Dell EMC PowerEdge MX840c

BIOS 和 UEFI 参考指南

部件号: E05B Series
管制类型： E05B001
December 2020
Rev. A00

DELL EMC

注意、小心和警告

注： “注意”表示帮助您更好地使用该产品的重要信息。

小心： **“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。**

警告： **“警告”表示可能会导致财产损失、人身伤害甚至死亡。**

目录

1

BIOS 和 UEFI

通过使用系统固件，可以在不引导至操作系统的情况下管理系统的基本设置和功能。

主题：

用于管理预操作系统应用程序的选项

系统提供了以下用于管理预操作系统应用程序的选项：

- 系统设置
- Dell Lifecycle Controller
- 引导管理器
- 预引导执行环境 (PXE)

系统设置

通过使用 **System Setup** 屏幕，您可以配置 BIOS 设置、iDRAC 设置、以及系统的设备设置。

注: 默认情况下，所选字段的帮助文本显示在图形浏览器中。要在文本浏览器中查看帮助文本，请按 F1。

您可以通过以下两种方法访问系统设置程序：

- 标准图形浏览器 — 默认设置下启用的浏览器。
- 文本浏览器 — 这种浏览器通过控制台重定向启用。

查看系统设置程序

要查看 **System Setup**（系统设置程序）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

系统设置程序详细信息

系统设置主菜单屏幕详细信息如下：

选项	说明
System BIOS（系统 BIOS）	允许您配置 BIOS 设置。
iDRAC Settings	允许您配置 iDRAC 设置。 iDRAC 设置设置程序是一种接口，用于使用 UEFI（统一扩展固件接口）设置和配置 iDRAC 参数。可使用 iDRAC 设置公用程序启用或禁用各种 iDRAC 参数。有关此实用程序的更多信息，请参阅 *Integrated Dell Remote Access Controller User's Guide（集成戴尔远程访问控制器用户指南）*，网址：www.dell.com/idracmanuals。
Device Settings（设备设置）	允许您配置设备设置，如网卡或存储控制器。

系统 BIOS

您可以使用 **System BIOS** 屏幕编辑特定功能，如引导顺序、系统密码、设置密码、设置 SATA 和 PCIe NVMeRAID 模式，以及启用或禁用 USB 端口。

查看系统 BIOS

要查看 **System Setup**（系统设置程序）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。

系统 BIOS 设置详细信息

关于此任务

System Profile Settings（系统配置文件设置）屏幕详细信息说明如下：

选项	说明
System Information（系统信息）	显示有关系统的信息，如系统型号名称、BIOS 版本、服务标签等。
Memory Settings	显示与所安装内存有关的信息和选项。
Processor Settings（处理器设置）	显示与处理器有关的信息和选项，如速度、高速缓存大小等。
SATA Settings	显示用于启用或禁用集成 SATA 控制器和端口的选项。
NVMe Settings	显示用于更改网络设置的选项。如果系统中包含的 NVMe 驱动器您想要配置在 RAID 阵列中,您必须在此字段和 **Embedded SATA (嵌入** 式 SATA)字段中设置 **SATA Settings (** SATA 设置)菜单上为 **RAID Mode**（RAID 模式)。您可能还需要的 **Boot Mode (引导模式**)设置更改为 **UEFI**。如果不是,则应将此字段设置为 **非 RAID** 模式。
Boot Settings（引导设置）	显示各选项以指定引导模式（BIOS 或 UEFI）。可让您修改 UEFI 和 BIOS 引导设置。

选项	说明
网络设置	指定用于管理 UEFI 网络设置和引导协议的选项。 传统 网络设置从 **Device Settings（设备设置）**菜单将受管。
Integrated Devices	显示用于管理集成设备控制器和端口的选项，以及指定相关的功能和选项。
Serial Communication	显示用于管理串行端口的选项，以及指定相关的功能和选项。
System Profile Settings	显示用于更改处理器电源管理设置、内存频率等等的选项。
System Security	显示用于配置系统安全设置的选项，如系统密码、设置密码、可信平台模块 (TPM) 安全和 UEFI 安全引导。它还可以管理系统上的电源按钮。
Redundant OS Control	设置冗余操作系统控制的冗余操作系统信息。
Miscellaneous Settings	指定更改系统日期和时间的选项。

System Information（系统信息）

您可以使用 **System Information**（系统信息）屏幕来查看系统属性，如服务标签、系统型号名称和 BIOS 版本。

查看系统信息

要查看 **System Information** 屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu** 屏幕中，单击 **System BIOS**。
4. 在 **System BIOS** 屏幕中，单击 **System Information**。

System Information（系统信息）的详细信息

关于此任务

System Information（系统信息）屏幕详细信息如下：

选项	说明
系统型号名称	指定系统的型号名称。
系统 BIOS 版本	指定系统上安装的 BIOS 版本。
系统 Management Engine 版本	显示 Management Engine 固件的当前版本。
系统服务标签	指定系统服务标签。
系统制造商	指示原始设备制造商 (OEM) 名称。
系统制造商联系人信息	指示原始设备制造商 (OEM) 的联系信息。
系统 CPLD 版本	指定系统复杂可编程逻辑设备 (CPLD) 固件的当前版本。

选项	说明
辅助系统 CPLD 版本	指定系统复杂可编程逻辑设备 (CPLD) 固件的当前版本。
UEFI 合规性版本	指定系统固件的 UEFI 合规性等级。

Memory Settings

您可以使用 **Memory Settings** 屏幕来查看所有内存设置以及启用或禁用特定内存功能，如系统内存测试和节点交叉。

查看内存设置

要查看 **Memory Settings**（内存设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Memory Settings**（内存设置）。

内存设置详细信息

关于此任务

内存设置屏幕详细信息如下：

选项	说明
系统内存大小	指定系统的内存大小。
系统内存类型	指定系统中安装的内存类型。
系统内存速度	指定系统内存速度。
系统内存电压	指定系统内存电压。
视频内存	指定视频内存容量。
系统内存测试	指定系统内存测试是否在系统引导期间运行。选项包括**已启用**和**已禁用**。该选项默认设置为**已禁用**。 **注:** 设置为**已启用**时，系统需要更长引导时间。引导时间取决于系统内存的大小。
Dram 刷新延迟	通过启用 **CPU 内存控制器**来推迟运行**刷新**命令，您可以提高一些工作负载的性能。通过最小化延迟时间，可确保内存控制器定期运行**刷新**命令。对于基于英特尔的服务器，此设置仅影响配置 DIMM（使用 8 Gb 密度 DRAM）的系统。
内存运行模式	指定内存运行模式。可用选项为**优化器模式**、**单列备用模式**、**多列备用模式**、**镜像模式**和**戴尔故障恢复模式**。该选项默认设置为**优化器模式**。 **注:** 根据系统内存配置，**内存运行模式**可能有不同的默认设置和可用选项。 **注:** **戴尔故障恢复模式**建立故障恢复内存区域。此模式可由支持加载关键应用程序或启用操作系统内核功能的操作系统使用，以最大化系统可用性。 **注:** 如果已安装 DC 傲腾永久性内存，则应只选择“优化器模式”。

