Guía del usuario HP TamperLock

Resumen

HP TamperLock brinda protección para evitar la apertura del chasis del equipo y la modificación maliciosa del hardware.

Primera edición: septiembre de 2020

Número de referencia del documento: M11669-E51

Tabla de contenido

1 Visión general

HP TamperLock brinda protección para evitar la apertura del chasis del equipo y la modificación maliciosa del hardware. HP TamperLock incluye sensores para detectar si el chasis se abrió, además de controles de política para configurar qué acción realizar si ocurre la apertura.

Las políticas de HP TamperLock incluyen las capacidades opcionales de bloqueo del arranque del sistema en el nivel del BIOS hasta que se introduzcan credenciales de administrador del BIOS válidas, borrado del HP Trusted Platform Module (TPM) para eliminar todas las claves de usuario (por ejemplo, las claves de BitLocker que hacen que los datos almacenados en la unidad local solo sean accesibles mediante una clave de recuperación de BitLocker almacenada de forma remota) y la capacidad de apagar el sistema de inmediato cuando se extrae la cubierta. Los eventos de apertura de la cubierta y el historial se almacenan en el hardware de la plataforma y un administrador remoto puede consultarlos.

Las políticas de HP TamperLock no pueden alterarse porque están protegidas mediante almacenamiento con protección, basado en el hardware del HP Endpoint Security Controller. El almacenamiento protegido brinda protección contra ataques físicos para los datos y las configuraciones del BIOS y el firmware almacenados en la memoria flash y relacionados con las configuraciones de HP TamperLock. Este recurso siempre está presente en los sistemas que admiten HP TamperLock y no puede deshabilitarse.

2 Funcionamiento

El recurso HP TamperLock está configurado para bloquear el sistema debido a acceso no autorizado. Brinda detección de apertura de la cubierta, independientemente del estado de energía del sistema durante la apertura no autorizada de la cubierta. Específicamente, HP TamperLock detectará un evento de apertura de la cubierta en todos los siguientes estados de energía del sistema cuando HP TamperLock esté configurado según las recomendaciones de HP.

- **Sistema encendido** (sistema operativo [SO] en ejecución)
- **Sistema apagado** (SO apagado o en estado de hibernación)
- **Sistema en estado de suspensión**

IMPORTANTE: Para obtener los resultados óptimos descritos en este documento, configure HP TamperLock según las recomendaciones de la tabla 4-1.

Además, el sensor de apertura de la cubierta de HP TamperLock se activa incluso en caso de que se retiren todas las fuentes de energía mientras se extrae la cubierta, incluida la batería interna y la celda de moneda del reloj en tiempo real (RTC).

NOTA: La pérdida de energía de RTC activa de forma automática el recurso del sensor de apertura de la cubierta de HP TamperLock. Por lo tanto, los sistemas que permanecen en el almacenamiento sin ninguna fuente de alimentación conectada durante más de 2 años activarán el sensor de apertura de la cubierta de HP TamperLock, incluso si no se ha extraído la cubierta.

Cuando HP TamperLock detecta que se ha abierto la cubierta mientras el sistema está encendido o en estado de suspensión, el sistema se apaga de inmediato y se pierden los datos que no se han guardado. Si la política opcional para borrar el estado del TPM en la detección de apertura de la cubierta está **Habilitada**, el BIOS borra el TPM. El BIOS no inicia el SO después de que se detecta la apertura de la cubierta y, en su lugar, solicita al usuario local que introduzca la contraseña de administrador del BIOS o (en modo de Sure Admin) un PIN de uso único para desbloquear el sistema y arrancar normalmente.

Puede obtener el estatus de HP TamperLock a través de una consulta de la configuración del BIOS asociada o mediante el Visor de eventos de Windows cuando está instalado el software HP Notifications.

3 Secuencia

Aquí se describe la secuencia de HP TamperLock.

1. HP TamperLock detecta que se ha abierto la cubierta del chasis.
2. Si el sistema está encendido o en suspensión, HP TamperLock fuerza un apagado sin la opción de cancelar.
3. El evento de apertura de la cubierta da como resultado que el hardware del sistema ingrese en un estado de bloqueo.
4. Cuando se vuelve a colocar la cubierta, el sistema se puede volver a encender. Cuando el sistema se enciende a continuación, se producen los siguientes eventos:
    1. Si la política para borrar el TPM está habilitada, el BIOS borrará el TPM.
    2. Se notifica al usuario local sobre la apertura de la cubierta.
    3. Se solicitan las credenciales del administrador del BIOS:
        - Si se proporcionan credenciales, el sistema se inicia normalmente.
        - Si no se proporcionan credenciales, el sistema no se iniciará en el SO.
5. La entrada de registro de auditoría está sincronizada con el registro de eventos de Windows® si el software HP Notifications está instalado.

4 Configuración de políticas

Puede utilizar las herramientas de HP Client Management para ver y configurar las políticas de HP TamperLock como configuraciones del BIOS. Las configuraciones asociadas controlan la habilitación del recurso HP TamperLock, así como las acciones tomadas cuando se extrae la cubierta.

