HP TamperLock 使用指南

摘要

HP TamperLock 可防止攻擊者打開您的電腦機殼並以惡意方式修改硬體。

第一版：2020 年 9 月

文件編號：M11669-AB1

目錄

1 概觀

HP TamperLock 可防止攻擊者打開您的電腦機殼並以惡意方式修改硬體。HP TamperLock 包含可偵測機殼是否開啟的感應器，以及用來設定發生此類情況後所要採取動作的原則控制項。

HP TamperLock 原則包含下列選擇性功能：在 BIOS 層級封鎖系統開機，直到輸入有效的 BIOS 管理員認證、清除 HP 信任平台模組 (TPM) 以刪除所有使用者金鑰（例如，可轉換僅能透過遠端儲存 BitLocker 復原金鑰存取之本機磁碟機上資料的 BitLocker 金鑰），以及拆卸蓋板時立即關閉系統的功能。蓋板開啟事件與歷程記錄會儲存在平台硬體中，且可由遠端管理員進行查詢。

HP TamperLock 原則可防止 HP Endpoint Security Controller 硬體中受保護的儲存裝置在破解後遭到變更。受保護的儲存裝置可針對 BIOS 與韌體資料，以及儲存在快閃記憶體中與 HP TamperLock 設定相關的設定，提供實體攻擊保護。此功能一律會顯示在支援 HP TamperLock 的系統上，且無法停用。

2 作業

HP TamperLock 功能設定為在未經授權存取時鎖定系統，能提供蓋板開啟偵測，而且不論未經授權蓋板開啟期間的系統電源狀態為何。具體而言，當使用 HP 建議的設定對 HP TamperLock 進行設定時，HP TamperLock 將會在下列所有系統電源狀態下偵測蓋板開啟事件。

- **系統開啟**（作業系統 [OS] 正在執行）
- **系統關閉**（作業系統關閉，或作業系統處於休眠狀態）
- **系統處於「睡眠」狀態**

重要：為能獲得如本文件所述的最佳效果，請將 HP TamperLock 設定為 HP 推薦的設定，如表格 4-1 中所示。

此外，即便在蓋板拆卸時所有供電來源（包含內部電池與即時時鐘 (RTC) 鈕扣電池）已拔除/失去電力，仍可觸發 HP TamperLock 蓋板開啟感應器。

附註：RTC 電力中斷會自動觸發 HP TamperLock 蓋板開啟感應器功能。因此，當系統放置在未連接任何電源的儲存環境中超過 2 年，即便蓋板並未遭到拆卸，仍將觸發 HP TamperLock 蓋板開啟感應器。

當 HP TamperLock 偵測到蓋板開啟且系統已開啟或電腦處於「睡眠」狀態時，系統會立即關閉，且任何未儲存的資料均會遺失。若蓋板開啟偵測上的清除 TPM 狀態選擇性原則設為**啟用**，則 BIOS 會清除 TPM。BIOS 不會在偵測到蓋板開啟後啟動至作業系統，而是會提示本機使用者輸入 BIOS 管理員密碼或一次性 PIN 碼（Sure Admin 模式下）以解除鎖定系統並正常啟動。

若已安裝 HP Notifications 軟體，您可以透過相關聯的 BIOS 設定查詢，或透過 Windows 事件檢視器來取得 HP TamperLock 狀態。

3 順序

此處概述 HP TamperLock 的順序。

1. HP TamperLock 會偵測機座蓋板是否已遭開啟。
2. 若系統已開啟或處於「睡眠」模式，則 HP TamperLock 會強制關閉且不會顯示取消的選項。
3. 蓋板開啟事件會導致系統硬體進入鎖定狀態。
4. 更換蓋板時，系統可能會再次開啟。當系統再次開啟時，便會發生下列事件：
    1. 若清除 TPM 的原則已啟用，則 BIOS 會清除 TPM。
    2. 系統會通知本機使用者蓋板開啟。
    3. 此時會要求 BIOS 管理員認證：
        - 若提供認證，則系統會正常啟動。
        - 若未提供認證，則系統不會啟動至作業系統。
5. 若已安裝 HP Notifications 軟體，則稽核記錄項目會與 Windows® 事件記錄同步。

4 原則設定

您可以使用 HP Client Management 工具來檢視和設定 HP TamperLock 原則，如同 BIOS 設定一般。這些相關聯的設定可控制 HP TamperLock 功能的啟用，以及蓋板拆卸後所要採取的動作。

