

F-Secure Mobile Security™ for S60

1. Telepítés és aktiválás

Előző verzió Nincs szükség az F-Secure Mobile Anti-Virus előző verziójának eltávolítására. Az új verzió telepítése előtt ellenőrizze az F-Secure Mobile Security beállításait.

Telepítés **Telepítés:**

- Töltse le a telepítőfájlt a számítógépre, majd helyezze át az eszközre,
- töltse le a telepítőfájlt a számítógépre, majd telepítse a terméket a Nokia PC Suite szoftvercsomag használatával, vagy
- töltse le a telepítőfájlt közvetlenül a kívánt eszközre. A telepítés automatikusan elindul.

A telepítés után indítsa újra a készüléket, ha a szoftver felszólítja erre. A telepítés befejezése után a terméket aktiválni kell. Aktiválás nélkül a termék nem védi az eszközt.

Aktiválás **Az aktiválás elindítása:**

1. Nyissa meg az alkalmazást. Megjelenik az üdvözlő képernyő.
2. Kattintson a **Folytatás** gombra.
3. Válassza ki a használni kívánt aktiválástípust:
 - A termék kizárólag a Lopásvédelem funkció használatára való aktiválásához válassza a **Csak lopásvédelem** aktiválási típust, majd válassza a **Folytatás** lehetőséget.
 - A teljes, licencelt verzió elindításához válassza az **Előfizetői szám** aktiválástípust, majd nyomja meg a **Folytatás** gombot. Adja meg előfizetői számát, majd nyomja meg az **OK** gombot.
4. Nyomja meg az **Igen** gombot, válassza ki az az internet-hozzáférési pontot, amelyen keresztül csatlakozni kíván a frissítési szolgáltatáshoz, majd kezdje el a frissítések letöltését.

Az alkalmazás csatlakozik a frissítési szolgáltatáshoz, és elküldi az előfizetői számot. Az első frissítés során az alkalmazás letölti a legújabb vírusdefiníciós adatbázist.
5. Miután a termék minden szükséges frissítést letöltött, az alkalmazás használatra készen áll. Válassza a **Folytatás** lehetőséget az aktiválás befejezéséhez.

Az aktiválás elvégzése után végezzen vírusvizsgálatot az eszközön, hogy az biztosan vírusmentes legyen. További információt az alábbi, [Vírusvizsgálat](#) című szakaszban talál.



Minden alkalommal, amikor az alkalmazás erre felkéri, ajánlott vizsgálatot végeznie az eszközön.

2. Vírusvizsgálat

Az F-Secure Mobile Security a háttérben működik, és automatikusan vizsgálja a fájlokat.

1. Az F-Secure Mobile Security értesíti, ha a valós idejű vizsgálat során vírusot talál. Válassza az **Igen** lehetőséget a fertőzött fájlok azonnali, illetve a **Nem** lehetőséget azok későbbi megtekintéséhez.
2. A fertőzések nézete tartalmazza az eszközön található fertőzött fájlok listáját, valamint megjeleníti, hogy a fájlok karanténban vannak-e vagy elengedett állapotúak.

További információk megjelenítése a fertőzött fájlal kapcsolatban:

1. Görgessen a fertőzött fájlhoz, és nyomja meg a kijelölő billentyűt.
2. Válassza a **Megtekintés** lehetőséget.
3. A Fertőzés részletei nézetben megjelenik a fertőzött fájl elérési útja és neve, valamint a fájl megfertőző vírus neve is.

A fertőzött fájlok feldolgozása

A fertőzött fájlok feldolgozása:

1. A fertőzések nézetében görgessen a feldolgozni kívánt fertőzött fájlhoz.
2. Nyomja meg a kiválasztó gombot.
3. 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.

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 igényei szerint módosíthatja a védelem szintjét.


A biztonsági szint kiválasztása

A biztonsági szint kiválasztása:

1. Keresse meg a **Beállítások** menüt, majd nyomja le a kiválasztó billentyűt.
2. A beállítások listájából válassza a **Tűzfal** elemet.
3. Válassza ki a használni kívánt tűzfalszintet:
 - **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 szabályok módosításához válassza a **Beállítások > Egyéni szabályok szerkesztése** menüpontot, 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 könnyen eltávolíthatók, ezért a bizalmas információkat mindig az eszköz belső memóriájában tárolja, mivel ez zárolható és törölhető a lopásvédelem segítségével.*

A eszközzárolás használata

A lopásvédelem automatikusan zárolja a készüléket, ha kicserélik a benne található SIM-kártyát. A zárolt eszköz csak a saját zárolási kódjával oldható fel.