选项	说明
内存运行模式的当前状态	指定内存运行模式的当前状态。
故障恢复模式内存大小 [%]	选择此选项可定义在**内存运行模式**中选择故障恢复模式时必须使用的总内存大小的百分比。未选择**故障恢复模式**时，此选项将呈灰色显示，并且不会被**故障恢复模式**使用。
节点交叉存取	指定是否支持非一体化内存体系结构 (NUMA)。如果此字段为**已启用**，则在安装对称内存配置的情况下支持内存交叉存取。如果为**已禁用**，则系统支持 NUMA（非对称）内存配置。该选项默认设置为**已禁用**。
ADDDC 设置	启用或禁用 **ADDDC 设置**功能。已启用自适应双 DRAM 设备纠正 (ADDDC) 时，将动态映射故障 DRAM。当设置为**已启用**时，在特定工作负载下可能对系统性能造成一些影响。此功能仅适用于 x4 DIMM。该选项默认设置为**已启用**。
16 Gb DIMM 的本机 tRFC 时间	支持 16 Gb 密度 DIMM 以按照其编程行刷新周期时间 (tRFC) 运行。启用此功能可提高某些配置的系统性能。但是，启用此功能将不会对具有 16 Gb 3DS/TSV DIMM 的配置产生影响。该选项默认设置为**已启用**。
伺机自刷新	启用或禁用伺机自刷新功能。该选项默认设置为**已禁用**。
可纠正的错误日志记录	启用或禁用可纠正内存阈值错误的日志记录。该选项默认设置为**已启用**。
永久性内存	此字段控制永久性内存上的系统。如果在系统中安装了永久性内存模块，则可以使用此选项。

永久性内存详细信息

关于此任务

永久性内存屏幕详细信息如下所述：

选项	说明
永久性内存	启用或禁用 NVDIMM-N 的持久性。如果此选项设置为**关闭**，则所有 NVDIMM-N 的持久性已禁用且未呈现给操作系统（数据将不保留）。如果此选项被设置为**非易失性 DIMM**，则所有 NVDIMM-N 的持久性已启用且呈现给操作系统（数据将保留）。默认情况下，该选项设置为**非易失性 DIMM**。
永久性内存清理	在开机自检过程中启用永久性内存的轮询清理。
清除所有 NVDIMM	启用或禁用 NVDIMM-N 上的数据清除。如果设置为**启用**，NVDIMM-N 上的所有数据都会丢失。此选项用于上移除数据 NVDIMM-N，重新利用系统。该选项默认设置为**禁用**。
NVDIMM-N 只读	启用或禁用 NVDIMM-N 的只读选项。如果设置为**启用**，强制所有 NVDIMM-N 为只读。只读旨在是调试或维护时客户想要访问 NVDIMM-N 数据，并以将其锁定，无法更新。该选项默认设置为**禁用**。
NVDIMM-N 交叉存取	在 NVDIMM-N 上启用或禁用交叉存取。易失性 RDIMM 交叉存取策略未受此选项的影响。该选项默认设置为**禁用**。
电池状态	指示 NVDIMM-N 电池是否已就绪。**电池状态**可以显示以下状态之一： • **存在且已就绪** • **存在且脱机** • **未就绪** 以下设置适用于系统中存在的每个 NVDIMM-N。
NVDIMM-N 内存位置	在每个通道中指定 NVDIMM-N 的位置。
NVDIMM-N 内存大小	指定有关 NVDIMM-N 容量的信息。
NVDIMM-N 内存速度	指定有关 NVDIMM-N 的速度的信息。
NVDIMM-N 内存固件版本	指定有关 NVDIMM-N 上当前固件版本的信息。
NVDIMM-N 内存序列号	指定有关 NVDIMM-N 的序列号的信息。

选项	说明
剩余额定写寿命 [%]	以百分比的形式指定剩余 NVDIMM-N 快擦写寿命时间的信息。
Sanitize NVDIMM	启用清除特定的 NVDIMM-N 上的数据,并会导致特定 NVDIMM-N 上的数据丢失。

永久性内存屏幕详情可在 *NVDIMM-N User Guide* 和 *DCPMM User Guide* 中查看，网址：www.dell.com/poweredgemanuals。

Processor Settings（处理器设置）

您可以使用 **Processor Settings（处理器设置）**屏幕查看处理器设置和执行特定功能，如启用虚拟化技术、硬件预取器逻辑处理器空闲和随机自刷新。

查看处理器设置

要查看 **Processor Settings**（处理器设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Processor Settings**（处理器设置）。

处理器设置详细信息

关于此任务

处理器设置屏幕详细信息如下：

选项	说明
逻辑处理器	启用或禁用逻辑处理器并显示逻辑处理器的数量。如果此选项设置为**已启用**，BIOS 会显示所有逻辑处理器。如果此选项设置为**已禁用**，BIOS 只会显示每个核心的一个逻辑处理器。该选项默认设置为**已启用**。
CPU 互联速度	使您能够在系统中的 CPU 之间不事先通知之间的通信链接的频率。 **注:** 标准 和基本 bin 处理器支持较低的链路频率。 可用的选项是 **最大数据速率**、 **10.4 GT / s**、和 **9.6 GT / s**。该选项的默认设置为**全面**。 最大数据率表示 BIOS 以处理器支持的最大频率运行通信链路。您也可以选择特定的频率的处理器支持,该驱动器可以有所不同。 为获得最佳性能,您应选择**最大数据速率**。任何通信链路频率下降会影响非本地内存访问的性能和高速缓存一致性流量。此外，它会降低从特定 CPU 访问非本地 I/O 设备的速度。 但是，如果节能比性能重要，您可能需要降低 CPU 通信链路之间的频率。如果您执行此操作,您应本地化内存和 I / O 访问连接到最近的 NUMA 节点以最小化到系统性能的影响。
虚拟化技术	启用或禁用的处理器虚拟化技术。。该选项默认设置为**已启用**。
相邻的高速缓存行预先访存	针对需要大量使用顺序内存访问的应用程序优化系统。该选项默认设置为**已启用**。您可以禁用需要大量使用随机内存访问的应用程序的此选项。
硬件预取器	启用或禁用硬件预取器。该选项默认设置为**已启用**。
软件预取器	启用或禁用软件预取器。该选项默认设置为**已启用**。

