 	如果 Numlock 开启, 则键盘默认具有数字输入功能。
Parallel Port	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用并行端口。
PCI Latency Timer	<ul style="list-style-type: none"> • 32 • 64 • 96 • 128 • 160 • 192 • 224 • 248 	为总线控制设置 PCI 延迟时钟。 按时钟周期数来限制 PCI 设备可以控制 PCI 总线的时间。 仅适用于旧版 PCI 设备。
Secondary LAN	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用板载辅助 LAN 控制器。
Serial Port	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用串行端口。
Serial Port 2	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用第二个串行端口。 <i>此 BIOS 设置仅适用于包含两个串行端口的英特尔® 台式机主板。</i>

Skull Backlighting	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用板载骷髅头指示灯上的背光功能。</p> <p><i>此 BIOS 设置仅适用于英特尔® 台式机主板的某些至尊版系列。</i></p>
Thunderbolt™ Controller	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用板载 Thunderbolt™ 控制器。</p> <p><i>这项 BIOS 设置仅适用于包含 Thunderbolt 控制器的英特尔® 台式机主板。</i></p>
Trusted Platform Module	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用可信平台模块 (TPM)。</p> <p><i>此 BIOS 设置仅适用于支持可信平台模块 (TPM) 的英特尔® 台式机主板。</i></p> <p><i>有关 TPM 的信息, 请访问</i> http://en.wikipedia.org/wiki/Trusted_Platform_Module</p>

Configuration > On-Board Devices > Audio

BIOS 设置	选项	说明/用途
Front Panel Audio	<ul style="list-style-type: none"> • Auto • High Definition Front Panel • Legacy Front Panel • Disable 	<p>自动或手动选择所安装音频前面板的类型。</p> <p>Auto: 尝试检测所安装的音频前面板是否存在及其类型</p> <p>High Definition Front Panel: 将音频前面板配置为“High Definition Mode”</p> <p>Legacy Front Panel: 将音频前面板配置为“Legacy Mode”</p> <p>Disable: 禁用音频前面板</p>
HDMI/Display Port Audio	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: HDMI/DisplayPort 输出包括音频和视频。</p> <p>Disable: HDMI/DisplayPort 输出仅包括视频。</p>

Configuration > On-Board Devices > Parallel Port

BIOS 设置	选项	说明/用途
Mode	<ul style="list-style-type: none"> • Output only • Bi-directional • EPP • ECP 	<p>允许选择并行端口的模式。此选项仅在启用了并行端口时才可用。</p> <p>Output Only: 在 AT* 兼容模式下运行。</p> <p>Bi-directional: 在 PS/2 兼容模式下运行。</p> <p>EPP: 增强型并行端口模式, 这是非打印机外设的高速双向模式。</p> <p>ECP: 扩展性能端口模式, 这是打印机和扫描仪的高速双向模式。</p>

Configuration > On-Board Devices > Skull Backlighting

BIOS 设置	选项	说明/用途
Skull Eye Hard Drive Activity	<ul style="list-style-type: none"> • Enable • Disable 	<p>根据硬盘的活动状态点亮骷髅头的眼睛。</p> <p><i>此 BIOS 设置仅适用于英特尔® 台式机主板的某些至尊版系列。</i></p>

Configuration > On-Board Devices > USB

BIOS 设置	选项	说明/用途
Backward Compatibility Mode	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 使用旧版 USB 控制器模式，它与旧版或稳定性较弱的 USB 设备的兼容性可能更好。此模式还将禁用 USB 端口的单独控制，并会导致英特尔® 主动管理技术的一些功能（如 KVM）无法正常工作。</p>
Charging Scheme	<ul style="list-style-type: none"> • Auto • USB-Compliant • Alternative 	<p>选择当 Portable Device Charging Mode 处于活动状态时要使用的电气方案：</p> <p>Auto: 尝试自动检测兼容性最好的收费方案。</p> <p>USB-Compliant: 使用 USB 兼容的收费方案。</p> <p>Alternative: 使用其他收费方案。</p>
Portable Device Charging Mode	<ul style="list-style-type: none"> • Off • Charging in S3/S4/S5 • Charging Only 	<p>标为黄色的 USB 端口以较高的最大电流支持一种移动设备收费模式。</p> <p>Off: 正常 USB 操作：USB 端口在 S3/S4/S5 中不提供额外的电源</p> <p>Charging in S3/S4/S5: USB 端口在 S3/S4/S5 中提供额外的电源</p> <p>Charging Only: USB 端口将一直提供额外的电源，但不能用来传输数据</p>
Secondary USB 3.0 Controller	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用辅助 USB 3.0 控制器以及所有路由到它的 USB 端口。这并不影响路由到芯片组 USB 3.0 控制器的 USB 端口。</p>
USB 3.0 Controller	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用所有 USB 3.0 端口和 USB 3.0 控制器。USB 3.0 端口为蓝色，位于后面板上，在图中表示为 USB*。</p>
USB Legacy	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 USB 传统支持。</p> <p>USB 传统支持允许在本身不支持 USB 的操作系统上支持 USB。禁用 USB 传统支持将不会在 BIOS 开机自检期间禁用 USB 键盘，包括 BIOS SETUP 和选项 ROM。</p>

USB Port x	<ul style="list-style-type: none"> • Enable • Disable • No Detect 	<p>用于启用或禁用单个 USB 端口。</p> <p>如果将 USB 键盘连接到已在 BIOS 中禁用的 USB 端口，则将在开机自检和 Setup 期间启用该端口，但会在操作系统启动之前禁用该端口。</p> <p>在开机自检和 Setup 期间以及在操作系统中将禁用所有非键盘设备。这意味着连接到已禁用 USB 端口的驱动器将不会出现在 Setup 的 BIOS 启动顺序中。</p> <p>No Detect: 在 POST 期间跳过所选端口上的 USB 设备检测。操作系统仍然能检测和使用所有插入系统的 USB 设备。这样可以更快地启动，同时仍可以在操作系统中使用 USB 设备。</p>
------------	--	---

Configuration > PCI/PCIe Add-In Slots

BIOS 设置	选项	说明/用途
FLR Capability	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用功能级重置 (FLR)，可允许单独重置 PCH 设备。
PCI/PCIe Slot Information	仅供参考	<p>对于主板上的每个插槽，都会显示以下信息：</p> <ul style="list-style-type: none"> • 插槽编号（必须与主板的丝网印刷面匹配） • 插槽类型（PCI 或 PCIe） • PCIe 插槽电气宽度 • PCIe 插槽协商宽度 • 数据传输速度

Configuration > SATA Drives

BIOS 设置	选项	说明/用途
Back Panel 61XX eSATA (Gen 2)	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用后面板 eSATA 接口。
Chipset-SATA Mode	<ul style="list-style-type: none"> • IDE • RAID • AHCI 	<p>IDE: 兼容模式下会禁用 AHCI 支持。</p> <p>AHCI: 支持高级 SATA 功能，例如全速命令队列 (Native Command Queuing)。</p> <p>RAID: 允许将多个驱动器合并到较大的卷中以提高性能和/或可靠性。始终启用 AHCI。</p> <p>警告：如果安装操作系统后更改了此设置，则操作系统可能无法启动。</p>
Detected Discrete-SATA Device	仅供参考	显示设备标识字符串、容量 (GB) 和连接到离散 SATA 端口的设备的协商速度（1.5Gb/秒、3.0Gb/秒或 6.0Gb/秒）。
Detected RAID Volume	仅供参考	如果配置了 RAID，将显示每个 PCH SATA RAID 卷的名称和容量 (GB)。

