HP TamperLock 用户指南

摘要

HP TamperLock 可以防止攻击者打开您的 PC 机箱，恶意修改硬件。

版权和许可

第一版：2020 年 9 月

文档部件号：M11669-AA1

目录

1 概述

HP TamperLock 可以防止攻击者打开您的 PC 机箱，恶意修改硬件。HP TamperLock 包括传感器和策略控制。传感器用于检测机箱盖是否被打开；而策略控制用于配置发生此类开盖操作时要采取的操作。

HP TamperLock 策略包括各种可选功能：在 BIOS 级别阻止系统启动，直到输入有效的 BIOS 管理员凭据；清除 HP Trusted Platform Module (TPM) 以删除所有用户密钥（例如，呈现本地驱动器存储数据的 BitLocker 密钥，而该本地驱动器只可通过远程存储的 BitLocker 恢复密钥访问）；以及在取下机箱盖后立即关闭系统的功能。开盖事件和历史记录存储在平台硬件中，远程管理员可以对其进行查询。

HP Endpoint Security Controller 中的受保护存储可防止 HP TamperLock 策略遭到更改。受保护存储可使存储在与 HP TamperLock 设置相关的闪存上的 BIOS 和固件数据及设置免受物理攻击。此功能始终存在于支持 HP TamperLock 的系统并且无法被禁用。

2 操作

HP TamperLock 功能配置为未经授权擅自打开机箱盖时锁定系统。不管系统的电源状态如何，在未经授权擅自打开机箱盖时，它都能提供开盖检测。具体地说，当 HP TamperLock 使用 HP 的推荐设置进行配置时，在以下所有系统电源状态中，HP TamperLock 都将检测开盖事件。

- **系统打开**（操作系统 [OS] 正在运行）
- **系统关闭**（操作系统关闭或处于休眠状态）
- **系统处于睡眠状态**

切记：为获得本文档所述的最佳结果，请使用 HP 的推荐设置配置 HP TamperLock，如表 4-1 所示。

此外，即便所有电源都已拆除，包括内置电池和实时时钟 (RTC) 微型电池，此时取下机箱盖也会触发 HP TamperLock 开盖传感器。

注：实时时钟断电会自动触发 HP TamperLock 开盖传感器功能。因此，即使未取下机箱盖，而且系统存放两年以上没有连接任何电源，这样仍会触发 HP TamperLock 开盖传感器。

当系统处于启动或睡眠状态时，如果 HP TamperLock 检测到机箱盖被打开，系统将立即关闭，并且任何未保存的数据都将丢失。如果开盖时清除 TPM 状态的可选策略设置为**已启用**，则 BIOS 将清除 TPM。检测到机箱盖被打开后，BIOS 不会启动到操作系统，而是提示本地用户输入 BIOS 管理员密码或（在 Sure Admin 模式下）一次性 PIN 来解锁系统并正常启动。

您可以通过查询相关 BIOS 设置或在安装 HP Notifications 软件的情况下通过 Windows 事件查看器，获取 HP TamperLock 状态。

3 序列

此处概述了 HP TamperLock 的运行序列。

1. HP TamperLock 检测到机箱盖已打开。
2. 如果系统处于启动或睡眠状态，HP TamperLock 将强制系统关闭，并且无法选择取消。
3. 开盖事件会导致系统硬件进入锁定状态。
4. 更换机箱盖后，系统可再次启动。当系统下次启动时，会发生以下事件：
    1. 如果启用了清除 TPM 的策略，BIOS 将清除 TPM。
    2. 本地用户会在开盖时收到通知。
    3. 要求提供 BIOS 管理员凭据：
        - 如果提供了凭据，系统将正常启动。
        - 如果未提供凭据，系统将无法启动至操作系统。
5. 如果安装了 HP Notifications 软件，审核日志条目将与 Windows® 事件日志同步。

4 策略设置

您可以使用 HP Client Management 工具查看 HP TamperLock 策略并将其配置为 BIOS 设置。相关设置可控制 HP TamperLock 的功能是否启用以及在取下机箱盖时执行的操作。

