ESET MOBILE SECURITY

AZ ANDROID RENDSZERHEZ

Telepítési kézikönyv és felhasználói útmutató

Ide kattintva letöltheti a dokumentum legújabb verzióját

Tartalom

ESET **MOBILE SECURITY**

Terméktámogatás: http://www.eset.hu/tamogatas

REV. 7. 10. 2011

1. Az ESET Mobile Security telepítése

Ha az ESET Mobile Security programot szeretné telepíteni az Android rendszerhez, a mobilkészüléknek az alábbi követelményeknek kell megfelelnie:

	Minimális rendszerkövetelmények
Operációs rendszer	Android 2.0/2.1 (Éclair) és újabb verziói
CPU	600 MHz
RAM	256 MB
Belső szabad tárhely	5 MB

Az Android 3.0 (Honeycomb) nem támogatott.

1.1 Telepítés

Az ESET Mobile Security telepítéséhez végezze el az alábbi műveletek valamelyikét:

- Keresse meg az **ESET Mobile Security** (vagy egyszerűen az **Eset**) programot itt: Android Market. Az alkalmazás az **Applications** > **Tools** listában található.
- Töltse le az ESET Mobile Security telepítőfájlját *(ems.apk)* a számítógépére az ESET weboldaláról. USB- vagy Bluetooth-kapcsolaton keresztül csatlakoztassa mobilkészülékét a számítógéphez, és másolja a fájlt a kívánt helyre.
- Töltse le az *ems.apk* fájlt az alábbi QR-kód ellenőrzésével a mobilkészüléke és egy alkalmazás, például a QR Droid vagy a Barcode Scanner használatával.

ESET Mobile Security **QR-kód**

Ha manuálisan telepíti az ESET Mobile Security programot, koppintson az indítóikonra az Android kezdőképernyőjén (vagy lépjen a **Védelem állapota** > **Menü** pontra), koppintson a **Beállítások** > **Alkalmazások** lehetőségre, és válassza az **Ismeretlen források** elemet. Keresse meg az *ems.apk* fájlt például az ASTRO File Manager vagy az ES File Explorer alkalmazással. Nyissa meg a fájlt, és koppintson a **Telepítés** lehetőségre. Az alkalmazás telepítése után koppintson a **Megnyitás** lehetőségre.

A sikeres telepítést követően aktiválja az ESET Mobile Security programot a Licenc aktiválása 4 című részben ismertetett lépésekkel.

1.2 Eltávolítás

Ha el szeretné távolítani az ESET Mobile Security programot a készülékről, kövesse az alábbi lépéseket:

1. Koppintson az indítóikonra az Android kezdőképernyőjén (vagy lépjen a **Védelem állapota** > **Menü** pontra), koppintson a **Beállítások** > **Hely és biztonság** > **Eszközkezelők kiválasztása** lehetőségre, törölje az **EMS** bejelölését, és koppintson a **Deaktiválás** gombra. Amikor a program kéri, írja be az ESET Mobile Security jelszavát. (Ha nem állította be az ESET Mobile Security programot eszköz-rendszergazdaként, hagyja ki ezt a lépést.)
2. Lépjen vissza a **Beállítások** lapra, és koppintson az **Alkalmazások** > **Alkalmazások kezelése** > **ESET Security** > **Eltávolítás** gombra.

A program véglegesen eltávolítja az ESET Mobile Security programot és a karanténmappát a mobilkészülékről.

2. Licenc aktiválása

A sikeres telepítést követően aktiválni kell az ESET Mobile Security programot. Koppintson az **Aktiválás** lehetőségre az ESET Mobile Security főképernyőjén.

Az ESET Mobile Security beszerzési módjától függően háromféle aktiválási mód közül választhatja ki a megfelelőt.

- **Aktiválás próba üzemmódban** – válassza ezt a lehetőséget, ha nem rendelkezik licenccel, és a vásárlás előtt ki szeretné próbálni az ESET Mobile Security programot. Írja be az **E-mail** címét az ESET Mobile Security korlátozott időtartamra szóló aktiválásához. A licenc sikeres aktiválását követően egy megerősítő e-mailt fog kapni. Mobilkészülékenként csak egyszer aktiválható a próbaverzió licence.
- **Aktiválás aktiválási kulcs segítségével** – ha az ESET Mobile Security programot egy új eszközzel együtt (vagy dobozos termékként) szerezte be, a vásárláskor aktiválási kulcsot kapott hozzá. Írja be a kapott adatokat az **Aktiválási kulcs** mezőbe és az aktuális címét az **E-mail** mezőbe. Új hitelesítési adatai (felhasználóneve és jelszava) automatikusan felváltják az aktiválási kulcsot, és a rendszer a megadott e-mail címre is elküldi azokat.
- **Aktiválás felhasználónév és jelszó segítségével** – ha terjesztőtől szerezte be a programot, a vásárláskor kapott egy felhasználónevet és egy jelszót. Írja be a kapott adatokat a **Felhasználónév** és a **Jelszó** mezőbe. Írja be az aktuális kapcsolattartási címét az **E-mail** mezőbe.
- **Megvásárolom** – válassza ezt a lehetőséget, ha még nincs licence, és szeretne vásárolni egyet.