Detected SATA Drive	仅供参考	显示设备标识字符串、容量 (GB) 和连接到 SATA 端口的设备的协商速度 (1.5Gb/秒、3.0Gb/秒或 6.0Gb/秒)。
Detected Secondary SATA Device	仅供参考	显示设备标识字符串、容量 (GB) 和连接到辅助 SATA 端口的设备的协商速度 (1.5 Gb/s、3.0 Gb/s 或 6.0 Gb/s)。
Discrete SATA	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用 Discrete SATA Controller。 BIOS 屏幕中显示的其他帮助文本将随主板而异。
Discrete SATA Mode	<ul style="list-style-type: none"> • IDE • RAID 	IDE: 兼容模式下会禁用 RAID 支持。 RAID: 允许将多个驱动器合并到较大的卷中以提高性能和/或可靠性。 Warning: 如果安装操作系统后更改了此设置, 则操作系统可能无法启动。
eSATA Controller Mode	<ul style="list-style-type: none"> • IDE • RAID 	后面板 eSATA 端口支持 BIOS 中的 IDE 和 RAID (无 AHCI) 模式。 引导至加载了驱动程序的操作系统后, 所有 SATA 控制器支持将取决于操作系统驱动程序。 注意: 不能跨 SATA 驱动程序控制器共享 RAID 阵列 (x6 ICH10 2 代黑色端口、x2 离散型 3 代蓝色端口以及 x2 eSATA 2 代红色端口)。
eSATA Port x Hot Plug Capability	<ul style="list-style-type: none"> • Enable • Disable 	如果启用此功能, SATA 端口将被报告为支持热插拔。
eSATA Ports	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用外部 SATA (eSATA) 端口。 有关 eSATA 的信息, 请访问 http://en.wikipedia.org/wiki/Esata#External_SATA
External eSATA Port	仅供参考	显示设备标识字符串、容量 (GB) 和连接到 SATA 端口的设备的协商速度 (1.5 Gb/秒、3.0 Gb/秒或 6.0 Gb/秒)。如果未连接设备, 将显示 [Not Installed] 字符串。
Hard Disk Pre-Delay	<ul style="list-style-type: none"> • Disable • 3 Seconds • 6 Seconds • 9 Seconds • 12 Seconds • 15 Seconds • 21 Seconds • 30 Seconds 	硬盘初始化之前的延迟时间 (秒)。 此设置可用于延长 BIOS 启动屏幕的显示时间。 可用的时间选项可能因具体主板而异。
Internal 91XX Blue SATA (Gen 3)	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用内部的蓝色 SATA 接口。
mSATA Port	仅供参考	显示设备标识字符串、容量 (GB) 和连接到 SATA 端口的设备的协商速度 (1.5 Gb/秒、3.0 Gb/秒或 6.0 Gb/秒)。如果未连接设备, 将显示 [Not Installed] 字符串。
mSATA Port x Hot Plug Capability	<ul style="list-style-type: none"> • Enable • Disable 	如果启用此功能, SATA 端口将被报告为支持热插拔。

No SATA Devices Detected	仅供参考	启用了离散 SATA，但在离散 SATA 端口未检测到设备时会出现此设置。
S.M.A.R.T.	<ul style="list-style-type: none"> • Auto • Disable • Enable 	<p>启用或禁用对硬盘 S.M.A.R.T.（自我监测分析与报告技术）功能的支持。当前所有硬盘都支持 S.M.A.R.T.。使用 S.M.A.R.T.，可以对即将发生的硬盘故障提前进行预测并发出警告。</p> <p>如果要使用支持 S.M.A.R.T. 的实用程序来监测硬盘的状态，则应该启用该功能。</p> <p><i>有关 S.M.A.R.T. 的信息，请访问</i> http://en.wikipedia.org/wiki/Self-Monitoring,_Analysis,_and_Reporting_Technology</p>
SATA Controller Mode	<ul style="list-style-type: none"> • IDE • AHCI 	<p>在 BIOS Setup 中仅可选择 IDE 和 AHCI，但 SATA Gen 3 controller Option ROM 中提供 RAID mode（在启动时按 Control-M 进入菜单）。</p> <p>注：不能跨 SATA 驱动程序控制器共享 RAID 阵列（x6 ICH10 2 代黑色端口、x2 离散型 3 代蓝色端口以及 x2 eSATA 2 代红色端口）。</p>
SATA Port x	仅供参考	显示设备标识字符串、容量 (GB) 和连接到 SATA 端口的设备的协商速度（1.5 Gb/秒、3.0 Gb/秒或 6.0 Gb/秒）。如果未连接设备，将显示 [Not Installed] 字符串。
SATA Port x Hot Plug Capability	<ul style="list-style-type: none"> • Enable • Disable 	如果启用此功能，SATA 端口将被报告为支持热插拔。
Secondary SATA	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用辅助 SATA 控制器。辅助 SATA 控制器支持后面板上的 2 个蓝色内部 SATA 端口和 2 个 eSATA 端口。</p> <p>BIOS 画面中将提供有关主板的更多帮助内容。</p>
Secondary SATA Mode	<ul style="list-style-type: none"> • IDE • AHCI • RAID 	<p>IDE: 兼容模式下会禁用 RAID 支持。</p> <p>AHCI: 支持高级 SATA 功能，例如本机命令队列 (Native Command Queuing)。</p> <p>RAID: 允许将多个驱动器合并到较大的卷中以提高性能和/或可靠性。</p> <p>Warning: 如果安装操作系统后更改了此设置，则操作系统可能无法启动。</p>

Configuration > Video

BIOS 设置	选项	说明/用途
Detected Video Device Priority	将列出检测到的视频设备	将主视频适配器设置为 Manual 时，检测到的每个视频设备都将在此处列出，您可以选择启动期间使用的视频设备的优先顺序。

<p>IGD DVMT Memory</p>	<ul style="list-style-type: none"> • 32 MB • 64 MB • 128 MB • 256 MB • Maximum DVMT 	<p>动态视频内存技术 (DVMT) - 允许您选择分配给集成显卡 (IGD) 视频的系统内存量。</p> <p>英特尔动态视频内存技术 3.0 (DVMT3.0) 允许根据应用程序的需要来分配用于显卡的额外内存。应用程序关闭后，将释放分配给显卡的内存，并且这些内存可供系统使用。</p> <p>可用选项可能因主板而异。</p> <p><i>有关 DVMT 的信息，请参考 Intel® Graphics Media Accelerator 900 White Paper</i> http://www.intel.com/design/chipsets/applnots/30262403.pdf</p>
<p>IGD Flat Panel</p>	<ul style="list-style-type: none"> • Disable • LVDS • eDP 	<p>Disable: 禁用视频 BIOS LVDS 与电子数据处理输出。BIOS 将使用“IGD Primary Video Port” (IGD 主视频端口) 以实现多显示器支持配置。</p>
<p>IGD Primary Video Port</p>	<ul style="list-style-type: none"> • Auto • VGA Analog • DVI-I (Blue) • Analog DVI-I (Blue) • Digital DVI-D (White) • HDMI • LVDS • DisplayPort 	<p>允许在系统启动时选择集成显卡 (IGD) 显示界面所使用的首选项。</p> <p>Auto: 尝试检测连接的监视器，且最多可在两个端口上显示视频。</p>
<p>IGD Secondary Video Port</p>	<ul style="list-style-type: none"> • None • VGA Analog • DVI-I (Blue) • Analog DVI-I (Blue) • Digital DVI-D (White) • HDMI • LVDS • DisplayPort 	<p>允许在系统启动时选择已镜像集成显卡 (IGD) 显示界面所使用的首选项。</p>
<p>Integrated Graphics Device</p>	<ul style="list-style-type: none"> • Enable if Primary • Always Enable • Always Disable 	<p>Enable if Primary: 如果未将集成显卡 (IGD) 选为主视频适配器，则将其禁用。</p> <p>Always Enable: 即使未选为主视频适配器，也始终启用 IGD。</p> <p>Always Disable: 即使未安装其他视频设备，也始终禁用 IGD。</p>
<p>No Video Detected Error Beeps</p>	<ul style="list-style-type: none"> • Enable • Disable 	<p>未检测到视频时，启用或禁用主板喇叭蜂鸣声。</p>

PAVP	<ul style="list-style-type: none"> • Lite • Disable 	使用硬件加速来进行视频解码时，受保护音频视频路径 (PAVP) 可对内容进行保护。该设置需要支持 PAVP 的处理器/芯片组。此 BIOS 设置项目不会显示在 BIOS Setup 中，并且只能通过英特尔® 集成商工具包 (ITK) 进行访问。
Primary Video Adapter	<ul style="list-style-type: none"> • Auto • Int Graphics (IGD) • Ext PCIe Graphics (PEG) • Ext PCI Graphics • Manual 	<p>允许将特定视频控制器选为显示设备，在系统启动时将激活该设备。</p> <p>选项可能因具体配置而异。</p>

