Manuel de l'utilisateur HP TamperLock

RESUME

HP TamperLock protège contre toute attaque d'ouverture du boîtier de votre PC et toute modification du matériel de manière malveillante.

Première édition : septembre 2020

Numéro de référence du document : M11669-051

Sommaire

1 Présentation

HP TamperLock protège contre toute attaque d'ouverture du boîtier de votre PC et toute modification du matériel de manière malveillante. HP TamperLock inclut des capteurs pour détecter si le boîtier a été ouvert et des contrôles de stratégie pour configurer l'action à effectuer si cela se produit.

Les stratégies HP TamperLock incluent des capacités facultatives de blocage du démarrage du système au niveau du BIOS jusqu'à ce que des informations d'authentification de l'administrateur du BIOS valides soient saisies. d'effacement du HP Trusted Platform Module (TPM) pour supprimer toutes les clés utilisateur (par exemple, les clés BitLocker qui rendent les données stockées sur le disque local accessibles uniquement via une clé de récupération BitLocker stockée à distance), et la possibilité d'éteindre le système immédiatement lorsque le capot est retiré. Les événements d'ouverture du capot et l'historique sont stockés sur une plate-forme matérielle et peuvent être interrogés par un administrateur distant.

Les stratégies HP TamperLock ne peuvent pas être modifiées par un stockage protégé enraciné dans le matériel du contrôleur HP Endpoint Security. Le stockage protégé fournit une protection contre les attaques physiques contre les données et les paramètres du BIOS et du microprogramme stockées dans la mémoire flash associée aux paramètres de HP TamperLock. Cette fonctionnalité est toujours présente sur les systèmes qui prennent en charge HP TamperLock et ne peut pas être désactivée.

2 Fonctionnement

La fonction HP TamperLock est configurée pour verrouiller le système en cas d'un accès non autorisé, elle fournit une détection d'ouverture du capot, quel que soit l'état d'alimentation du système lors d'une ouverture du capot non autorisée. Plus particulièrement, HP TamperLock détectera un événement d'ouverture du capot dans tous les états suivants d'alimentation du système lorsque HP TamperLock est configuré avec les paramètres recommandés par HP.

- **Système activé** (système d'exploitation [SE] en cours d'exécution)
- **Système désactivé** (arrêt du système d'exploitation ou système d'exploitation en mode veille prolongée)
- **Système en mode veille**

IMPORTANT : Pour obtenir les résultats optimaux décrits dans ce document, configurez HP TamperLock avec les paramètres recommandés par HP, comme indiqué dans le tableau 4-1.

En outre, le capteur d'ouverture du capot HP TamperLock est déclenché même dans un scénario où toutes les sources d'alimentation sont retirées alors que le capot est retiré, y compris la batterie interne et la pile bouton de l'horloge en temps réel (RTC).

REMARQUE : La perte d'alimentation RTC déclenche automatiquement la fonction du capteur d'ouverture du capot HP TamperLock. Par conséquent, les systèmes qui demeurent stockés sans source d'alimentation pendant plus de 2 ans déclenchent le capteur d'ouverture du capot HP TamperLock, même lorsque le capot n'a pas été retiré.

Lorsque HP TamperLock détecte une ouverture du capot lorsque le système est activé ou en mode veille, le système est immédiatement désactivé et les données non enregistrées sont perdues. Si la stratégie facultative d'effacer l'état du TPM à la détection d'ouverture du capot est définie sur **Activé**, le BIOS efface le TPM. Le BIOS ne démarre pas sur le système d'exploitation une fois que l'ouverture du capot est détectée et invite plutôt l'utilisateur local à entrer le mot de passe d'administrateur du BIOS ou (en mode Sure Admin) un code PIN à utilisation unique pour déverrouiller le système et démarrer normalement.

Vous pouvez obtenir l'état de HP TamperLock via une requête sur le paramètre du BIOS associé ou via l'observateur d'événements Windows lorsque le logiciel HP Notifications est installé.

3 Séquence

La séquence de HP TamperLock est décrite ici.

1. HP TamperLock détecte lorsque le capot du châssis a été ouvert.
2. Si le système est sous tension ou en mode veille, HP TamperLock force un arrêt sans option d'annulation.
3. L'événement d'ouverture du capot entraîne l'entrée du système matériel en mode verrouillé.
4. Le capot étant replacé, le système peut à nouveau être mis sous tension. Lorsque le système est à nouveau sous tension, les événements suivants se produisent :
    1. Si la stratégie pour effacer le TPM est activée, le BIOS efface le TPM.
    2. L'utilisateur local est notifié de l'ouverture du capot.
    3. Les informations d'authentification de l'administrateur BIOS sont demandées :
        - Si des informations d'authentification sont fournies, le système démarre normalement.
        - Si les informations d'authentification ne sont pas fournies, le système ne démarre pas avec le système d'exploitation.
5. L'entrée du journal d'audit est synchronisée avec le journal des événements Windows® si le logiciel HP Notifications est installé.

4 Paramètres de stratégie

Vous pouvez utiliser les outils HP Client Management pour afficher et configurer les stratégies HP TamperLock en tant que paramètres du BIOS. Les paramètres associés contrôlent l'activation de la fonction HP TamperLock, ainsi que les actions effectuées lors du retrait du capot.

