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
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

1.2 导航键

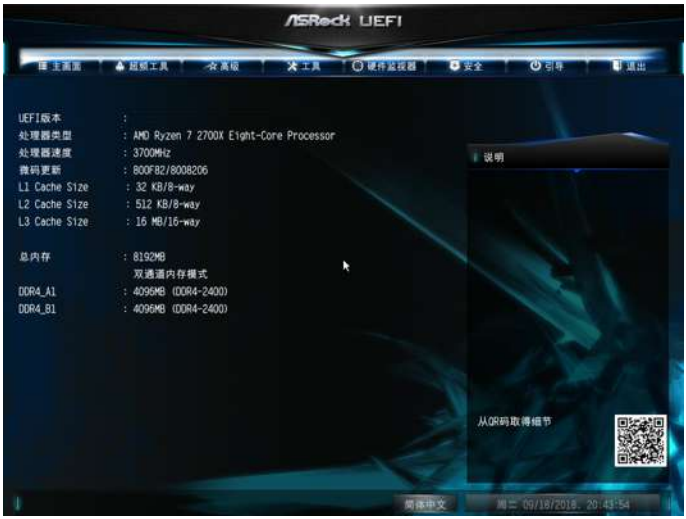
使用 < ← > 键或 < → > 键选择菜单栏上的选项，并使用 < ↑ > 键或 < ↓ > 键上下移动光标以选择项目，然后按 <Enter> 进入子屏幕。您也可以使用鼠标单击需要的项目。

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。

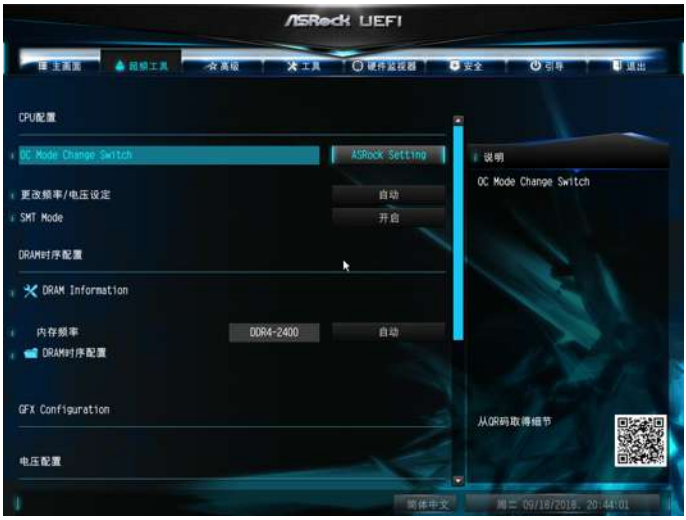


我的收藏

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

3 OC Tweaker 屏幕

在 OC Tweaker 屏幕中，您可以设置超频功能。



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。

CPU Configuration (CPU 配置)

CPU Frequency and Voltage Change（CPU 频率与电压更改）

若此项目设置为 [手动]，倍数与电压将根据用户选择来设置。最终结果根据 CPU 能力而定。

SMT Mode（SMT 模式)

此项目可用来关闭对称多线程技术。要开启对称多线程（SMT），将此项目设置为【自动】然后重启系统。
警告: 若系统开启 SMT 功能则不支持 S3。

DRAM Timing Configuration(DRAM 时序配置)

内存信息

浏览 DDR4 内存模块的 SPD（serial presence defect）。

DRAM Frequency(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。

GFX Clock Frequency(GFX 时钟频率)

本项目用来切换 GPU 频率。

GFX Core Voltage(GFX 核心电压)

本项目用来切换 GPU 电压。

Voltage Configuration (电压配置)

CPU SOC Voltage(CPU SOC 电压) (仅适用于 X370M-HDV R4.0 / AB350M-HDV R3.0)

本项目用来设置 VID 需求 CPU SOC 供应水平的电压。

DRAM Voltage (DRAM 电压)

使用它可配置 DRAM 电压。默认值是 [Auto]（自动）。

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)

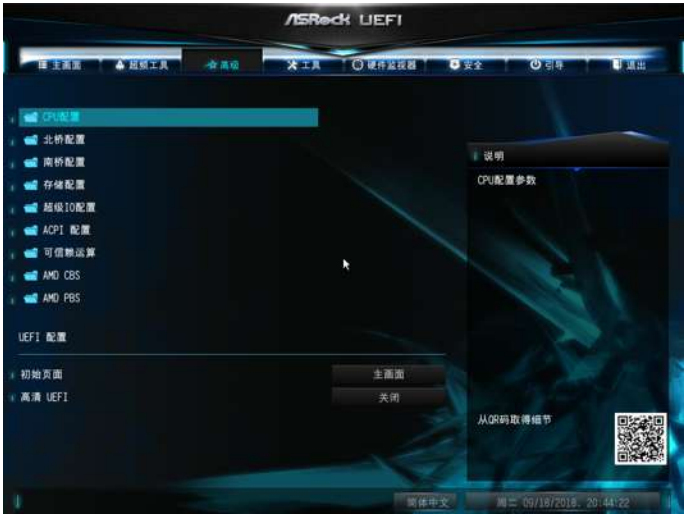
将当前 UEFI 设置作为用户默认配置文件保存到磁盘。

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。

4 Advanced(高级) 屏幕

在此部分中，您可以配置以下项目：CPU Configuration（中央处理器设置），North Bridge Configuration（北桥设置），South Bridge Configuration（南桥设置），Storage Configuration（存储设置），SuperIO Configuration（高级输入输出设置），ACPI Configuration（ACPI 电源管理设置），Trusted Computing(信任计算)，AMD CBS 和 AMD PBS.