Configuration > Video > Advanced Flat Panel Display Settings

BIOS 设置	选项	说明/用途
Backlight-Off to Power-Down Delay Time (ms)	数值	指定从背光关闭到面板断电的延迟。
Brightness Steps	数值	设置向操作系统报告的显示器亮度调整步骤数。
EDID Data Source	<ul style="list-style-type: none"> • Flat Panel Display • Custom Payload • Pre-Defined 	平板显示器参数将从选定的源读取。
eDP Data Rate	<ul style="list-style-type: none"> • 1.62 Gbps • 2.70 Gbps 	设定嵌入式 DisplayPort(eDP) 链路的数据传输速率。如果信号表明链接训练期间无需 AUX 握手，则使用此设置。
eDP Interface Type	<ul style="list-style-type: none"> • Single-Lane • Dual-Lane • Quad-Lane 	设置嵌入式 DisplayPort(eDP) 连接。
Flat Panel Configuration Changes	<ul style="list-style-type: none"> • Unlocked • Locked 	锁定后，只能由英特尔® 集成商工具包来解锁。
Inverter Frequency (Hz)	数值	请参阅高压板和显示器技术指标以了解适当的值。警告：使用不支持的值可能会导致硬件受损。
Inverter Polarity	<ul style="list-style-type: none"> • Normal • Inverted 	<p>Normal: PWM = 0% (暗)</p> <p>Inverted: PWM=0% (亮)</p> <p>请参阅高压板技术指标以了解适当的值。</p>
LVDS Spread Spectrum Control	<ul style="list-style-type: none"> • Disable • +/- 0.5% Center Spread • 1.0% Center Spread 	配置 LVDS 展频时脉。

Max Inverter Current Limit (%)	数值	设置可接受的最大 PWM 以驱动高压板，该值充当显示器背光灯的电流上限值。 请参阅高压板和显示器技术指标以了解适当的值。警告：使用不支持的值可能会导致硬件受损。
Min Inverter Current Limit (%)	数值	设置可接受的最小 PWM 以驱动高压板，该值充当显示器背光灯的电流下限值。 请参阅高压板和显示器技术指标以了解适当的值。警告：使用不支持的值可能会导致硬件受损。
Panel Power Cycle Delay Time (ms)	数值	指定面板电源周期的延迟。
Panel Power-Down Delay Time (ms)	数值	指定面板断电的延迟。
Panel Power-On Delay Time (ms)	数值	指定从系统通电到面板通电的延迟。
Power-On to Backlight Enable Delay Time (ms)	数值	指定从面板加电到背光点亮的延迟。
Pre-Defined EDID Configuration	多种平板类型	允许您从视频 BIOS 中嵌入的列表内选择一种预定义 EDID 配置。

Configuration > Video > LVDS Settings

BIOS 设置	选项	说明/用途
Color Depth	<ul style="list-style-type: none"> • 18-bpp • 24-bpp (VESA) • 24-bpp (JEIDA) 	设置平板显示器色深（位/像素，bpp）和数据映射。 <i>注： 如果不支持 JEIDA，24-bpp (VESA) 将显示为“24-bpp”。</i>
LVDS Interface Type	<ul style="list-style-type: none"> • Single-Channel • Dual-Channel 	设置 LVDS 连接。
Maintain Aspect Ratio	<ul style="list-style-type: none"> • Yes • No 	允许在显卡驱动程序初始化之前选择宽高比。 Yes: 原始宽高比 No: 全屏 <i>此 BIOS 设置仅适用于支持 LVDS 的英特尔® 台式机主板。</i>

Screen Brightness	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用面板背光亮度设置。</p> <p><i>此 BIOS 设置仅适用于支持 LVDS 的英特尔® 台式机主板。</i></p>
-------------------	---	---

Exit

BIOS 设置	选项	说明/用途
Discard Changes	Continue? (Y/N)	放弃更改，但不退出 Setup。将使用计算机启动时已存在的选项值。
Exit Discarding Changes	Continue? (Y/N)	退出 BIOS setup，但不保存所做的任何更改。
Exit Saving Changes	Continue? (Y/N)	保存所有更改并退出 BIOS setup。
Load Custom Defaults	Continue? (Y/N)	BIOS 将加载 Setup 默认值。如果存在用户自定义默认值，则使用这些值。
Load Optimal Defaults	Continue? (Y/N)	BIOS 将加载 Setup 默认值。如果存在 OEM 自定义默认值，则使用这些值。此项目等效于 F9 BIOS Setup 快捷键。此项目不会对 BIOS 密码、硬盘密码或英特尔® 管理引擎菜单下的任何内容产生影响。
Save Custom Defaults	Continue? (Y/N)	BIOS 会将现有 Setup 配置保存为用户自定义默认值。

Intel® ME

BIOS 设置	选项	说明/用途
Change Intel® Management Engine Password	用户自定义	<p>必须先更改英特尔® 管理引擎的默认密码，然后再访问其他管理引擎选项。</p> <p>系统所有者应记录新的英特尔管理引擎密码，并将其存储在安全位置（保管库、保险箱或异地存储）以供将来使用。更改密码后，应更新此文档。</p>
Enter Intel® Management Engine Password	用户输入	必须先输入英特尔® 管理引擎的密码，然后再访问英特尔® 管理引擎页面上的其他选项。

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration

BIOS 设置	选项	说明/用途
Partial Intel® AMT Reset	Continue? (Y/N)	将所有英特尔® AMT 配置设置重置为出厂默认值，但不包括英特尔® 管理引擎密码、PSK (PID/PPS)、域名和主机名。
Set PRTC	用户自定义	<p>设置英特尔® AMT PRTC（受保护实时时钟）。</p> <p>以格林威治标准时间 (GMT) 格式输入 PRTC： YYYY:MM:DD:HH:MM:SS</p>

Setup and Configuration Mode	<ul style="list-style-type: none"> • Local • Remote 	<p>Local: 执行 AMT 配置, 而不与服务器通信</p> <p>Remote: 通过与服务器通信来执行 AMT 配置</p>
------------------------------	---	---

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > KVM Configuration

BIOS 设置	选项	说明/用途
Enable KVM	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 允许键盘、视频和鼠标通过 IP 重定向。视频从本地客户端重定向到远程控制台。键盘和鼠标从远程控制台重定向到本地客户端。</p> <p>Disable: 不允许使用 KVM 功能。</p>
Remote Control of Opt-in Policy	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 允许远程用户设置用户自愿加入策略。</p> <p>Disable: 阻止远程用户设置用户自愿加入策略。</p>
User Consent for Opt-in Session	<ul style="list-style-type: none"> • Required • Not Required 	<p>Required: 必须获得本地用户同意, 才能远程建立 KVM 会话。</p> <p>Not Required: 允许不经本地用户同意远程建立会话。</p>

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > Local Setup and Configuration

BIOS 设置	选项	说明/用途
Computer Name	用户自定义	设置计算机名称。
Domain Name	用户自定义	设置域名 (计算机连接到的网络的名称)。
Dynamic DNS TTL	数值	启用 DNS 动态更新后, 将设置 DDNS (动态 DNS) 存在时间值。如果设为零, 该值将为内部默认值 15 分钟或 DHCP 租用时间的 1/3。
Dynamic DNS Update	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 英特尔® 管理引擎尝试使用 DNS 动态更新协议在 DNS (域名系统) 中注册其 IP 地址和 FQDN。</p> <p>Disable: 英特尔® 管理引擎将不更新 DNS。IPv6 需要 DDNS (动态 DNS) 的专用 FQDN。</p>
Periodic Update Interval	数值	启用动态 DNS 更新后, 此设置设定发送 DDNS (动态 DNS) 更新的间隔时间
Shared/Dedicated FQDN	<ul style="list-style-type: none"> • Shared • Dedicated 	<p>Shared: 英特尔® 管理引擎与主机操作系统共享 FQDN (完全限定域名)</p> <p>Dedicated: FQDN 为英特尔® 管理引擎专用。</p>

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > Local Setup and Configuration > IPv4 TCP/IP Configuration

