UEFI SETUP UTILITY

1 简介

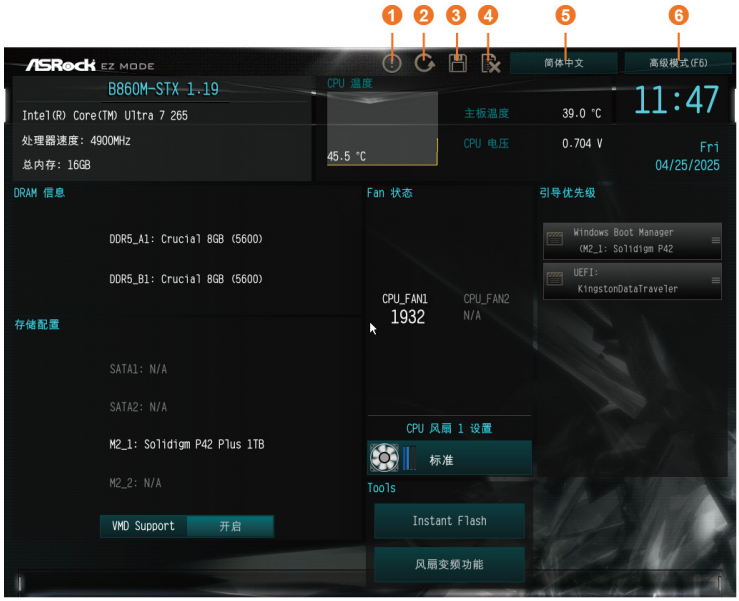
本节介绍如何使用 UEFI SETUP UTILITY 配置您的系统。打开计算机电源后按 <F2> 或 <Del> ，您可以运行 UEFI SETUP UTILITY，否则，开机自检 (POST) 将继续其测试例程。如果您想要在 POST 后进入 UEFI SETUP UTILITY，可按 <Ctl> + <Alt> + <Delete> 或按系统机箱上的重置按钮重新启动系统。也可以通过关闭系统后再开启来重新启动它。

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。

2 EZ 模式

默认情况下，进入 BIOS 设置程序时，EZ Mode (EZ 模式）屏幕会出现。 EZ 模式是一个仪表盘，包含系统当前状态的多个读数。 您可以检查系统最重要的信息，如：CPU 速度、DRAM 频率、SATA 信息、风扇速度等。

按 <F6> 或单击屏幕右上角的“Advanced Mode (高级模式）”按钮可以切换到“高级模式”，访问更多选项。



编号	功能
1	Help (帮助）
2	Load UEFI Defaults (加载 UEFI 默认值）
3	Save Changes and Exit (保存更改并退出）
4	Discard Changes (放弃更改）
5	Change Language (更改语言）
6	Switch to Advanced Mode (切换到高级模式）

3 高级模式

高级模式提供更多选项来配置 BIOS 设置。 请参阅以下部分了解详细配置。

要访问 EZ 模式，请按 <F6> 或单击屏幕右上角的“EZ Mode (EZ 模式)”按钮。

3.1 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
超频工具	超频配置
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
安全	安全设置
引导	配置引导设置和引导优先级
退出	退出当前屏幕或 UEFI Setup Utility

3.2 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

4 主画面

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

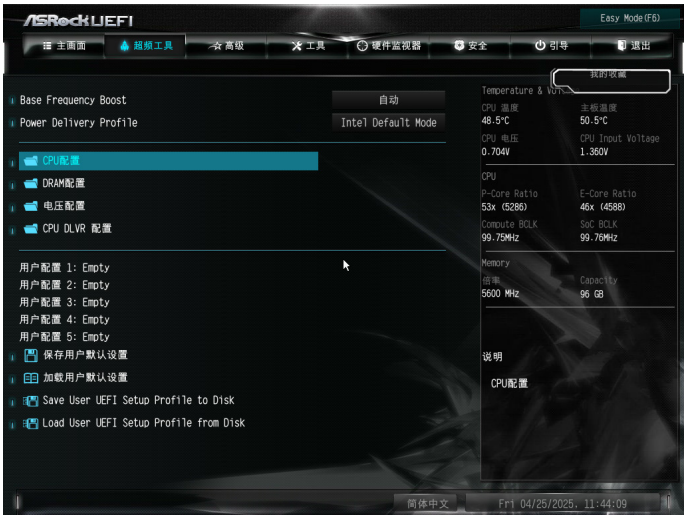
BIOS 设置是否可用及其路径根据不同的型号与 BIOS 版本而定。

我的收藏

显示您所收藏的 BIOS 项目。按下 <F5> 可添加 / 移除收藏的项目。

3.3 OC Tweaker 屏幕

在 OC Tweaker 屏幕中，您可以设置超频功能。



CPU Indicator（CPU 指示灯）

CPU 指示器根据 CPU 的性能和功能分配分数，对 CPU 进行评级，从而帮助用户优化超频设置，提高性能。

CPU Configuration（CPU 配置）

CPU Turbo Ratio Information（CPU 加速倍频信息）

按下 [Enter] 查看 CPU 加速倍频信息。

CPU P-Core Ratio（CPU E-Core 倍频）

CPU P-Core 倍频乘以 BCLK 确定 CPU 速度。增加 CPU P-Core 倍频可增加内部 CPU 时钟速度且不会影响其它组件的时钟速度。

配置选项：[Auto]（自动）[All-core]（所有内核）[Per-core]（每个内核）[Specific Per Core]

AVX2 Ratio Offset（AVX2 比率偏移）

AVX2 比率偏移用于指定 AVX 工作负载的 CPU 倍频负偏移量。AVX 是一种压力更高的工作负载，通过降低 AVX 比率保证 SSE 工作负载的最大可用比率。

CPU E-Core Ratio（CPU E-Core 比率）

E-Core 速度乘以 BCLK 确定 E-Core 倍频。增加 E-Core 倍频可增加内部 E-Core 时钟速度且不会影响其它组件的时钟速度。

配置选项：[Auto]（自动）[All-core]（所有内核）[Per-core]（每个内核）[Specific Per Core]

CPU Cache Ratio（CPU 缓存比率）

CPU 内部总线速比。最大值应与 CPU 比率相同。

Min Cache Ratio（最小缓存比率）

CPU 内部总线最小速比。若要使缓存比率与非 K 系列 CPU 的 P-Core 限值一致，可将最小缓存比率限值与 CPU 缓存比率同步。

MemSS Max OC Ratio（MemSS 最大超频比）

允许为内存子系统设置最大超频比。范围：非加速倍频最大值 - 109。

NGU Max OC Ratio（NGU 最大超频比）

允许为 NGU 设置最大超频比。范围：非加速倍频最大值 - 34。

GT Frequency（GT 频率）

允许配置集成 GPU 频率（单位 MHz）。此项目会在用户使用板载图形时显示。

CPU D2D Ratio（CPU D2D 比）

允许设置 CPU D2D 比，范围为 15 到 40。

BCLK Aware Adaptive Voltage（BCLK 感知自适应电压）

允许将 BCLK 感知自适应电压设置为启用或禁用。启用后，在计算 CPU V/F 曲线时 pcode 会获知 BCLK 频率。这也是避免 BCLK OC 出现高电压倍频的理想方式。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Boot Max Frequency（引导最大频率）