表格 4-1 TamperLock 原則設定

設定	說明	預設值	HP 建議
蓋板開啟感應器	• **停用**—蓋板拆卸時不採取任何動作。 • **通知使用者**—當蓋板開啟時，在下一次啟動時顯示警告訊息。 • **管理員認證**—此設定會要求輸入管理員密碼或一次性 PIN 碼（當 HP Sure Admin 啟用時），然後才能在蓋板開啟後繼續啟動。若要啟用此設定，您必須設定密碼或啟用 HP Sure Admin 增強型 BIOS 驗證模式並搭配本機存取金鑰組。 • **管理員密碼**—與管理員認證行為相同（系統會顯示此設定以維持與支援蓋板開啟感應器之舊版設定管理軟體的相容性）。	停用	管理員認證或管理員密碼
蓋板開啟時關閉電源	僅在蓋板開啟感應器並未設為「停用」時才能使用。 **停用**—若蓋板拆卸時系統已開啟或處於「睡眠」狀態，則它會維持該狀態。 **啟用**—當系統已開啟或處於「睡眠」（S3 或新式待命）狀態時，若蓋板已拆卸，則系統會立即關閉。	停用	啟用
蓋板開啟後在開機時清除 TPM	僅在蓋板開啟感應器並未停用時才能使用。 • **停用**—當蓋板拆卸時不會變更 TPM 狀態。 • **啟用**—蓋板拆卸後系統會在下一次啟動時清除 TPM。系統會清除 TPM 中的所有客戶金鑰。 **附註：**僅在您可從遠端備份進行手動復原，或您不想要復原的情況下，才啟用此設定。若 BitLocker 已啟用，則磁碟機需要 BitLocker 復原金鑰才能解密。	停用	視客戶要求而定。
開機前 DMA 保護	**僅 Thunderbolt**—輸入輸出記憶體管理單元 (IOMMU) 硬體式 DMA 保護會在 BIOS 開機前環境中啟用，適用於已連接 Thunderbolt 的 PCI-e 裝置。	僅 Thunderbolt	所有 PCI 裝置

表格 4-1 TamperLock 原則設定 （續）

設定	說明	預設值	HP 建議
	所有 PCIe 裝置—輸入輸出記憶體管理單元 (IOMMU) 硬體式 DMA 保護會在 BIOS 開機前環境中啟用，適用於所有已連接 PCI 的內部與外部裝置。		
DMA 保護	**停用**—BIOS 將不會設定輸入輸出記憶體管理單元 (IOMMU) 硬體以供支援 DMA 保護的作業系統使用。 **啟用**—BIOS 將會設定輸入輸出記憶體管理單元 (IOMMU) 硬體以供支援 DMA 保護的作業系統使用。	啟用	啟用

5 狀態

您可以使用現有的 BIOS 設定管理工具來查詢 BIOS 設定，藉此判斷 HP TamperLock 的狀態。清除此設定的唯一方法是提供 BIOS 管理員密碼或 BIOS 管理員認證（Sure Admin 模式）。

表格 5-1

設定	說明
上次蓋板開啟和計數	當蓋板開啟感應器並未設為「停用」時，此設定會回報自 BIOS 管理員上次清除設定起計算的上一次蓋板拆卸時間與已確認的拆卸次數。格式項目為 MM/DD/YYYY HH:MM:SS。X 次。視系統因素（例如電腦已關閉）而定，接連的蓋板開啟情況將不會累加至計數。日期與時間在無法判斷值的情況下將會全數回報為 0 值，例如即時時鐘已失去電力後的情況。

事件稽核記錄檔

若已安裝 HP Notifications 軟體，則您可以用 Windows 事件檢視器檢視 HP Sure Start 資料夾中的下列事件記錄。

表格 5-2 稽核記錄

來源 ID	事件 ID	事件	事件記錄檔
0x8A	0x1E	HP TamperLock - 系統偵測到蓋板已遭開啟。	警告
	0x1F	HP TamperLock - 使用者已確認指出蓋板遭到開啟的 BIOS POST 通知。	參考資訊
	0x20	HP TamperLock - 根據目前的 HP TamperLock 原則設定，TPM 已因蓋板開啟而遭到清除。	參考資訊