BIOS 设置	选项	说明/用途
Alternate DNS Address	用户自定义	输入点分十进制格式的地址 (例如: 255.255.255.0)
Default Gateway Address	用户自定义	输入点分十进制格式的地址 (例如: 255.255.255.0)
DHCP	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用英特尔® 管理引擎的 DHCP (动态主机配置协议)。
IPv4 Address	用户自定义	输入点分十进制格式的地址 (例如: 192.168.0.10)。如果已禁用 DHCP, 则该 IP 地址应该与主机操作系统 IP 地址不同。
Preferred DNS Address	用户自定义	输入点分十进制格式的地址 (例如: 255.255.255.0)
Subnet Mask	用户自定义	输入点分十进制格式的地址掩码 (例如: 255.255.255.0)

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > Local Setup and Configuration > IPv6 TCP/IP Configuration

BIOS 设置	选项	说明/用途
Alternate DNS IPv6 Address	用户自定义	输入有效的地址 (例如: 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00)
Enable IPv6	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 英特尔® 管理引擎 IPv6 地址为专用地址, 不与主机操作系统共享。</p> <p>Disable: 与主机操作系统共享英特尔® 管理引擎 IPv6 地址。</p>

IPv6 Address	用户自定义	输入有效的地址（例如： 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00）
IPv6 Default Router	用户自定义	输入有效的地址（例如： 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00）
IPv6 Interface ID	<ul style="list-style-type: none"> • Random ID • Intel ID • Manual ID 	Random ID: 随机生成 ID。 Intel ID: 使用 MAC 地址生成 ID。 Manual ID: 允许输入 64 位有效值。
IPv6 Manual Interface ID	用户自定义	如果 IPv6 Interface ID 设为 Manual ID，则允许输入 64 位有效值（例如： 1122:3344:5566:7788）。
Preferred DNS IPv6 Address	用户自定义	输入有效的地址（例如： 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00）

Intel® ME > Intel® Active（或 Standard）Management Technology Configuration > Remote Setup and Configuration

BIOS 设置	选项	说明/用途
Delete TLS Pre-Shared Key (PSK) PID/PPS	Continue? (Y/N)	删除 TLS 预共享密钥 (PSK) PID/PPS，以便可以重新设定。
Fully Qualified Domain Name (FQDN)	用户自定义	特定配置服务器的完全限定域名 (FQDN)。 FQDN 必须包含主机名和域名。
PKI DNS Suffix	用户自定义	PKI（公钥基础结构）的域名系统后缀。 该值用于验证配置服务器的证书中的 FQDN（例如： name.com）。
Provisioning Mode	仅供参考	显示当前配置模式： PKI 或 PSK 。

Provisioning Server Address IPv4/IPv6	用户自定义	输入点分十进制格式的地址。 例如, 192.168.0.10
Provisioning Server Mode	<ul style="list-style-type: none"> • OTC uses TLS-PSK • Remote Configuration uses TLS-PKI 	根据英特尔® AMT 部署策略, 选择一键配置 (使用采用预共享密钥的传输层安全协议) 或远程配置 (使用采用公钥基础结构的传输层安全协议)。
Provisioning Server Port	数值	输入配置服务器的端口。 端口号范围为 0 - 65535。
TLS Pre-Shared Key (PSK) PID	用户自定义	<p>PID (配置标识符) 是由 8 位字母数字字符组成的以破折号分隔的字符串 (例如: ABCD-123K)。</p> <p>必须同时设置 PID 和 PPS (配置口令), 才能建立安全 TLS-PSK 会话。</p>
TLS Pre-Shared Key (PSK) PPS	用户自定义	<p>PPS (配置口令) 是由 32 位字母数字字符组成的以破折号分隔的字符串 (例如: EGET-GZFF-C6A6-ORRR-HQXP-C9JI-RJGB-KBS8)。</p> <p>必须同时设置 PID (配置标识符) 和 PPS, 才能建立安全 TLS-PSK 会话。</p>

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > Remote Setup and Configuration > Manage Permanent Certificates

BIOS 设置	选项	说明/用途
Active Certificate	<ul style="list-style-type: none"> • Yes • No 	<p>确定证书哈希是否处于活动状态。 活动证书可用于远程配置 PKI 过程。</p> <p>Yes: 活动</p> <p>No: 不活动</p>
Certificate Algorithm	仅供参考	显示证书算法: SHA1、SHA256 或 SHA384。
Hash Value	仅供参考	显示永久证书或用户定义证书的哈希值。

Permanent Certificate Name	仅供参考	显示永久证书的名称。
----------------------------	------	------------

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > Remote Setup and Configuration > Manage User Defined Certificates

BIOS 设置	选项	说明/用途
Active Certificate	<ul style="list-style-type: none"> • Yes • No 	确定证书哈希是否处于活动状态。 活动证书可用于远程配置 PKI 过程。 Yes: 活动 No: 不活动
Certificate Algorithm	<ul style="list-style-type: none"> • Empty • SHA1 • SHA256 • SHA384 	算法类型必须与生成的证书哈希相匹配
Hash Value	仅供参考	显示永久证书或用户定义证书的哈希值。
User Hash Certificate #x	用户自定义	用于跟踪证书哈希的唯一可读取标识符。 可使用字母数字组成。

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > SOL/IDER Configuration

BIOS 设置	选项	说明/用途
Redirection Mode	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用重定向模式。 如果使用适用于 AMT5.0 或更早版本的旧版 SMB 重定向控制台，则必须启用重定向模式。
SOL/IDER Authentication Mode	<ul style="list-style-type: none"> • Enable • Disable 	选择 IDER 和 SOL 操作对 LAN 上接口的验证和安全保护方式。 Enable: 需要 Kerberos。 Disable: 允许采取用户名和密码身份验证。

Intel® ME > Intel® Active (或 Standard) Management Technology Configuration > View Provisioning Record

BIOS 设置	选项	说明/用途
Cert. Serial Number	仅供参考	显示证书序列号。
Cert. Type	仅供参考	显示证书类型： User Defined 、 Permanent Default 或 Not Defined 。
Date	仅供参考	显示配置日期。
Hash Data	仅供参考	将显示哈希数据。
Hash Type	仅供参考	将显示以下哈希类型： MD5 、 SHA1 、 SHA256 、 SHA512 或 Not Defined 。
Host Initiated	仅供参考	显示主机启动的状态： Yes 、 No 或 Invalid 。
Mode	仅供参考	显示配置模式： TLS-PSK 、 TLS-PKI 或 Not Defined 。
Provisioning Record Details	仅供参考	将显示以下配置信息： <ul style="list-style-type: none"> • Mode • Server IP Address • Server FQDN • Date • Time Validity Pass • Secure DNS • Host Initiated • Hash Data • Hash Type • Cert. Serial Number • Cert. Type
Secure DNS	仅供参考	显示安全 DNS： Yes 、 No 或 Invalid 。

Server FQDN	仅供参考	显示配置服务器 FQDN。
Server IP Address	仅供参考	显示配置服务器的 IP 地址。
Time Validity Pass	仅供参考	显示时间有效性检查通过: Yes 、 No 或 Invalid 。

Intel® ME > Intel® Management Engine Configuration

BIOS 设置	选项	说明/用途
Deep S4/S5	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 deep S4/S5。</p> <p>启用此设置将处于 S4/S5 睡眠状态, 耗电量较少, 但只能通过电源按钮或 RTC 警报从 S4/S5 唤醒。</p>
Idle Timeout	用户自定义	<p>0 和 65535 之间的值。设置英特尔® 管理引擎进入睡眠状态之前的空闲时间 (分钟)。</p> <p>默认值为 0。使用此设置, 英特尔® 管理引擎将不会进入睡眠状态, 因此无法节电。</p> <p><i>此选项仅在启用了“Turn on Intel® ME in Sleep States”时才可用。</i></p>
Manageability Feature	<ul style="list-style-type: none"> • None • Intel® AMT • Intel® Standard Manageability 	<p>None: 为默认值; 在此设置下, 您可以启用/禁用板载 LAN。</p> <p>Intel® AMT: 启用英特尔® 主动管理技术 – 有关更多信息, 请访问 http://www.intel.com/technology/platform-technology/intel-amt/</p> <p>Intel® Standard Manageability: 启用标准可管理性功能。</p> <p>选择 AMT 还是 Standard Manageability 取决于所安装的处理器的芯片组。</p>
ME Wake from S3, S4, S5	<ul style="list-style-type: none"> • Enable • Disable 	<p>确定系统处于睡眠状态时英特尔® 管理引擎的状态。</p> <p>Enable: 允许在 S3、S4 或 S5 期间唤醒管理引擎。</p> <p>Disable: 阻止在 S3、S4 或 S5 期间唤醒管理引擎。</p>