选项	说明
DCU 流转化器预取器	启用或禁用数据高速缓存设备 (DCU) 流转化器预取器。该选项默认设置为**已启用**。
DCU IP 预取器。	启用或禁用数据高速缓存设备 (DCU) IP 预取器。该选项默认设置为**已启用**。
子 NUMA 群集	子 NUMA 群集 (SNC) 功能可根据地址范围将 LLC 划分为分离的群集，其中每个群集绑定到系统中内存控制器的子集。它可以改进 LLC 的平均延迟。启用或禁用子 NUMA 群集。该选项默认设置为**已禁用**。
UPI 预先访存	支持您尽早获取 DDR 总线上的内存读数。超路径互连 (UPI) Rx 路径会直接将推测内存读数蔓延到集成内存控制器 (iMC)。该选项默认设置为**已启用**。
LLC 预取	启用或禁用所有线程上的 LLC 预取。该选项默认设置为**已禁用**。
截止日期 LLC Alloc	启用时，它将适时填充 LLC 中的死行。禁用时，它永远不会填充 LLC 中的死行。该选项默认设置为**已启用**。
目录 AToS	AToS 优化可以减少重复读取访问的远程读取延迟，而不影响写入。该选项默认设置为**已禁用**。
FastGo	允许您选择 CR OOS 配置配置文件。
IRQ 限制	允许您限制针对远程地址的本地请求。
逻辑处理器空闲	可让您以提高系统。它使用操作系统核心休眠算法，并将系统中的一些逻辑处理器置于休眠状态，这反过来又允许相应的处理器核心数转换为低功耗空闲状态。仅当操作系统支持它可以启用此选项。该选项默认设置为**已禁用**。 **注:** 如果“CPU 电源管理”设置为“最大性能”，此功能不受支持。
可配置的 TDP	允许您配置 TDP 级别。可用选项包括**标称**、**级别 1** 和**级别 2**。该选项默认设置为**标称**。 **注:** 此选项仅在处理器的某些库存单位 (SKU) 上可用。
x2APIC 模式	启用或禁用 x2APIC 模式。该选项默认设置为**已启用**。
L2 RFO 预先访存技术	启用或禁用 L2 RFO（读取所有权）预取。该选项默认设置为**已启用**。RFO 是将高速缓存行从内存读取高速缓存后再写入高速缓存的过程。 **注:** 仅当安装了四个处理器时，才支持此功能。
戴尔受控涡轮	控制涡轮增压。只有在**系统配置文件**设置为**性能**时才启用此选项。 **注:** 根据安装的 CPU 数量，可能会有多达两个处理器列表。
戴尔 AVX 调节技术	允许您配置戴尔 AVX 调节技术。该选项默认设置为 **0**。
AVX ICCP 预授予	允许系统在英特尔提供的不同 AVX ICCP 转换级别之间进行选择。默认级别为 128 繁重。
每个处理器的核心数量	控制处理器中已启用的核心数。在某些情况下，当您减少启用的内核数量时，您可能会看到对英特尔睿频加速技术的受限性能改进，并受益于潜在的更高共享高速缓存。大多数计算环境都将受益于更多的处理内核数量，因此您必须认真衡量禁用的内核数量，以实现标称性能增强功能。
处理器核心速率	显示处理器的内核速度。
进程总线速度	显示处理器的总线速度。
处理器 n	以下设置仅对系统中安装的每个处理器显示：

选项	说明
系列-型号-步进编号	显示英特尔定义的处理器系列、型号和步进。
品牌	显示品牌名称。
2 级高速缓存	显示 L2 高速缓存总和。
3 级高速缓存	显示 L3 高速缓存总和。
核心数量	显示每个处理器的内核数。
最大内存容量	指定每个处理器的最大内存容量。
微码	指定微码。

SATA 设置

您可以使用 **SATA Settings** 屏幕来查看 SATA 设备的 SATA 设置并在系统上启用 SATA 和 PCIe NVMe RAID 模式。

查看 SATA 设置

要查看 **SATA Settings**（SATA 设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **SATA Settings**（SATA 设置）。

SATA 设置详细信息

关于此任务

SATA Settings 屏幕详细信息如下所述：

选项	说明
Embedded SATA	支持将嵌入式 SATA 选项设置为 **Off**、**AHCI** 或 **RAID** 模式。此选项默认设置为 **AHCI Mode**。
Security Freeze Lock	在开机自测过程中将安全冻结锁定命令发送给嵌入式 SATA 驱动器。此选项仅适用于 AHCI 模式。此选项默认设置为 **Enabled**。
Write Cache	在 POST 过程中启用或禁用嵌入式 SATA 驱动器的命令。该选项默认设置为 **Disabled**。
Port n	设置所选设备的驱动器类型。 对于 **AHCI Mode** 或 **RAID Mode**，总是启用 BIOS 支持。

选项	说明
Model	指定所选设备的驱动器型号。 **注:** 如果未安装设备，则显示 **Unkown**。
Drive Type	指定连接至 SATA 端口的驱动器类型。 **注:** 如果未安装设备，则显示 **Unkown Device**。
Capacity	指定驱动器的总容量。对于可移动介质设备，如光盘驱动器，此字段未定义。 **注:** 如果未安装设备，则显示 **N/A**。

NVMe Settings

NVMe 设置允许您将 NVMe 驱动器设置为 **RAID** 模式或 **Non-RAID** 模式。

注: 要将这些驱动器配置为 RAID 驱动器，单击 **System BIOS Settings** > **SATA Settings** > **Embedded SATA Option** 并启用 **RAID** 模式。否则，必须将此字段设置为 **Non-RAID** 模式。

查看 NVMe 设置

要查看 **NVMe Settings（NVMe 设置）**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 <F2> 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS（系统 BIOS）**屏幕中，单击 **NVMe Settings（NVMe 设置）**。

NVMe 设置详细信息

关于此任务

“NVMe Settings”（NVMe 设置）屏幕详细信息如下所述：

选项	说明
NVMe 模式	使您可以设置 NVMe 模式。此选项默认设置为 **Non RAID**（非 RAID）。

Boot Settings（引导设置）

您可以使用 **Boot Settings (引导** 设置)屏幕设置为 **BIOS** 或 **UEFI 的引导模式**。它还允许您指定引导顺序。

- **BIOS**：**BIOS Boot Mode（BIOS 引导模式）**是传统引导模式。此位置支持向后兼容性。
- **UEFI**:统一可扩展固件接口(UEFI)都是一个新接口之间的操作系统和平台固件。接口由与平台相关信息的数据表组成,也引导和运行时服务电话转接至操作系统及其 加 载程序的可用。以下参数仅在 **System Profile**（系统配置文件）设置为 **Custom**（自定义）时才可用。
  - 支持大于 2 TB 的驱动器分区。
  - 增强的安全性(例如, UEFI 安全引导)。
  - 更快的引导时间。

注: 您必须使用 UEFI 引导模式，以便从 NVMe 驱动器进行引导。

查看引导设置

要查看 **Boot Settings**（引导设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Boot Settings**（引导设置）。