允许启用或禁用 CPU Strap 中的引导最大频率。

Boot Performance Mode（启动性能模式）

默认为最大非智能加速性能模式。在该模式下，可使 CPU 保持弹性倍频直至操作系统接管为止。最大电池模式会将 CPU 倍频设置为 x8 直至操作系统接管为止。若 BCLK 为超频，则建议启用此选项。

配置选项：[Max Battery]（最大电池）、[Max Non-Turbo Performance]（最大非智能加速性能）、[Turbo Performance]（智能加速性能）

CPU BGREF Mode（CPU BGREF 模式）

允许在“正常”和“避开带隙”之间选择 CPU 带隙参考模式。CPU 带隙参考模式 - 默认电压为“正常”。

配置选项：[Normal]（正常）、[Bandgap Bypassed]（避开带隙）

VCCIA Boot Voltage（VCCIA 引导电压）

允许在“标称电压”和“高电压”之间选择 VCCIA 引导电压。VCCIA 引导电压 - 默认电压为标称电压，为了支持高电压，BIOS 可通过程序设定大于 1.65v（最大 2.01v）的 VCCIA 引导电压。

VCCSA Boot Voltage（VCCSA 引导电压）

允许在“标称电压”和“高电压”之间选择 VCCSA 引导电压（最大 1.2/1.3V)。VCCSA 引导电压 - 默认电压为标称电压，为了支持高压，BIOS 可通过程序设定 EPOC2 位，以将电压提升为最大 1.2/1.3V。0 - 标称电压。1 - 高电压（最大 1.2/1.3V）。

配置选项：[Nominal]（标称电压）、[High Voltage]（高电压）

Ring to Core Ratio Offset（环形总线至内核比率偏移）

禁用“环形总线至内核比率偏移”后，环形总线和内核可以在相同频率下运行。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

FLL Overclock Mode（FLL 超频模式）

允许在 1 至 3 范围内选取 FLL 模式数值。
0x0 = 不超频。

0x1 = 在标称 (0.5-1x) 基准时钟频率下超频；
0x2 = BCLK 在极高 (3-5x) 基准时钟频率下超频，限值为 63。

SA PLL Frequency（SA PLL 频率）

允许配置 SA PLL 频率。

配置选项：[Auto]（自动）、[3200 MHz]、[1600 MHz]

BCLK TSC HW Fixup（BCLK TSC HW 固定）

在 TSC 从 PMA 复制到 APIC 时，将禁用“BCLK TSC HW 固定”。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel SpeedStep Technology（Intel 动态节能技术）

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。当 Intel SpeedStep Technology（Intel SpeedStep 技术）设置为 Disabled（禁用）且 Intel Turbo Boost Technology（Intel 智能加速技术）设置为 Enabled（启用）时，
可以使 CPU 加速倍频固定。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel Turbo Boost Technology（Intel 智能加速技术）

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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel Speed Shift Technology（Intel 变速技术）

允许启用或禁用 Intel 变速技术支持。启用时将显示 CPPC v2 界面，通过该界面可进行硬件效能控制。要获得对 Intel Turbo Boost Max Technology 3.0（Intel 智能加速技术 3.0）最佳支持，必须启用 Intel 变速技术。若 CPU 不支持 ITMBT 3.0，该选项仍为灰显状态。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel Turbo Boost Max Technology 3.0（Intel 智能加速技术 3.0）

允许启用或禁用 Intel 智能加速技术 3.0 (ITBMT 3.0) 支持。禁用时，将报告 _CPC 对象中的最慢内核的最大倍频。支持 ITBMT 3.0 功能的处理器中至少有一个内核的最大频率高于其他内核。

配置选项：[Auto]（自动）、[Enabled]（启用）、 [Disabled]（禁用）

Intel Dynamic Tuning Technology（Intel 动态调谐技术）

允许启用或禁用 Intel 动态平台热框架。

Intel Thermal Velocity Boost Voltage Optimizations（Intel 热速度加速电压优化）

该服务用于控制支持 Intel 热速度加速 (TVB) 特性的处理器的热速度电压优化。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Enhanced Thermal Velocity Boost（增强热速度加速）

启用此项目后，当温度达到产品支持的默认阈值时，用户将被删除。建议超频时禁用此项目。此项目显示与否由您主板上的 CPU 型号决定。

配置选项：[Auto]（自动）、[Enabled]（启用）、[Disabled]（禁用）

CPU Tj（CPU Tj 最大值）

允许设置 CPU Tj 最大值以调节 TCC 目标温度。该选项支持的 Tj 最大值范围为 62 至 115 摄氏度。

Long Duration Power Limit（长持续时间功率限制）

允许配置封装功率限制 1（瓦）。超过此限制时，在一段时间后 CPU 倍频会降低。较低限制可保护 CPU 和节能，较高限制可提高性能。

Long Duration Maintained（维持的长持续时间）

允许配置超过长持续时间功率限制时经过多长时间 CPU 倍频降低。

Short Duration Power Limit（短持续时间功率限制）

允许配置封装功率限制 2（瓦）。超过此限制时，CPU 倍频将被立即降低。较低限制可保护 CPU 和节能，较高限制可提高性能。

CPU Core Current Limit（CPU 内核电流限制）

调压器电流限制。该数值代表在任意给定时间允许的最大瞬时电流。

GT Current Limit（GT 电流限制）

调压器电流限制。该数值代表在任意给定时间允许的最大瞬时电流。此项目会在用户使用板载图形时显示。

IA CEP Enable（IA CEP 启用）

允许启用或禁用 CEP（电流偏移保护）支持。

GT CEP Enable（GT CEP 启用）

允许启用或禁用 CEP（电流偏移保护）支持。

Process Vmax Limit（过程 Vmax 限值）

此选项允许用户禁用 P-core 功率密度限制，以达到超频目的。禁用后，BIOS 无法在

同一重置周期内启用此选项。启用进行热重置或冷重置才能再次启用保护。

P-core Power Density Throttle（P-core 功率密度限制）

为实现超频目的而进行限制。禁用后，BIOS 无法在同一重置周期内启用此选项。启用进行热重置或冷重置才能再次启用保护。

DRAM Configuration（DRAM 配置）

Memory Information（内存信息）

允许用户浏览内存模块的串行存在检测 (SPD) 和 Intel 极限内存配置文件 (XMP)。

DRAM Timing Configuration（DRAM 时序配置）

Memory Ratio（内存比）

频率将等于 PLL 比 * 档位比（2 或 4） * 基准时钟 (33.33)。

DRAM Frequency（DRAM 频率）

如果选择 [Auto]（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。

DRAM Gear Mode（DRAM 档位模式）

允许选择 DRAM 档位模式。高档位适用于高频率。

配置选项：[Auto]（自动）、[2]、[4]