在此部分中设置错误的值可能会造成系统故障。

UEFI Configuration(UEFI 设置)

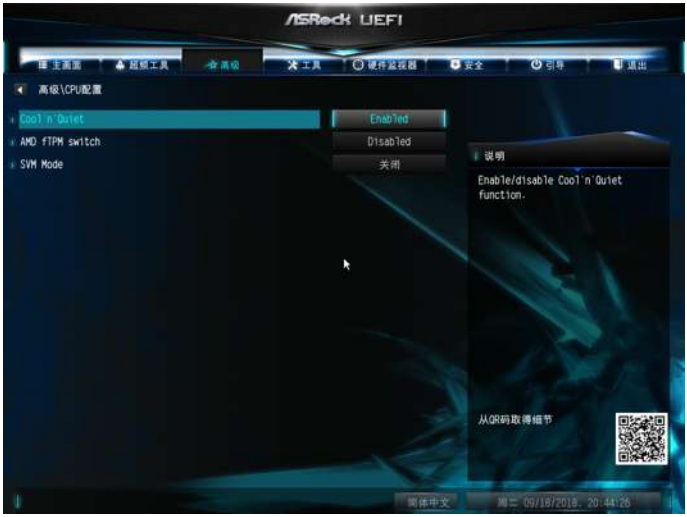
Active Page on Entry(初始页面)

选择进入 UEFI 设置实用程序时的默认页面。

Full HD UEFI(高清 UEFI)

当设置为 [自动] 时，若显示器支持全高清分辨率，则 UEFI 显示分辨率将为 1920 x 1080。若显示器不支持全高清分辨率，则 UEFI 显示分辨率为 1024 x 768。当设置为 [关闭] 时，UEFI 显示分辨率将为 1024 x 768。

4.1 CPU 配置



Cool ‘n’ Quiet(AMD 冷静设置)

使用此项打开或关闭 “AMD Cool ‘n’ Quiet Configuration” (AMD 冷静设置) 功能。默认值为 [Enabled](开启)。设定值有 :[Enabled](开启) 和 [Disabled](关闭)。如果您安装 Windows OS 并想开启这项功能 , 请将此项设置为 [Enabled](开启)。请注意开启这项功能可能会降低 CPU 电压和内存频率 , 并带来一些内存条或电源方面的系统稳定性或兼容性问题。如果出现上述问题 , 请将此项设置为 [Disabled](关闭)。

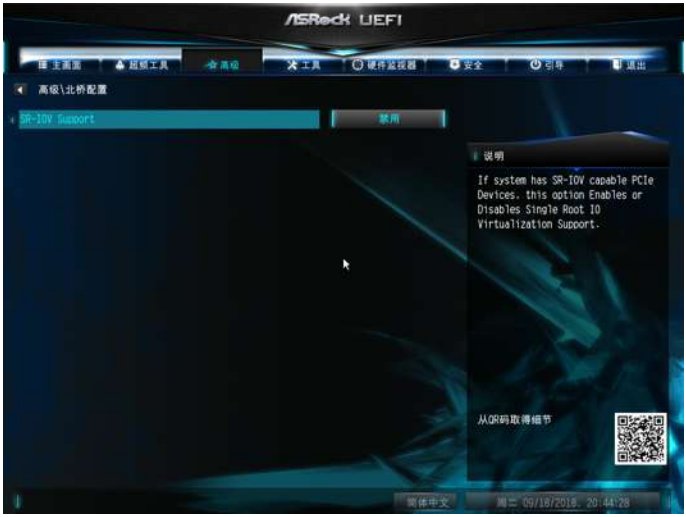
AMD fTPM Switch

使用此项打开或关闭 AMD fTPM Switch。

SVM(安全虚拟机)

当此项设为 [Enabled](开启) 时 ,VMM(Virtual Machine Architecture, 虚拟机架构) 可以利用 AMD-V 提供的额外硬件性能。设置选项 :[Enabled](开启) 和 [Disabled] (关闭)。