引导设置详细信息

关于此任务

Boot Settings（引导设置）屏幕详细信息如下所述：

选项	说明
Boot Mode	允许您配置引导顺序以及启用或禁用单独的引导选项。可用的选项为 **BIOS** 和 **UEFI**。此选项默认设置为 **UEFI**。
Boot Sequence Retry	启用或禁用引导顺序重试功能。如果上次尝试引导失败，系统会在 30 秒超时后立即执行冷重置或重试，具体取决于 **Reset** 或 **Enabled** 设置。此选项默认设置为 **Enabled（已启用）**。
Hard-Disk Failover	指定在驱动器发生故障的情况下进行引导的驱动器。所选中的设备 **引导选项设置上 Hard - Disk Drive Sequence (硬盘驱动器顺序**)菜单。此选项设置为 **Disabled（已禁用）**时，将仅尝试引导列表中的第一个驱动器。此选项设置为 **Enabled（已启用）**时，将尝试按顺序引导 **Hard-Disk Drive Sequence（硬盘驱动器顺序）**中已选的所有驱动器。未为 **UEFI 引导模式已启用此选项**。该选项默认设置为 **Disabled（已禁用）**。
Generic USB Boot	启用或禁用 USB 引导选项。该选项默认设置为 **Disabled（已禁用）**。
Hard-disk Drive Placeholder	启用或禁用硬盘占位符选项。此选项默认设置为 **disabled**。

UEFI 引导设置

UEFI Boot Settings 屏幕允许您指定 UEFI 引导顺序。

关于此任务

选项	说明
UEFI Boot Sequence	允许您更改 **UEFI** 引导设备的顺序。
Boot Options Enable/Disable	允许您启用或禁用 **UEFI** 引导设备。

选择系统引导模式

系统设置程序也能让您指定其中一个用于安装操作系统的引导模式：

- BIOS 引导模式是标准的 BIOS 级引导接口。
- UEFI 引导模式（默认）是标准的 BIOS 级引导接口。

  如果您已将系统配置为引导至 UEFI 模式，则会更换系统 BIOS。

1. 单击**系统设置程序主菜单**中的**引导设置**，然后选择**引导模式**。
2. 选择您希望系统引导至的 UEFI 引导模式。

   小心: 如果操作系统不是在同一种引导模式下安装，则切换引导模式可能会阻止系统引导。
3. 在系统以指定引导模式引导后，从该模式安装操作系统。

注: 操作系统必须与 UEFI 兼容才能从 UEFI 引导模式安装。DOS 和 32 位操作系统不支持 UEFI，只能通过 BIOS 引导模式进行安装。

注: 有关支持的操作系统的最新信息，请访问 **Dell.com/ossupport**。

更改引导顺序

关于此任务

如果您想从 USB 盘或光盘驱动器引导，您可能需要更改引导顺序。如果您已选择了 **BIOS Boot Mode**（引导模式），则此处给出的说明可能会有所不同。

步骤

1. 在 **System Setup Main Menu（系统设置主菜单）**屏幕上，单击 **System BIOS（系统 BIOS）** > **Boot Settings（引导设置）** > **UEFI/BIOS Boot Settings（UEFI/BIOS 引导设置）** > **UEFI/BIOS Boot Sequence（UEFI/BIOS 引导顺序）**。
2. 使用箭头键选择引导设备，然后使用加号 (+) 和减号 (-) 将设备按顺序向下或向上移动。
3. 单击 **Exit（退出）**，然后单击 **Yes（是）**以在退出后保存设置。

网络设置

您可以使用 **Network Settings（网络设置）**屏幕修改 UEFI PXE、iSCSI 和 HTTP 引导设置。Network Settings（网络设置）选项仅在 UEFI 模式下可用。

注: BIOS 不会在 BIOS 引导模式下控制网络设置。对于 BIOS 引导模式，网络控制器的可选的引导 ROM 可以处理网络设置。

查看网络设置

要查看 **Network Settings**（网络设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Network Settings**（网络设置）。

Network Settings（网络设置）屏幕详细信息

Network Settings（网络设置）屏幕详细信息如下所述：

关于此任务

选项	说明
UEFI PXE Settings（UEFI PXE 设置）	允许您控制 UEFI PXE 设备的配置。
PXE Device n (n = 1 to 4)	启用或禁用此设备。启用时，则为设备创建 UEFI PXE 引导选项。
PXE Device n Settings(n = 1 to 4)	允许您控制 PXE 设备的配置。
UEFI HTTP Settings（UEFI HTTP 设置）	启用或禁用此设备。启用时，则为设备创建 UEFI HTTP 引导选项。
HTTP Device n Settings (n = 1 to 4)	允许您控制 HTTP 设备的配置。
UEFI iSCSI 设置	允许您控制 iSCSI 设备的配置。

表. 1: UEFI iSCSI Settings（UEFI iSCSI 设置）屏幕详细信息

选项	说明
iSCSI 启动器名称	指定 iSCSI 启动器的名称（IQN 格式）。

选项	说明

表. 1: UEFI iSCSI Settings（UEFI iSCSI 设置）屏幕详细信息（续）

选项	说明
iSCSI 设备 1	启用或禁用 iSCSI 设备。禁用后，将为 iSCSI 设备自动创建 UEFI 引导选项。该选项默认设置为 **Disabled**。
iSCSI 设备 1 设置	允许您控制 iSCSI 设备的配置。

TLS Authentication Configuration	查看和/或修改此设备的引导 TLS 身份验证模式。“无”表示 HTTP 服务器和客户端不会针对此引导为对方进行身份验证。“单向”表示 HTTP 服务器将通过客户端进行身份验证，而客户端将不会由服务器进行身份验证。该选项默认设置为 **None**。

集成设备

您可以使用 **Integrated Devices** 屏幕来查看和配置所有集成设备的设置，包括视频控制器、集成 RAID 控制器和 USB 端口。

查看集成设备

要查看 **Integrated Devices**（集成设备）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 <F2> 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Integrated Devices**（集成设备）。

集成设备详细信息

关于此任务

集成设备屏幕详细信息如下所述：

选项	说明
用户可访问 USB 端口	禁用前端用户可访问 USB 端口。选择**禁用所有端口**将禁用所有 USB 端口；选择**禁用所有端口（动态）**将在 POST 期间禁用所有 USB 端口，并且获得授权的用户可以动态启用或禁用正面端口，无需重设系统。 在引导过程中 USB 键盘和鼠标在某些 USB 端口中仍可正常工作，具体取决于选择。引导过程完成后，USB 端口将根据设置启用或禁用。
内部 USB 端口	启用或禁用内部 USB 端口。该选项默认设置为**立即**。
iDRAC Direct USB 端口	iDRAC Direct USB 端口由 iDRAC 专门管理，主机不可见。此选项设置为**启用**或**禁用**。当设置为**禁用**时，iDRAC 无法检测到此管理端口中安装的任何 USB 设备。该选项默认设置为**立即**。
集成 RAID 控制器	启用或禁用集成 RAID 控制器。该选项默认设置为**已启用**。
I/OAT DMA 引擎	启用或禁用 I/O 加速技术 (I/OAT) 选项。I/OAT 是一组旨在加速网络流量和降低 CPU 利用率的 DMA 功能。仅在硬件和软件均支持此功能时启用。
I/O 监听推迟响应	允许您选择 PCI I/O 可以从 CPU 取消监听请求的周期数，以允许时间完成其自己的写入到 LLC。此设置可帮助改进性能上的吞吐量和延迟严重的工作负载。

