

# F-Secure Mobile Security™ for Windows Mobile

## 1. Telepítés és aktiválás

**Előző verzió** Ha telepítette az F-Secure Mobile Security egy korábbi verzióját, be kell zárnia azt. Az előző verzió a telepítés során automatikusan el lesz távolítva.

**Telepítés** **Telepítés:**

1. Vigye át a .cab telepítőfájlt az eszközre.
2. Keresse meg, és válassza ki a .cab fájlt az eszköz Intéző alkalmazásában.
3. Ha erre vonatkozó kérdést kap, az **Igen** lehetőség kiválasztásával engedélyezze a telepítést.
4. Válassza az **Igen** lehetőséget a licenc feltételeinek elfogadásához.
5. Az alkalmazás telepítése után indítsa újra az eszközt, amikor a telepítő ezt kéri. Select **Igen**.
6. A telepítés befejezése után a terméket aktiválni kell. Aktiválás nélkül a termék nem védi az eszközt.


**Aktiválás** **Az aktiválás elindítása:**


1. Select Válassza az **Igen** lehetőséget az eszköz a F-Secure Mobile Security telepítését követő első bekapcsolásakor megjelenő aktiválási értesítésen.
2. Válassza ki a használni kívánt aktiválástípust:
  - A próbaidőszak megkezdéséhez válassza az **Ingyenes próbaverzió** lehetőséget, és válassza a **Következő** lehetőséget, VAGY
  - Teljes licencelt verzió beszerzéséhez válassza az **Előfizetői szám** lehetőséget az aktiválási típusnál, majd válassza a **Tovább** lehetőséget. Adja meg előfizetői számát, majd válassza a **Tovább** lehetőséget.
3. Válassza az **Igen** lehetőséget a frissítési szolgáltatáshoz való kapcsolódáshoz. Az alkalmazás csatlakozik a frissítési szolgáltatáshoz, és elküldi az előfizetői számot. Az első frissítés során az alkalmazás letölti a legújabb vírusdefiníciós adatbázist.
4. A letöltés befejeztével egy üzenet jelzi, hogy a letöltés sikeres volt, és az alkalmazást sikerült aktiválni. Válassza az **OK** lehetőséget az aktiválás befejezéséhez.
5. Az aktiválás befejezése után végezzen víruskeresést az eszközén annak biztosításához, hogy az tiszta. További információkért tekintse meg a következő szakaszt: **Víruskeresés**.

Ha rendelkezik érvényes előfizetői kóddal és jelenleg az alkalmazás ingyenes próbaverzióját használja, indítsa el a **Vásárlás** parancsot a menüből, és írja be előfizetési kódját az előfizetés aktiválásához.

## A termék elindítása

A F-Secure Mobile Security aktiválását követően az eszköz minden bekapcsolásakor automatikusan elindul.

1. Ha a Windows Mobile Professional vagy Classic kiadását használja, válassza a **Start→ Programok→  Mobile Security** parancsot.

Ha a Windows Mobile Standard kiadását használja, válassza a **Start→  Mobile Security** parancsot.

2. Válassza az **Igen** lehetőséget, ha a program megkérdezi, hogy futtassa-e a víruskeresést.

## 2. Víruskeresés

A F-Secure Mobile Security a háttérben működik, és automatikusan ellenőrzi a fájlokat, amikor a valós idejű keresés be van kapcsolva.

1. Ha a program vírusot talál a valós idejű keresés során, egy üzenetet jelenít meg. Válassza az **Igen** lehetőséget a fertőzött fájlok megtekintéséhez, vagy a **Nem** lehetőséget a nézet bezárásához.
2. A Fertőzések nézet az eszközön talált fertőzött fájlok listáját tartalmazza. A lista elemei esetében az állapot (karanténba helyezve, elengedve) és a fertőzött fájl neve jelenik meg.
3. Válassza ki a fertőzött fájl az arra vonatkozó részletes információk megtekintéséhez.
  - Ha a Windows Mobile Professional vagy Classic kiadást használja, koppintson a **Részletek megjelenítése** elemre.
  - Ha a Windows Mobile Standard kiadását használja, válassza a **Menü→Részletek megjelenítése** lehetőséget.

## A fertőzött fájlok feldolgozása

**A fertőzött fájlok feldolgozása:**

1. A fő nézetben nyissa meg a **Vírusvédelem** lehetőséget.
2. A **Vírusvédelem** menüben válassza a Fertőzött fájlok lehetőséget.
3. A **Fertőzött fájlok** nézetben válassza ki a feldolgozni kívánt fertőzött fájlt.
4. Az alábbi műveletek közül választhat:
  - **Törlés** – a fertőzött fájl törlése. Ez az ajánlott lehetőség. A fájlt a program teljes mértékben eltávolítja az eszközről.
  - **Karantén** – a fertőzött fájl karanténba helyezése, ha még nem történt meg. A karanténba helyezett fájl zárolt, és nem károsíthatja az eszközt az F-Secure Mobile Security működése alatt.
  - **Elengedés** – a karanténba helyezett fájl elengedése. Ha elenged egy fájlt, akkor a későbbiekben az nem lesz zárolva. Csak saját felelősségére nyissa meg a fájlt.