Az eszközzárolás beállítása:

1. Keresse meg a **Beállítások** menüt, majd nyomja le a kiválasztó billentyűt.
2. A beállítások listájából válassza a **Lopásvédelem** elemet.
3. Adjon meg egy **Zárolási kódot**. A biztonsági kódnak legalább 5 karakter hosszúnak kell lennie. Tárolja biztonságos helyen.

-  *A lopásvédelmi beállításokat a zárolási kód védi. A lopásvédelmi beállítások módosítása előtt mindig meg kell adnia zárolási kódját.*

4. Ha zárolni szeretné az eszköz a SIM-kártya lecserélésekor, válassza az **Igen** lehetőséget a **Zárolás, ha megváltozik a SIM-kártya** beállításhoz.

A távoli lopásvédelem használata

A távoli lopásvédelem használatához elküldhet egy SMS üzenetet a zárolási kóddal az eszközre annak megkereséséhez vagy zárolásához, illetve elküldheti a törlési kódot az összes adat törléséhez.

A távoli zárolás beállítása:

1. Keresse meg a **Beállítások** menüt, majd nyomja le a kiválasztó billentyűt.
2. A beállítások listájából válassza a **Lopásvédelem** elemet.
3. Ha lehetővé kívánja tenni az eszköz távoli zárolását, kövesse az alábbi utasításokat:

- a. Írjon be egy **Zárolási kódot**, ha még nem hozta létre.
- b. Kapcsolja be a **Távoli zárolást**.

A zárolt eszköz csak a saját zárolási kódjával oldható fel.


4. Ha lehetővé kívánja tenni az eszköz távoli törlését, kövesse az alábbi utasításokat:
 - a. Adjon meg egy **Törlési kódot**. A törlési kódnak legalább 8 karakter hosszúnak kell lennie. Tárolja biztonságos helyen.
 - b. Kapcsolja be a **Távoli törlést**.

Az eszköz törlése során a rajta tárolt összes adatot eltávolítja a program.

Az eszköz zárolása vagy tartalmának törlése távolról:

Küldje el a következő SMS üzenetet az eszközére.


- Az eszköz zárolásához küldje el a következőt:
#LOCK#<zárolási kód> (például: #LOCK#abcd1234)
- Az eszköz tartalmának törléséhez küldje el a következőt:
#WIPE#<törlési kód> (például: #WIPE#abcd1234)
- Az eszköz megkereséséhez küldje el a következőt:
#LOCATE#<zárolási kód> (például: #LOCATE#abcd1234)

-  *A Lopásvédelem semmilyen helyadatot nem tárol, az egyetlen helyre vonatkozó adat az elküldött SMS üzenetben szereplő információ.*

5. A webböngészés védelme

A böngészővédelem segít a személyes információk, például személyes adatok, hitelkártyaszámok, a felhasználói fiókra vonatkozó információk és jelszavak eltulajdonításával próbálkozó webhelyek elleni védekezésben.

A böngészővédelem azokat a webhelyeket ellenőrzi, amelyeket az eszköz alapértelmezett böngészőjével látogat meg. Ha valamilyen harmadik féltől származó böngészőt használ, a böngészővédelem nem nyújt védelmet.

 *A böngészővédelem használatának megkezdése előtt kapcsolja ki a webböngészőt, és törölje annak gyorsítótárát.*

A böngészővédelem bekapcsolása:


1. Keresse meg a **Beállítások** menüt, majd nyomja le a kiválasztó billentyűt.
2. A beállítások listájából válassza a **Böngészővédelem** elemet.
3. Kapcsolja be a **Böngészővédelem** lehetőséget.
4. A **Használandó hálózat** területen határozza meg, hogy mindig használni kívánja a böngészővédelmet, vagy csak akkor, amikor saját hálózatán böngészi a webet:
 - Válassza a **Csak a saját szolgáltatóm** lehetőséget a Böngészővédelem kizárólag a saját hálózaton való használatához.
 - Válassza **Az összes szolgáltató** beállítást a védelem bekapcsolásához utazás és a sajáttól eltérő hálózat használata során.

