HP TamperLock-brugerhåndbog

OVERSIGT

HP TamperLock beskytter mod uautoriserede forsøg på at åbne kabinettet på din pc og ændre hardwaren på en ondsindet måde.

Første udgave: September 2020

Dokumentets bestillingsnummer: M11669-081

Indholdsfortegnelse

1 Oversigt 1

2 Drift 2

3 Rækkefølge 3

4 Politikindstillinger 4

5 Status 6

Hændelsesovervågningslogfil 6

1 Oversigt

HP TamperLock beskytter mod uautoriserede forsøg på at åbne kabinettet på din pc og ændre hardwaren på en ondsindet måde. HP TamperLock indeholder sensorer, der registrerer, om kabinettet er blevet åbnet, og politikkontrol, der gør det muligt at konfigurere, hvad du skal gøre, hvis det sker.

HP TamperLock-politikker omfatter valgfrie muligheder for at blokere systemopstart på BIOS-niveau, indtil gyldige BIOS-administratorlegitimationsoplysninger indtastes, mulighed for at lade HP Trusted Platform-modulet (TPM) slette alle brugernøgler (f.eks. BitLocker-nøgler, der gengiver data på det lokale drev, som kun er tilgængelige via en eksternt gemt BitLocker-genoprettelsesnøgle) og mulighed for at slukke systemet øjeblikkeligt, hvis dækslet fjernes. Dækselåbningshændelser og -historik gemmes i platformhardwaren, og en fjernadministrator kan sende forespørgsler.

HP TamperLock-politikker beskyttes mod ændring ved hjælp af et beskyttet lager, som er indlejret i HP Endpoint Security Controller-hardware. Det beskyttede lager giver beskyttelse mod fysiske angreb til BIOS og firmwaredata samt indstillinger, der er gemt i flashhukommelsen, som er relaterede til HP TamperLock-indstillinger. Denne funktion findes altid på systemer, der understøtter HP TamperLock og kan ikke deaktiveres.

2 Drift

HP TamperLock-funktionen er konfigureret til at låse systemet på grund af uautoriseret adgang og registrerer altid, om dækslet åbnes – uanset systemets strømtilstand – hvis det sker uden tilladelse. HP TamperLock vil specifikt registrere en dækselåbning i alle følgende systemstrømtilstande, når HP TamperLock er konfigureret med HP's anbefalede indstillinger.

- **System tændt** (operativsystem [OS] kører)
- **System slukket** (operativsystemet afsluttes eller er i dvaletilstand)
- **System i slumretilstand**

VIGTIGT: For at opnå de bedste resultater, der er beskrevet i dette dokument, skal du konfigurere HP TamperLock med HP's anbefalede indstillinger som vist i tabel 4-1.

Desuden aktiveres HP TamperLocks dækselåbningssensor også i et scenarie, hvor alle strømkilder fjernes, mens dækslet er fjernet, herunder indbyggede batterier og RTC-møntceller (Real-Time Clock).

BEMÆRK: Fjernelse af RTC-strømkilden udløser automatisk HP TamperLocks dækselåbningssensor. Det betyder, at hvis systemer opbevares uden strømforsyning i mere end to år, aktiveres HP TamperLocks dækselåbningssensor – også selvom dækslet ikke er blevet fjernet.

Når HP TamperLock registrerer, at dækslet åbnes, mens systemet er tændt eller i slumretilstand, slukkes systemet øjeblikkeligt, og ikke-gemte data går tabt. Hvis den valgfrie politik for rydning af TPM-tilstanden ved registrering af dækselåbning er indstillet til **Aktiveret**, vil BIOS'en rydde TPM. BIOS'en starter ikke operativsystemet, efter at dækselåbningen er registreret, og beder i stedet den lokale bruger om at indtaste BIOS-administratoradgangskoden eller (i sikker administratortilstand) en engangspinkode for at låse systemet op og starte normalt.

Du kan få oplyst HP TamperLock-statussen ved at sende en forespørgsel om den tilknyttede BIOS-indstilling eller via Windows Logbog, når HP Notifications-softwaren er installeret.

3 Rækkefølge

HP TamperLock-rækkefølgen er beskrevet her.

1. HP TamperLock registrerer, at kabinettets dæksel er blevet åbnet.
2. Hvis systemet er tændt eller i slumretilstand, gennemtvinger HP TamperLock en nedlukning, som ikke kan annulleres.
3. Åbningen af dækslet medfører, at systemets hardware låses.
4. Når dækslet er sat på igen, kan systemet igen tændes. Følgende sker, næste gang systemet tændes:
    1. Hvis politikken for rydning af TPM er aktiveret, rydder BIOS'en TPM.
    2. Den lokale bruger får besked om, at dækslet er åbnet.
    3. BIOS-administratorens legitimationsoplysninger skal indtastes:
        - Hvis legitimationsoplysninger angives, starter systemet normalt.
        - Hvis legitimationsoplysninger ikke angives, startes systemet ikke i operativsystemet.
5. Punktet i overvågningslogfilen synkroniseres med Windows®-hændelsesloggen, hvis HP Notifications-softwaren er installeret.

4 Politikindstillinger

Du kan bruge HP Client Management-værktøjer til at se og konfigurere HP TamperLock-politikker som BIOS-indstillinger. De tilknyttede indstillinger gør det muligt vælge, hvilke funktioner i HP TamperLock der kan aktiveres, samt hvilke handlinger der skal udføres, når dækslet fjernes.