SAGV

允许启用或禁用系统代理 Geyserville。启用时，会出现以下选项供配置：

SA GV Mask（SA GV 屏蔽）

System Agent Geyserville（系统代理 Geyserville）此项允许设置在频率切换中使用点的 BIT。

配置选项：

[Enable Points: 1st and 2nd]（启用点：第 1 点和第 2 点）

[Enable Points: 1st, 2nd and 3rd]（启用点：第 1 点、第 2 点和第 3 点）

[Enable All Points: 1st, 2nd, 3rd, and 4th]（启用全部点：第 1 点、第 2 点、第 3 点和第 4 点）

1st Point Frequnecy（第 1 点频率）

允许指定给定点的频率。

1st Point Gear（第 1 点档位）

该 SAGV 点的档位比。

配置选项：[Auto]（自动）、[2]、[4]

2nd Point Frequnecy（第 2 点频率）

允许指定给定点的频率。

2nd Point Gear（第 2 点档位）

该 SAGV 点的档位比。

配置选项：[Auto]（自动）、[2]、[4]

3rd Point Frequnecy（第 3 点频率）

允许指定给定点的频率。

3rd Point Gear（第 3 点档位）

该 SAGV 点的档位比。

配置选项：[Auto]（自动）、[2]、[4]

4th Point Frequnecy（第 4 点频率）

允许指定给定点的频率。

4th Point Gear（第 4 点档位）

该 SAGV 点的档位比。

配置选项：[Auto]（自动）、[2]、[4]

Primary Timing（第一时序）

CAS# Latency (tCL)（列地址选通脉冲时间延迟）

发送列地址到内存与回应数据开始之间的时间。

RAS# to CAS# Delay (tRCD)（内存行地址传输到列地址的延迟时间）

RAS# to CAS# Delay（内存行地址传输到列地址的延迟时间）：开启内存行到访问内存中的列之间需要的时钟周期数。

Row Precharge (tRP)（行预充电）

发出 precharge（预充电）命令到打开下一行之间需要的时钟周期数。

RAS# Active Time (tRAS)（行地址动态时间）

bank active 命令与发出 precharge（预充电）命令之间需要的时钟周期数。

RAS# Cycle Time (tRC)（RAS# 循环时间）

允许配置最短激活至激活 / 刷新时间。

Command Rate (CR)（命令速率）

选择内存芯片和可以发出第一个 active 命令之间的延迟。

Secondary Timing（第二时序）

Write Recovery Time (tWR)（写入恢复时间）

在完成有效写入操作之后，可以预充电 active bank（有效存储单元）之前必须等待的
延迟时间。

Refresh Cycle Time 2 (tRFC2)（刷新周期时间 2）

从 Refresh（命令）命令直到第一个 Activate（激活）命令至相同等级的时钟数。

Refresh Cycle Time per Bank (tRFCpb)（刷新每个存储单元的循环时间）

从 Refresh（命令）命令直到第一个 Activate（激活）命令（每个存储单元）至相同等级的时钟数。

Refresh Delay Same Bank（相同存储单元刷新延迟）(tREFSBRD)

允许配置 tREFSBRD，相同存储单元刷新为 ACT 延迟。

Refresh Interval x9 (tREFIx9)（刷新间隔 x9）

允许配置 tREFIx9，以获得每个等级刷新之间的最大间隔时间。

Refresh Interval (tREFI)（刷新间隔）

允许配置平均周期间隔时间的刷新周期。

CAS to CAS CMD Delay (tCCD_L)（CAS 到 CAS CMD 延迟）

允许配置内部写入到读取命令的延迟时间。

Write CAS to CAS CMD Delay (tCCD_L_WR)（将 CAS 写入到 CAS CMD 的延迟）

允许配置内部写入到写入命令的延迟时间。

Write to Read Delay (tWTR_L)（写入到读取延迟）

最后一个有效写入操作到下一次读取命令至相同内部存储单元之间的时钟数。

Write to Read Delay (tWTR_S)（写入到读取延迟）

最后一个有效写入操作到下一次读取命令至相同内部存储单元之间的时钟数。

RAS to RAS Delay (tRRD_L)（RAS 到 RAS 延迟）

相同等级不同存储单元中激活的两行之间的时钟数。

RAS to RAS Delay (tRRD_S)（RAS 到 RAS 延迟）

相同等级不同存储单元中激活的两行之间的时钟数。

Read to Precharge (tRTP)（读取预充电）

读取命令至行预充电命令至相同等级之间插入的时钟数。

Four Activate Window (tFAW)（四个存储单元激活窗口）

允许相同等级四个存储单元激活的时间窗口。

CAS Write Latency (tCWL)（列地址写入延迟）

配置 CAS 写入延迟。

Power Down Timing（关机时序）

tCKE

配置 DDR5 在进入自刷新模式时从内部开始执行至少一个刷新命令的时段。

tXP

允许配置 tXP。

tCPDED

允许配置 tCPDED。

tRDPDEN

允许配置 tRDPDEN。

tWDPDEN

允许配置 tWDPDEN。

tCKCKEH

允许配置 tCKCKEH。

tCSH

允许配置 tCSH。

tCSH

允许配置 tCSH。

tCSL

允许配置 tCSL。

tCA2CS
允许配置 tCA2CS。

tPRPDEN
允许配置 tPRPDEN。

tOSCO
允许配置 tOSCO。

tMRR
允许配置 tMRR。

MISC Timing（MISC 时序）

tRPab
允许配置 tRPab。

tRDPRE
允许配置 tRDPRE。

tPPD
允许配置 tPPD。

tWRPRE
允许配置 tWRPRE。

DeratingExt
允许配置 DeratingExt。

DecTcwl
允许配置 DecTcwl。

AddTcwl
允许配置 AddTcwl。

tCCDByteCasDelta
允许配置 tCCDByteCasDelta。

tPrefRi
允许配置 tOrefRi。

RefreshHpWm

允许配置 RefreshHpWm。

RefreshPanicWm

允许配置 RefreshPanicWm。

RefreshPanicWm

允许配置 RefreshAbrRelease。

tRFM

允许配置 tRFM。

tXSR

允许配置 tXSR。

tSR

允许配置 tSR。

tXSDLL

允许配置 tXSDLL。

tZQCS

允许配置 tZQCS。

tZQCAL

允许配置 tZQCAL。

tZQCSPeriod

允许配置 tZQCSPeriod。

tMRD

允许配置 tMRD。

Turn Around Timing（周转时间）

TAT Training Value（TAT 训练值）

tRDRD_sg

配置模块读取和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tRDRD_dg

配置模块读取和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tRDRD_dr

配置模块读取和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDRD_dd

配置模块读取和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_sg

配置模块读取和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dg

配置模块读取和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dr

配置模块读取和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dd

配置模块读取和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

tWRRD_sg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [511]

tWRRD_dg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [511]

tWRRD_dr

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRRD_dd

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_sg

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dg

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dr

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dd

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

TAT Runtime Value（TAT 运行值）

tRDRD_sg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tRDRD_dg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tRDRD_dr

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDRD_dd

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_sg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dr

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tRDWR_dd

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [255]

tWRRD_sg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [511]

tWRRD_dg

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [511]

tWRRD_dr

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRRD_dd

配置模块写入和读取延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_sg

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dg

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dr

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [127]

tWRWR_dd

配置模块写入和写入延迟。

配置选项：[Auto]（自动）、[0] - [255]