选项	说明
嵌入式视频控制器	启用或禁用“嵌入式视频控制器作为主要显示屏的使用”。当设置为**已启用**时，嵌入式视频控制器将用作主显示器，即使已安装附加式显卡。当设置为**已禁用**时，附加式显卡将用作主显示器。BIOS 在开机自检过程中和预引导环境中将输出显示为两个主要附加式视频和嵌入式视频。在操作系统引导之前，嵌入式视频将立即被禁用。该选项默认设置为**已启用**。 **注:** 当系统中已安装附加式显卡时，在 PCI 枚举过程中查找到的第一个卡已选中作为主视频。您可能需要重新排列插槽中的插卡，以便控制哪些插卡是主视频。
嵌入式视频控制器的当前状态	显示嵌入式视频控制器的当前状态。**嵌入式视频控制器的当前状态**选项为只读字段。如果嵌入式视频控制器是系统中唯一的显示功能（即没有安装附加显卡），那么即使**嵌入式视频控制器**设置为**已禁用**，嵌入式视频控制器设置也会自动用作主显示屏。
SR-IOV 全局启用	启用或禁用单根 I/O 虚拟化 (SR-IOV) 设备的 BIOS 配置。该选项默认设置为**已禁用**。
内部 SD 卡端口	启用或禁用内部双 SD 模块 (IDSDM) 的内部 SD 卡端口。该选项默认设置为**立即**。
内部 SD 卡冗余	在内部双 SD 模块 (IDSDM) 中找到 SD 卡连接器。如果设置为**镜像**模式，数据将同时写入两张 SD 卡。数据写入两个 SD 卡中。一旦其中一个卡发生故障或对故障的卡进行了更换，在系统引导期间活动卡上的数据就被复制到脱机卡中。 时内部 SD 卡冗余设置为**已禁用**,则仅主要 SD 卡到操作系统可见。该选项默认设置为**已禁用**。
内部 SD 主要卡	**冗余**设置为**已禁用**时，可选择将自身作为大容量存储设备,方法是设置其的其中一台 SD 卡是主卡。默认情况下,选中主要 SD 卡为 SD 卡 1。如果 SD 卡 1 不存在，则该控制器将选择 SD 卡 2 作为主要 SD 卡。
OS 监督计时器	如果系统停止响应，则此监督计时器可帮助恢复操作系统。此选项设置为**已启用**时，操作系统会初始化计时器。此选项设置为**已禁用**（默认）时，计时器不会对系统造成任何影响。该选项默认设置为**已禁用**。
空插槽取消隐藏	启用或禁用 BIOS 和操作系统可访问的所有空插槽的根端口。该选项默认设置为**已禁用**。
内存映射的 I/O 大于 4 GB	启用或禁用需要大量内存的 PCIe 设备的支持。启用此选项仅适用于 64 位操作系统。该选项默认设置为**已启用**。
内存映射的 I/O 基座	设置为 **12 TB** 时，系统将 MMIO 基座映射为 12 TB。对于需要 44 位 PCIe 寻址的操作系统启用此选项。 **注:** 将**内存映射的 I/O 基座**设置为 **512 GB** 需要低于 512 GB 的物理内存，否则系统将无法执行 POST。
夹层插槽禁用	插槽禁用功能控制指定插槽中安装的夹层卡的配置。仅系统中存在的夹层卡插槽可用于控制。

串行通信

使用 **Serial Communication** 屏幕可查看串行通信端口的属性。

查看串行通信

要查看 **Serial Communication**（串行通信）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 <F2> 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Serial Communication**（串行通信）。

串行通信详细信息

关于此任务

串行通信屏幕详细信息如下所述：

选项	说明
串行通信	BIOS 中的串行通信设备（串行设备 1 和串行设备 2）。也可以启用 BIOS 控制台重定向,并可指定端口地址。此选项默认设置为 **关闭**。 允许您启用 **COM** 端口或**控制台重定向**选项。
串行端口地址	允许您设置串行设备的端口地址。此字段可将串行端口地址设置为 COM1 或 COM2（COM1=0x3F8、COM2=0x2F8）。此选项默认设置为**串行设备 1=COM1**。 **注:** 只能将串行设备 2 用于 LAN 上串行 (SOL) 功能。要通过 SOL 使用控制台重定向，请为控制台重定向和串行设备配置相同的端口地址。
外部串行连接器	您可以使用此选项将外部串行连接器与**串行设备 1**、**串行设备 2** 或**远程访问设备**关联起来。该选项的默认设置为**串行设备 1**。 **注:** 只能将串行设备 2 用于 LAN 上串行 (SOL)。要通过 SOL 使用控制台重定向，请为控制台重定向和串行设备配置相同的端口地址。 **注:** 每次系统启动时，BIOS 中同步 iDRAC 中保存的串行 MUX 设置。串行 MUX 设置可单独在 iDRAC 中进行更改。因此，从 BIOS 设置实用程序加载 BIOS 默认设置并不总会将此设置转换为设置为串行设备 1 的默认设置。 您可以将外部串行连接器与串行设备 1 关联起来。
故障保护波特率	显示用于控制台重定向的故障保护波特率。BIOS 尝试自动确定波特率。仅当尝试失败时才使用故障保护波特率且不得更改此值。该选项默认设置为 **115200**。
远程终端类型	允许您设置远程控制台终端类型。此选项默认设置为 **VT100/VT220**。
引导后重定向	允许您在载入操作系统后启用或禁用 BIOS 控制台重定向。此选项默认设置为**已启用**。

系统配置文件设置

您可以使用 **System Profile Settings** 屏幕启用特定系统的性能设置，如电源管理。

查看系统配置文件设置

要查看 **System Profile Settings**（系统配置文件设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 <F2> 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **System Profile Settings**（系统配置文件设置）。