Tabel 4-1 Indstillinger i TamperLock-politik

Indstillinger	Beskrivelse	Standard	HP anbefalet
Dækselåbningssensor	• **Deaktiveret** – ingen handling udføres, når dækslet fjernes. • **Giv brugeren besked** – viser en advarsel ved næste opstart, når dækslet åbnes. • **Administrator-legitimationsoplysninger**– denne indstilling kræver, at der indtastes en administratoradgangskode eller engangspinkode (når HP Sure Admin er aktiveret), før opstarten kan fortsættes, når dækslet er åbnet. Hvis du vil aktivere denne indstilling, skal du angive en adgangskode eller aktivere HP Sure Admin Enhanced BIOS Authentication Mode med et lokalt adgangsnøglesæt. • **Administratoradgangskode** – samme adfærd som administrator-legitimationsoplysninger (dette indstillingsnavn vises for at sikre kompatibiliteten med tidligere software til administration af indstillinger, der understøttede dækselåbningssensoren).	Deaktiveret	Administrator-legitimationsoplysninger eller administratoradgangskode
Sluk ved dækselåbning	Kun tilgængelig, når dækselåbningssensoren ikke er sat til Deaktiveret. **Deaktiveret** – hvis systemet er tændt eller er i slumretilstand, når dækslet fjernes, forbliver det i denne tilstand. **Aktiveret** – systemet slukker øjeblikkeligt, hvis dækslet fjernes, mens systemet er tændt eller er i slumretilstand (S3 eller moderne standby).	Deaktiveret	Aktiveret
Ryd TPM ved opstart efter dækselåbning	Kun tilgængelig, når dækselåbningssensoren ikke er deaktiveret. • **Deaktiveret** – ingen ændring i TPM-tilstand, når dækslet fjernes. • **Aktiveret** – TPM ryddes ved næste opstart, når dækslet er fjernet. Alle kundenøgler i TPM ryddes. **BEMÆRK:** Aktivér kun denne indstilling, når manuel gendannelse er mulig via ekstern sikkerhedskopiering, eller når du ikke vil gendanne. Hvis BitLocker er aktiveret, kan drevet ikke dekrypteres uden BitLocker-gendannelsesnøglen.	Deaktiveret	Afhænger af kundekrav.

Tabel 4-1 Indstillinger i TamperLock-politik (fortsat)

Indstillinger	Beskrivelse	Standard	HP anbefalet
DMA-beskyttelse før opstart	**Kun Thunderbolt** – IOMMU-hardwarebaseret DMA-beskyttelse (Input-Output Memory Management Unit) er aktiveret i BIOS'ens pre-boot-miljø for Thunderbolt-tilsluttede PCI-e-enheder. **Alle PCIe-enheder** – IOMMU-hardwarebaseret DMA-beskyttelse (Input-Output Memory Management Unit) er aktiveret i BIOS'ens pre-boot-miljø for alle interne og eksterne PCI-tilsluttede enheder.	Kun Thunderbolt	Alle PCI-enheder
DMA-beskyttelse	**Deaktiveret** – BIOS konfigurerer ikke IOMMU-hardware (Input-Output Memory Management Unit) til brug af operativsystemer, der understøtter DMA-beskyttelse. **Aktiveret** – BIOS konfigurerer IOMMU-hardware (Input-Output Memory Management Unit) til brug af operativsystemer, der understøtter DMA-beskyttelse.	Aktiveret	Aktiveret

5 Status

Du kan sende en forespørgsel om BIOS-indstillingen for at se statussen for HP TamperLock ved hjælp af de eksisterende administrationsværktøjer til BIOS-opsætning. Denne indstilling kan kun ryddes, hvis der angives en BIOS-administratoradgangskode eller BIOS-administrator-legitimationsoplysninger (Sure Admin-tilstand).

Tabel 5-1

Indstilling	Beskrivelse
Seneste dækselåbning og antal	Når dækselåbningssensoren er deaktiveret, rapporterer denne indstilling den sidste gang, hvor dækslet blev fjernet, samt hvor mange gange det blev fjernet og bekræftet, siden BIOS-administratoren sidst ryddede den. Indtastningen skal være i følgende format: MM/DD/ÅÅÅÅ TT:MM:SS. X gange. Afhængigt af systemfaktorerne (f.eks. hvis computeren er slukket) øges antallet af dækselåbninger i træk ikke. Dato og klokkeslæt rapporteres som 0, hvis værdien ikke kan fastslås, f.eks. efter et strømsvigt i realtidsperioden.

Hændelsesovervågningslogfil

Hvis HP Notifications-softwaren er installeret, kan du se følgende hændelseslogfiler i Windows Logbog i mappen HP Sure Start.

Tabel 5-2 Overvågningslogfil

Kilde-ID	Hændelses-id	HÃ¦ndelse	Hændelseslogfilens type
0x8A	0x1E	HP TamperLock – systemet har registreret, at dækslet blev åbnet.	Advarsel
	0x1F	HP TamperLock – brugeren har bekræftet en BIOS-POST-meddelelse om, at dækslet var blevet åbnet.	Oplysning
	0x20	HP TamperLock – TPM blev ryddet, fordi dækslet er blevet åbnet, baseret på de aktuelle HP TamperLock-politikindstillinger.	Oplysning