Ha a Windows Mobile Professional vagy Classic kiadást futtatja, használja a megfelelő gombot.

Ha a Windows Mobile Standard kiadást használja, válassza a **Menü** lehetőséget, majd válassza ki a kívánt műveletet.

### 3. A jogosulatlan hálózati forgalom letiltása

Az F-Secure Mobile Security tűzfala csendben, a háttérben dolgozik. Folyamatosan figyeli a bejövő és a kimenő internetes és hálózati forgalmat, és megóvja az eszközt a behatolási kísérletektől. Az előre definiált tűzfalszintek segítségével azonnal módosíthatja a védelem szintjét.

#### A biztonsági szint kiválasztása

##### A biztonsági szint kiválasztása:

1. A fő nézetben nyissa meg a **Tűzfal** lehetőséget.
2. A Tűzfal menüben válassza a **Beállítások** lehetőséget.
3. Válassza a következő tűzfalszintek egyikét:
  - **Minden letiltása** – minden hálózati forgalmat letilt.
  - **Magas** – a legtöbb általánosan használt alkalmazás engedélyezése, és a bejövő forgalom blokkolása.
  - **Normál** – minden kimenő forgalom engedélyezése, és minden bejövő forgalom blokkolása.
  - **Minden engedélyezése** – a teljes hálózati forgalom engedélyezése.
  - **Egyéni** – hálózati forgalom engedélyezése egyéni szabályok alapján. Az egyéni szabálykészlet szerkesztéséhez válassza az **Egyéni szabályok szerkesztése** lehetőséget, amikor az **Egyéni** biztonsági szint van kiválasztva.

### 4. Bizalmas információk védelme

A lopásvédelem segítségével még az eszköz ellopása esetén sem használhatják fel az adatokat, illetve magát az eszközt.



*Mivel a memóriakártyák könnyedén eltávolíthatók, bizalmas információit az eszköz memóriájában tárolja.*

#### Biztonsági kód

A biztonsági kód segítségével távolról megkeresheti vagy zárolhatja az eszközt, illetve törölheti annak tartalmát.

A biztonsági kódnak legalább 8 karakterből kell állnia. Olyan kódot válasszon, amit nem fog elfelejteni, mások viszont nehezen találják ki. Tartsa biztonságos helyen a biztonsági kódot.

#### Távoli Anti-theft

A távoli lokátor úgy működik, hogy SMS-t küld az elveszett készülékre, így határozza meg annak helyét.

A távoli zárolás segítségével távolról is zárolhatja a rendszert egy SMS üzenet elküldésével. A távoli zárolás használatához tartsa bekapcsolva az eszközzárolást.

A távoli törlés segítségével távolról törölheti az eszköz tartalmát egy SMS üzenet elküldésével. Az eszköz törlése során a rajta tárolt összes adatot eltávolítja a program.

#### A távoli zárolás és törlés beállításához:

1. A fő nézetben nyissa meg az **Anti-theft** lehetőséget.
2. Az Anti-theft menüben válassza a **Beállítások** lehetőséget.
3. Válassza ki a bekapcsolni kívánt funkciókat:
  - Ha szeretné távolról meghatározni a készülék helyét, válassza a **Lokátor engedélyezése** elemet.
  - Ha szeretné távolról törölni a készülék adatait, válassza a **Távoli törlés engedélyezése** elemet.
  - Ha szeretné távolról zárolni a készüléket, válassza a **Távoli zárolás engedélyezése** elemet.



*Csak az eszközzárolás bekapcsolt állapota mellett engedélyezheti a távoli zárolást.*

4. Adja meg a **Biztonsági kód** értékét, majd írja be azt újra a megerősítéshez.

#### Az eszköz megkeresése, zárolása vagy tartalmának törlése távolról:

- Az eszköz helyének meghatározásához küldje el az eszközre az alábbi üzenetet:  
#LOCATE#<biztonsági kód> (például: #locate#12345678)
- Az eszköz zárolásához küldje el az eszközre az alábbi üzenetet:  
#LOCK#<biztonsági kód> (például: #lock#12345678)
- Az eszköz tartalmának törléséhez küldje el az eszközre az alábbi üzenetet:  
#WIPE#<biztonsági kód> (például: #wipe#12345678)

#### SMS-figyelmeztetés

Az Anti-theft figyelmeztetést küldhet, ha valaki kicseréli a SIM-kártyát az eszközben. Az SMS-figyelmeztetés használatához kapcsolja be az **SMS-figyelmeztetés SIM cseréjekor** beállítást, és adja meg azt a telefonszámot, amelyre az SMS-t kéri, ha az eszközben lévő SIM-kártyát kicserélik.