Round Trip Timing（往返时间）

Round Trip Level（往返延迟等级）

配置往返延迟等级。

配置选项：[Tightest]（最紧密）、[Tighter]（更紧密）、[Tight]（紧密）、[Normal]（正常）、[Loose]（松散）、[Looser]（更松散）、[Loosest]（最松散）

Initial RTL IO Delay Offset（初始 RTL IO 延迟偏移）

配置往返延迟 IO 延迟初始偏移。

Initial RTL FIF0 Delay Offset（初始 RTL FIF0 延迟偏移）

配置往返延迟 FIF0 延迟初始偏移。

Initial RTL（初始 RTL）(MC0 A1)

配置往返延迟初始值。

Initial RTL（初始 RTL）(MC0 A1)

配置往返延迟初始值。

Initial RTL（初始 RTL）(MC1 B1)

配置往返延迟初始值。

Initial RTL（初始 RTL）(MC1 B1)

配置往返延迟初始值。

RTL (MC0 C0 A1)

配置往返延迟。

RTL (MC0 C1 A1)

配置往返延迟。

RTL (MC1 C0 B1)

配置往返延迟。

RTL (MC1 C1 B1)

配置往返延迟。

ODT Setting（ODT 设置）

Force Reset Type（强制重置类型）

F10 保存更改并退出后强制重置类型

配置选项：[Auto]（自动）、[Cold Reset]（冷重置）、[Warm Reset]（暖重置）、[Shut Down Reset]（关机重置）、[Platform Specific Reset]（平台特定重置）

Retrain on Fast Fail（快速失败时重新训练）

如果 SW MemTest 在快速流程期间失败，则在冷模式下重新启动 MRC。默认选项设为“启用”。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Retrain to Working Channel（重新训练到工作通道）

禁用失败通道后在冷模式下重新启动 MRC。默认选项设为“禁用”。

Exit On Failure（发生故障时退出）(MRC)

为 MRC 训练步骤配置“发生故障时退出”。

Force ColdReset（强制冷重置）

强制冷重置或选择 MrcColdBoot 模式，MRC 执行期间需要进行冷启动。注：如果存在 ME 5.0MB，则需要 ForceColdReset！

Reset for MRC Failed（MRC 重置失败）

MRC 训练失败后重置系统。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

MRC Training on Warm Boot（热启动时 MRC 训练）

启用后，将在热启动时执行内存训练。

配置选项：[Auto]（自动）、[Enabled]（启用）、 [Disabled]（禁用）

MRC Fast Boot（MRC 快速引导）

启用后，尽可能跳过部分内存引用代码以提高引导速度。

配置选项：[Auto]（自动）、[Enabled]（启用）、 [Disabled]（禁用）

Voltage Configuration（电压配置）

Voltage Mode（电压模式）

[OC Mode]（OC 模式）：增大超频电压范围。

[Stable Mode]（稳定模式）：减小稳定系统电压范围。

CPU GT Voltage（CPU GT 电压）

允许外部调压器供应的处理器输入电压。

配置选项：[Auto]（自动）、[Offset Mode]（偏移模式）、[Fixed Mode]（固定模式）

CPU GT Load-Line Calibration（CPU GT 负载线路校准）

CPU GT Load-Line Calibration（CPU GT 负载线路校准）可帮助防止系统负载较大时 GT 电压下降。

配置选项：[Auto]（自动）、[Level 1]（1 级）、[Level 2]（2 级）、[Level 3]（3 级）、[Level 4]（4 级）、[Level 5]（5 级）
*[Level 1]（1 级）和 [Level 2]（2 级）选项是否显示由主板上使用的 CPU 决定。

System Agent Voltage（系统代理电压）

外部调压器供应的处理器输入电压。

配置选项：[Auto]（自动）、[Offset Mode]（偏移模式）、[Fixed Mode]（固定模式）

System Agent Load-Line Calibration（系统代理负载线路校准）

系统代理负载线路校准可帮助防止系统负载较大时系统代理电压下降。

配置选项：[Auto]（自动）、[Level 1]（1 级）、[Level 2]（2 级）、[Level 3]（3 级）、[Level 4]（4 级）、[Level 5]（5 级）

Vcore Offset（Vcore 热偏移）

运行配置 Vcore 偏移。

VCCGT Voltage（VCCGT 电压）

允许配置 VCCGT 电压。

VDD_CPU Voltage（VDD_CPU 电压）

允许配置 VDD_CPU 电压。

MRC Voltage Configuration（MRC 电压配置）

Vdd2Mv Voltage（Vdd2Mv 电压）

VR 导轨连接到 DRAM。该电压通常等于或小于 VDD2 电压。

Vddq Voltage（Vddq 电压）

允许配置 CPU FIVR TX Vddq。

Vcclog Voltage（Vcclog 电压）

允许配置 CPU FIVR VCC IOG。

VccClk Voltage（VccClk 电压）

允许配置 CPU FIVR VCC CLK。

DDR5 PMIC Configuration（DDR5 PMIC 配置）

PMIC Voltage Option（PMIC 电压选项）

[United]（组合）允许综合调节 DIMM PMIC。
[Separate]（分开）允许单独调节 DIMM PMIC。

VDD Voltage（VDD 电压）

允许配置 DRAM 侧由 PMIC 支持的 VDD 电压。可通过 PMIC ADC 以 0.015V 为增量测量 VDD 输出。VDD 信息包含在内存 SPD 和 XMP 中，可通过内存信息 (Memory Information) 工具进行查看。

VDD Voltage Range（VDD 电压范围）

JEDEC 标准范围为 0.800V 至 1.435V。OC 需求范围为 0.800V 至 2.070V。若 PMIC OC CAP 为 JEDEC PMIC，则 OC 需求不适用。可通过内存信息 (Memory Information) 工具进行查看。

配置选项：[JEDEC Standard]（JEDEC 标准）、[OC Demand]（OC 需求）

VDDQ Voltage（VDDQ 电压）

允许配置 DRAM 侧由 PMIC 支持的 VDDQ 电压。可通过 PMIC ADC 以 0.015V 为增量测量 VDDQ 输出。VDDQ 信息包含在内存 SPD 和 XMP 内。可通过内存信息 (Memory Information) 工具进行查看。

配置选项：[JEDEC Standard]（JEDEC 标准）、[OC Demand]（OC 需求）

VDDQ Voltage Range（VDDQ 电压范围）

JEDEC 标准范围为 0.800V 至 1.435V。OC 需求范围为 0.800V 至 2.070V。若 PMIC OC CAP 为 JEDEC PMIC，则 OC 需求不适用。可通过内存信息 (Memory Information) 工具进行查看。

配置选项：[JEDEC Standard]（JEDEC 标准）、[OC Demand]（OC 需求）

VPP Voltage（VPP 电压）

允许配置 DRAM 侧由 PMIC 支持的 VPP 电压。可通过 PMIC ADC 以 0.015V 为增量测量 VPP 输出。VPP 信息包含在内存 SPD 和 XMP 内。可通过内存信息 (Memory Information) 工具进行查看。