Main

BIOS 设置	选项	说明/用途
Active Processor Cores	<ul style="list-style-type: none"> • All • 1 • 2 	<p>用于选择每个处理器封装中要启用的内核数。</p> <p><i>此 BIOS 设置仅在安装了多核处理器时才显示。</i></p>
BIOS Version	仅供参考	显示当前安装的 BIOS 版本。
Host Clock Frequency	仅供参考	显示默认主机时钟频率 (MHz)
Intel® Hyper-Threading Technology	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用超线程技术。</p> <p>如果禁用，每个活动内核将只有一个可用线程。</p> <p><i>如果安装了支持超线程技术的处理器，此 BIOS 设置仅适用于支持超线程技术的英特尔® 台式机主板。</i></p> <p><i>有关超线程技术的信息，请访问</i> http://en.wikipedia.org/wiki/Hyperthreading</p>
L3 Cache RAM	仅供参考	<p>显示所安装处理器的三级高速缓存内存总量 (MB)。</p> <p><i>此设置在所安装的处理器支持三级高速缓存时才可用。</i></p>
Memory Channel x Slot y	仅供参考	<p>显示 Channel x Slot y 中所安装系统的内存大小 (GB)。</p> <p>会针对主板上的每个内存插槽显示一行。这些行会根据内存插槽与处理器的距离按顺序显示，离处理器最近的插槽显示在最前面。</p> <p>实例： Memory Channel A Slot 0 2 GB Memory Channel B Slot 0 1 GB</p>
Memory Speed	仅供参考	显示当前内存速度。定义为当前主机时钟频率乘以内存倍频。
Overridden Host Clock Frequency	仅供参考	<p>显示当前主机时钟频率。</p> <p><i>此 BIOS 设置仅适用于主机时钟频率已被非默认值覆盖的英特尔® 台式机主板。</i></p>
Overridden Memory Speed	仅供参考	<p>显示当前内存速度。定义为当前主机时钟频率乘以内存倍频。</p> <p><i>此 BIOS 设置仅适用于主机时钟频率和内存倍频被覆盖的英特尔® 台式机主板。</i></p>

Overridden Processor Speed	仅供参考	显示当前设置的处理器最大速度。 定义为当前主机时钟频率乘以最大非 Turbo 比率。 <i>此 BIOS 设置仅适用于主机时钟频率或最大非 Turbo 比率被覆盖的英特尔® 台式机主板。</i>
Overridden Processor Turbo Speed	仅供参考	显示当前设置的处理器最大速度。 定义为当前主机时钟频率乘以单核活动 Turbo 比率。 <i>此 BIOS 设置仅适用于主机时钟频率或 Turbo 比率被覆盖的英特尔® 台式机主板。</i>
Processor Turbo Speed	仅供参考	显示当前设置的处理器最大速度。 定义为当前主机时钟频率乘以单核活动 Turbo 比率。
Total Memory	仅供参考	显示所安装系统的内存大小总量 (GB)。
L2 Cache RAM	仅供参考	显示所安装处理器的二级高速缓存内存总量 (MB)。 如果安装的是多核处理器，该内存量会显示为内核数乘以每个内核的二级高速缓存量。 <i>此设置仅当所安装的处理器支持二级高速缓存时才可用。</i>
Processor Speed	仅供参考	显示当前设置的处理器最大速度。 定义为当前主机时钟频率乘以最大非 Turbo 比率。
Processor Type	仅供参考	显示从 CPUID 指令获取的处理器品牌字符串。
SODIMMx	仅供参考	以千兆字节为单位显示 SODIMM 插槽中安装的系统内存大小。
System Date	月、日、年	从实时时钟显示和更改系统日期。 RTC 日期以 [MM/DD/YYYY] 格式显示。 可用 Tab 键选择各个字段。 + 和 - 键可用于增加/减少所选字段的值。 更改日期后，更改的值将立即提交到 RTC，而不是等待按 Save & Exit Setup/F10 键。 仅当 RTC 报告了无效日期，或者电池或 CMOS 校验失败时，才加载默认日期。 加载其他 Setup 默认值 (F9 键等) 时，无法加载默认日期。

System Time	时、分、秒	<p>从实时时钟显示和更改系统时间。</p> <p>RTC 时间会以 24 小时制 [HH:MM:SS] 显示。可用 Tab 键选择各个字段。+ 和 - 键可用于增加/减少所选字段的值。更改日期后，更改的值将立即提交到 RTC，而不是等待按 Save & Exit Setup/F10 键。仅当 RTC 报告了无效时间，或者电池或 CMOS 校验失败时，才加载默认时间。加载其他 Setup 默认值（F9 键等）时，无法加载默认时间。</p>
-------------	-------	---

Main > System Identification Information

BIOS 设置	选项	说明/用途
Microcode Update Revision	仅供参考	显示十六进制格式的 32 位处理器微代码更新版本。
Onboard LAN MAC Address	仅供参考	显示十六进制格式的板载 LAN 设备的 MAC 地址。
Processor Family x Model y Stepping z	仅供参考	显示十六进制格式的处理器家族、型号和步进编号（包括扩展的家族/型号）。这些是从 EAX 设为 1 时采用 CPUID 指令的 EAX 寄存器输出中派生的。
Processor Signature	仅供参考	显示十六进制格式的 32 位处理器签名；从 EAX 设为 1 时采用 CPUID 指令的 EAX 寄存器输出中复制。

Main > System Identification Information > Chassis Information

BIOS 设置	选项	说明/用途
Asset Tag	仅供参考	显示 SMBIOS Type 3 结构的机箱资产标签字符串。
Manufacturer	仅供参考	显示 SMBIOS Type 3 结构的机箱制造商字符串。
Serial Number	仅供参考	显示 SMBIOS Type 3 结构的机箱制造商序列号字符串。
SKU Number	仅供参考	显示 SMBIOS Type 3 结构的 SKU 编号字符串。
Version	仅供参考	显示 SMBIOS Type 3 结构的机箱制造商字符串。

Main > System Identification Information > Desktop Board Information

BIOS 设置	选项	说明/用途
Asset Tag	仅供参考	显示 SMBIOS Type 2 结构的主板资产标签字符串。

Manufacturer	仅供参考	显示 SMBIOS Type 2 结构的主板制造商字符串。
Product Name	仅供参考	显示 SMBIOS Type 2 结构的主板产品名称字符串。
Serial Number	仅供参考	显示 SMBIOS Type 2 结构的主板序列号字符串。
Version	仅供参考	显示 SMBIOS Type 2 结构的主板版本字符串。

Main > System Identification Information > Intel® Management Engine Information

BIOS 设置	选项	说明/用途
Firmware Version	仅供参考	显示当前安装的英特尔® 管理引擎固件版本。 <i>此 BIOS 设置仅适用于支持英特尔® 管理引擎 (Intel® ME) 的主板。</i>

Main > System Identification Information > System Information

BIOS 设置	选项	说明/用途
系列	仅供参考	显示 SMBIOS Type 1 结构的家族字符串
Manufacturer	仅供参考	显示 SMBIOS Type 1 结构的系统制造商字符串。
Product Name	仅供参考	显示 SMBIOS Type 1 结构的系统产品名称字符串。
Serial Number	仅供参考	显示 SMBIOS Type 1 结构的系统序列号字符串。
SKU Number	仅供参考	显示 SMBIOS Type 1 结构的 SKU 编号。
UUID	仅供参考	显示 SMBIOS Type 1 结构的 UUID/GUID。
Version	仅供参考	显示 SMBIOS Type 1 结构的系统版本字符串。