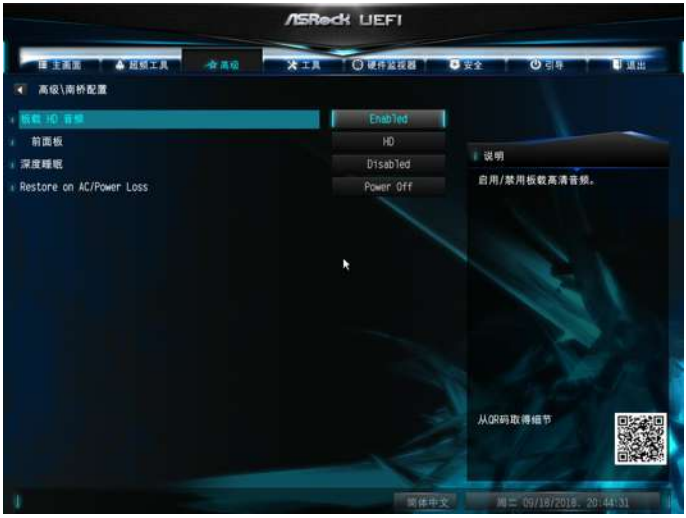
4.2 北桥芯片配置



SR-IOV 支持

在系统配有具备 SR-IOV 功能的 PCIe 设备时，启用 / 禁用 SR-IOV（单根 IO 虚拟化支持）。

4.3 南桥芯片配置



Onboard HD Audio (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。

Front Panel (前面板)

启用 / 禁用前面板高清音频。

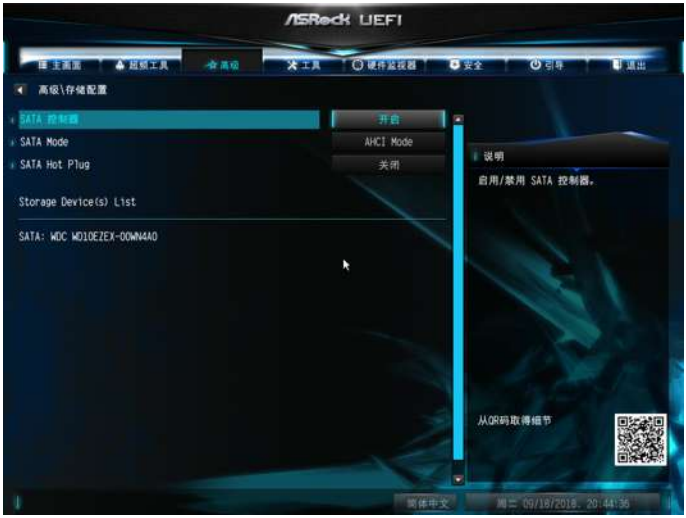
Deep Sleep (深度睡眠)

在计算机关闭时，配置深度睡眠模式以节能。

Restore on AC/Power Loss (断电后恢复)

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

4.4 存储配置



SATA Controller(s)(SATA 控制器)

启用 / 禁用 SATA 控制器。

SATA Mode(SATA 模式)

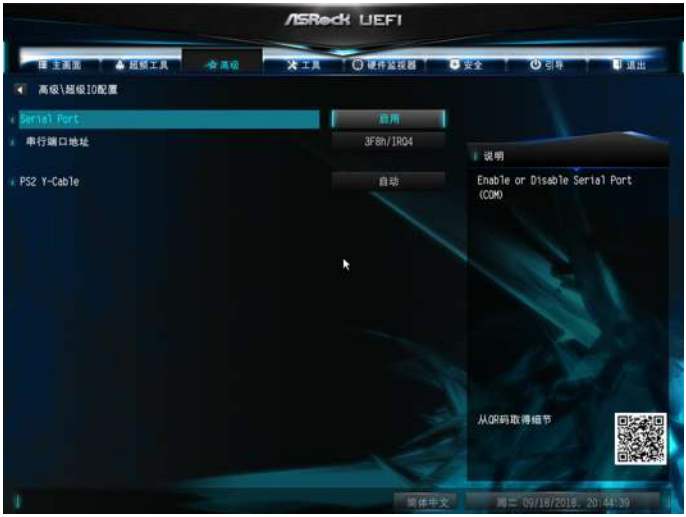
AHCI: 支持可提升性能的新功能。

RAID: 将多个磁盘驱动器合并到一个逻辑单元。

SATA Hot Plug(SATA 热插拔)

本项目用来开启 / 关闭 SATA 接口的热插拔功能。

4.5 超级 IO 配置



Serial Port (串行端口)

启用或禁用串行端口。

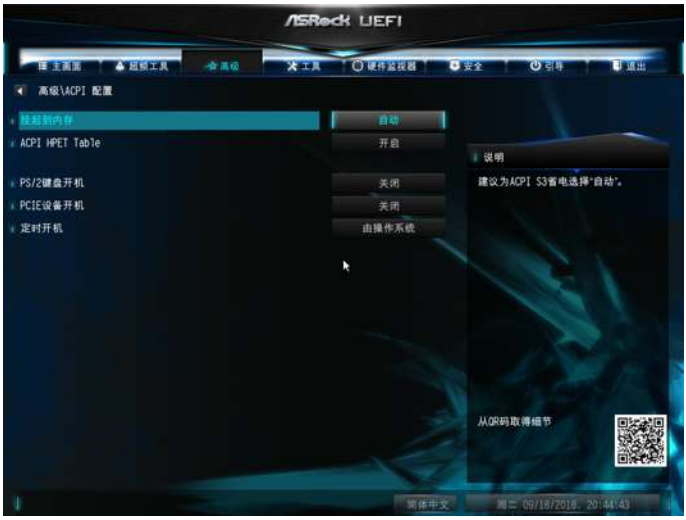
Serial Port Address (串行端口地址)