PMIC Protection Unlock（PMIC 保护解锁）

允许配置 PMIC 保护解锁设置。

配置选项：[Auto]（自动）、[Enabled]（启用）

Current Limiter VDD（电流限制器 VDD）

允许配置输出电流限制器警告阈值设置。

配置选项：[Auto]（自动）[3.0 A] [3.5 A] [4.0 A] [Max TDC]（最大 TDC）

Current Limiter VDD（电流限制器 VDD）

允许配置输出电流限制器警告阈值设置。

配置选项：[Auto]（自动）[3.0 A] [3.5 A] [4.0 A] [Max TDC]（最大 TDC）

Current Limiter VPP（电流限制器 VPP）

允许配置输出电流限制器警告阈值设置。

配置选项：[Auto]（自动）、[0.5 A]、[Reserved]（保留）、[Max TDC]（最大 TDC）

PLL Voltage Configuration（PLL 电压配置）

P-Core PLL Voltage Offset（P-Core PLL 电压偏移）

PLL 电压偏移数值范围为 0 至 15，每个单元为 17.5mV。

E-Core PLL Voltage Offset（E-Core PLL 电压偏移）

PLL 电压偏移数值范围为 0 至 15，每个单元为 17.5mV。

SOC System Agent PLL Voltage Offset（SOC 系统代理 PLL 电压偏移）

PLL 电压偏移数值范围为 0 至 15，每个单元为 17.5mV。

CPU System Agent PLL Voltage Offset（CPU 系统代理 PLL 电压偏移）

PLL 电压偏移数值范围为 0 至 15，每个单元为 17.5mV。

Memory Controller PLL Voltage Offset（内存控制器 PLL 电压偏移）

PLL 电压偏移数值范围为 0 至 15，每个单元为 17.5mV。

P-Core PLL IRefTune Offset（P-Core PLL IRefTune 偏移）

PLL 电流参考调谐偏移，范围 0-15。此字段中提供的值会与 PLL 保险丝值相加。加上偏移后的值不能超过 0xF，如果超过，FW 会先将该值截为值 0xF，然后再将值写入保险丝。

E-Core PLL IRefTune Offset（E-Core PLL IRefTune 偏移）

PLL 电流参考调谐偏移，范围 0-15。此字段中提供的值会与 PLL 保险丝值相加。加上偏移后的值不能超过 0xF，如果超过，FW 会先将该值截为值 0xF，然后再将值写入保险丝。

Ring PLL IRefTune Offset（环形总线 PLL IRefTune 偏移）

PLL 电流参考调谐偏移，范围 0-15。此字段中提供的值会与 PLL 保险丝值相加。加上偏移后的值不能超过 0xF，如果超过，FW 会先将该值截为值 0xF，然后再将值写入保险丝。

AVX Configuration（AVX 配置）

AVX2 Voltage Guardband Scale Factor（AVX2 电压保护频带比例系数）

AVX2 电压保护频带比例系数用于控制施加于 AVX2 负载的电压保护频带。数值大于 1.00 时将增大电压保护频带，小于 1.00 时将减小电压保护频带。

Max Voltage Configuration（最大电压配置）

P-Core Max Voltage Limits（P-Core 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

E-Core Max Voltage Limits（E-Core 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

Ring Max Voltage Limits（环形总线最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

GT Max Voltage Limits（GT 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

SA Max Voltage Limits（SA 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

EMemSS Max Voltage Limits（EMemSS 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

NGU Max Voltage Limits（NGU 最大电压限值）

配置最大电压限值。最大电压应比 Vfused P0 大 200mV。

VR Configuration（VR 配置）

IA AC Loadline（IA AC 负载线路）

通过 AC 负载线路可以调整 CPU VID 标称电压。AC 交流负载线路值越高，相应地 VID 越高，高频或高负载条件下尤为明显。AC 负载线路值的单位为兆欧。数值范围为 0-20.00。默认 0 = AUTO/HW。

IA DC Loadline（IA DC 负载线路）

通过 DC 负载线路可以调节 CP 计算的功率值。DC 负载线路值的单位为兆欧。数值范围为 0-20.00。默认 0 = AUTO/HW。

CPU DLVR Configuration（CPU DLVR 配置）

CPU DLVR Mode（CPU DLVR 模式）

允许选择 CPU DLVR 模式。

配置选项：[Regulation Mode]（调节模式）、[Bypassed Mode]（避开模式）

Voltage Mode（电压模式）

允许选择电压模式。

配置选项：
[OC Mode]（OC 模式）：增大超频电压范围。
[Stable Mode]（稳定模式）：减小稳定系统电压范围。

Core Input Voltage（内核输入电压）

允许配置外部调压器供应的处理器输入电压。

配置选项：[Auto]（自动）、[Offset Mode]（偏移模式）、[Fixed Mode]（固定模式）

Core Input Voltage Load-Line Calibration（内核输入电压负载线路校准）

CPU Load-Line Calibration（CPU 负载线路校准）可帮助防止系统负载重时的 CPU 电压下降。

配置选项：[Auto]（自动）、[Level 1]（1 级）、[Level 2]（2 级）、[Level 3]（3 级）、[Level 4]（4 级）、[Level 5]

Save User Default（保存用户默认值）

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。

Load User Default（加载用户默认值）

加载以前保存的用户默认值。

Save User UEFI Setup Profile to Disk（将用户 UEFI 设置配置文件保

存到磁盘）

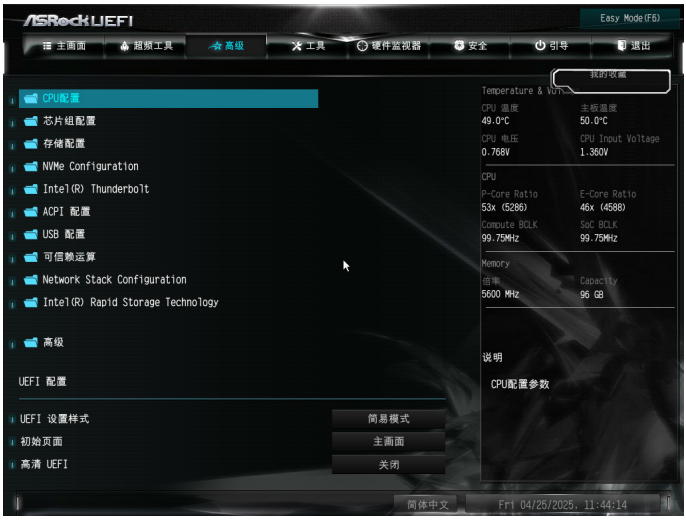
帮助您将当前 UEFI 设置作为用户配置文件保存到磁盘。

Load User UEFI Setup Profile from Disk（从磁盘中加载用户 UEFI 设置配置文件）

您可以从磁盘加载以前保存的配置文件。

3.4 Advanced（高级）屏幕

在此部分中，您可以配置以下项目：CPU Configuration（CPU 配置）、Chipset Configuration（芯片集配置）、Storage Configuration（存储配置）、Intel(R) Thunderbolt、ACPI Configuration（ACPI 配置）、USB Configuration（USB 配置）、Trusted Computing（信任计算）、Network Stack Configuration（网络堆栈配置）和 Intel(R) Rapid Storage Technology（Intel(R) 快速存储技术）。



