

## McAfee Encrypted USB

Biztonság mobil eszközök számára



Manapság a nagyvállalatok az érzékeny adataikat számtalan helyen tárolják, hiszen a mobilitás előnyt jelent a versenytársakhoz képest. E miatt az USB eszközökön is számos érzékeny, vállalati tulajdonú képező információ található, ráadásul az USB eszközök mérete is drasztikusan megnőtt (egyetlen USB stick is lehet akár 32 GB-os).

Belátható, hogy ezen eszközök védelme, központi menedzsmentje szintén szükséges a biztonságos működéshez.

### Jellemzők

- Biztosítja a vállalati biztonsági szabályzatnak, az adatkezelési szabályzatnak, és az iparági előírásoknak való megfelelést.
- Mobil eszközök biztonságos használatát segíti.
- Központi felületet (McAfee ePolicy Orchestrator) biztosít a titkosított USB eszközök menedzselésére, auditálására, szabályrendszer kikényszerítésére, valamint lehetőséget biztosít a riportok egységes kezelésére.
- Kétfaktoros autentikációval növeli a biztonságot.
- Biztonságos algoritmusok és tanúsítványok használatával (AES-256, FIPS 140-2) valósítja meg az erős autentikációt.

### Védelem az adatnak és a vállalatnak

Az USB eszközök, a kis méretük és a nagy kapacitásuk miatt a biztonsági szakemberek rémálma. Naponta hagyhatja el sok fontos adat a vállalatot anélkül, hogy arról bárki tudna, és bárki védené (mondjuk lopás esetén) az adatokat.

A McAfee Encrypted USB eszközeivel az információ speciális, hardveresen védett eszközön tárolódik, melyhez szabályozható a hozzáférés akár több azonosítási lépéssel.

Ezen modulokkal az információ minden körülmények között védett (akár lopás, akár utazás, akár más gépen történő használat esetén). Plusz, a biometrikus jellemzők is az eszközön, teljes biztonságban tárolódnak.

### Központi menedzsment McAfee ePolicy Orchestrator szerverrel

Ezen USB eszközök bevezetése, kiosztása, jogosultságának kezelése meglehetősen komplex dolog, mivel az USB eszközök menedzselése általában nem az IT osztály feladata. E miatt az adatok gyakran nem kellően védettek, akár titkosítás és azonosítás nélkül is elérhetőek. Az ePo szerver segítségével mindezen probléma kiküszöbölhető, hiszen egyetlen konzolról megvalósítható a teljes eszközmenedzsment.

Az ePo szerver és a McAfee Encrypted USB eszközök párhuzamos használata növeli a biztonságot, egységesíti a kiosztott eszközöket, miközben kisebb a TCO.

### Adatok biztonságosan erős autentikációval

A McAfee Encrypted USB eszközön lévő adat hozzáféréséhez a felhasználónak autentikálni kell magát vagy jelszóval, vagy ujjlenyomattal. A fokozott biztonság miatt akár kombinálható is e kettő megoldás. Azonban ha a felhasználó elfelejtette a jelszavát, vagy valamilyen ok miatt nem képes az ujjlenyomatát "bemutatni" a McAfee ePO konzolon keresztül könnyedén visszaállíthatóak az adatok az adminisztrátor segítségével (vagy akár egy központi webes felületen keresztül).

A megbízható algoritmusok használata miatt a kulcsok nem visszafejthetőek, nem másolhatóak, nem kerülhetnek ki az eszközből.

### Compliance report

Köszönhetően az integrált McAfee ePo menedzsment konzolnak, a McAfee Encrypted USB termékek minden iparági előírás megfelelését ellenőrizni képes (a vállalati biztonsági előírásoktól a törvényi adatvédelmi szabályzásokig). Az adatbiztonságot tovább növeli, hogy még az ellopott, elhagyott USB eszközön lévő adatok sem hozzáférhetőek illetéktelenek számára.

### Tulajdonságok

- Advanced Encryption Standard (AES)-256 alapú hardveres védelmet biztosít McAfee USB eszközök számára.

**Rendszerkövetelmények**

**Standard Driverless Encrypted USB**

- Operációs rendszer:
- Microsoft Windows Vista
  - Microsoft Windows XP
  - Microsoft Windows 2000

- Kapacitás:
- 1 GB és 2 GB

**Zero-Footprint and Hard Disk**

- Operációs rendszer:
- Microsoft Windows Vista
  - Microsoft Windows XP
  - Microsoft Windows 2000
  - Mac OS X

- Kapacitás:
- Stick: 1 GB-tól 16 GB-ig
  - HDD: 80 GB-tól 320 GB-ig

**McAfee ePolicy Orchestrator követelmények**

- ePO 4.0, vagy újabb (Encrypted USB Extension szükséges)

- Operációs rendszer:
- Microsoft Windows Vista
  - Microsoft Windows XP
  - Microsoft Windows 2003
  - Microsoft Windows 2000

- Adatbázis:
- Microsoft SQL Server 2000, vagy 2005
  - Microsoft SQL Express
  - Informix





- Böngésző:
- Microsoft Internet Explorer 6.0, vagy 7.0

- LDAP címtár:
- Microsoft Windows 2003 Active Directory, vagy újabb
  - Microsoft ADAM

- A maximális biztonság érdekében jelszavaink biztonságát, hosszát, illetve a biometrikus jellemezőket is képes ellenőrizni, hogy csökkentsük az adatvesztés kockázatát.
- Rugalmasság a zero-client footprint modullal, mellyel elkerülhető kliens oldali alkalmazások telepítése, vagy adminisztrátori jogkör megadása.
- A kétfaktoros azonosítással a nem megfelelő jogosultságú egyének elől biztonságban vannak az adataink.
- A használathoz szükséges szoftverek szintén az USB eszközön (védett helyen) találhatóak, melyek ráadásul bővíthetők VPN klienssel, internet böngészővel, vékonyklienssel.
- A beépített kulcsgeneráló, ellenőrző, tároló modul megvédi a kulcsokat az illetéktelen hozzáférésektől, hiszen a kulcsok nem hagyják el az eszközt, de lehetőség van külső kulcsok importálására is.

**McAfee Encrypted USB eszközök**

A következő táblázat mutatja a teljes McAfee Encrypted USB portfóliót. Az USB stick-ek kapacitása 1 és 16 GB között van, a HDD-k mérete pedig 80 és 320 GB között.

	Standard Driverless	Zero-Footprint Non-BIO	Zero-Footprint BIO	USB Hard Disk
				
Password Authentication	•	•	•	•
Biometric Authentication			•	•
Hardware Encryption	•	•	•	•
Digital Identity and Crypto Services		•	•	•
Managed by McAfee ePolicy Orchestrator	•	•	•	•

*Az USB eszközök moduljai*

**További információkért keresse a McAfee Encrypted USB weboldalát:**

[http://www.mcafee.com/uk/enterprise/products/data\\_protection/data\\_encryption/encrypted\\_usb.html](http://www.mcafee.com/uk/enterprise/products/data_protection/data_encryption/encrypted_usb.html)