Minden aktiválás meghatározott ideig érvényes. Ha az aktiválás lejár, meg kell újítania a program licencét (a program erről előzetes értesítést küld).

MEGJEGYZÉS: Az aktiválás során az eszköznek kapcsolódnia kell az internethez. Kis mennyiségű adatot le kell tölteni. Erre az adatátvitelre a mobilszolgáltatóval kötött szolgáltatási szerződés alapján érvényes díj vonatkozik.

3. Antivírus

Készülék ellenőrzése

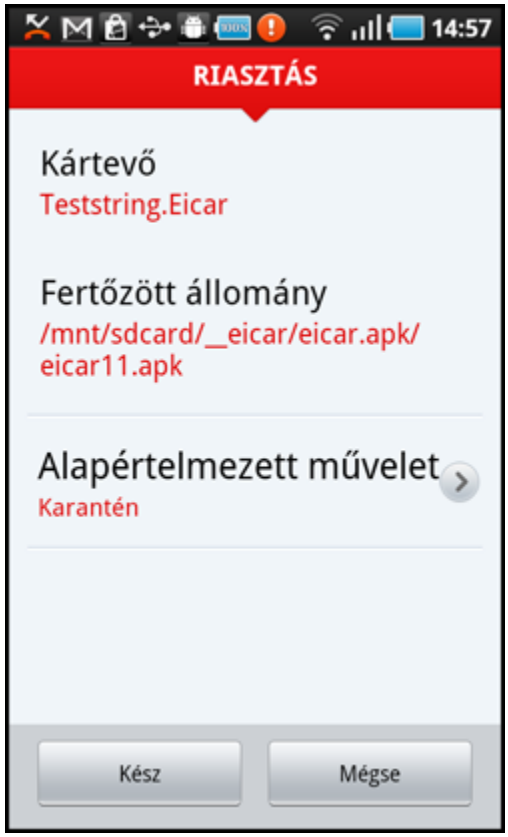
A **Készülék ellenőrzése** beállítással ellenőrizheti, hogy észlelhető-e fertőzés a mobilkészülékén.

A program egyes előre megadott fájltípusokat alapértelmezés szerint ellenőriz. A teljes készülék ellenőrzése során a program ellenőrzi a memóriát, a futó folyamatokat és a futásukhoz szükséges dinamikus csatolású függvénytárakat, valamint a belső és a cserélhető adattárolókon található állományokat. Az ellenőrzés befejezése után megjelenik róla egy rövid összesítés (vagyis az ellenőrzött és a fertőzött állományok száma, az ellenőrzés időtartama stb.).

Ha meg szeretne szakítani egy folyamatban lévő ellenőrzést, koppintson a **Mégse** gombra.

Mappa ellenőrzése

Ha adott mappákat szeretne ellenőrizni a készüléken, koppintson a **Mappa ellenőrzése** lehetőségre. Keresse meg az ellenőrizendő mappákat, jelölje be a jelölőnégyzeteiket a jobb oszlopban, majd koppintson az **Ellenőrzés** elemre.



Az ESET Mobile Security

Vírusellenőrzések naplói

A **Vírusellenőrzések naplói** szakaszban a befejezett ellenőrzési feladatokról átfogó adatokat tartalmazó naplók találhatók. A rendszer naplókat hoz létre az egyes kézzel indított ellenőrzések után vagy abban az esetben, ha a valós idejű ellenőrzés fertőzést észlel.

Az egyes naplók tartalma:

- az esemény dátuma és időpontja;
- ellenőrzött állományok száma;
- fertőzött állományok száma;
- a fertőzött állományok elérési útjának teljes neve;
- az ellenőrzés időtartama;
- a végrehajtott műveletek és az ellenőrzés során tapasztalható hibák.