Adatvédelmi mód

A böngészővédelem képes a káros tartalmakkal rendelkező webhelyekre vonatkozó információk elemzésre való automatikus elküldésére a szolgáltatás minőségének fenntartásához. Kiválaszthatja, hogy mely adatokat kívánja elemzésre elküldeni.

Az adatvédelmi mód módosítása:

1. Keresse meg a **Beállítások** menüt, majd nyomja le a kiválasztó billentyűt.
2. Válassza az **Egyéb beállítások** lehetőséget a beállításválasztó listából.
3. Az Adatvédelmi mód területén válassza a következők egyikét:
 - Válassza a **Csak statisztika** lehetőséget a böngészővédelmi statisztika és a kiszolgálókapcsolatra vonatkozó információk elküldéséhez.
 - Válassza a **Minden engedélyezése** lehetőséget a statisztika, valamint a nem elemzett vagy káros tartalmakkal rendelkező webhelyekre vonatkozó információk elküldéséhez.

 *A legjobb minőségű szolgáltatás érdekében javasoljuk, hogy az adatvédelmi mód esetében válassza a **Minden engedélyezése** beállítást.*

Adatvédelmi szabályzat

Az adatküldés nem veszélyezteti személyes adatait.

Habár bizonyos szempontok szerint az elküldött adatok személyesnek ítéltetők, adatai a folyamat során mindvégig védelmet élveznek. Az adatokat biztonságosan továbbítjuk, eltávolítjuk az összes szükségtelen személyes adatot, emellett névtelenül, összesítetten dolgozzuk fel az adatokat. Így az információ semmilyen módon nem köthető a felhasználóhoz. Az elküldött információk nem tartalmaznak a felhasználói fiókra és az IP-címre vonatkozó adatokat, illetve licencinformációkat. Az információ átvitelekor titkosítással is védjük az adatait.

Az elküldött információval javítjuk a szolgáltatások és termékek védelmi képességeit.

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 kézi frissítése:

1. Keresse meg a **Vírusvédelem** menüt, majd nyomja le a kiválasztó billentyűt.
2. Válassza a **Frissítés most** parancsot.
3. Válassza ki, hogy melyik internet-hozzáférési ponton keresztül kíván csatlakozni a frissítési kiszolgálóhoz. Az alkalmazás letölti a legfrissebb vírusdefiníciós adatbázist, és azonnal használni kezdi azt.
4. A letöltés befejezése után nyomja meg az **Igen** gombot az eszköz ellenőrzéséhez, ha az alkalmazás felszólítja erre. További információt a fenti, **Vírusvizsgálat** című szakaszban talál.

Verzió-frissítések

Amikor megjelenik az F-Secure Mobile Security egy új verziója, az alkalmazás egy üzenetben megkérdezi, hogy letöltse-e az újabb verziót. A frissítés befejeződésekor az alkalmazás újraindul.

Technikai ügyfélszolgálat

A fő nézet a biztonságra vonatkozó áttekintést és a jelenlegi állapotra vonatkozó információkat tartalmaz.

Ha a megjelenített állapot szerint az eszköz nem védett, kövesse a következő utasításokat:

1. Keresse meg a **Biztonság áttekintése** lehetőséget, majd nyomja le a kiválasztó billentyűt.
2. Válassza ki a piros vagy sárga ikonnal rendelkező elemet, majd nyomja meg a kiválasztó billentyűt a probléma megoldásához.

További információért töltsse le az (angol nyelven elérhető) *F-Secure Mobile Security for S60 User's Guide* kézikönyvet a <http://mobile.f-secure.com/> webhelyről.

Amennyiben olyan kérdései merülnének fel, amelyekre nem található válasz az útmutatókban vagy az online szolgáltatások között, lépjen kapcsolatba helyi F-Secure viszonteladójával, vagy közvetlenül az F-Secure Corporation vállalattal.

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 telhetőt 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 © 2009 F-Secure Corporation. Minden jog fenntartva