Maintenance

BIOS 设置	选项	说明/用途
Clear BIOS Passwords	Continue? (Y/N)	如果选择此项，将清除 BIOS 管理员密码和 BIOS 用户密码。 将完整保留与 BIOS 相关的其他密码（英特尔® 管理引擎密码、硬盘密码等）。
Clear Trusted Platform Module	<ul style="list-style-type: none"> • No • Yes 	<p>清除存储的所有加密密钥和 TPM 所有者。 如果您正在将平台所有权转让给新的所有者，可使用此选项清除 TPM。</p> <p><i>此 BIOS 设置仅适用于支持可信平台模块 (TPM) 并且启用了 TPM 的英特尔® 台式机主板。</i></p> <p><i>有关更多信息，请参阅《可信平台模块快速参考指南》。</i></p>
Fixed Disk Boot Sector	<ul style="list-style-type: none"> • Normal • Write Protect 	Write Protect 提供某些反病毒保护
Force On-board LAN Disable	<ul style="list-style-type: none"> • Enable • Disable 	<p>强制禁用板载 LAN 和所有主动管理技术功能。</p> <p><i>这项 BIOS 设置仅适用于支持英特尔® 主动管理技术的主板。</i></p>
Intel Enhanced Debug	<ul style="list-style-type: none"> • Enable • Disable 	Enable: 允许对可能与处理器相关的系统问题执行操作系统级别的调试。
DIMM n (Memory Channel x Slot y)	仅供参考	<p>以 GB 为单位显示 DIMM n (Channel x Slot y) 中所安装的系统内存大小（例如： 2 GB）。</p> <p>对主板上的每个内存插槽显示一行。 这些行会根据内存插槽与处理器的距离按顺序显示，离处理器最近的插槽显示在最前面。 DIMM 根据建议的内存加载顺序进行编号，并且应与主板丝网印刷面上的标签匹配。</p>
Reset Intel® AMT to default factory settings	Continue? (Y/N)	将所有英特尔® AMT 配置设置全都重置为出厂默认值。 如果选择此项，BIOS 将取消设置 AMT 并加载英特尔® 管理引擎默认设置。
Reset Intel® Standard Manageability to default factory settings	Continue? (Y/N)	将所有英特尔® 标准可管理性配置设置全都重置为出厂默认值。 如果选择此项，BIOS 将取消设置标准可管理性功能并加载英特尔管理引擎默认设置。
Unlock Intel® QST	<ul style="list-style-type: none"> • Yes • No 	如果选择 Yes ，则允许使用软件更改风扇的控制设置。
Use Maximum Multiplier	<ul style="list-style-type: none"> • Automatic • Disable 	仅用于未锁定的处理器： 将 CPU 速度设置为最小额定倍频或额定倍频（速度）

Performance

BIOS 设置	选项	说明/用途
Core Max Multiplier	仅供参考	显示默认、建议及当前的内核最大倍频。
Failsafe Watchdog	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用失败保障看门狗。</p> <p>如果启用了失败保障看门狗，则启动失败后，系统将使用用户最后设置的值重新引导至 BIOS 设置。</p>
Graphics Dynamic Frequency (GHz)	仅供参考	显示建议的、当前的以及默认的显卡动态频率。
Graphics Max Multiplier	数值	选择 Graphics Dynamic Frequency: $\text{Host Clock Frequency} \times 0.5 \times \text{Graphics Max Multiplier} = \text{Graphics Dynamic Frequency}$
Host Clock Frequency (MHz)	数值	<p>主机时钟频率 \times 处理器倍频 = 处理器速度</p> <p>主机时钟频率 \times 内存倍频 = 内存速度</p> <p>注意：要在增加基本时钟频率的基础上增强稳定性，需要减小处理器倍频或内存倍频。</p>
Host Clock Frequency Override	<ul style="list-style-type: none"> • Automatic • Manual 	<p>Manual: 允许覆盖主机时钟频率</p> <p><i>此 BIOS 设置仅适用于可覆盖其主机时钟频率的英特尔® 台式机主板。</i></p>
Intel® Turbo Boost Technology	仅供参考	显示默认、建议及当前的英特尔® 睿频加速技术状态。
Internal PLL Voltage Override	<ul style="list-style-type: none"> • Enable • Disable 	<p>Disable: 保持处理器内部 PLL 的默认电压。</p> <p>Enable: 增大处理器内部 PLL 的电压。这样可能会提高处理器在以至尊版处理器频率运行时的稳定性。</p> <p>警告：如果启用 Internal PLL Voltage Override, ACPI S3 睡眠状态将被禁用。</p>
Memory	仅供参考	显示默认、建议及活动的内存电压。
Multiplier	仅供参考	显示默认、建议及当前的内存倍频。

Overclocking Assistant	<ul style="list-style-type: none"> • Manual • Automatic 	<p>Manual: 用户必须手动配置性能问题。</p> <p>Automatic: 除 Processor Speed (GHz)、Internal Graphics Speed (GHz) 和 Memory Speed (MHz) 外, 所有性能问题 (包括子画面中的问题) 都将灰显; 以下问题的设置如下:</p> <ul style="list-style-type: none"> • Failsafe Watchdog - Enable • Host Clock Frequency (MHz) - 100 • Processor Voltage Override Type - None • Intel® Turbo Boost Technology - Enable • Sustained Mode Time (Seconds) - 1 • IGD Current Limit (Amps) - 64 • Active Core-Based Ratio Limits - Disable
PCH Core	仅供参考	显示默认、建议及活动的 PCH 核心电压。
Processor Core	仅供参考	显示默认、建议及当前的处理器核心电压。
Processor System Agent	仅供参考	显示默认、建议及当前的处理器系统代理电压。
Speed	仅供参考	对于处理器: 显示默认、建议及当前的处理器速度。 对于内存: 显示默认、建议及当前的内存速度。
Watchdog Coverage for Host Clock	<ul style="list-style-type: none"> • Enable • Disable 	如果启用, 看门狗计时器将在检测到 POST 故障时捕获系统挂起和/或故障, 并重置系统。如果发生故障, 看门狗计时器断言应重置系统并使用默认设置启动, 同时显示警告消息。

Performance > Bus Overrides

BIOS 设置	选项	说明/用途
Allow Simultaneous PCIe x16 Video Card (PEG) and IGD	<ul style="list-style-type: none"> • Enable • Disable 	启用此设置可同时启用安装在 x16 插槽中的 PCIe x16 视频卡 (PEG) 和处理器集成视频 (IGD)。
PCH Core Voltage Override	多个电压值	在配置页面下增加 Uncore/QPI 电压以实现稳定操作时, 可能需要调整 PCH 核心电压。
PCI Bus Frequency	仅供参考	显示 PCI 总线频率

PCI Express Bus Frequency	<ul style="list-style-type: none"> • 110MHz • 109MHz • 108MHz • 107MHz • 106MHz • 105MHz • 104MHz • 103MHz • 102MHz • 101MHz • Default 	设置 PCI Express 时钟频率。旧的 PCI 时钟频率设为此频率的 1/3。
---------------------------	---	--

Performance > Memory Overrides

BIOS 设置	选项	说明/用途
ECC Event Logging	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用 ECC 事件的日志记录。
Memory Correction	<ul style="list-style-type: none"> • Non-ECC • ECC 	<p>如果系统以及所安装的全部内存均支持 ECC（错误更正代码），则可以开启或关闭错误报告功能。</p> <p><i>此 BIOS 设置仅适用于安装 ECC DIMM 后支持 ECC 内存的台式机主板。</i></p>
Performance Memory Profiles	<ul style="list-style-type: none"> • Automatic • Manual – User Defined • Profile x: XMP-Frequency 	<p>要使用 DIMM SPD 的默认内存设置，需要手动覆盖内存设置或选择 XMP 配置文件。</p> <p>Automatic: BIOS 自动配置所有内存参数 Manual – User Defined: 允许用户完全控制内存参数 Profile x: XMP-Frequency: BIOS 根据所选 XMP 配置文件配置内存参数</p>
Uncore Multiplier	数值	Uncore 倍频会影响处理器功能（如三级高速缓存、内存控制器和集成显卡）的性能和稳定性。
Uncore Voltage Override	多个电压值	允许调整 CPU Uncore 电压。

Performance > Memory Overrides > Performance Memory Profiles

BIOS 设置	选项	说明/用途
Command Rate	<ul style="list-style-type: none"> • Auto • 1T • 2T 	Auto: 根据内存模式进行调整。2T 通常更加稳定。
Memory Multiplier	<ul style="list-style-type: none"> • Auto • Multiplier: DDRx-Frequency 	<p>Auto: BIOS 根据主机时钟频率、已安装处理器支持的倍频以及 DIMM 支持的内存频率来选择内存倍频。</p> <p>Multiplier: DDRx-Frequency: BIOS 将使用特定的内存倍频。如果选择随附的倍频，则内存将以所显示的频率运行。</p>