选择串行端口的地址。

PS2 Y-Cable

启用 PS2 Y 型电缆或将此选项设置为 [自动]。

4.6 ACPI 配置



Suspend to RAM(挂起到 RAM)

建议选择自动以实现 ACPI S3 节能。

ACPI HPET Table

启用 High Precision Event Timer（高精度事件计时器）以取得更好性能和通过 WHQL 测试。

PS/2 Keyboard Power On(PS/2 键盘开机)

允许通过 PS/2 键盘唤醒系统。

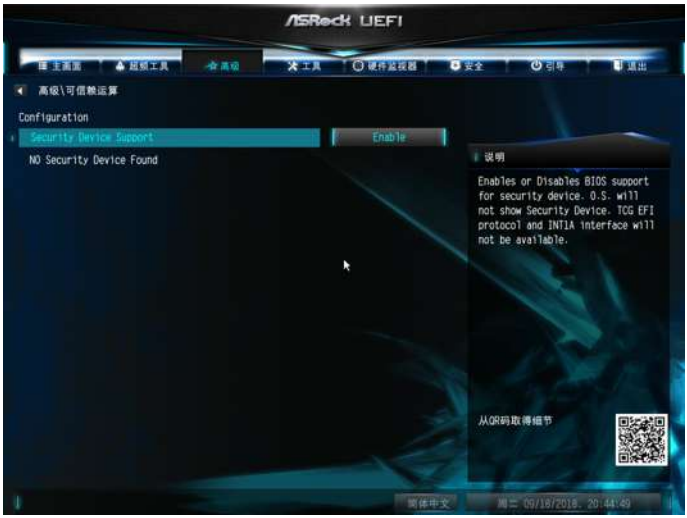
PCIE Devices Power On(PCIE 设备开机)

允许通过 PCIE 设备唤醒系统，并启用网上唤醒。

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。

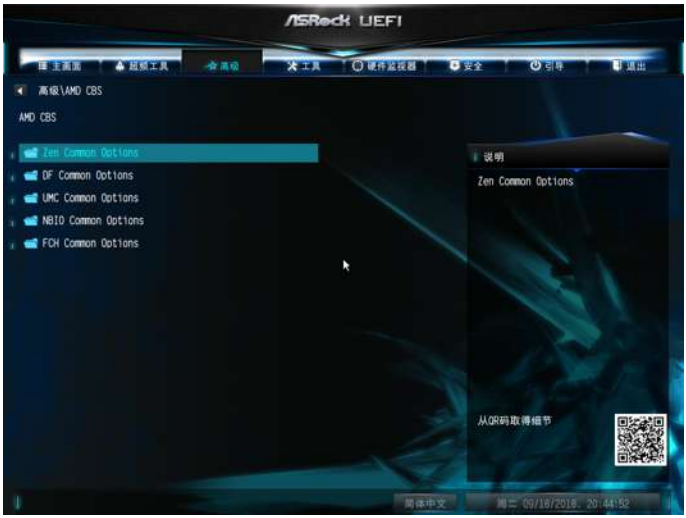
4.7 信任计算



Security Device Support(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。

4.8 AMD CBS



Zen Common Options（Zen 一般选项）

RedirectForReturnDis（ReturnDis 重定向）

从 CZ A0 上的 XV Core 的 GCC/C000005 问题的工作区，将 MSRC001_1029 解码设置 (DE_CFG) bit 14 [DecfgNoRdrctForReturns] 设置为 1。

L2 TLB Associativity（L2 TLB 结合）

0 - L2 TLB ways [11:8] 完全可结合。 1 - =L2 TLB ways [11:8] 仅支持 4K。

Platform first Error Handling（平台第一错误处理）

开启或关闭平台第一错误处理，遮盖单独 bank，掩盖来自每个 bank 的不同的错误干扰。

Core Performance Boost（核心性能加速）

本项目用来关闭 CPB。

Enable IBS（开启 IBS）

通过 MSRC001_1005[42] 开启 IBS，以及通过 MSRC001_1020[54] 关闭 SpecLockMap。

Global C-state Control（全部 C-State 控制）

本项目用来控制 IO C-state 生成和 DF C-State。

Opcache Control（Opcache 缓存控制）

本项目用来开启或关闭 Opcache 缓存。

OC Mode（超频模式）

OC1 - 16 cores/3.6GHz on 1.3375V

OC2 - 8 cores/3.7GHz on 1.369V

OC3 - 4 cores/3.75GHz on 1.374V\nMax Stress - 16 cores/3.8GHz on 1.400V

SEV-ES ASID Space Limit（SEV-ES ASID 空间限制）

使用在此空间限制下的 ASID 的 SEV VM 必须开启 SEV-ES 功能。有效值从 0x1 (1) - 0x10 (16)。

Core/Thread Enablement（核心 / 线程开启）

Downcore control（减核控制）

设置使用的核心数。若使用此项目移除任意核心，需重启系统使之后的设置生效。

SMTEN

此项目可用来关闭对称多线程技术。要开启对称多线程（SMT），将此项目设置为【自动】然后重启系统。

警告：若系统开启 SMT 功能则不支持 S3。

Streaming Stores Control（流存储控制）

开启或关闭流存储功能。

DF Common Options（DF 一般选项）

DRAM scrub time（内存除尘时间）

设置内存除尘的时间值。

Redirect scrubber control（重定向除尘器控制）

控制 DF::RedirScrubCtrl[EnRedirScrub]

Disable DF sync flood propagation（关闭 DF 拒绝服务攻击传播）

控制 DF::PIEConfig[DisSyncFloodProp].