在此部分中设置错误的值可能会造成系统故障。

UEFI Configuration（UEFI 配置）

UEFI Setup Style（UEFI 设置风格）

允许选择进入 UEFI 设置实用程序时的默认模式。
配置选项：[Easy Mode]（简单模式）、[Advanced Mode]（高级模式）

Active Page on Entry（进入时的初始页）

允许选择进入 UEFI 设置实用程序时的默认页面。

配置选项：[My Favorite]（我的收藏）、[Main]（主画面）、[OC Tweaker]、[Advanced]（高级）、[Tool]（工具）、[H/W Monitor]（硬件监视器）、[Security]（安全）、[Boot]（引导）、[Exit]（退出）

Full HD UEFI（全高清 UEFI）

[Auto]（自动）

选择 [Auto]（自动）时，如果显示器支持全高清分辨率，分辨率将设为 1920 x 1080。如果显示器不支持全高清分辨率，分辨率将设为 1024 x 768。

[Disabled]（禁用）

选择 [Disabled]（禁用）时，分辨率将直接设为 1024 x 768。

3.4.1 CPU Configuration（CPU 配置）

Processor P-Core Information（处理器 P-Core 信息）

按下 [Enter] 查看 P-Core 信息。

Processor E-Core Information（处理器 E-Core 信息）

按下 [Enter] 查看 E-Core 信息。

Active P-Cores（有效 P-Core）

允许选择在每个处理器封装中启用的内核数。注：P-Core 和 E-Core 数量将同时锁定。当二者均为 {0,0} 时，Pcode 将启用所有内核。

Active Processor E-Cores（有效处理器内核）

选择在每个处理器封装中启用的 E-Core 数量。注: P-Core 和 E-Core 数量将同时锁定。当二者均为 {0,0} 时，Pcode 将启用所有内核。

CPU C States Support（CPU C 状态支持）

允许启用 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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

C-State Auto Demotion（C 状态自动降级）

允许配置 C 状态自动降级。

配置选项：[C1][Disabled]（禁用）

CState Un-demotion（CState 取消降级）

允许配置 C 状态取消降级。

配置选项：[C1][Disabled]（禁用）

Package C State Demotion（封装 C 状态降级）

允许启用或禁用封装 C 状态降级。

Package CState Un-demotion（封装 CState 取消降级）

允许启用或禁用封装 C 状态取消降级。

CState Pre-Wake（C 状态预唤醒）

允许启用或禁用 C 状态预唤醒。禁用 - 到 1 可禁用 C 状态预唤醒。

IO MWAIT Redirection（IO MWAIT 重定向）

允许配置 IO MWAIT 重定向。设置后，会将发送到 IO 寄存器 PMG_IO_BASE_ADDRBASE+ 偏移 的 IO_read 指令映射到 MWAIT（偏移）。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Package C State Support（封装 C 状态支持）

允许启用 CPU、PCIe、内存、图形 C 状态支持以达到节能目的。

DC6 Latency WA（DC6 延迟 WA）

允许配置 DC6 延迟 WA。

CPU Thermal Throttling（CPU 过热降频保护）

允许启用 CPU 内部温度控制机制，以防 CPU 过热。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel AVX/AVX2

允许启用或禁用 Intel AVX 和 AVX2 指令。其仅适用于大核心。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Intel Virtualization Technology（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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

X2APIC Enable（APIC 启用）

允许启用或禁用 X2APIC 操作模式。\n 此选项配置为 Enabled（启用）时，“VT-d”选项必须为“Enabled”（启用），“X2APIC Opt Out”选项必须为“Disabled”（禁用）。\n“VT-d”选项配置为“Disabled”（禁用）时，此选项将呈灰色显示。

Legacy Game Compatibility Mode（传统游戏兼容性模式）

启用后，按下滚动锁定键将切换高效内核状态 - 当滚动锁 LED 亮起时高效内核挂起，LED 熄灭时高效内核取消挂起。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

3.4.2 Chipset Configuration（芯片集配置）

Re-Size BAR Support（支持调整 BAR 大小）

如果系统包含 BAR 大小可调整的 PCIe 设备，此选项可启用或禁用对大小可调整 BAR 的支持。

VT-d

Intel® Virtualization Technology for Directed I/O（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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

SR-IOV Support（SR-IOV 支持）

若系统包含具有 SR-IOV 功能的 PCIe 设备 利用此选项可启用或禁用 Single Root IO 虚拟化支持。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

DMI Link Speed（DMI 连接速度）

允许配置 DMI 插槽链接速度。

配置选项：[Gen1]、[Gen2]、[Gen3]、[Gen4]

PCI Express Native Control（PCI Express 本地控制）

选择启用后将增强 PCI Express 在操作系统下的节电性能。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

PCIE ASPM Support（PCIE ASPM 支持）

该选项可用于控制所有 CPU 下游设备的 ASPM 支持。

配置选项：[Disabled]（禁用）、[L0s]、[L1]、[L0sL1] [Auto]（自动）

PCH PCIE ASPM Support（PCH PCIE ASPM 支持）

该选项可用于控制所有 PCH 下游设备的 ASPM 支持。

配置选项：[Disabled]（禁用）、[L0s]、[L1]、[L0sL1] [Auto]（自动）

PCH DMI ASPM Support（PCH DMI ASPM 支持）

允许启用或禁用所有 PCH DMI 设备的 ASPM 支持。

配置选项：[Disabled]（禁用）、[L0s]、[L1]、[L0sL1] [Auto]（自动）

DMI ASPM Support（DMI ASPM 支持）

允许配置 PCH DMI ASPM 设置。

配置选项：[Disabled]（禁用）、[L0s]、[L1]、[L0sL1] [Auto]（自动）

PCIE Bifurcation（PCIE 分叉）

允许选择 DPCIE1 的宽度。

Onboard HD Audio（板载高清音频）

允许启用或禁用板载高清音频控制器。将此项目设为 Auto（自动）启用板载高清并在安装了声卡时自动禁用它。

配置选项：[Auto]（自动）、[Enabled]（启用）、 [Disabled]（禁用）

Front Panel（前面板）

允许选择前面板类型。

[HD]（高清）用于将前面板音频接头模式设置为高清音频。

[AC 97] 用于将前面板音频接头模式设置为 legacy AC'97。]

Onboard HDMI HD Audio（板载 HDMI 高清音频）

允许启用或禁用板载数字输出的音频。
此项目会在主板上安装了显卡时显示。

配置选项：[Enabled]（启用）、[Disabled]（禁用）。

Realtek 2.5G Ethernet Controller（Realtek 2.5G 以太网控制器）

允许启用或禁用板载 LAN。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Onboard WAN Device（板载 WAN 设备）