Karantén

A karantén fő feladata a fertőzött állományok biztonságos tárolása. Az állományokat akkor kell a karanténba helyezni, ha nem tisztíthatók meg, ha törlésük kockázattal jár vagy nem ajánlott, illetve ha az ESET Mobile Security tévesen észlelte őket.

A karanténban tárolt fájlok megtekinthetők egy naplóban, amely tartalmazza a fertőzött állomány nevét és eredeti helyét, valamint a karanténba helyezés dátumát és időpontját.

Ha egy karanténba helyezett állományt vissza szeretne állítani az eredeti helyére, koppintson az állományra, és válassza a **Visszaállítás** lehetőséget. Ez a beállítás nem javasolt.

Ha véglegesen el szeretne távolítani a készülékéről egy karanténba helyezett állományt, koppintson az állományra, és válassza a **Törlés** parancsot. A karanténban tárolt összes állomány eltávolításához nyomja meg a **MENÜ** gombot, és koppintson **Az összes törlése** parancsra.

Beállítások

A **Kézi indítású keresés** beállításai lehetővé teszik a kézzel indított ellenőrzés paramétereinek a módosítását.

A **Figyelmeztető üzenetek megjelenítése** beállítással minden alkalommal megjeleníthetők a kártevőkkel kapcsolatos riasztások, amikor a kézi indítású ellenőrzés új kártevőt talál.

Ha a készüléken telepített összes alkalmazást (*.apk* fájlt) szeretné ellenőrizni, válassza az **Alkalmazások ellenőrzése** beállítást.

A **Proaktív védelem** olyan algoritmikus észlelési módszer, amely elemzi a kódokat, és jellegzetes vírustevékenységek után kutat. Fő előnye, hogy képes az aktuális vírusdefiníciós adatbázis számára egyelőre ismeretlen kártevő szoftverek azonosítására. A proaktív védelem engedélyezése esetén több időre van szükség az ellenőrzés befejezéséhez.

A **Tömörített állományok ellenőrzésének mélysége** beállítás lehetővé teszi az ellenőrizendő többszörösen tömörített fájlok (*.zip* fájlok) mélységének megadását. Minél magasabb a szám, annál mélyebb az ellenőrzés.

A **Tárolt naplók** beállítás segítségével megadhatja a **Vírusellenőrzések naplói** 5 szakaszban tárolandó naplók maximális számát.

Megadhatja a fertőzött fájlok észlelésekor automatikusan elvégzendő **alapértelmezett műveletet**. Az alábbi lehetőségek közül választhat:

- **Mellőzés** – semmilyen műveletet nem hajt végre a program a fertőzött állományon (ez a beállítás nem javasolt).
- **Törlés** – a program eltávolítja a fertőzött állományt.
- **Karantén** – (alapértelmezett) a program a **karanténba** 5 helyezi a fertőzött állományt.

A **Kiterjesztések** beállításai megjelenítik az Android platformon a fertőzéseknek leginkább kitett általános fájltípusokat. Jelölje ki az ellenőrizendő fájltípusokat, illetve szüntesse meg a kiterjesztések kijelölését, ha ki szeretné zárni azokat az ellenőrzésből. Ezek a beállítások egyaránt vonatkoznak a kézi indítású és a valós idejű ellenőrzésekre:

- **Csak indítható állományok** – ha törli a beállítás kiválasztását, a program az összes fájltípust ellenőrzi. A fájlok ellenőrzése akkor is megtörténik, ha nem voltak más fájltípusnak álcázva. Ekkor hosszabb ellenőrzési időre van szükség.
- **DEX (Alkalmazások forráskódú fájljai)** – az Android operációs rendszerhez írt lefordított kódot tartalmazó végrehajtható fájlformátum.
- **SO (könyvtárak)** – a fájlrendszer kijelölt helyeire mentett és olyan programok által hivatkozott megosztott könyvtárak, amelyeknek szükségük van a funkcióikra.
- **Tömörített állományok** – a Zip tömörítés használatával tömörített fájlok.
- **Egyéb lehetőségek** – egyéb ismert fájltípusok.

A **Valós idejű védelem** beállításaiban konfigurálhatja a fájlrendszervédelmi ellenőrzés paramétereit. A fájlrendszervédelem valós idejű ellenőrzést végez a kommunikációban részt vevő állományokon. Automatikusan ellenőrzi az SD-kártya *letöltési* mappáját, az *.apk* telepítési fájlokat és az SD-kártyán a csatlakoztatása után meglévő fájlokat (ha a **Csatlakoztatott SD kártya ellenőrzése** beállítás engedélyezve van). A fájlrendszervédelem automatikusan bekapcsol a rendszer indításakor.