系统配置文件设置详情

关于此任务

系统配置文件设置屏幕详细信息如下所述：

选项	说明
系统配置文件	允许您设置系统密码。如果将**系统配置文件**选项设置为除自定义外的其它模式，BIOS 将自动设置其余选项。仅在模式设置为**自定义**时，才可更改其余选项。此选项默认设置为**性能功耗比优化 (DAPC)**。DAPC 是 Dell Active Power 控制器。其他选项包括**性能功耗比 (OS)**、**性能**和**工作站性能**。 **注:** 只有在**系统配置文件**选项设置为**自定义**时，系统配置文件设置屏幕上的所有参数方可用。
CPU 电源管理	设置 CPU 电源管理。此选项默认设置为**系统 DBPM (DAPC)**。DBPM 是基于需求的电源管理。其他选项包括 **OS DBPM** 和**最大性能**。
内存频率	设置系统内存的速度。您可以选择**最大性能**、**最大可读性**，或特定速度。此选项默认设置为**最大性能**。
睿频加速	启用或禁用处理器在睿频加速模式下运行。此选项默认设置为**已启用**。
C1E	允许您在处理器处于闲置状态时启用或禁用处理器切换至最低性能状态。此选项默认设置为**已启用**。
C 状态	允许您启用或禁用处理器在所有可用电源状态下运行。此选项默认设置为**已启用**。
写入数据 CRC	启用或禁用写入数据 CRC。该选项默认设置为**已禁用**。
内存轮巡	允许您设置内存轮巡检查频率。此选项默认设置为**标准**。
内存刷新率	将“内存刷新率”设置为 1x 或 2x。此选项默认设置为 **1x**。
非核心频率	可用于选择**处理器非核心频率**选项。 **动态模式**使处理器能够在运行时跨核心和非核心优化电源资源。优化非核心频率以节省电力或优化性能的效果受到**能源效率策略**选项设置的影响。
能效策略	可用于选择**能效策略**选项。 CPU 会使用该设置来操作处理器的内部行为并确定是定位更高的性能还是更好的节能效果。此选项默认设置为**平衡性能**。
处理器 1 已启用睿频加速核心的数量	**注:** 如果系统中安装了四个处理器，将显示适用于**处理器 4 启用睿频加速技术的核心数**的条目。 控制处理器 1 启用睿频加速技术的核心数。默认启用的最大核心数量是全部。
Monitor/Mwait	启用处理器中的 Monitor/Mwait 指令。对于所有系统配置文件（**自定义**除外），此选项默认设置为**已启用**。 **注:** 仅当 **C 状态**选项在**自定义**模式下设置为**已禁用**时，才能禁用此选项。 **注:** 当 **C 状态**在**自定义**模式下设置为**已启用**时，更改 Monitor/Mwait 设置不会影响系统电源或性能。
CPU 互连总线链路电源管理	启用或禁用 CPU 互连总线链路电源管理。此选项默认设置为**已启用**。
PCI ASPM L1 链路电源管理	启用或禁用 PCI ASPM L1 链路电源管理。此选项默认设置为**已启用**。
英特尔永久性内存 CR QoS	控制服务质量 (QoS) 旋钮的调整功能。默认设置为**已禁用**建议将**方法 1** 用于 App-Direct 中的 2-2-2 内存配置。建议将**方法 2** 用于 App-Direct 中的其他内存配置。建议将**方法 3** 用于每个通道 1 个 DIMM 配置。
英特尔永久性内存性能设置	控制在接近 (RDIMM/LRDIMM) 和远离 (DCPMM) 内存之间触发切换的阈值。**BW 优化**，默认情况下已选择，可优化 RDIMM/LRDIMM 和 DCPMM 带宽。**延迟优化**可在 DCPMM 存在时提供更好的 RDIMM/LRDIMM 延迟。**平衡配置文件**可优化内存模式配置的 DCPMM 的性能。

System Security

您可以使用 **System Security** 屏幕来执行特定的功能，如设置系统密码、设置密码和禁用电源按钮。

查看系统安全

要查看 **System Security**（系统安全）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。

2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **System Security**（系统安全）。

“系统安全设置”详细信息

关于此任务

系统安全设置屏幕详细信息如下所述：

选项	说明
CPU AES-NI	通过使用高级加密标准指令集 (AES-NI) 执行加密和解密来提高应用程序速度。默认设置为已启用。此选项默认设置为**已启用**。
系统密码	设置系统密码。此选项默认设置为**已启用**，并且如果系统上未安装密码跳线，此选项为只读。
设置密码	设置系统密码。如果系统上未安装密码跳线，此选项为只读。
密码状态	锁定系统密码。该选项默认设置为**所有**所有。
TPM 信息	**注:** TPM 菜单仅在安装 TPM 模块时可用。 使您能够控制可信平台模块 (TPM) 的报告模式。默认情况下，**TPM 安全**选项设置为 **关**。如果 **TPM 状态**字段设置为**开，进行预引导测量**或**开，不进行预引导测量**，则仅可修改“TPM 状态”和“TPM 激活”和“英特尔 TXT”字段。 已安装 TPM 1.2 时，**TTPM 安全保护**选项设置为**关**、**开，进行预引导测**或**开，不进行预引导测量**。

表. 2: TPM 1.2 安全信息

TPM 信息	说明
TPM 信息	允许您更改 TPM 的操作状态。该选项默认设置为**无更改**。
TPM 固件	指示 TPM 的固件版本。
TPM 状态	指定 TPM 状态。
TPM 命令	安装可信平台模块 (TPM)。当设置为**无**时，不会将命令发送到 TPM。当设置为**激活**时，将启用并激活 TPM。当设置为**停用**时，将禁用并取消激活 TPM。当设置为**清除**时，将清除 TPM 的所有内容。此选项默认设置为**无**。

安装了 TPM 2.0 时，**TPM 安全**选项设置为**打开**或**关闭**。该选项默认设置为**关闭**。

表. 3: TPM 2.0 安全信息

TPM 信息	说明
TPM 信息	允许您更改 TPM 的操作状态。该选项默认设置为**无更改**。
TPM 固件	指示 TPM 的固件版本。
TPM 层级结构	启用、禁用或清除存储和认可层级结构。当设置为**已启用**时，存储和认可层级结构可以使用。 当设置为**已禁用**时，存储和认可层级结构无法使用。 当设置为**清除**时，存储和认可层级结构中的任何值都被清除，然后重设为**已启用**。

TPM 高级设置	当 TPM 安全保护设置为开时，此设置已启用。

选项 **说明**

表. 4: TPM 高级设置详情

选项	说明
TPM PPI 绕过配置	当设置为**已启用**时，允许操作系统绕过物理存在接口 (PPI)，并且在发出 PPI 高级配置和电源接口 (ACPI) 配置操作时进行提示。该选项默认设置为**已禁用**。
TPM PPI 绕过清除	当设置为**已启用**时，允许操作系统绕过物理存在接口 (PPI)，并且在发出 PPI 高级配置和电源接口 (ACPI) 配置操作时进行提示。该选项默认设置为**已禁用**。

英特尔® TXT

启用或禁用英特尔可信执行技术 (TXT)。要启用此**英特尔 TXT** 选项，必须启用虚拟化技术以及进行预引导测量的 TPM 安全保护。该选项默认设置为**关闭**。

安装了 TPM 2.0 时，**TPM 2 算法**选项可用。它可让您选择散列算法 TPM 支持从这些(SHA 1, SHA 256)。**TPM 2 算法**选项必须设置为 **SHA 256**，以启用 TXT。