允许启用或禁用板载 WAN 设备。

配置选项：[Enabled]（启用）、[Disabled]（禁用）。

Deep Sleep（深度睡眠）

允许在计算机关闭时，配置深度睡眠模式以节能。我们建议禁用“深度睡眠”以取得更好的系统兼容性和稳定性。

配置选项: [Enabled]（启用）、[Enabled in S5]（S5 中启用）、[Enabled in S4 & S5]（S4 & S5 中启用）

Restore on AC/Power Loss（断电后恢复）

允许选择电源出现故障后的电源状态。

[Power Off]（关机）用于在电源恢复后使电源保持关闭。

[Power On]（开机）用于在电源恢复后启动系统。

NPU Device（NPU 设备）

允许启用或禁用 NPU （神经处理单元）设备。

3.4.3 Storage Configuration（存储配置）

SATA Controller(s) (SATA 控制器)

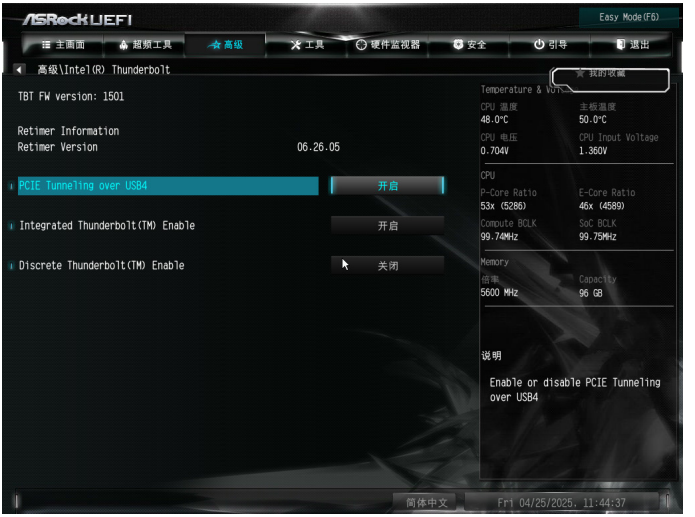
启用 / 禁用 SATA 控制器。

SATA Aggressive Link Power Management（SATA 积极链路电源管理）

SATA 积极链路电源管理允许 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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

3.4.4 Intel(R) Thunderbolt



PCIE Tunneling over USB4（通过 USB4 进行 PCIE 隧道传输）

允许启用或禁用通过 USB4 进行 PCIE 隧道传输。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Integrated Thunderbolt(TM) Enable（集成 Thunderbolt(TM) 启用）

允许启用或禁用集成 Thunderbolt(TM)。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Discrete Thunderbolt(TM) Enable（离散 Thunderbolt(TM) 启用）

允许启用或禁用离散 Thunderbolt(TM)。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

当此选项设为启用时，会出现以下选项供配置。

3.4.5 ACPI Configuration（ACPI 配置）

Suspend to RAM（挂起到 RAM）

允许对 ACPI 挂起类型 S1 选择 [Disabled]（禁用）。建议选择自动以实现 ACPI S3 节能。

配置选项：[Auto]（自动）[Disabled]（禁用）

PCIE Devices Power On（PCIE 设备开机）

允许通过 PCIE 设备唤醒系统，并启用网上唤醒。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

RTC Alarm Power On（自动定时开机）

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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）、[By OS]（通过操作系统）

USB Keyboard Power On（USB 键盘开机）

允许通过键盘或遥控器唤醒系统。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

USB Mouse Power On（USB 鼠标开机）

允许通过 USB 鼠标唤醒系统。

3.4.6 USB Configuration（USB 配置）

XHCI Hand-off（XHCI 接管）

对于无 XHCI 接管支持的操作系统，可选用此选项。XHCI 所有权变更应通过 XHCI 驱动程序声明。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

3.4.7 Trusted Computing（信任计算）

注：选项因所连接的 TPM 模块版本而异。

Security Device Support（安全设备支持）

允许启用或禁用 BIOS 安全设备支持。O.S. 将不会显示安全设备。TCG EFI 协议和 INT1A 接口将不可用。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Active PCR banks（有效 PCR 存储单元）

此项会显示有效 PCR 存储单元。

Available PCR Banks（可用 PCR 存储单元）

此项会显示可用 PCR 存储单元。

SHA256 PCR Bank（SHA256 PCR 存储单元）

允许启用或禁用 SHA256 PCR 存储单元。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

SHA384 PCR Bank（SHA384 PCR 存储单元）

允许启用或禁用 SHA384 PCR 存储单元。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

SM3_256 PCR Bank（SM3_256 PCR 存储单元）

允许启用或禁用 SM3_256 PCR 存储单元。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Pending Operation（待执行操作）

允许预定对安全设备的操作。

注：重新启动期间，计算机将重新引导，以更改设备状态。

配置选项：[None]（无）[TPM Clear]（TPM 清空）

Platform Hierarchy（平台层级）

允许启用或禁用平台层级。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Storage Hierarchy（存储层级）

允许启用或禁用存储层级。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Endorsement Hierarchy（批准层级）

允许启用或禁用批准层级。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Physical Presence Spec version（实际存在规范版本）

选择此项目将告知 OS 支持 PPI 规范版本 1.2 或 1.3。请注意，一些 HCK 测试可能不支持版本 1.3。

配置选项：[1.2] [1.3]

TPM 2.0 InterfaceType（TPM 2.0 接口类型）

允许查看 TPM 2.0 设备的通信接口：CRB 或 ITS。

Device Select（设备选择）

允许选择支持的 TPM 设备。

[TPM 1.2] 可限制对 TPM 1.2 设备的支持。

[TPM 2.0] 可限制对 TPM 2.0 设备的支持。

[Auto]（自动）同时支持 TPM 1.2 和 TPM 2.0 设备，默认支持 TPM 2.0 设备。如果未找到 TPM 2.0 设备，将枚举 TPM 1.2 设备。

3.4.8 Network Stack Configuration（网络堆栈配置）

Network Stack（网络堆栈）

允许启用或禁用 UEFI 网络堆栈。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

3.4.9 Intel(R) Rapid Storage Technology（Intel(R) 快速存储技术）

该表单集允许用户管理 Inter(R) RAID 控制器上的 RAID 卷。如果有磁盘连接到系统，该页面会显示磁盘信息。

Create RAID Volume（创建 RAID 卷）

按 [Enter] 可进入用于创建 RAID 卷的页面。

Name（名称）

输入不含特殊字符且长度不超过 16 个字符的唯一卷名称。

RAID Level（RAID 级别）

利用此项目可选择 RAID 级别。选项因连接的磁盘而异。

配置选项: [RAID0 (Stripe)]（RAID0（条带））、[RAID1 (Mirror)]（RAID01（镜像））、[RAID5 (Parity)]（RAID5（奇偶校验））

Select Disks（选择磁盘）

使用此项选择要包含在 RAID 阵列中的硬盘。

Stripe Size（条带大小）

使用此项选择 RAID 阵列的条带大小。

Create Volume（创建卷）

创建采用上面指定的设置的卷。

3.5 Tools（工具）

Media Sanitization（介质净化）

使用此工具安全擦除 SSD。此工具仅会列出支持安全擦除功能的 SSD。对 SSD 进行清理后，SSD 上的所有用户数据将永久销毁，无法恢复。

Auto Driver Installer

允许自动下载并安装所有必要的驱动程序。

[Enabled]（启用）

选择此项可启用 Auto Driver Installer 工具。如果已启用此项，进入可访问 Internet 的 Windows 后，Auto Driver Installer 工具将自动出现。