Tableau 4-1 Paramètres de stratégie TamperLock

Paramètres	Description	Défaut	Recommandé par HP
Capteur d'ouverture du capot	• **Désactivé** : Aucune action n'est effectuée lorsque le capot est retiré. • **Notifier l'utilisateur** : Affiche un message d'avertissement au prochain démarrage lors de l'ouverture du capot. • **Informations d'authentification de l'administrateur** : Ce paramètre nécessite d'entrer le mot de passe administrateur ou le code PIN unique (lorsque HP Sure Admin est activé) avant de continuer le démarrage une fois le capot ouvert. Pour activer ce paramètre, vous devez définir un mot de passe ou activer le mode d'authentification du BIOS amélioré HP Sure Admin Enhanced avec un jeu de clés d'accès local. • **Mot de passe administrateur** : Même comportement que Informations d'authentification de l'administrateur (Ce nom de paramètre est présent pour maintenir la compatibilité avec les logiciels de gestion des paramètres antérieurs qui prenaient en charge le capteur d'ouverture du capot).	Désactivé	Informations d'authentification de l'administrateur ou Mot de passe administrateur
Mise hors tension lors de l'ouverture du capot	N'est disponible que lorsque le capteur d'ouverture du capot n'est pas défini sur Désactivé. **Désactivé** : Si le système est activé ou en mode veille lorsque le capot est retiré, il reste dans cet état. **Activé** : Le système s'éteint immédiatement si le capot est retiré lorsque le système est activé ou en veille (S3 ou Veille moderne).	Désactivé	Activé
Effacer le TPM au démarrage après ouverture du capot	N'est disponible que lorsque le capteur d'ouverture du capot n'est pas désactivé. • **Désactivé** : aucun changement à l'état du TPM lorsque le capot est retiré. • **Activé** : le TPM est effacé lors du prochain démarrage une fois le capot retiré. Toutes les clés client du TPM sont effacées.	Désactivé	Dépend des exigences des clients.

Tableau 4-1 Paramètres de stratégie TamperLock (suite)

Paramètres	Description	Défaut	Recommandé par HP
	REMARQUE : Activez ce paramètre uniquement lorsque vous pouvez effectuer une récupération manuelle à partir de la sauvegarde à distance ou lorsque vous ne souhaitez pas effectuer de récupération. Si BitLocker est activé, le lecteur ne peut pas être déchiffré sans la clé de récupération BitLocker.		
Protection DMA avant amorçage	**Thunderbolt uniquement** : La protection DMA matérielle de l'unité de gestion de mémoire entrées/sorties (IOMMU) est activée dans l'environnement de préamorçage du BIOS pour les périphériques PCI-e connectés par Thunderbolt. **Tous les périphériques PCIe** : la protection DMA matérielle de l'unité de gestion de mémoire entrées/sorties (IOMMU) est activée dans l'environnement de préamorçage du BIOS pour tous les périphériques connectés au PCI interne et externe.	Thunderbolt uniquement	Tous les périphériques PCI
Protection DMA	**Désactivé** : Le BIOS ne configure pas le matériel de l'unité de gestion de mémoire entrées/sorties (IOMMU) pour une utilisation par les systèmes d'exploitation qui prennent en charge la protection DMA. **Activé** : Le BIOS configure le matériel de l'unité de gestion de mémoire entrées/sorties (IOMMU) pour une utilisation par les systèmes d'exploitation qui prennent en charge la protection DMA.	Activé	Activé

5 État

Vous pouvez interroger le paramétrage du BIOS pour déterminer l'état de HP TamperLock à l'aide des outils de gestion des paramètres BIOS existants. La seule façon d'effacer ce paramètre consiste à fournir le mot de passe d'administrateur du BIOS ou les informations d'authentification de l'administrateur du BIOS (mode Sure Admin).

Tableau 5-1

Réglages	Description
Dernière ouverture du capot et comptage	Lorsque le capteur d'ouverture du capot n'est pas défini sur Désactivé, ce paramètre indique la dernière fois où le capot a été retiré et le nombre de fois où il a été retiré et reconnu depuis que l'administrateur du BIOS l'a effacé pour la dernière fois. L'entrée est au format MM/JJ/AAAA HH:MM:SS. X fois. Selon les facteurs système (tels que l'ordinateur est éteint), les ouvertures de capot consécutives n'incrémenteront pas ce comptage. La date et l'heure seront toutes signalées à 0s dans les cas où la valeur ne peut pas être déterminée, par exemple après une perte de puissance de l'horloge en temps réel.

Journal d'audit d'évènement

Si le logiciel HP Notifications est installé, vous pouvez afficher les journaux des événements suivants dans l'observateur d'événements Windows dans le dossier HP Sure Start.

Tableau 5-2 Journal d'audit

ID source	ID de l'événement	Événement	Type de journal des événements
0x8A	0x1E	HP TamperLock - Le système a détecté l'ouverture du capot.	Avertissement
	0x1F	HP TamperLock - L'utilisateur a pris connaissance d'une notification POST BIOS indiquant que le capot avait été ouvert.	Informatif
	0x20	HP TamperLock - Le TPM a été effacé en raison de l'ouverture du capot en fonction des paramètres de stratégie HP TamperLock actuels.	Informatif