HP TamperLock User Guide

SUMMARY

HP TamperLock protects against an attacker opening the case of your PC and modifying the hardware in a malicious manner.

Copyright and License

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: September 2020

Document Part Number: M11669-001

Table of contents

1 Overview

HP TamperLock protects against an attacker opening the case of your PC and modifying the hardware in a malicious manner. HP TamperLock includes sensors to detect whether the case was opened and policy controls to configure what action to take if it occurs.

HP TamperLock policies include the optional abilities of blocking system boot at the BIOS level until valid BIOS administrator credentials are entered, clearing the HP Trusted Platform Module (TPM) to delete all user keys (for example, BitLocker keys that render the data stored on the local drive accessible only via a remotely stored BitLocker recovery key), and the ability to turn off the system immediately when the cover is removed. Cover opening events and history are stored in platform hardware and can be queried by a remote administrator.

HP TamperLock policies are protected from being changed by protected storage rooted in the HP Endpoint Security Controller hardware. Protected storage provides physical attack protection for BIOS and firmware data and settings stored in flash memory related to HP TamperLock settings. This capability is always present on systems that support HP TamperLock and cannot be disabled.

2 Operation

The HP TamperLock feature is configured to lock the system due to unauthorized access, it provides cover opening detection regardless of the power state of the system during unauthorized cover opening. Specifically, HP TamperLock will detect a cover opening event in all the following system power states when HP TamperLock is configured with HP recommended settings.

- **System On** (operating system [OS] running)
- **System Off** (OS shutdown, or OS in hibernated state)
- **System in Sleep state**

IMPORTANT: For the optimum results described in this document, configure HP TamperLock with HP's recommended settings, as shown in Table 4-1.

Additionally, the HP TamperLock cover opening sensor is triggered even in a scenario where all power sources are removed while the cover is removed, including internal battery and Real-Time Clock (RTC) coin cell.

NOTE: RTC power loss automatically triggers the HP TamperLock cover opening sensor feature. Therefore, systems that remain in storage without any power supply attached for longer than 2 years will trigger HP TamperLock cover opening sensor, even when the cover has not been removed.

When HP TamperLock detects a cover opening while the system is on or in in the Sleep state, the system is immediately turned off and any unsaved data will be lost. If the optional policy to clear the TPM state on cover opening detection is set to **Enabled**, the BIOS clears the TPM. The BIOS does not boot to the OS after the cover opening is detected and instead prompts the local user to enter the BIOS administrator password or (in Sure Admin mode) a one-time-use PIN to unlock the system and boot normally.

You can obtain the HP TamperLock status via a query of the associated BIOS setting or via the Windows Event Viewer when HP Notifications software is installed.

3 Sequence

The sequence of HP TamperLock is outlined here.

1. HP TamperLock detects that the chassis cover has been opened.
2. If the system is on or in Sleep, HP TamperLock forces a shutdown without the option to cancel.
3. The cover opening event results in the system hardware entering a locked state.
4. With the cover replaced, the system can once again be turned on. When the system is next turned on, the following events occur:
    1. If the policy to clear TPM is enabled, the BIOS clears the TPM.
    2. The local user is notified of the cover opening.
    3. BIOS Admin Credentials are requested:
        - If credentials are provided, the system boots normally.
        - If credentials are not provided, the system does not boot to the OS.
5. Audit log entry is synced with the Windows® event log if HP Notifications software is installed.

4 Policy settings

You can use HP Client Management tools to view and configure HP TamperLock policies as BIOS settings. The associated settings control the HP TamperLock capability enablement as well as the actions taken when the cover is removed.

Table 4-1 TamperLock policy settings

Settings	Description	Default	HP Recommended
Cover opening sensor	- **Disabled**—No action taken when cover is removed. - **Notify the user**—Displays warning message on the next startup when the cover is opened. - **Administrator Credential**—This setting requires entering the administrator password or the one-time-PIN (when HP Sure Admin is enabled) before continuing startup after the cover is opened. To enable this setting, you must set a password or enable HP Sure Admin Enhanced BIOS Authentication Mode with a local access key set. - **Administrator Password**—Same behavior as Administrator Credential (This setting name is present to maintain compatability with earlier setting management software that supported the cover opening sensor).	Disabled	Administrator Credential or Administrator Password
Power off upon cover opening	Only available when cover opening sensor is not set to Disabled. **Disabled**—if system is in on or sleep state when cover is removed, it remains in that state. **Enabled**—the system immediately turns off if the cover is removed while the system is on or sleep (S3 or Modern Standby).	Disabled	Enabled
Clear TPM on boot after cover opening	Only available when cover opening sensor is not disabled. - **Disabled**—No change to TPM state when cover is removed. - **Enabled**—TPM is cleared on the next startup after the cover is removed. All customer keys in the TPM are cleared. **NOTE:** Enable this setting only when manual recovery is possible from remote backup or when you do not want recovery. If BitLocker is enabled, the drive cannot be decrypted without the BitLocker recovery key.	Disabled	Depends on Customer requirements.
Pre-boot DMA protection	**Thunderbolt Only**—Input-Output Memory Management Unit (IOMMU) hardware-based DMA	Thunderbolt Only	All PCI-Devices

Table 4-1 TamperLock policy settings (continued)

Settings	Description	Default	HP Recommended
	protection is enabled in BIOS preboot environment for Thunderbolt-attached PCI-e devices. **All PCIe devices**—Input-Output Memory Management Unit (IOMMU) hardware-based DMA protection is enabled in BIOS preboot environment for all internal and external PCI-attached devices.		
DMA Protection	**Disabled**—BIOS will not configure Input-Output Memory Management Unit (IOMMU) hardware for use by operating systems that support DMA protection. **Enabled**—BIOS will configure Input-Output Memory Management Unit (IOMMU) hardware for use by operating systems that support DMA protection.	Enabled	Enabled

5 Status

You can query the BIOS setting to determine the status of HP TamperLock by using existing BIOS setting management tools. The only way to clear this setting is to provide the BIOS administrator password or BIOS Administrator Credential (Sure Admin mode).

Table 5-1

Setting	Description
Last cover opening and count	When cover opening sensor is not set to Disabled, this setting reports the last time the cover was removed and how many times it was removed and acknowledged since the BIOS administrator last cleared it. The format entry is MM/DD/YYYY HH:MM:SS. X times. Depending on system factors (such as the computer is off), consecutive cover openings will not increment the count. The date and time will be reported as all 0s in cases where the value cannot be determined, such as after a real-time clock power loss.

Event audit log

If HP Notifications software is installed, you can view the following event logs in Windows Event Viewer in the HP Sure Start Folder.

Table 5-2 **Audit log**

Source ID	Event ID	Event	Event Log Type
0x8A	0x1E	HP TamperLock - The system detected that the cover was opened.	Warning
	0x1F	HP TamperLock - The user acknowledged a BIOS POST notification that the cover had been opened.	Informational
	0x20	HP TamperLock - The TPM was cleared due to cover opening based on current HP TamperLock policy settings.	Informational