Freeze DF module queues on error（错误时冻结 DF 模块队列）

控制 DF::PIEConfig[DisImmSyncFloodOnFatalError]

禁用此项目设置 DF:PIEConfig[DisImmSyncFloodOnFatalError].

GMI encryption control（GMI 加密控制）

GMI 加密控制。

Control GMI link encryption（控制 GMI 链接加密）

xGMI 加密控制。

Control xGMI link encryption（控制 xGMI 链接加密）

CC6 memory region encryption（CC6 内存区域加密）

控制 CC6 保存 / 恢复内存是否加密。

Location of private memory regions（私人内存区域位置）

控制私人内存区域 (PSP, SMU and CC6) 是否在内存顶端或被分配。请注意，被分配需要所有内存芯片。另外，无论此项目设置为何，如果某些芯片没有内存它将始终在内存顶部。

System probe filter（系统调查筛选）

本项目用来控制调查筛选是否开启。关闭系统筛选的地方不会对零件产生任何影响。

Memory interleaving（内存交叉存储）

控制内存交叉存取的质地层（自动、无、通道、芯片、插槽）。注意：通道、芯片和插槽对内存安装有要求，且若内存不支持所选设置则该设置将被忽略。

Memory interleaving size （内存交叉存储容量）

控制内存交叉存储容量。有效值为自动、 256 bytes、512 bytes、1 Kbytes 或 2Kbytes。此设置决定了交叉存储的起始地址（bit 8, 9, 10 或 11）。

Channel interleaving hash（通道交叉存储散列）

控制地址位是否在通道交叉存储模式中进行散列。只有当交叉存储设置为通道，且交叉存储容量为 256 或 512 byte 时此区域才可使用。

Memory Clear（内存清除）

若关闭此项目，BIOS 不会在内存训练后进行内存清除（除非使用 non-ECC 内存条）。

UMC Common Options（UMC 一般选项）

DDR4 Common Options（DDR4 一般选项）

DRAM Controller Configuration（内存控制器设置）

内存控制器设置。

DRAM Power Options（内存电源选项）

Cmd2T

在 ADDR/CMD 上选择 1T 或 2T 模式。

Gear Down Mode（降档模式）

设置降档模式。

CAD Bus Configuration（CAD 总线设置）

CAD Bus Timing User Controls（CAD 总线时序用户控制）

设置 CAD 总线信号的时间为自动或手动。

CAD Bus Drive Strength User Controls（CAD 总线驱动强度用户控制）

设置 CAD 总线信号的驱动强度为自动或手动。

Data Bus Configuration（数据总线设置）

Data Bus Configuration User Controls（数据总线设置用户控制）

将驱动强度模式设置为自动或手动。

Common RAS（一般 RAS）

Data Poisoning（数据中毒）

开启或关闭数据中毒： UMC_CH::EccCtrl[UcFatalEn] UMC_CH::EccCtrl[WrEccEn]

应同时开启或关闭。

Security （安全性）

TSME

透明 SME: AddrTweakEn = 1; ForceEncrEn =1; DataEncrEn = 0

Data Scramble（数据扰频）

数据扰频 : DataScrambleEn

DRAM Memory Mapping （DRAM 内存寻址）

Chipselect Interleaving（芯片选择交叉存储）

在 node 0 选择的 DRAM 芯片组之间交叉存取内存区块。

BankGroupSwap（Bank 群组交换）

设置 Bank 群组交换。

BankGroupSwapAlt

设置 BankGroupSwapAlt。

Address Hash Bank（地址散列 Bank）

设置 bank 地址散列 .

Address Hash CS（地址散列 CS）

设置 CS 地址散列。

NVDIMM

Memory MBIST（内存 MBIST）

MBIST Enable（MBIST 开启）

设置内存 MBIST。

MBIST SubType Test（MBIST 子类型测试）

选择 MBIST 子测试 – 单一芯片选择，多芯片选择，地址行测试或执行所有测试。

MBIST Aggressors（MBIST 侵略）

本项目用来设置 MBIST Aggressor 测试。

MBIST Per Bit Slave Die Reporting（MBIST 每位从属芯片报告）

开启或关闭 MBIST 每位从属芯片结果报告。

NBIO Common Options（NBIO 一般选项）

NB Configuration（北桥设置）

IOMMU

使用此项目开启或关闭 IOMMU。默认设置值为【关闭】。

Determinism Slider（决定滑块）

【自动】
使用默认的性能决定设置。

cTDP Control

【自动】
使用融合 cTDP。

【手动】
用户可以自定义设置 cTDP。

Fan Control（风扇控制）

【自动】
使用默认的风扇控制器设置。

【手动】
用户可以自定义设置风扇控制器。

PSI

关闭 PSI。

ACS Enable（ACS 开启）

开启 ACS。

PCIe ARI Support（PCIe ARI 支持）

Enables Alternative Routing-ID Interpretation（开启 Alternative Routing-ID Interpretation）