- **Valós idejű fájlrendszervédelem** – ha engedélyezve van (alapértelmezés szerint), a fájlrendszervédelmi ellenőrzés a háttérben fut.
- **Figyelmeztető üzenetek megjelenítése** – minden alkalommal megjeleníti a kártevőkkel kapcsolatos riasztásokat, amikor a fájlrendszervédelmi ellenőrzés új kártevőt talál.
- **Csatlakoztatott SD kártya ellenőrzése** – azt megelőzően ellenőrzi a fájlokat, hogy megnyitná vagy az SD-kártyára mentené azokat.
- **Proaktív védelem** – ezt választva alkalmazhatja a heurisztikai ellenőrzési eljárásokat. A heurisztika proaktívan azonosítja a vírusdefiníciós adatbázisban még nem szereplő új kártevőket oly módon, hogy elemzi a kódot, és felismeri a vírus tipikus viselkedését. A proaktív védelem engedélyezése esetén több időre van szükség az ellenőrzés befejezéséhez.
- **Tömörített állományok ellenőrzésének mélysége** – lehetővé teszi az ellenőrizendő többszörösen tömörített fájlok (*.zip* fájlok) mélységének megadását. Minél magasabb a szám, annál mélyebb az ellenőrzés.
- **Alapértelmezett művelet** – megadhatja, hogy milyen alapértelmezett műveletet végezzen el a program automatikusan, ha a fájlrendszervédelmi ellenőrzés fertőzött állományt észlel. A **Mellőzés** beállítás választásakor semmilyen műveletet nem hajt végre a program a fertőzött állományon (ez a beállítás nem javasolt). A **Törlés** választása esetén a program eltávolítja a fertőzött állományt. A **Karantén** beállítás választása esetén a program a **karanténba** 5 helyezi a fertőzött állományt.

Az ESET Mobile Security megjeleníti az értesítési ikonját  a képernyő bal felső sarkában (Android állapotsor). Ha nem szeretné megjeleníteni ezt az ikont, lépjen az ESET Mobile Security főképernyőjére, nyomja meg a **MENÜ** gombot, koppintson az **Értesítési beállítások** parancsra, és kapcsolja ki az **Értesítési ikon megjelenítése** beállítást. Ne feledje, hogy ez nem kapcsolja ki a vörös figyelmeztető ikont, amelyen egy felkiáltójel látható, és egy biztonsági kockázatról értesíti (pl. a valós idejű vírusellenőrzés vagy a SIM ellenőrzés le van tiltva.).

4. Spamszűrő

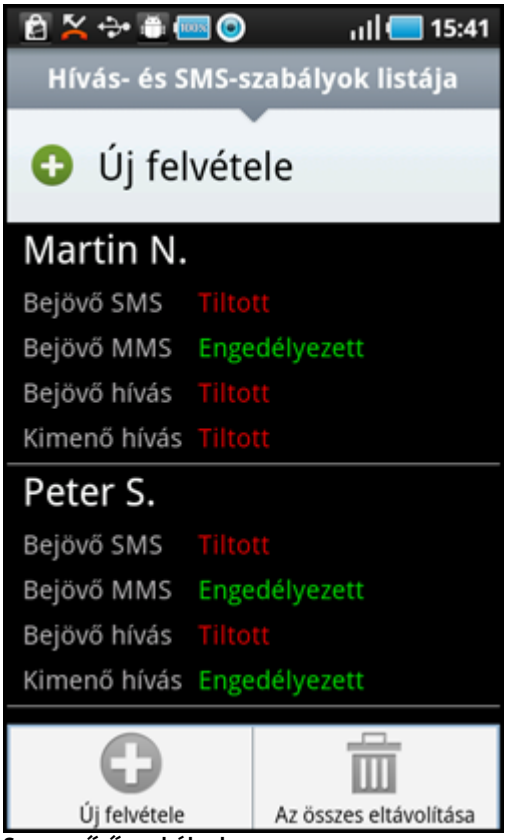
A **Spamszűrő** modul a felhasználó szabályai alapján blokkolja az SMS/MMS-üzeneteket és a bejövő vagy kimenő hívásokat.