Tabla 4-1 Configuración de políticas de TamperLock

Configuración	Descripción	Predeterminado	Recomendado por HP
Sensor de apertura de la cubierta	• **Deshabilitado**: no se toma ninguna acción cuando se extrae la cubierta. • **Notificar al usuario**: muestra el mensaje de advertencia en el siguiente inicio cuando se abre la cubierta. • **Credencial de administrador**: esta configuración requiere introducir la contraseña de administrador o el PIN único (cuando HP Sure Admin está activado) antes de continuar con el inicio, después de que se ha abierto la cubierta. Para habilitar esta configuración, debe definir una contraseña o habilitar el modo de autenticación mejorada del BIOS de HP Sure Admin con un conjunto de claves de acceso local. • **Contraseña de administrador**: el mismo comportamiento que la credencial de administrador (este nombre de configuración está presente para mantener la compatibilidad con el software anterior de administración de configuraciones que admitía el sensor de apertura de la cubierta).	Deshabilitado	Credencial de administrador o contraseña de administrador
Apagado al abrirse la cubierta	Solo está disponible cuando el sensor de apertura de la cubierta no está establecido como Deshabilitado. **Deshabilitado**: si el sistema está encendido o en estado de suspensión cuando se extrae la cubierta, permanece en ese estado. **Habilitado**: el sistema se apaga de inmediato si se extrae la cubierta mientras el sistema está encendido o en suspensión (modo de espera S3 o moderno).	Deshabilitado	Habilitado
Borrar el TPM en el arranque después de la apertura de la cubierta	Solo está disponible cuando el sensor de apertura de la cubierta no está deshabilitado. • **Deshabilitado**: no hay cambios en el estado del TPM cuando se extrae la cubierta. • **Habilitado**: el TPM se borra en el siguiente arranque después de que se ha extraído la cubierta. Todas las teclas de cliente del TPM se borran.	Deshabilitado	Depende de los requisitos del cliente.

Tabla 4-1 Configuración de políticas de TamperLock (continuación)

Configuración	Descripción	Predeterminado	Recomendado por HP
	NOTA: Habilite esta configuración solamente cuando la recuperación manual sea posible desde copias de seguridad remotas o cuando no desee realizar una recuperación. Si BitLocker está activado, la unidad no se puede desencriptar sin la tecla de recuperación de BitLocker.		
Protección de DMA previo al inicio	**Solo Thunderbolt**: la protección de DMA basada en hardware de la Unidad de administración de memoria de entrada y salida (IOMMU) está habilitada en el entorno de preinicio del BIOS para dispositivos PCI-e conectados con Thunderbolt. **Todos los dispositivos PCIe**: la protección de DMA basada en hardware de la Unidad de administración de memoria de entrada y salida (IOMMU) está habilitada en el entorno de preinicio del BIOS para todos los dispositivos internos y externos conectados con PCI.	Solo Thunderbolt	Todos los dispositivos PCI
Protección de DMA	**Deshabilitado**: el BIOS no configurará el hardware de la Unidad de administración de memoria de entrada y salida (IOMMU) para el uso de los sistemas operativos que admiten la protección de DMA. **Habilitado**: el BIOS configurará el hardware de la Unidad de administración de memoria de entrada y salida (IOMMU) para el uso de los sistemas operativos que admiten la protección de DMA.	Habilitado	Habilitado

5 Estado

Puede consultar la configuración del BIOS para determinar el estatus de HP TamperLock mediante las herramientas existentes de administración de configuraciones del BIOS. La única forma de eliminar esta configuración es proporcionar la contraseña de administrador del BIOS o la credencial de administrador del BIOS (modo Sure Admin).

Tabla 5-1

Ajuste	Descripción
Conteo y última vez que se abrió la cubierta	Cuando el sensor de apertura de la cubierta no está Deshabilitado, esta configuración informa sobre la última vez que se extrajo la cubierta y la cantidad de veces que ha sido extraída y se ha detectado desde la última vez que el administrador del BIOS borró los datos. La entrada del formato es MM/DD/AAAA HH:MM:SS. X veces. Según factores del sistema (como el hecho de que el equipo esté apagado), las aperturas consecutivas de la cubierta no aumentarán el conteo. La fecha y la hora se indicaran con 0 en los casos en los que no se pueda determinar el valor, por ejemplo, si falta energía en el reloj en tiempo real.

Registro de auditoría de eventos

Si el software HP Notifications está instalado, puede ver los siguientes registros de eventos en el Visor de eventos de Windows, en la carpeta de HP Sure Start.

Tabla 5-2 Registro de auditoría

ID de origen	ID del evento	Evento	Tipo de registro de eventos
0x8A	0x1E	HP TamperLock: el sistema detectó que se abrió la cubierta.	Advertencia
	0x1F	HP TamperLock: el usuario reconoció una notificación del BIOS POST de que se había abierto la cubierta.	Informativo
	0x20	HP TamperLock: el TPM se borró debido a la apertura de la cubierta basada en la configuración actual de la política de HP TamperLock.	Informativo