CLDO_VDDP Control（CLDO_VDDP 控制）

【手动】
若选择此项目，用户可自定义 CLDO_VDDP 电压。

HD Audio Enable（高保真音频开启）

开启高保真音频。

FCH Common Options（FCH 一般选项）

SATA Configuration Options（SATA 设置选项）

SATA Controller（SATA 控制器）

开启或关闭板载 SATA 控制器。

Sata RAS Support（SATA RAS 支持）

开启或关闭 SATA RAS 支持。

Sata Disabled AHCI Prefetch Function（SATA 关闭 AHCI 预取功能）

设置 SATA 关闭 AHCI 预取功能。

Aggresive SATA Device Sleep Port 0（Aggressive SATA 设备睡眠端口 0）

设置 Aggressive SATA 设备睡眠端口 0。

Aggresive SATA Device Sleep Port 1（Aggressive SATA 设备睡眠端口 1）

设置 Aggressive SATA 设备睡眠端口 1。

USB Configuration Options（USB 设置选项）

XHCI controller enable（XHCI 控制器开启）

设置 USB3 控制器。

SD (Secure Digital) Options（SD 选项）

SD Configuration Mode（SD 配置模式）

选择 SD 模式。

Ac Power Loss Options（Ac 掉电选项）

选择 Ac 失控方法。

I2C Configuration Options（I2C 设置项目）

Uart Configuration Options（Uart 设置项目）

ESPI Configuration Options（ESPI 设置项目）

XGBE Configuration Options（XGBE 设置项目）

eMMC Options（eMMC 选项）

NTB Common Options（NTB 一般选项）

DRAM Memory Mapping（DRAM 内存寻址）

Chipselect Interleaving（芯片选择交叉存储）

在 node 0 选择的 DRAM 芯片组之间交叉存取内存区块。

BankGroupSwap（Bank 群组交换）

设置 Bank 群组交换。

BankGroupSwapAlt

设置 BankGroupSwapAlt。

Address Hash Bank（地址散列 Bank）

设置 bank 地址散列。

Address Hash CS（地址散列 CS）

设置 CS 地址散列。

NVDIMM

Memory MBIST（内存 MBIST）

MBIST Enable（开启 MBIST）

本项目用来设置内存 MBIST。

MBIST SubType Test（MBIST 子类型测试）

选择 MBIST 子测试 – 单一芯片选择，多芯片选择，地址行测试或执行所有测试。

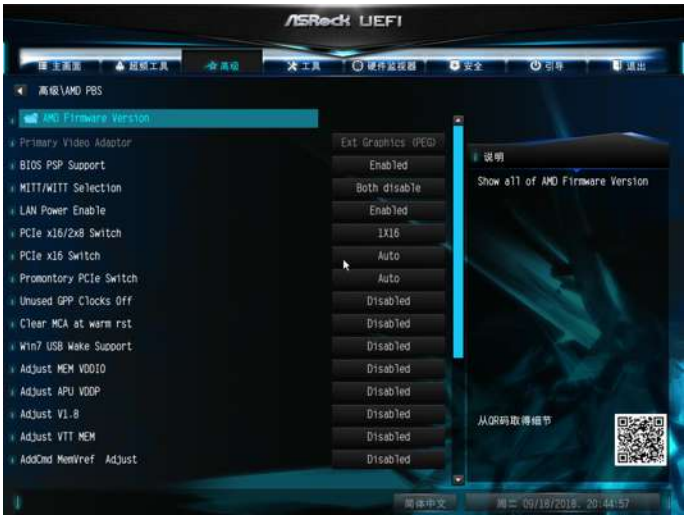
MBIST Aggressors（MBIST 侵略）

本项目用来设置 MBIST Aggressor 测试。

MBIST Per Bit Slave Die Reporting（MBIST 每位从属芯片报告）

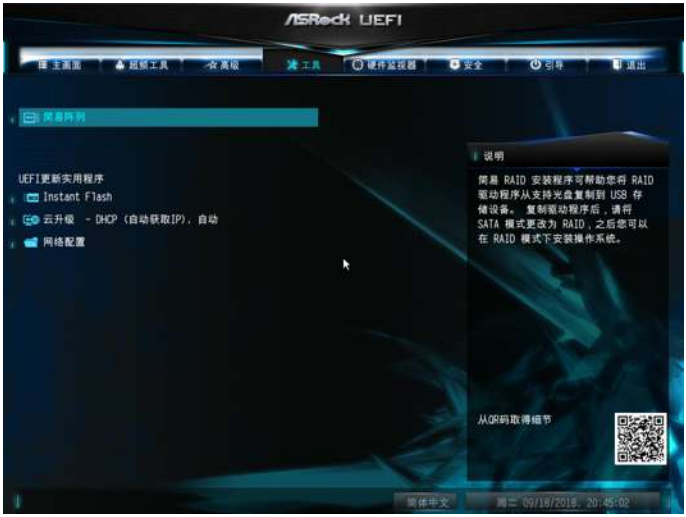
本项目用来设置 MBIST 每位从属芯片报告。

4.9 AMD PBS



AMD PBS 菜单可用来设置 AMD 特定功能。

5 Tools(工具)



Easy RAID Installer (简易阵列)