A kéretlen üzenetek közé általában a mobilszolgáltató cégek által küldött reklámok és az ismeretlen vagy nem megadott felhasználóktól érkező üzenetek tartoznak. A *kapcsolatok blokkolása* kifejezés alatt a bejövő üzeneteknek a **spamszűrő naplóiba** 7 történő automatikus áthelyezését értjük. Az ESET Mobile Security nem jelenít meg értesítést, ha blokkol egy beérkező üzenetet. Ennek az előnye abban rejlik, hogy Önt nem zavarják a kéretlen információk, ugyanakkor mindig ellenőrizheti a naplókban, hogy a program nem blokkolt-e tévedésből üzeneteket.

Új spamszűrő felvételéhez koppintson a **Hívás- és SMS-szabályok listája** > **Új felvétele** lehetőségre. Írja be a blokkolni kívánt telefonszámot, vagy koppintson a **+** gombra, és válassza ki a számot a névjegyalbumból. Az üzenetek és hívások engedélyezésével vagy blokkolásával szabja testre a szabályt, és koppintson a **Kész** gombra.

Meglévő szabálybejegyzés szerkesztéséhez vagy eltávolításához érintse meg hosszan a bejegyzést, és válassza ki a kívánt műveletet. Ha el szeretné távolítani az összes spamszűrő szabályt, nyomja meg a **MENÜ** gombot, és koppintson **Az összes eltávolítása** parancsra.

MEGJEGYZÉS: A telefonszámnak a tényleges szám előtt tartalmaznia kell a nemzetközi hívószámot (például +16101001OO).



Spamszűrő szabályok

Beállítások

Hívószám nélküli bejövő hívások blokkolása – jelölje be ezt a jelölőnégyzetet, ha a CLIR (Calling Line Identification Restriction, Hívófél-azonosítás letiltása) szolgáltatással blokkolni szeretné a telefonszámukat szándékosan elrejtő hívókat.

Megadott kapcsolatok blokkolása – ezzel a beállítással blokkolhatja a névjegyalbumában szereplő kapcsolatok üzeneteit és hívásait.

Ismeretlen kapcsolatok blokkolása – blokkolja a névjegyalbumában nem szereplő kapcsolatok üzeneteit és hívásait. Ezzel a beállítással blokkolhatja a kéretlen telefonhívásokat (pl. reklámcélú hívásokat), illetve akadályozhatja meg, hogy a gyermekek ismeretlen számokat hívjanak. (Ehhez javasolt **jelszóval** 10 védeni a spamszűrő beállításait.)

A **Spamszűrő naplói** részen megnézheti a Spamszűrő által blokkolt hívásokat és üzeneteket. Minden napló tartalmazza az esemény nevét, a megfelelő telefonszámot, az esemény dátumát és időpontját. A blokkolt SMS-üzenetek az üzenet törzsét is tartalmazzák.

5. Lopásvédelem

A **Lopásvédelem** funkció biztosítja mobiltelefonja védelmét a jogosulatlan hozzáféréssel szemben.

Ha elveszíti vagy ellopják a telefonját, és SIM kártyáját egy újra (nem megbízhatóra) cserélik, az ESET Mobile Security azonnal zárolja a telefont, és titokban figyelmeztető üzenetet küld a felhasználó által meghatározott telefonszám(ok)ra. Az üzenet tartalmazza az aktuálisan behelyezett SIM kártya telefonszámát, az IMSI (International Mobile Subscriber Identity, nemzetközi mobil-előfizetői azonosító) számot és az IMEI (International Mobile Equipment Identity, nemzetközi mobilkészülék-azonosító) számot. A jogosulatlan felhasználó nem szerez értesülést az üzenet elküldéséről, mivel az automatikusan törlődik az **Üzenetek kezelése** folyamataiból. Emellett lekérheti az elveszett telefon GPS-koordinátáit, illetve törölheti a készüléken tárolt összes adatot.

Megbízható SIM kártyák

Ha a mobiltelefonban aktuálisan behelyezett SIM kártyát megbízhatóként szeretné menteni, koppintson a **Hozzáadás > Jelenlegi hozzáadása** lehetőségre. Ha egynél több SIM kártyát használ, célszerű megkülönböztetni azokat a **SIM kártya elnevezése** érték módosításával (például *Iroda*, *Otthon* stb.).

