



Korisnički priručnik za HP TamperLock

SAŽETAK

HP TamperLock štiti od napadača koji otvaraju kućište računala i zlonamjerno izmjenjuju hardver.

Autorsko pravo i licenca

© Autorsko pravo 2020 HP Development Company, L.P.

Povjerljivi računalni softver. Za posjedovanje, korištenje ili kopiranje potrebna je valjana licenca tvrtke HP. U skladu s odredbama FAR 12.211 i 12.212, komercijalni računalni softver, dokumentacija računalnog softvera i tehnički podaci za komercijalne stavke licencirani su na američku vladu u sklopu dobavljačeve standardne komercijalne licence.

Informacije navedene u ovom dokumentu podložne su promjenama bez najave. Jedina jamstva za HP-ove proizvode i usluge iznesena su u izričitim jamstvenim izjavama koje prate takve proizvode i usluge. Ništa u ovom dokumentu ne smije se tumačiti kao dodatno jamstvo. HP ne snosi odgovornost za tehničke ni uredničke pogreške ili propuste u ovom tekstu.

Prvo izdanje: rujan 2020.

Šifra dokumenta: M11669-BC1

Sadržaj

1 Pregled	1
2 Rad pogona	2
3 Slijed	3
4 Postavke pravila	4
5 Status	6
Zapisnik o nadzoru događaja	6

1 Pregled

HP TamperLock štiti od napadača koji otvaraju kućište računala i zlonamjerno izmjenjuju hardver. HP TamperLock obuhvaća senzore koji otkrivaju je li kućište otvoreno i kontrole pravila kojima se konfiguriraju radnje koje je potrebno poduzeti u slučaju otvaranja.


Pravila značajke HP TamperLock obuhvaćaju dodatne mogućnosti blokiranja pokretanja sustava na razini BIOS-a dok se ne unese valjana administratorska vjerodajnica za BIOS, čišćenje funkcije HP Trusted Platform Module (TPM) da bi se izbrisali svi korisnički ključevi (na primjer, ključevi značajke BitLocker pomoću kojih je podacima pohranjenima na lokalnom pogonu moguće pristupiti samo putem BitLocker ključa za oporavak koji nije lokalno pohranjen) i mogućnost isključivanja sustava čim se poklopac ukloni. Događaji i povijest otvaranja poklopca pohranjuju se na hardverskoj platformi i udaljeni administrator im može pristupiti.

Pravila značajke HP TamperLock zaštićena su od promjena pomoću zaštićene pohrane ukorijenjene u hardveru HP Endpoint Security Controller. Zaštićena pohrana osigurava zaštitu od fizičkog napada na podatke iz BIOS-a i firmvera te postavke pohranjene u izbrisivoj memoriji koje se odnose na postavke značajke HP TamperLock. Ta je mogućnost uvijek prisutna na sustavima koji podržavaju HP TamperLock i ne može se onemogućiti.


2 Rad pogona

Značajka HP TamperLock konfigurirana je za zaključavanje sustava zbog neovlaštenog pristupa, omogućuje otkrivanje otvaranja poklopca bez obzira na stanje napajanja sustava tijekom neovlaštenog otvaranja poklopca. Točnije, HP TamperLock prepoznat će događaj otvaranja poklopca u svim stanjima napajanja sustava ako se HP TamperLock konfigurira uz HP-ove preporučene postavke.

- **Sustav je uključen** (pokrenut je operacijski sustav [OS])
- **Sustav je isključen** (OS je isključen ili u stanju hibernacije)
- **Sustav u stanju mirovanja**

 **VAŽNO:** za optimalne rezultate opisane u ovom dokumentu konfigurirajte HP TamperLock s HP-ovim preporučenim postavkama, kao što je prikazano u tablici 4–1.

Osim toga, senzor za otvaranje poklopca HP TamperLock aktivira se čak i ako su svi izvori napajanja uklonjeni dok se poklopac uklanja, uključujući unutarnju bateriju i dugmastu bateriju za sat u stvarnom vremenu (RTC).