## 5. A webböngészés védelme

A böngészővédelem segít a személyes adatok, például a hitelkártyaszámok, a felhasználói fiók adatai és a jelszavak eltulajdonításával próbálkozó webhelyek elleni védekezésben.

A böngészővédelem ellenőrzi az Internet Explorer programmal megnyitott webhelyeket. A böngészővédelem az F-Secure Mobile Security aktiválása után automatikusan bekapcsol, ha az Internet Explorer van beállítva alapértelmezett böngészőként. Ha valamilyen harmadik féltől származó böngészőt használ, a böngészővédelem nem nyújt védelmet.

#### A böngészővédelem beállítása:

1. A fő nézetben nyissa meg a **Böngészővédelem** lehetőséget.
2. Válassza a Böngészővédelem menü **Beállítások** elemét.
3. A böngészővédelem bekapcsolásához válassza a **Böngészővédelem engedélyezése** lehetőséget.

4. A **Használandó hálózat** területen határozza meg, hogy mindig használni kívánja-e a böngészővédelmet, vagy csak akkor, amikor saját hálózatán böngészi a webet:
  - Válassza a **Csak a saját szolgáltatóm** lehetőséget, ha a böngészővédelmet kizárólag a saját hálózatán kívánja használni.
  - Válassza **Az összes szolgáltató** beállítást, ha a védelmet bekapcsolva szeretné hagyni utazás közben és a sajáttól eltérő hálózat használata során is.

## 6. A termék naprakészen tartása

### Automatikus frissítések

A F-Secure Mobile Security része egy automatikus frissítési szolgáltatás, amely gondoskodik az alkalmazás vírusdefiníciós adatbázisainak rendszeres frissítéséről. Csak a naprakészen tartott vírusdefiníciós adatbázissal biztosított a legújabb vírusok elleni védelem. A termék az aktiválás után használja az automatikus frissítéseket.

A frissítések letöltéséhez az alkalmazásnak aktív internetkapcsolatra van szüksége. Amikor kapcsolódik az internethez, az alkalmazás ellenőrzi, hogy mikor frissítette legutóbb a vírusdefiníciós adatbázist, és szükség esetén letölti a megfelelő frissítéseket.

### Kézi frissítések

Az alkalmazás és a vírusdefiníciós adatbázis kézzel is frissíthető:

1. Válassza a **Menü→Frissítés** parancsot a fő nézetben.
2. Válassza az **Igen** lehetőségét a legutóbbi frissítés beszerzésére vonatkozó kérdés megerősítéséhez.
3. Ha elérhető új alkalmazásfrissítés, a megjelenő kérdésnél válassza az **Igen** lehetőséget annak letöltéséhez.
4. Amikor a frissítés befejeződött, válassza az **Igen** lehetőséget víruskeresés futtatásához az eszközön. További információt a következő szakaszban talál: [Víruskeresés](#).

## További információ

További információért töltsse le a termék User's Guide című útmutatóját (angol nyelven érhető el) a <http://mobile.f-secure.com/> weboldalról.

## Technikai ügyfélszolgálat

Ha bármilyen kérdése van, amelyre nem kap választ a kézikönyvben vagy a <http://mobile.f-secure.com/> online szolgáltatásaival, keresse fel az F-Secure helyi terjesztőjét, vagy közvetlenül az F-Secure Corporation vállalatot.

---

JOGI NYILATKOZAT

Az „F-Secure” név és a háromszögszimbólum az F-Secure Corporation bejegyzett védjegye. Az F-Secure terméknevek és szimbólumok, valamint emblémák az F-Secure Corporation védjegyei vagy bejegyzett védjegyei. Az említett terméknevek a megfelelő tulajdonosok védjegyei vagy bejegyzett védjegyei. Az F-Secure Corporation tulajdonjogilag nem érdekelt mások neveivel és termékneveivel kapcsolatban. Noha az F-Secure Corporation minden tőle telhetőleg megtesz az itt szereplő információ pontosságáért, az ennek ellenére mégis fellelhető hiányosságokért és hibákért nem vállal felelősséget. Az F-Secure Corporation a jelen dokumentumban említett jellemzők előzetes értesítés nélküli módosításának jogát fenntartja.

Az itt szereplő példákban használt cégek, nevek és adatok kitalált információk, hacsak azt külön nem jelöltük. Az F-Secure Corporation kifejezett írásos engedélye nélkül a jelen dokumentum egyetlen része sem sokszorosítható vagy másolható semmilyen módon és formában, sem elektronikus, sem mechanikus úton, semmilyen célra.

E termék az F-Secure szabadalmi közül egy vagy több hatálya alá eshet, ilyenek például a következők:

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2010 F-Secure Corporation. Minden jog fenntartva