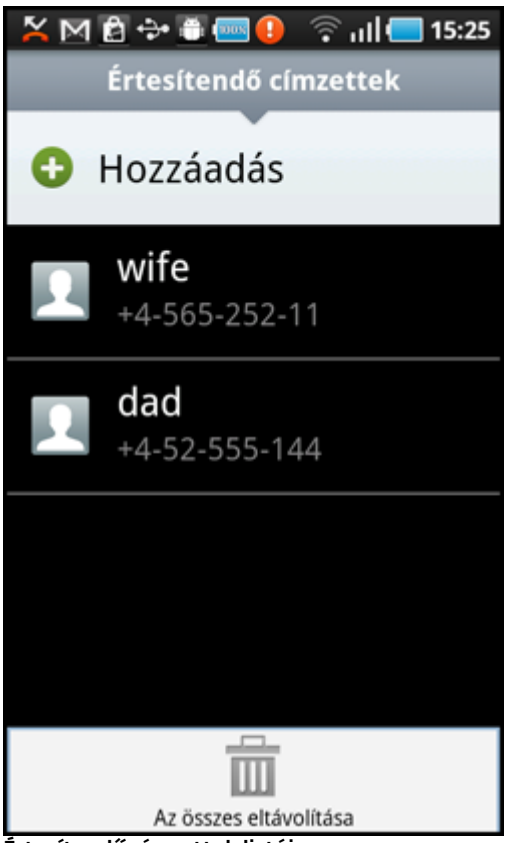
Meglévő SIM-bejegyzés **szerkesztéséhez** vagy **eltávolításához** érintse meg hosszan a bejegyzést, és válassza ki a kívánt műveletet. Ha el szeretné távolítani a listából az összes bejegyzést, nyomja meg a **MENÜ** gombot, és koppintson **Az összes eltávolítása** parancsra.

Értesítendő címzettek

Az **Értesítendő címzettek** listában **vegye fel** azokat a telefonszámokat, amelyekre figyelmeztető SMS küldendő azt követően, hogy egy nem megbízható SIM kártyát helyeznek a készülékbe. Írja be a nevet a **Címzett neve** mezőbe és a telefonszámot a **Telefonszám** mezőbe, vagy koppintson a **+** gombra, és válassza ki a kapcsolatot a névjegyalbumból. Ha a kapcsolathoz több telefonszám tartozik, a program minden számra küld figyelmeztető SMS üzenetet.

Meglévő bejegyzés **szerkesztéséhez** vagy **eltávolításához** érintse meg hosszan a bejegyzést, és válassza ki a kívánt műveletet. Ha el szeretné távolítani a listából az összes bejegyzést, nyomja meg a **MENÜ** gombot, és koppintson **Az összes eltávolítása** parancsra.

MEGJEGYZÉS: A telefonszámnak a tényleges szám előtt tartalmaznia kell a nemzetközi hívószámot (például +161010010O).



Értesítendő címzettek listája

Beállítások

Ha olyan készülékkel rendelkezik, amelyben nincs SIM kártya (például táblaszámítógép vagy CDMA telefon), válassza a **SIM ellenőrzés mellőzése** beállítást. Ez a beállítás kikapcsolja a vörös *Biztonsági kockázat!* figyelmeztetéseket (*SIM ellenőrzés ki van kapcsolva* és *nincs megadva megbízható SIM*) az ESET Mobile Security főképernyőjén. (Ne feledje, hogy a SIM ellenőrzés mellőzése beállítás nem érhető el a CDMA-alapú készülékeken.)

Ha engedélyezni szeretné a behelyezett SIM kártya ellenőrzését (és a figyelmeztető SMS küldését), jelölje be a **SIM ellenőrzés bekapcsolása** lehetőséget.

A **Figyelmeztető SMS üzenet szövege** mezőben módosíthatja az előre megadott telefonszámokra azt követően küldendő szöveges üzenetet, miután egy nem megbízató SIM kártyát helyeztek a készülékébe.

SMS parancsok

A távoli SMS parancsok (wipe, lock és find) csak akkor működnek, ha az **SMS parancsok engedélyezése** beállítás ki van választva.

Az **SMS jelszó-visszaállítás bekapcsolása** beállítás lehetővé teszi biztonsági jelszavának visszaállítását oly módon, hogy SMS üzenetet küld az **Értesítendő címzettek** listában mentett mobilról az Ön mobilszámára. Az SMS formátumának az alábbinak kell lennie:
eset remote reset

Ha elveszíti telefonját, és szeretné azt zárolni, küldjön egy távoli lock SMS parancsot bármely mobilkészülékről az Ön telefonszámára az alábbi formátumban:
eset lock jelszó
A *jelszó* helyére írja be a **Jelszó** 10 szakaszban megadott saját jelszavát. A jogosulatlan felhasználók nem tudják használni a telefont, mivel ahhoz meg kell adni a jelszavát.