电源按钮

允许您启用或禁用系统前面的电源按钮。此选项默认设置为**已启用**。

交流电源恢复

设置系统恢复交流电源后系统如何反应。该选项默认设置为**持续**。

UEFI 可变访问

提供保护 UEFI 变量的各种度。当设置为**标准**（默认值）时，可以按照 UEFI 规范在操作系统中访问 UEFI 变量。当设置为**受控**时，所选 UEFI 变量在环境中受保护，并且新的 UEFI 引导条目强制为当前引导顺序的末端。

带内可管理性界面

设置为**已禁用**时，此设置将对操作系统隐藏管理引擎 (ME)、HECI 设备和系统的 IPMI 设备。这会导致操作系统无法更改 ME 电源上限设置，并阻止访问所有带内管理工具。所有管理应通过带外进行管理。此选项默认设置为**已启用**。

注: BIOS 更新需要 HECI 设备正常运行，并且 DUP 更新需要 IPMI 界面正常工作。此设置需要设置为**已启用**，以避免更新错误。

安全引导

启用安全引导，BIOS 使用安全引导策略中的证书来验证每个预引导映像。安全引导在默认设置下已禁用。安全引导策略默认设置为**标准**。

安全引导策略

当安全引导策略设置为**标准**时，BIOS 将使用系统制造商密钥和证书来验证预引导映像。当安全引导策略设置为**自定义**时，BIOS 将使用用户定义的密钥和证书。安全引导策略默认设置为**标准**标准。

安全引导模式

配置 BIOS 如何使用安全引导策略对象（PK、KEK、db、dbx）。

如果当前模式设置为**部署模式**时，则可用的选项为**用户模式**和**部署模式**。如果当前模式设置为**用户模式**时，则可用的选项为**用户模式**、**审核模式**和**部署模式**。

选项	说明
用户模式	在**用户模式**下，PK 必须安装并且 BIOS 在编程尝试更新策略对象时执行签名验证。 BIOS 允许不需要身份验证的编程模式之间转换。
部署模式	**部署模式**是最安全的模式。在**部署模式**中，PK 必须安装并且 BIOS 在编程尝试更新策略对象时执行签名验证。 **部署模式**限制编程模式转换。
审核模式	在**审计模式**下，PK 不存在。BIOS 不验证策略对象的编程更新,并模式之间转换。 **审核模式**对于以编程方式确定一组策略工作有帮助。 BIOS 在预引导映像上执行签名验证并在映像执行信息表上记录结果，但无论它们通过还是验证失败都会执行映像。

安全引导策略摘要

显示安全引导用于验证映像的证书和哈希值列表。

安全引导自定义策略设置

配置安全引导自定义策略。要启用此选项，将安全引导策略设置为**自定义**选项。

创建系统密码和设置密码

前提条件

请确保 密码 跳线已启用。密码跳线用于启用或禁用系统密码和设置密码功能。有关更多信息，请参阅“系统板跳线设置”部分。

注: 如果密码跳线设置已禁用，将删除现有系统密码和设置密码，无需提供系统密码即可引导系统。

步骤

1. 要进入系统设置，请在开机或重新启动后立即按 F2。
2. 在**系统设置主菜单**屏幕中，单击**系统 BIOS** > **系统安全**。
3. 在**系统安全保护**屏幕中，验证**密码状态**是否设置为**已解锁**。
4. 在**系统密码**字段中，输入系统密码，然后按 Enter 或 Tab。
   采用以下原则设定系统密码：
   - 一个密码最多可包含 32 个字符。密码可包含 ASCII 字符集中的任意字符。

   将显示一条消息，提示您重新输入系统密码。
5. 重新输入系统密码，然后单击**确定**。
6. 在**设置密码**字段中，输入系统密码，然后按 Enter 或 Tab。
   将显示一条消息，提示您重新输入设置密码。
7. 重新输入设置密码，然后单击**确定**。
8. 按 Esc 键返回系统 BIOS 屏幕。再按一次 <Esc> 键。
   将出现一条消息，提示您保存更改。
   注: 重新引导系统之后，密码保护才能生效。

使用系统密码保护系统安全

前提条件

如果已分配设置密码，系统会将设置密码视为备选系统密码。

步骤

1. 打开或重新引导系统。
2. 键入系统密码，然后按 Enter 键。

后续步骤

如果 **Password Status（密码状态）**设置为 **Locked（已锁定）**，则必须在重新引导时根据提示键入系统密码并按 Enter 键。

注: 如果键入错误的系统密码，则系统会显示一条消息并提示您重新输入密码。您有三次机会键入正确的密码。第三次尝试失败后，系统将显示一条错误消息，表示系统已停止工作，必须关机。即使您关闭并重新启动系统，系统仍然会显示该错误信息，直到输入正确的密码。

删除或更改系统密码和设置密码

前提条件

注: 如果**密码状态**设置为**已锁定**，则无法删除或更改现有系统密码或设置密码。

步骤

1. 要进入系统设置程序，请在开启或重新启动系统后立即按 F2 键。
2. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS** > **系统安全**。
3. 在**系统安全**屏幕中，确保**密码状态**设置为**已解锁**。
4. 在**系统密码**字段中，更改或删除现有系统密码，然后按 Enter 或 Tab 键。

5. 在**设置密码**字段中，更改或删除现有设置密码，然后按 Enter 或 Tab 键。
   如果更改系统密码和/或设置密码，将出现一则信息，提示您重新输入新密码。如果删除系统密码和/或设置密码，将出现一则信息，提示您确认删除操作。
6. 按 Esc 键返回**系统 BIOS** 屏幕。再按一次 Esc 键，将出现提示您保存更改的消息。
7. 选择**设置密码**，更改或删除现有设置密码并按 Enter 或 Tab 键。

   注: 如果更改系统密码或设置密码，将出现一则信息，提示您重新输入新密码。如果删除系统密码和/或设置密码，将出现一则信息，提示您确认删除操作。

在已启用设置密码的情况下进行操作

如果将**设置密码**设置为**已启用**，则必须输入正确的设置密码才能修改系统设置选项。

如果您尝试输入三次密码，但均不正确，系统会显示以下信息：

```
Password Invalid.
```

```
Number of unsuccessful password attempts: <3> Maximum number of password attempts exceeded.
System Halted!
```

即使您关闭并重新启动系统，系统仍然会显示该错误信息，直到键入正确的密码。支持以下选项：

- 如果未将**系统密码**设置为**已启用**，并且未通过**密码状态**选项加以锁定，则您可以设定系统密码。有关更多信息，请参阅系统的“安全设置屏幕”部分。
- 您不能禁用或更改现有的系统密码。

注: 您可以将密码状态选项与设置密码选项配合使用，以防止他人擅自更改系统密码。

冗余操作系统控制

您可以使用 **Redundant OS Control** 屏幕来设置冗余操作系统控制的冗余操作系统信息。它允许您在系统上设置物理恢复磁盘。

查看冗余操作系统控制

要查看 **Redundant OS Control（冗余操作系统控制）**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