简易阵列安装程序可帮助您将 RAID 驱动程序从支持光盘复制到 USB 存储设备。复制驱动程序后，请将 SATA 模式更改为 RAID，之后您可以在 RAID 模式下安装操作系统。

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。

Network Configuration(网络配置)

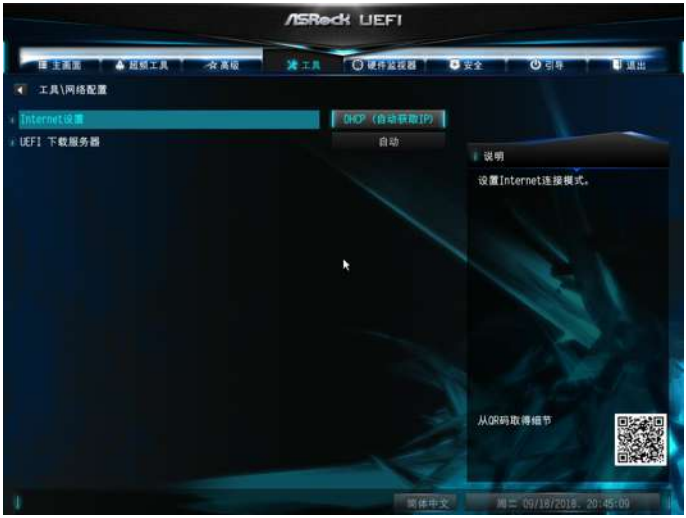
使用它可配置云升级的网络连接设置。

Internet Setting(Internet 设置)

在设置实用程序中启用或禁用声效。

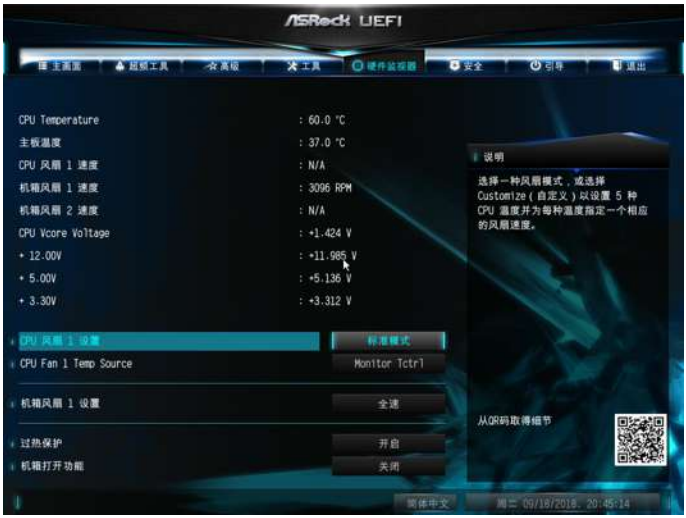
UEFI Download Server(UEFI 下载服务器)

选择一个服务器来下载 UEFI 固件。



6 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。



CPU Fan 1 Setting (CPU 风扇 1 设置)

选择 CPU 风扇 1 模式或选择 Customize(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 Temp Source (CPU 风扇 1 溫度來源)

选择 CPU 风扇 1 1 温度來源。

Chassis Fan 1 Setting (机箱风扇 1 设置)

选择机箱风扇 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。

Chassis Fan 1 Temp Source (机箱风扇 1 溫度來源)

选择机箱风扇 1 温度來源。

Over Temperature Protection (过热保护)

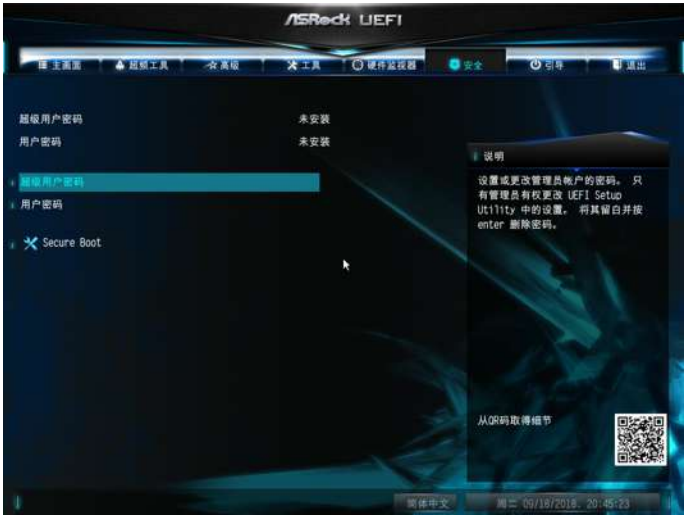
启用过热保护时，在主板过热时系统会自动关闭。

Case Open Feature (開箱偵測功能)