Ha le szeretné kérni mobilkészüléke GPS-koordinátáit, küldjön egy távoli find SMS parancsot a mobilkészülékére vagy a jogosult felhasználó mobilkészülékére (attól függően, hogy a SIM kártya már ki lett-e cserélve):
eset find jelszó
A rendszer küld egy SMS üzenetet a GPS-koordinátákkal és a Google Térkép alkalmazásra mutató hivatkozással, amely megjeleníti a mobilkészülék pontos helyét. Ne feledje, hogy csak akkor tudja fogadni a GPS-koordinátákat, ha előzőleg aktiválta a telefonon a GPS modult.

Ha a készüléken és az aktuálisan behelyezett összes cserélhető adathordozón tárolt összes adatot törölni szeretné, küldjön egy távoli wipe SMS parancsot:
eset wipe jelszó

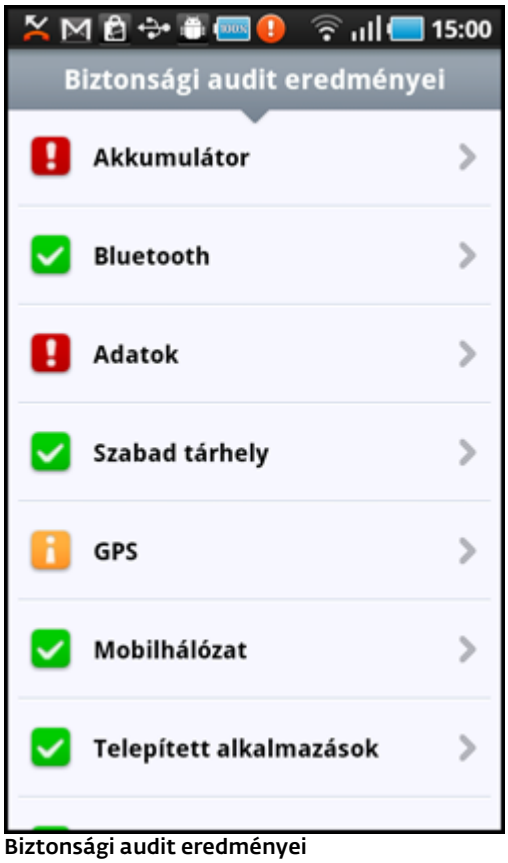
Minden kapcsolat, üzenet, e-mail, telepített alkalmazás, Google Fiókja és az SD-kártya tartalma véglegesen törlődik a készülékről. Ha az ESET Mobile Security nincs eszköz-rendszergazdaként beállítva, csak a kapcsolatok, üzenetek és az SD-kártya tartalma törlődik.

MEGJEGYZÉS: A jelszóban meg kell különböztetni a kis- és nagybetűket. A jelszót pontosan a Jelszó szakaszban megadott módon kell megadni.

6. Biztonsági audit

A **Biztonsági audit** ellenőrzi a telefon állapotát, beleértve az akkumulátor töltöttségi szintjét, a Bluetooth állapotát, a szabad tárhelyet stb.

A biztonsági audit kézzel történő futtatásához koppintson az **Audit indítása** elemre. A program részletes jelentést fog megjeleníteni.



Biztonsági audit eredményei

Az egyes elemek mellett látható zöld pipa jelzi, hogy az érték meghaladja a határértéket, illetve hogy az elem nem jelent biztonsági kockázatot.

Sárga ikon jelzi, hogy legalább egy elem a határérték alatt van, illetve hogy az elem lehetséges biztonsági kockázatot jelenthet. Koppintson az elemre a részletes adatok megjelenítéséhez.

Vörös felkiáltójel jelzi, hogy az elem határérték alatti, illetve biztonsági kockázatot jelent, és beavatkozásra van szükség.

Ha javítani szeretné a vörössel kiemelt elem állapotát, koppintson az elemre, és erősítse meg az **Igen** lehetőségre koppintással.

Beállítások

A biztonsági audit alapértelmezés szerint rendszeresen 24 óránkénti futtatásra van ütemezve. Ha ki szeretné kapcsolni az audit rendszeres futtatását, törölje a **Rendszeres audit** beállítás bejelölését.

Az **Automatikus javítás** beállítás bekapcsolása esetén az ESET Mobile Security automatikusan megkísérli a kockázatot jelentő elemek (pl. a bluetooth állapot) javítását felhasználói beavatkozás nélkül. Ez a beállítás csak rendszeres (ütemezett) auditokra vonatkozik.

A **Tárolt naplók** beállítás segítségével megadhatja az **Auditok naplói** szakaszban tárolandó naplók maximális számát.