   ```
   F2 = System Setup
   ```

   注: 如果按 F2 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS（系统 BIOS）**屏幕中，单击 **Redundant OS Control（冗余操作系统控制）**。

冗余 OS Control (操作系统控制)屏幕详细信息

冗余 操作系统控制屏幕详尽的解释如下：

关于此任务

选项	说明
Redundant OS Location	可让您选择从以下设备的备份磁盘,请执行以下操作: • **无**

选项	说明
	• **内部 SD 卡** • **AHCI Mode（AHCI 模式中的 SATA 端口** • **BOSS PCIe 卡（内部 M.2 驱动器）** • **内置 USB** **注:** RAID 配置和 NVMe 卡不 BIOS 中包含不具备以区分将这些配置中的各个驱动器的功能。
Redundant OS State	**注:** 如果 NIC 选择设置为专用，则此选项被禁用。 时设置为 **可见**,备份磁盘到引导列表中可见和操作系统。当设置为 **隐藏**、备份磁盘已禁用且到的引导列表和操作系统中不可见。该选项默认设置为 **可见**。 **注:** BIOS 将在硬件中禁用设备, 因此 它由操作系统 无法 访问。
Redundant OS Boot	**注:** 如果冗余操作系统的位置设置为无，或者冗余操作系统状态设置为隐藏，此选项将被禁用。 如果**冗余操作系统的位置**设置为**启用**，BIOS 将使用指定的位置引导设备。如果此选项设置**禁用**，BIOS 会保留当前引导列表设置。该选项默认设置为 **已禁用**。

Miscellaneous Settings

您可以使用 **Miscellaneous Settings** 屏幕来执行特定功能，如更新资产标签以及更改系统日期和时间。

查看其他设置

要查看 **Miscellaneous Settings**（ 其他设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

注: 如果按 <F2> 键之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并重试。

3. 在 **System Setup Main Menu**（系统设置程序主菜单）屏幕中，单击 **System BIOS**（系统 BIOS）。
4. 在 **System BIOS**（系统 BIOS）屏幕中，单击 **Miscellaneous Settings**（其他设置）。

其他设置详细信息

关于此任务

Miscellaneous Settings 屏幕详细信息如下所述：

选项	说明
System Time	允许您设置系统时间。
System Date	允许您设置系统日期。
Asset Tag	指定资产标签，并且允许您出于安全保护和跟踪目的修改资产标签。
Keyboard NumLock	允许您设置系统引导是否启用或禁用 NumLock（数码锁定）。该选项默认设置为 **On**。 **注:** 此选项不适用于 84 键键盘。
F1/F2 Prompt on Error	启用或禁用 F1/F2 Prompt on Error（发生错误时 F1/F2 提示）。此选项默认设置为 **Enabled**。F1/F2 提示还包括键盘错误。

选项	说明
Load Legacy Video Option ROM	使您能够确定系统 BIOS 是否从视频控制器加载旧式视频 (INT 10H) 选项 ROM。如果操作系统不支持 UEFI 视频输出标准，则选择 **Enabled**。此字段仅适用于 UEFI 引导模式。如果已启用 **UEFI Secure Boot** 模式，您无法将此选项设置为 **Enabled**。该选项默认设置为 **Disabled**。
Dell Wyse P25/P45 BIOS Access	启用或禁用 Dell Wyse P25/P45 BIOS 的访问权限。此选项默认设置为 **Enabled**。
Power Cycle Request	启用或禁用电源关闭后重启请求。该选项默认设置为 **None**。

iDRAC 设置公用程序

iDRAC 设置公用程序是使用 UEFI 设置和配置 iDRAC 参数的接口。可使用 iDRAC 设置公用程序启用或禁用各种 iDRAC 参数。

注: 访问 iDRAC 设置公用程序中的某些功能需要升级 iDRAC Enterprise 许可证。

有关使用 iDRAC 的更多信息，请参阅 *Dell Integrated Dell Remote Access Controller User's Guide（戴尔集成远程访问控制器用户指南）*，网址：www.dell.com/idracmanuals。

Device Settings（设备设置）

Device Settings（设备设置）可用于配置设备参数。

Dell Lifecycle Controller

Dell Lifecycle Controller (LC) 可提供高级嵌入式系统管理功能，包括系统部署、配置、更新、维护和诊断。LC 是 iDRAC 带外解决方案和戴尔系统嵌入式统一可扩展固件接口 (UEFI) 应用程序的一部分。

嵌入式系统管理

Dell Lifecycle Controller 在系统的整个生命周期提供高级嵌入式系统管理。Dell Lifecycle Controller 可在引导顺序期间启动，并可独立于操作系统工作。

注: 某些平台配置可能不支持 Dell Lifecycle Controller 提供的整套功能。

有关设置 Dell Lifecycle Controller、配置硬件和固件以及部署操作系统的更多信息，请参阅 Dell Lifecycle Controller 文档，网址：www.dell.com/idracmanuals。

引导管理器

Boot Manager（引导管理器）屏幕允许您选择引导选项和诊断公用程序。

查看引导管理器

关于此任务

要进入引导管理器，请执行以下操作：

步骤

1. 开启或重新启动系统。
   在此处输入步骤的结果（可选）。
2. 显示以下消息时按 F11 键：

F11 = Boot Manager

如果按 F11 键之前已开始加载操作系统，请让系统完成引导，然后重新启动系统并重试。

引导管理器主菜单

菜单项	说明
Continue Normal Boot（持续正常引导）	系统尝试从引导顺序中的第一项开始引导至设备。如果引导尝试失败，系统将继续从引导顺序中的下一项进行引导，直到引导成功或者找不到引导选项为止。
One-Shot Boot Menu（一次性 UEFI 引导菜单）	支持您访问 UEFI 引导菜单并选择要引导的一次性引导选项。
Launch System Setup（启动系统设置）	允许您访问系统设置程序。
Launch Lifecycle Controller（启动 Lifecycle Controller）	退出 Boot Manager（引导管理器），并启动 Lifecycle Controller 程序。
System Utilities（系统公用程序）	通过该菜单项可以启动系统公用程序菜单，例如系统诊断和 UEFI shell。

One-Shot Boot Menu（一次性 UEFI 引导菜单）

One-shot UEFI Boot menu（一次性 UEFI 引导菜单）支持您访问 UEFI 引导菜单并选择要引导的一次性引导选项。

System Utilities（系统公用程序）

System Utilities（系统公用程序）包含以下可以启动的公用程序：

- 启动诊断程序
- BIOS 更新文件资源管理器
- 重新引导系统

PXE 引导

您可使用预引导执行环境 (PXE) 选项来远程引导和配置联网的系统。

要访问 **PXE boot（PXE 引导）**选项，请引导系统并在 POST 期间按 F12，而不是从 BIOS 设置程序使用标准引导顺序。它不拉动任何菜单或允许管理网络设备。