[Disabled]（禁用）

选择此项可禁用 Auto Driver Installer 工具。

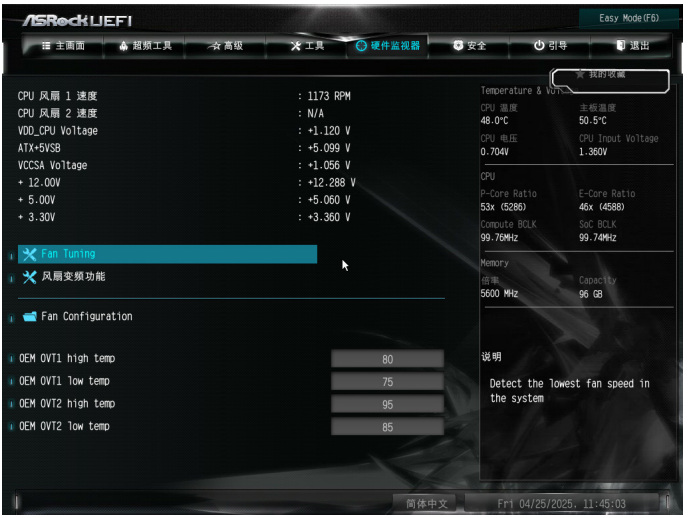
UEFI Update Utility（UEFI 更新实用程序）

Instant Flash

允许将 UEFI 文件保存在 USB 存储设备上，然后运行 Instant Flash（即时刷新）以更新您的 UEFI。请注意，USB 存储设备必须为 FAT32/16/12 文件系统。

3.6 Hardware Health Event Monitoring（硬件运行状况事件监控）屏幕

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。



注：选项因主板功能而异。

Fan Tuning（风扇调节）

选择此项后，BIOS 将继续检测连接到主板的风扇中速度最低的风扇。此过程将需要几分钟才能完成。

Fan-Tastic Tuning (变频风扇)

选择 CPU 风扇模式或选择自定义以设置 5 种 CPU 温度并为每种温度指定一个相应的风扇速度。

CPU Fan 1 Setting (CPU 风扇 1 设置)

选择 CPU 风扇 1 模式或选择自定义以设置 5 种 CPU 温度并为每种温度指定一个相应的风扇速度。

CPU Fan 2 Setting (CPU 风扇 2 设置)

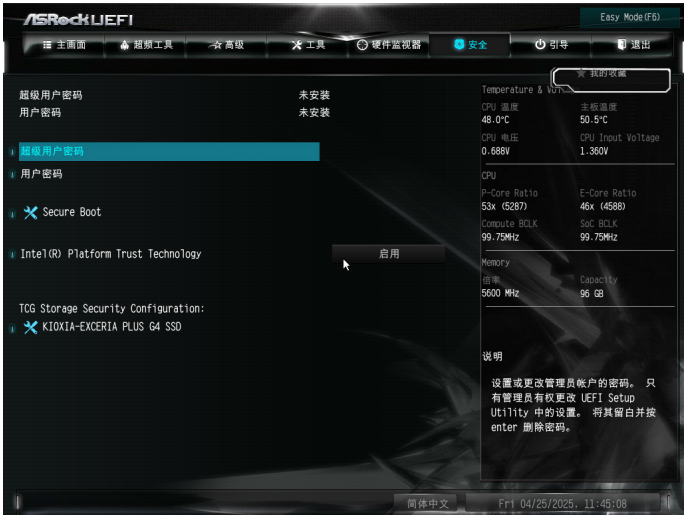
选择 CPU 风扇 2 模式，或选择自定义以设置 5 种 CPU 温度并为每种温度指定一个相应的风扇速度。

CPU Fan 2 Temp Source (CPU 风扇 2 溫度來源)

选择 CPU 风扇 2 的风扇温度源。

3.7 Security（安全）屏幕

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。



Supervisor Password（监督人密码）

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。

User Password（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。

Secure Boot（安全引导）

按 [Enter] 可配置 Secure Boot Settings（安全启动设置）。此功能可在 POST 期间保护系统免遭未授权访问和恶意软件破坏。

Intel(R) Platform Trust Technology（Intel(R) 平台信任技术）

允许启用或禁用 Intel PTT 功能。

[Enabled]（启用）用于启用 ME 中的 Intel PTT。

[Disabled]（禁用）用于禁用 ME 中的 Intel PTT。使用离散 TPM 模块。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

3.8 Boot（引导）屏幕

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。

Fast Boot（闪速启动）

快速启动可加快计算机的启动时间，但无法通过 USB 存储设备启动。只有 UEFI OS 或更高版本支持 Ultra Fast（超快）模式，如使用外部图形卡，还必须使用支持 UEFI GOP 的 VBIOS。请注意，Ultra Fast（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。

配置选项：[Disabled]（禁用）、[Ultra Fast]（超快）

Boot From Onboard LAN（从板载 LAN 引导）

允许通过板载 LAN 唤醒系统。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Setup Prompt Timeout（设置提示超时）

允许配置等待 UEFI 设置实用程序的秒数。

配置选项： [1] - [65535]

Bootup Num-Lock（启动数字锁定键）

允许选择在系统启动时 Num Lock（数字锁定键）关闭还是打开。

配置选项：[On]（开）、[Off]（关）

Boot Beep（引导蜂鸣声）

允许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。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Full Screen Logo（全屏标志）

[Enabled]（启用）选择此项可显示启动标志。

[Disabled]（禁用）选择此项可显示正常 POST 消息。

Boot Failure Guard Message（引导故障防护消息）

如果计算机多次引导失败，则系统会自动恢复默认设置。

配置选项：[Enabled]（启用）、[Disabled]（禁用）

Boot Failure Guard Count（引导故障防护计数）

允许配置系统自动恢复默认设置之前的引导尝试次数

配置选项：[2] - [250]

3.9 Exit（退出）屏幕

Save Changes and Exit（保存更改并退出）

选择此选项时以下信息 “Save configuration changes and exit setup?”（保存配置更改并退出设置？）会弹出。按下 <F10> 键或选择 [Yes]（是）将保存变更并退出 UEFI SETUP UTILITY。

Discard Changes and Exit（放弃更改并退出）

选择此选项时以下信息 “Discard changes and exit setup?”（放弃更改并退出设置？）会弹出。按下 <ESC> 键或选择 [Yes]（是）将不保存变更直接退出 UEFI SETUP UTILITY。

Discard Changes（放弃更改）

选择此选项时以下信息 “Discard changes?”（放弃更改？）会弹出。按下 <F7> 键或
选择 [Yes]（是）将放弃所有变更。

Load UEFI Defaults（加载 UEFI 默认值）

允许加载所有选项的 UEFI 默认值。可以使用 F9 键执行此操作。

Launch EFI Shell from filesystem device（从文件系统设备启动 EFI Shell）

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