Memory Voltage	多个电压值	更改内存电压可能会实现超频和/或提高内存兼容性。
System Agent Voltage Override	使用 +/- 键更改值	更改系统代理电压可能会实现内存超频。
tCL	使用 +/- 键更改值	CAS Latency: 数据请求和数据读取之间的周期数
tFAW	使用 +/- 键更改值	Four Active Window: 允许向新内存条发出第 5 个连续 ACTIVE 命令之前的时间段
tRASmin	使用 +/- 键更改值	Minimum RAS Active Tim: 预充电和内存条激活之间的周期数
tRC	使用 +/- 键更改值	Row Cycle Delay: 对同一内存条发出连续 ACTIVE 命令的最小时间间隔
tRCD	使用 +/- 键更改值	RAS-to-CAS Delay: 激活和读/写操作之间的周期数
tRFC	使用 +/- 键更改值	RAS Refresh: 从行刷新到行激活之间的周期数
tRP	使用 +/- 键更改值	RAS Pre-Charge: 关闭一行和打开下一行之间的周期数。
tRRD	使用 +/- 键更改值	RAS to RAS Delay: 用于激活同一级中下一个内存条的周期数
tRTP	使用 +/- 键更改值	Read to Precharge Delay: 向同一级内存发送读取和预充电命令之间的周期数
tWR	使用 +/- 键更改值	Write Recovery: 写入和预充电之间的周期数
tWTR	使用 +/- 键更改值	Write to Read: 写入命令和下一个读取命令之间的周期数；与 tCL 相关

Performance > Processor Overrides

BIOS 设置	选项	说明/用途
CPU Idle State	<ul style="list-style-type: none"> • High Performance • Low Power 	<p>High Performance 强制操作系统始终使用最大倍频。</p> <p>Low Power 允许操作系统将倍频调低。</p>
CPU Voltage Override	多个电压值	<p>设置处理器电压。</p> <p>警告: 更改此设置的默认值会缩短处理器的使用寿命。强烈建议使用默认值。</p>

CPU Voltage Override Type	<ul style="list-style-type: none"> • None • Static • Dynamic 	<p>None: 允许处理器利用默认上限管理用电情况。</p> <p>Static: 使处理器始终保持在用户指定的具体电压。</p> <p>Dynamic: 允许处理器管理自己的电压级别，但需遵守用户指定的上限。</p>
CPU VREG Droop Control	<ul style="list-style-type: none"> • Low V-droop (Performance) • Mid v-droop • High V-Droop (Power Saving) 	选择的 V-droop 越低，为 CPU 提供的总功率越大。这会 增加热量，但可使 CPU 更稳定。
Intel® Turbo Boost Technology	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 如果处理器内核运转时未达到功率、电流和温度限值，该设置可使处理器内核的运行频率高于基本工作频率。</p> <p>Disable: 使用最大非 Turbo 比率</p>
Maximum Non-Turbo Ratio	数值	<p>非 Turbo 处理器最大速度 = 最大非 Turbo 比率 x 主机时钟频率</p> <p>未使用英特尔® 睿频加速技术时，可使用此参数和主机时钟频率来确定处理器的最大速度。</p>

Performance > Processor Overrides > Intel® Turbo Boost Technology

BIOS 设置	选项	说明/用途
1-Core Ratio Limit 2-Core Ratio Limit 3-Core Ratio Limit 4-Core Ratio Limit	数值	x 个内核处于活动状态时，英特尔® 睿频加速技术使用的最大处理器倍频。
Long Duration Power Limit Override (Watts)	数值	显示持续功率限制时间窗口时，英特尔® 睿频加速技术将使用此功率限制。
Long Duration Power Limit Time Window	数值	显示持续功率限制时间窗口（以秒为单位）时，英特尔® 睿频加速技术将使用持续功率限制覆盖。
Short Duration Power Limit Override (Watts)	数值	英特尔® 睿频加速技术将在极短的时间内使用此功率限制。此后，推荐使用持续功率限制。
TDC Current Limit Override (Amps)	数值	如果处理器运转时超过此电流限制，将停止使用英特尔® 睿频加速技术。
TDP Power Limit Override (Watts)	数值	如果处理器运转时超过此功率限制，将停止使用英特尔® 睿频加速技术。

Power

BIOS 设置	选项	说明/用途
After Power Failure	<ul style="list-style-type: none"> • Stay Off • Last State • Power On 	<p>确定发生断电时，电源恢复后的操作模式。</p> <p>Stay Off: 电源恢复后，在按电源按钮之前系统将保持关闭状态。</p> <p>Last State: 电源恢复后，系统将返回到断电前的最后电源状态。</p> <p>Power On: 电源恢复后，系统自动接通电源。</p>
CPU C States	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 CPU C 状态。</p> <p>如果启用，BIOS 会将 C1 以下的 C 状态报告给操作系统。此设置可使处理器在空闲时进入低功耗状态，从而降低功耗和产热量。</p>
Deep S4/S5	<ul style="list-style-type: none"> • Enable • Disable 	<p>如果启用，系统在处于 S4/S5 睡眠状态时将使用较少电能，但仅通过电源按钮或 RTC 警报从 S4/S5 唤醒。</p>
Enhanced Halt State (C1E)	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用增强型深度休眠技术，它使处理器可以处于 C1E（暂停）空闲状态，从而减少耗电量和产热量。</p>
Enhanced Intel SpeedStep® Technology	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用增强型英特尔 SpeedStep® 技术 (EIST)，它使系统可以动态调整处理器电压和内核频率，从而减少平均功耗和平均产热量并降低噪音。</p> <p>有关 SpeedStep 的信息，请访问 http://en.wikipedia.org/wiki/Speedstep</p>
Flash Update Sleep Delay	<ul style="list-style-type: none"> • Enable • Disable 	<p>如果启用，系统将在闪存更新电源周期内休眠 20 秒。启用此功能可以提高与电源的兼容性。</p>

<p>Intel® Dynamic Power Technology</p>	<ul style="list-style-type: none"> • Energy Efficient Performance • Off • Custom 	<p>配置处理器电源管理功能。</p> <p>Energy Efficient Performance: 隐藏以下 BIOS 选项:</p> <ul style="list-style-type: none"> • Enhanced Intel SpeedStep® Technology • OS ACPI C2 Report • OS ACPI C3 Report <p>Sets the following BIOS options:</p> <ul style="list-style-type: none"> • Enhanced Intel SpeedStep® Technology to Enable • OS ACPI C2 Report to Enable • OS ACPI C3 Report to Disable • PCIe ASPM Support to Enable <p>Off: 隐藏以下 BIOS 选项:</p> <ul style="list-style-type: none"> • Enhanced Intel SpeedStep® Technology • OS ACPI C2 Report • OS ACPI C3 Report • Enhanced Intel SpeedStep® Technology to Disable • OS ACPI C2 Report to Disable • OS ACPI C3 Report to Disable • PCIe ASPM Support to Disable <p>Custom: 取消隐藏以下 BIOS 选项:</p> <ul style="list-style-type: none"> • Enhanced Intel SpeedStep® Technology • OS ACPI C2 Report • OS ACPI C3 Report
<p>OS ACPI C2 Report</p>	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 OS ACPI C2 报告功能。 如果启用, BIOS 将报告 ACPI C2 状态 (映射到处理器 C3 状态)。</p>
<p>PCIe ASPM L0s</p>	<ul style="list-style-type: none"> • Enable • Disable 	<p>PCIe Active State Power Management: L0 使 PCI Express 链路的一个方向进入低功率状态。</p>
<p>PCIe ASPM L1</p>	<ul style="list-style-type: none"> • Enable • Disable 	<p>PCIe Active State Power Management: L1 使 PCI Express 链路的两个方向都进入低功率状态。</p>
<p>PCIe ASPM Support</p>	<ul style="list-style-type: none"> • Disable • Enable • PEG Only 	<p>Disable: 禁用所有 PCIe 设备的 ASPM 支持。 Enable: 启用所有 PCIe 设备的 ASPM 支持。 PEG Only: 仅为安装在 PCI Express 图形 (PEG) 插槽中的设备启用 ASPM。</p>
<p>Processor C States</p>	<ul style="list-style-type: none"> • Enable • Disable 	<p>Enable: 将最大限度地发挥系统的节能功能。 Disable: 可提高系统性能, 并提高系统能源使用效率。</p> <p>仅在重新启动后生效。 需要使用 C 状态才能充分发挥 Processor Turbo Boost 的所有功能。</p>
<p>Processor Power Efficiency Policy</p>	<ul style="list-style-type: none"> • High Performance • Balanced • Low Power 	<p>配置处理器偏压以提高电源效率与性能。</p> <p>High Performance: 将 MSR 1B0h Bits 3:0 设置为 0h Balanced: 将 MSR 1B0h Bits 3:0 设置为 5h Low Power: 将 MSR 1B0h Bits 3:0 设置为 7h</p>