 **NAPOMENA:** gubitak napajanja za RTC automatski aktivira značajku senzora za otvaranje poklopca HP TamperLock. Stoga će sustavi koji ostanu u spremištu bez priključenog napajanja više od 2 godine aktivirati senzor za otvaranje poklopca HP TamperLock, čak i ako poklopac nije uklonjen.

Kada HP TamperLock prepozna otvaranje poklopca dok je sustav uključen ili u stanju mirovanja, sustav se odmah isključuje i gube se svi nespremljeni podaci. Ako je dodatno pravilo za brisanje stanja TPM-a pri otkrivanju otvaranja poklopca postavljeno na **Omogućeno**, BIOS će očistiti TPM. Nakon otkrivanja otvaranja poklopca BIOS ne pokreće OS, već od lokalnog korisnika traži da unese administratorsku lozinku za BIOS ili (u načinu rada Sure Admin) jednokratni PIN za otključavanje sustava i normalno pokretanje.

Status značajke HP TamperLock možete saznati prikazom povezane postavke BIOS-a ili putem preglednika događaja u sustavu Windows ako je instaliran softver HP Notifications.

3 Slijed

Ovdje je opisan slijed radnji značajke HP TamperLock.

1. HP TamperLock otkriva da je otvoren poklopac kućišta.
2. Ako je sustav uključen ili u stanju mirovanja, HP TamperLock prisilno isključuje sustav bez mogućnosti otkazivanja.
3. Kao posljedica događaja otvaranja poklopca, hardver sustava prelazi u zaključano stanje.
4. Kada se poklopac vrati na mjesto, sustav se može ponovno uključiti. Prilikom sljedećeg uključivanja sustava doći će do sljedećih događaja:
 1. Ako je omogućeno pravilo za brisanje TPM-a, BIOS čisti TPM.
 2. Lokalni korisnik prima obavijest o otvaranju poklopca.
 3. Traže se administratorske vjerodajnice za BIOS:
 - Ako se unesu vjerodajnice, sustav se pokreće normalno.
 - Ako se vjerodajnice ne unesu, sustav ne pokreće OS.
5. Stavka u zapisniku o nadzoru sinkronizira se sa zapisnikom događaja u sustavu Windows® ako je instaliran softver HP Notifications.

4 Postavke pravila

Pomoću alata HP Client Management pravila značajke HP TamperLock možete pregledavati i konfigurirati kao postavke BIOS-a. Povezane postavke kontroliraju omogućivanje značajke HP TamperLock, kao i radnje poduzete nakon uklanjanja poklopcu.

Tablica 4-1 Postavke pravila za TamperLock

Postavke	Opis	Zadano	HP-ova preporuka
Senzor za otvaranje poklopcu	<ul style="list-style-type: none">• Onemogućeno – ne poduzimaju se nikakve radnje nakon uklanjanja poklopcu.• Obavijestiti korisnika – prikazat će se poruka upozorenja prilikom sljedećeg pokretanja kada se poklopac otvori.• Administratorska vjerodajnica – ova postavka zahtijeva unos administratorske lozinke ili jednokratnog PIN-a (kada je omogućen HP Sure Admin) prije nastavka pokretanja nakon otvaranja poklopcu. Da biste omogućili tu postavku, morate postaviti lozinku ili omogućiti način rada provjere autentičnosti HP Sure Admin Enhanced BIOS s postavljenim ključem za lokalni pristup.• Administratorska lozinka – isto ponašanje kao i kad se traži administratorska vjerodajnica (navedeni naziv postavke prisutan je da bi novi sustav bio kompatibilan s prethodnim softverom za upravljanje postavkama koji je podržavao senzor za otvaranje poklopcu).	Onemogućeno	Administratorska vjerodajnica ili administratorska lozinka
Isključivanje nakon otvaranja poklopcu	Dostupno je samo kada senzor za otvaranje poklopcu nije onemogućen. Onemogućeno – ako je sustav uključen ili u stanju mirovanja kada se poklopac ukloni, ostaje u tom stanju. Omogućeno – sustav se odmah isključuje ako se poklopac ukloni dok je sustav uključen ili u stanju mirovanja (S3 ili moderno stanje pripravnosti).	Onemogućeno	Omogućeno
Brisanje TPM-a pri pokretanju nakon otvaranja poklopcu	Dostupno je samo kada senzor za otvaranje poklopcu nije onemogućen. <ul style="list-style-type: none">• Onemogućeno – nema promjene stanja TPM-a kada se poklopac ukloni.• Omogućeno – TPM se briše pri sljedećem pokretanju nakon uklanjanja poklopcu. Brišu se svi korisnički ključevi u TPM-u.	Onemogućeno	Ovisi o zahtjevima korisnika.