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。

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)

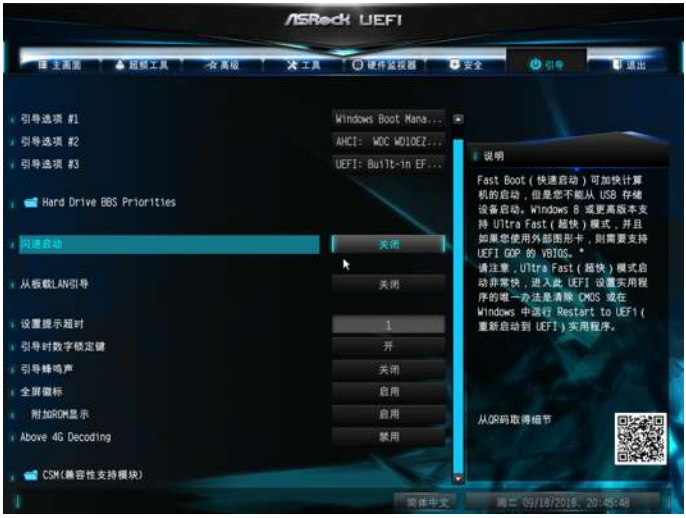
设置或更改用户帐户的密码。用户不能更改 UEFI Setup Utility 中的设置。将其留白并按 enter 删除密码。

Secure Boot(安全引导)

启用可支持安全引导。

8 Boot Screen(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)

Fast Boot（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。

Boot From Onboard LAN(从板载 LAN 引导)

允许通过板载 LAN 唤醒系统。

Setup Prompt Timeout(设置提示超时)

配置等待设置热键的秒数。

Bootup Num-Lock(启动数字锁定键)

选择在系统启动时 Num Lock（数字锁定键）关闭还是打开。

Boot Beep (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。

Full Screen Logo(全屏标志)

启用可显示引导标志，禁用可显示正常 POST 信息。

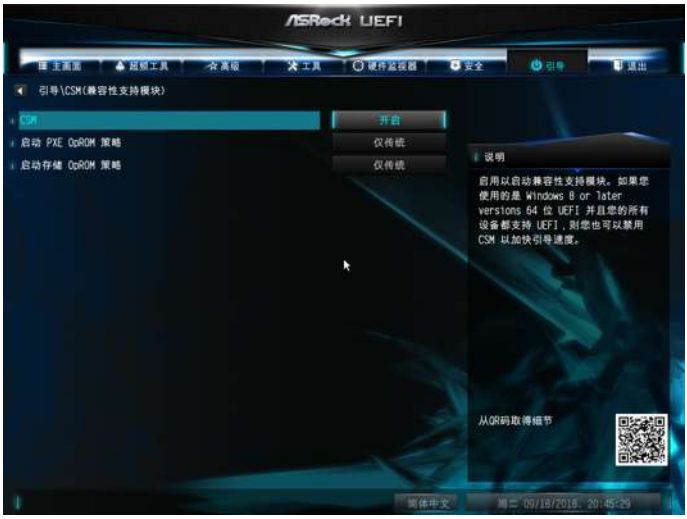
AddOn ROM Display(附加 ROM 显示)

启用 AddOn ROM Display（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标志）。禁用可取得更快引导速度。

大于 4G 地址空间的解码

启用 / 禁用要在大于 4G 地址空间中解码的 64 位功能设备。

CSM (兼容性支持模块)



CSM

启用可启动 Compatibility Support Module(兼容性支持模块)。请勿禁用它，除非您正在运行 WHCK 测试。

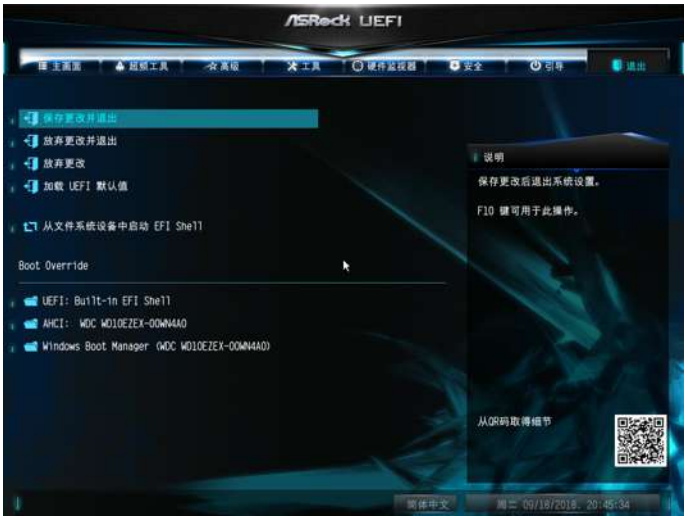
Launch PXE OpROM Policy (启动 PXE OpROM 策略)

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。

Launch Storage OpROM Policy (启动存储 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。

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。选择 [OK]（确定）可更改并退出 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。选择 [OK]（确定）可退出 UEFI SETUP UTILITY 而不保存任何更改。

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。选择 [OK]（确定）放弃所有更改。

Load UEFI Defaults(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。

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

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