表 4-1 TamperLock 策略设置

设置	说明	默认值	HP 推荐
开盖传感器	• **已禁用**—在取下机箱盖时不采取任何操作。 • **通知用户**—当机箱盖被打开时，下次启动时显示警告消息。 • **管理员凭据**—在机箱盖被打开后，此设置需要输入管理员密码或一次性 PIN（启用 HP Sure Admin 时），才能继续启动。要启用此设置，您必须设置密码或使用本地访问密钥集启用 HP Sure Admin 增强型 BIOS 身份验证模式。 • **管理员密码**—与管理员凭据相同的行为（此设置名称的存在是为了兼容支持开盖传感器的早期设置管理软件）。	已禁用	管理员凭据或管理员密码
开盖后关闭电源	仅在开盖传感器未设置为“已禁用”时可用。 **已禁用**—取下机箱盖时，如果系统处于启动或睡眠状态，则将继续保持此状态。 **已启用**—如果在系统处于启动或睡眠状态（S3 或现代待机）时取下机箱盖，则系统将立即关闭。	已禁用	已启用
开盖后启动时清除 TPM	仅在未禁用开盖传感器时可用。 • **已禁用**—在取下机箱盖时不会更改为 TPM 状态。 • **已启用**—在取下机箱盖后，下次启动时清除 TPM。TPM 中的所有客户密钥均会被清除。 **注：** 仅在可从远程备份手动恢复或不希望恢复时，才能启用此设置。如果启用 BitLocker，没有 BitLocker 恢复密钥则无法解密驱动器。	已禁用	取决于客户要求。
预启动 DMA 保护	**仅限 Thunderbolt**—在 BIOS 预启动环境中，为 Thunderbolt 连接的 PCIe 设备启用基于输入输出内存管理单元 (IOMMU) 硬件的 DMA 保护。	仅限 Thunderbolt	所有 PCI 设备

表 4-1 TamperLock 策略设置（续）

设置	说明	默认值	HP 推荐
	所有 PCIe 设备—在 BIOS 预启动环境中，为所有通过 PCI 连接的内置和外接设备启用基于输入输出内存管理单元 (IOMMU) 硬件的 DMA 保护。		
DMA 保护	**已禁用**—BIOS 不会配置输入输出内存管理单元 (IOMMU) 硬件来供支持 DMA 保护的操作系统使用。 **已启用**—BIOS 将配置输入输出内存管理单元 (IOMMU) 硬件来供支持 DMA 保护的操作系统使用。	已启用	已启用

5 状态

通过使用现有的 BIOS 设置管理工具，您可以查询 BIOS 设置来确定 HP TamperLock 的状态。清除此设置的唯一方法是提供 BIOS 管理员密码或 BIOS 管理员凭据（Sure Admin 模式）。

表 5-1

设置	说明
上次开盖和计数	如果开盖传感器未设置为“已禁用”，则此设置会报告上次取下机箱盖的时间，以及自从 BIOS 管理员上次对其进行清除以来，机箱盖被取下和确认了多少次。格式为 MM/DD/YYYY HH:MM:SS。X 次。根据系统因素（如计算机已关闭），连续打开机箱盖不会增加计数。如果无法确定日期和时间的数值，则日期和时间将全部归零，例如在实时时钟断电后。

事件审核日志

如果安装了 HP Notifications 软件，您可以在 HP Sure Start 文件夹的 Windows 事件查看器中查看以下事件日志。

表 5-2 审核日志

源 ID	事件 ID	事件	事件日志类型
0x8A	0x1E	HP TamperLock - 系统检测到机箱盖已打开。	警告
	0x1F	HP TamperLock - 用户确认了提示机箱盖已打开的 BIOS POST 通知。	信息
	0x20	HP TamperLock - 根据当前 HP TamperLock 策略设置，由于机箱盖被打开导致清除了 TPM。	信息