Tablica 4-1 Postavke pravila za TamperLock (Nastavak)

Postavke	Opis	Zadano	HP-ova preporuka
	<p>NAPOMENA: tu postavku omogućite samo kada je moguć ručni oporavak iz udaljene sigurnosne kopije ili kada ne želite oporaviti podatke. Ako je omogućen BitLocker, pogon se ne može dešifrirati bez ključa za oporavak značajke BitLocker.</p>		
DMA zaštita prije pokretanja	<p>Samo Thunderbolt – hardverska DMA zaštita jedinice za upravljanje ulazno-izlaznom memorijom (IOMMU) omogućena je u okruženju BIOS-a prije pokretanja sustava za PCI-e uređaje povezane putem sučelja Thunderbolt.</p> <p>Svi PCIe uređaji – hardverska DMA zaštita jedinice za upravljanje ulazno-izlaznom memorijom (IOMMU) omogućena je u okruženju BIOS-a prije pokretanja sustava za sve unutarnje i vanjske uređaje povezane putem sučelja PCI.</p>	Samo Thunderbolt	Svi PCI uređaji
DMA zaštita	<p>Onemogućeno – BIOS neće konfigurirati hardver jedinice za upravljanje ulazno-izlaznom memorijom (IOMMU) za upotrebu u operacijskim sustavima koji podržavaju DMA zaštitu.</p> <p>Omogućeno – BIOS će konfigurirati hardver jedinice za upravljanje ulazno-izlaznom memorijom (IOMMU) za upotrebu u operacijskim sustavima koji podržavaju DMA zaštitu.</p>	Omogućeno	Omogućeno

5 Status

Prema postavci BIOS-a možete odrediti status značajke HP TamperLock pomoću postojećih alata za upravljanje postavkama BIOS-a. Jedini je način za poništavanje te postavke navođenje administratorske lozinke za BIOS ili administratorske vjerodajnice za BIOS (u načinu rada Sure Admin).

Tablica 5-1

Postavka	Opis
Zadnje otvaranje poklopca i broj otvaranja	Kada senzor za otvaranje poklopca nije onemogućen, ova postavka izvještava o tome kada je poklopac zadnji put uklonjen te koliko je puta uklanjan s potvrdom od kada ju je administrator BIOS-a zadnji put poništio. Oblik unosa je MM/DD/GGGG HH:MM:SS. X puta. Ovisno o čimbenicima sustava (na primjer, računalo je isključeno), uzastopna otvaranja poklopca neće povećati broj. Datum i vrijeme bit će zabilježeni kao nule u slučajevima kada se vrijednost ne može utvrditi, na primjer nakon gubitka napajanja za sat u stvarnom vremenu.

Zapisnik o nadzoru događaja

Ako je instaliran softver HP Notifications, u pregledniku događaja u sustava Windows u mapi HP Sure Start možete pregledati sljedeće zapisnike događaja.

Tablica 5-2 Zapisnik o nadzoru

ID izvora	ID događaja	Događaj	Vrsta zapisa o događaju
0x8A	0x1E	HP TamperLock – sustav je otkrio da je poklopac otvoren.	Upozorenje
	0x1F	HP TamperLock – korisnik je potvrdio obavijest BIOS POST-a da je poklopac otvoren.	Informativno
	0x20	HP TamperLock – TPM je izbrisan zbog otvaranja poklopca na temelju trenutne postavke pravila značajke HP TamperLock.	Informativno