A **Audit készítés gyakorisága** beállítás lehetővé teszi a rendszeres (ütemezett) audit gyakoriságának megadását.

A **Minimális szabad tárhely** és a **Minimális akkutöltöttség** beállítás használatával módosíthatja azt a határértéket, amely esetében a szabad tárhely és az akkumulátor töltöttségi szintje alacsonynak tekintendő.

Az **Auditálandó elemek** lapon jelölje ki a rendszeres (ütemezett) audit során ellenőrizendő elemeket.

Az **Auditok naplói** szakaszban az elvégzett rendszeres és kézzel indított auditokról átfogó adatokat tartalmazó naplók találhatók. Az egyes naplók tartalmazzák az esemény dátumát és időpontját, valamint az egyes elemekre vonatkozó részletes adatokat.

A **Feladatkezelő** áttekintést nyújt a készüléken futó összes folyamatról, szolgáltatásról és feladatról. Az ESET Mobile Security segítségével leállíthatja azokat a folyamatokat, szolgáltatásokat és feladatokat, amelyeket nem a rendszer futtat. Ezeket egy vörös ikon (**x**) jelzi.

7. Frissítés

Az ESET Mobile Security a rendszeres frissítés biztosítására alapértelmezés szerint tartalmaz egy frissítési feladatot. A frissítés kézzel történő futtatásához koppintson a **Frissítés** lehetőségre.

Beállítások

A **Felhasználónév** és a **Jelszó** mezőnek a licencről értesítő e-mailben kapott adatokat kell tartalmaznia.

Az **Automatikus frissítés gyakorisága** beállításban megadhatja a vírusdefiníciós adatbázis automatikus frissítésének időközét.

MEGJEGYZÉS: A fölösleges sávszélesség-használat elkerülése érdekében a frissítéseket szükség szerint, egy új kártevő hozzáadása esetén bocsátjuk ki. A frissítések az aktív licenccel ingyenesek, az adatátvitelért azonban a mobilszolgáltató díjat számíthat fel.

8. Jelszó

Biztonsági jelszava megvédi beállításait a jogosulatlan módosításoktól. Jelszó szükséges:

- az ESET Mobile Security jelszóval védett szolgáltatásainak (Antivírus, Spamszűrő, Lopásvédelem és Biztonsági audit) eléréséhez;
- a telefon eléréséhez a zárolása esetén;
- SMS parancsok küldéséhez a készülékére;
- az ESET Mobile Security eltávolításához.

MEGJEGYZÉS: A védelem eltávolítása csak az Android 2.2 vagy újabb verziókban lehetséges.

Új biztonsági jelszó megadásához írja be azt a **Jelszó** és a **Jelszó megismétlése** mezőbe. A **Jelszó-emlékeztető** beállítás (ha meg van adva) megjelenít egy emlékeztetőt arra az esetre, ha elfelejtette a jelszavát.

FONTOS: Gondosan válassza meg a jelszót, mert a készülék zárolásának feloldásához és az ESET Mobile Security eltávolításához szükség lesz rá.

Az **Alkalmazás erre** lapon megadhatja, hogy mely modulok védelmét biztosítsa a jelszó.

Ha elfelejti a jelszavát, küldhet egy SMS üzenetet az **Értesítendő címzettek** listában mentett telefonszámról a saját mobilszámára. Az SMS formátumának az alábbinak kell lennie:
eset remote reset
A program visszaállítja a jelszavát.

9. Hibaelhárítás és támogatás

9.1 Terméktámogatás

Ha az ESET Mobile Security programmal vagy bármely más ESET biztonsági szoftverrel kapcsolatban adminisztrációs vagy technikai támogatásra van szüksége, az ESET ügyfélszolgálati szakemberei a rendelkezésére állnak.

A legtöbb gyakori kérdésre megtalálhatja a választ az ESET angol és magyar nyelvű tudástárában, melyek az alábbi címeken érhetők el:
http://kb.eset.com; http://www.eset.hu/tamogatas/gyik

A tudástár kategóriákba sorolt vagy részletes keresővel elérhető rengeteg hasznos, a leggyakoribb problémák megoldásával kapcsolatos információt tartalmaz.

Ha fel szeretné venni a kapcsolatot az ESET ügyfélszolgálatával, használja az alábbi címen elérhető űrlapot:
https://www.eset.hu/tamogatas/kapcsolat

Ha visszajelzést szeretne számunkra küldeni, lépjen az ESET Mobile Security főképernyőjére, nyomja meg a **MENÜ** gombot, és koppintson a **Terméktámogatás** lehetőségre.