QPI Power Management	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用 QPI 总线的电源管理。</p> <p><i>如欲了解更多信息，请参阅</i> http://en.wikipedia.org/wiki/intel_quickpath_interconnect</p>
S1 State Indicator	<ul style="list-style-type: none"> • Off • Blink • On • Alternate Color 	<p>确定在 S1 系统电源状态期间前面板 LED 的行为。</p>
S3 State Indicator	<ul style="list-style-type: none"> • Off • Blink • On • Alternate Color 	<p>确定在 S3 系统电源状态期间前面板电源 LED 的行为。</p>
Wake on LAN from S4/S5	<ul style="list-style-type: none"> • Stay off • Power On – Normal Boot • Power On – PXE Boot 	<p>配置在 S4/S5 期间收到 Wake on LAN 数据包时的行为。</p> <p>Stay off: 收到 Wake on LAN 数据包时，系统不会从 S4/S5 电源状态唤醒。</p> <p>Power On-Normal Boot: 收到 Wake on LAN 数据包时，系统将从 S4/S5 电源状态唤醒，并且将遵循正常的启动顺序。</p> <p>Power On-PXE Boot: 收到 Wake on LAN 数据包时，系统将从 S4/S5 电源状态唤醒，并且将尝试从 PXE 启动。</p> <p>还必须启用操作系统 LAN 驱动程序中的 Wake on LAN 功能；但如果启用了 Deep S4/S5，则禁用该功能。</p>
Wake system from S5	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用系统警报唤醒事件。如果启用，系统将在指定的时间（日/时/分/秒）唤醒。</p>
Wakeup Date	<p>数值范围 0 - 31</p>	<p>选择每个月的某一天唤醒系统。如果每天唤醒，则选择 0。</p>
Wakeup Hour	<p>数值范围 0 - 23</p>	<p>选择采用 24 小时制的唤醒时间（小时）。例如，15 表示下午 3 点。</p>
Wakeup Minute	<p>数值范围 0 - 59</p>	<p>选择用分钟表示的唤醒时间。</p>
Wakeup Second	<p>数值范围 0 - 59</p>	<p>选择用秒表示的唤醒时间。</p>

Security

BIOS 设置	选项	说明/用途
Chassis Intrusion	<ul style="list-style-type: none"> • Disable • Enable <p>or</p> <ul style="list-style-type: none"> • Disable • Log Only • Pause POST 	<p>启用或禁用机箱防盗功能。</p> <p>Disable: 忽略机箱防盗功能并且不记录事件。</p> <p>Log only: 在 BIOS 事件日志中创建条目。</p> <p>Pause POST: 创建 BIOS 事件日志条目并显示消息。</p>

Clear User Password	Continue? (Y/N)	清除用户密码。 <i>此 BIOS 设置仅在设置了用户密码时才显示。</i>
Execute Disable Bit	<ul style="list-style-type: none"> • Enable • Disable 	启用此功能可实现病毒防护技术。 <i>如欲了解更多信息, 请参阅</i> http://www.intel.com/technology/xdbit/
Hard Disk Drive Password	仅供参考	报告是否设置了硬盘密码。
Intel Trusted Execution Technology	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用英特尔® 可信执行技术, 该技术可提供基于硬件的机制, 有助于防止基于软件的攻击并保护数据的机密性和完整性。 如果启用了英特尔® TXT, 则还将启用英特尔® VT、英特尔® VT-d、英特尔® HT、所有处理器内核以及板载 TPM。启用英特尔® TXT 后, 必须先将其禁用才能禁用所需功能。 <i>有关可信执行技术的信息, 请访问</i> http://www.intel.com/technology/security/
英特尔® 虚拟化技术	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用虚拟化技术。必须重新启动才会生效。 <i>有关更多信息, 请访问</i> http://www.intel.com/cn/technology/virtualization/index.htm
Master Key Hard Disk Drive Password	仅供参考	报告是否设置了主密钥硬盘密码。
Set Hard Disk Drive Password	用户自定义	设置硬盘密码 如果已经创建了硬盘密码, 则每次启动时都必须输入该密码才能访问操作系统。硬盘密码不可恢复, 并且在没有原始密码的情况下无法将其删除。除非输入硬盘或主密钥硬盘密码, 否则无法访问该硬盘。
Set Master Key Hard Disk Drive Password	用户自定义	设置主密钥硬盘密码 仅在忘记了硬盘密码时, 才使用主密钥硬盘密码来解除硬盘的锁定。它本身并不会锁定硬盘。硬盘密码不可恢复, 并且在没有原始密码的情况下无法将其删除。除非输入硬盘或主密钥硬盘密码, 否则无法访问该硬盘。

Set Supervisor Password	用户自定义	<p>设置管理员密码。</p> <p>使用管理员密码可以无任何限制地查看和更改所有 Setup 选项。如果只设置了管理员密码，则在 Setup 的密码提示界面中按 <Enter> 键，将允许用户有限制地访问 Setup。如果同时设置了管理员密码和用户密码，则必须输入管理员密码或用户密码才能访问 Setup。根据输入的是管理员密码还是用户密码，即可相应地查看和更改 Setup 选项。</p>
Set User Password	用户自定义	<p>设置用户密码。</p> <p>设置用户密码以限制可以启动计算机的用户。计算机启动前，将显示密码提示。如果只设置了管理员密码，计算机启动时将不需要输入密码。如果同时设置了这两种密码，可以输入任一种密码启动计算机。</p>
Supervisor Password	仅供参考	报告是否设置了管理员密码。
User access Level	<ul style="list-style-type: none"> • Full • Limited • View Only • No Access 	<p>User Access Level 确定输入用户密码后可得到的 BIOS Setup 访问级别。</p> <p>Full: 用户密码授予对用户访问级 (User Access Level) 别外所有设置的访问权限。</p> <p>Limited: 用户密码授予对时间/日期/语言/用户密码问题等设置的访问权限。</p> <p>View Only: 用户密码仅授予对语言问题设置的访问权限且无法保存更改。</p> <p>No Access: 用户密码不能用来访问 Setup。</p> <p><i>此 BIOS 设置仅在设置了管理员密码时才显示。</i></p>
User Password	仅供参考	报告是否设置了用户密码。
XD Technology	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 XD 技术。</p> <p>英特尔® 病毒防护技术功能结合支持该技术的操作系统，有助于防止特定类型的恶意缓冲区溢出攻击。</p> <p><i>有关更多信息，请访问</i> http://www.intel.com/technology/xdbit/</p>

Security > Intel® VT for Directed I/O (VT-d)

BIOS 设置	选项	说明/用途
ATS	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用非 Isoch VT-d 引擎地址转换服务 (ATS) 支持
Coherency Support	<ul style="list-style-type: none"> • Enable • Disable 	启用或禁用非 Isoch VT-d 引擎相干性支持

Intel® VT for Directed I/O (VT-d)	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用英特尔® 定向 I/O 虚拟化技术 (VT-d)，该技术为管理 I/O 虚拟化提供其他硬件支持。如果启用，BIOS 将发布一个“DMA Remapping ACPI”表。</p> <p><i>有关英特尔® VT 的信息，请访问</i> http://www.intel.com/technology/advanced_comm/virtualization.htm</p>
Interrupt Remapping	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 VT-d 中断重映射支持</p>
Pass Thru DMA	<ul style="list-style-type: none"> • Enable • Disable 	<p>启用或禁用 Isoch/非 Isoch VT-d 引擎直通 DMA 支持</p>