

# F-Secure Mobile Security™ for S60

## 1. Installeren en activeren

**Vorige versie** U hoeft de vorige versie van F-Secure Mobile Anti-Virus niet te verwijderen. Controleer de instellingen van F-Secure Mobile Security nadat u de nieuwe versie hebt geïnstalleerd.

**Installatie** **Installeren:**

- Download het installatiebestand naar de computer en verplaats het naar het apparaat.
- Download het installatiebestand naar de computer en installeer het product via Nokia PC Suite. Of,
- download de installatie rechtstreeks naar het apparaat. De installatie start automatisch.

Na de installatie moet u het apparaat opnieuw opstarten als dit wordt gevraagd tijdens de installatie. Nadat de installatie is voltooid, moet u het product activeren. Uw apparaat wordt pas beveiligd als u het product activeert.

**Activering** **Activeren:**

1. Open de toepassing. Het welkomtscherm wordt weergegeven.
2. Druk op **Doorgaan**.
3. Selecteer het activeringstype:
  - Om het product te activeren met alleen de Anti-diefstalfunctie geactiveerd, selecteert u **Alleen Anti-diefstal** als het activeringstype en drukt u op **Doorgaan**.
  - Als u de volledige licentieversie wilt gebruiken, selecteert u **Abonnementsnummer** als activeringstype en kiest u **Doorgaan**. Geef uw abonnementsnummer op en drukt op **OK**.
4. Druk op **Ja** en selecteer het internettoegangspunt waarmee u verbinding wilt maken met de updateservice en begin met het downloaden van de updates.  
De toepassing maakt verbinding met de updateservice en verzendt uw abonnementsnummer. Tijdens de eerste update wordt de nieuwste virusdefinitiedatabase gedownload.
5. Als het product de benodigde updates heeft gedownload, is de toepassing voltooid. Druk op **Doorgaan** om de activering te voltooien.

Nadat de activering is voltooid, scant u het apparaat op virussen om er zeker van te zijn dat het apparaat geen virussen bevat. Zie het gedeelte **Scannen op virussen** hieronder.



*Scan het apparaat altijd als u hierom wordt gevraagd.*

## 2. Scannen op virussen

F-Secure Mobile Security wordt op de achtergrond uitgevoerd en bestanden worden automatisch gescand.

1. F-Secure Mobile Security geeft een melding als tijdens de real-time scan een virus wordt gevonden. Druk op **Ja** om geïnfecteerde bestanden meteen weer te geven of **Nee** om de bestanden later te bekijken.
2. De infectieweergave bevat een lijst met geïnfecteerde bestanden op het apparaat en er wordt aangegeven of het bestand in quarantaine is of is vrijgegeven.

Meer informatie over een geïnfecteerd bestand:

1. Blader naar het geïnfecteerde bestand en druk op de selectietoets.
2. Selecteer **Weergave**.
3. In de weergave met infectiegegevens worden het pad en de bestandsnaam van het geïnfecteerde bestand en de naam van het virus weergegeven.

### Verwerking geïnfecteerde bestanden

#### Geïnfecteerde bestanden verwerken:

1. Blader in de infectieweergave naar het geïnfecteerde bestand dat u wilt verwerken.
2. Druk op de selectietoets.
3. Kies een van de volgende acties:
  - **Verwijderen**: het geïnfecteerde bestand wordt verwijderd. U kunt het beste deze optie kiezen. Het bestand wordt definitief van het apparaat verwijderd.
  - **Isolatie** - het geïnfecteerde bestand in isolatie plaatsen als dit nog niet is gebeurd. Een geïsoleerd bestand wordt vergrendeld en kan het apparaat niet beschadigen als F-Secure Mobile Security is ingeschakeld.
  - **Vrijgeven**: het geïsoleerde bestand wordt vrijgegeven. Als u een bestand vrijgeeft, wordt dit niet meer vergrendeld. U opent het bestand op eigen risico.

## 3. Ongeautoriseerd netwerkverkeer voorkomen

De firewall in F-Secure Mobile Security werkt op de achtergrond. Deze houdt het binnenkomende en uitgaande internet- en netwerkverkeer in de gaten, en beschermt u tegen inbraakpogingen. Met de vooraf gedefinieerde firewallniveaus kunt u het beschermingsniveau naar wens aanpassen.


### Een beveiligings- niveau selecteren

#### Het beveiligingsniveau selecteren:

1. Blader naar **Instellingen** en druk op de selectietoets.
2. Selecteer **Firewall** in de selectielijst met instellingen.
3. Het gewenste firewallniveau selecteren:
  - **Alles weigeren**: houdt alle netwerkverkeer tegen.
  - **Hoog**: staat de meest voorkomende toepassingen toe en blokkeert al het verkeer dat binnenkomt.
  - **Normaal**: staat alle uitgaande verbindingen toe en blokkeert al het verkeer dat binnenkomt.
  - **Alles toestaan**: staat alle netwerkverkeer toe.
  - **Aangepast**: staat netwerkverkeer toe dat gebaseerd is op uw aangepaste regels. Als u de aangepaste regelset wilt aanpassen, selecteert u **Opties > Aangepaste regels bewerken** wanneer het beveiligingsniveau **Aangepast** is geselecteerd.

## 4. Vertrouwelijke gegevens beschermen

Met Anti-Theft kunt u ervoor zorgen dat uw apparaat of de gegevens die erop zijn opgeslagen, niet worden misbruikt als uw apparaat wordt gestolen.


 *Aangezien geheugenkaarten eenvoudig kunnen worden verwijderd, moet u uw vertrouwelijke gegevens opslaan in het apparaatgeheugen dat u kunt vergrendelen en wissen met Anti-Theft.*

### De Apparaat- vergrendeling gebruiken

Anti-Theft kan uw apparaat automatisch vergrendelen wanneer er een andere SIM-kaart in het apparaat wordt geplaatst. Het vergrendelde apparaat kan worden ontgrendeld met de vergrendelingscode.

#### De apparaatvergrendeling instellen:

1. Blader naar **Instellingen** en druk op de selectietoets.
2. Selecteer **Anti-Theft** in de selectielijst met instellingen.
3. Voer een **Vergrendelingscode** in. De vergrendelingscode moet uit minstens 5 tekens bestaan. Bewaar deze code op een veilige plek.

 *Uw vergrendelingscode beveiligt de instellingen voor Anti-Theft. U moet uw eigen vergrendelingscode opgeven voordat u de instellingen voor Anti-Theft kunt wijzigen.*

4. Als u uw apparaat wilt vergrendelen als de SIM-kaart wordt vervangen, selecteert u **Ja** bij **Blok. bij gew. SIM**.

### De anti-diefstal op afstand gebruiken

Met anti-diefstal op afstand kunt u een sms-bericht met de vergrendelingscode verzenden om het apparaat te lokaliseren, te vergrendelen of u kunt een wiscode verzenden om alle gegevens te wissen.

#### Externe vergrendeling instellen:

1. Blader naar **Instellingen** en druk op de selectietoets.
2. Selecteer **Anti-Theft** in de selectielijst met instellingen.
3. Als u uw apparaat op afstand wilt kunnen vergrendelen, gaat u als volgt te werk:
  - a. Voer een **vergrendelingscode** in als u deze nog niet hebt gemaakt.
  - b. Schakel **Vergrendeling op afstand** in.Het vergrendelde apparaat kan worden ontgrendeld met de vergrendelingscode.
4. Als u uw apparaat op afstand wilt kunnen wissen, gaat u als volgt te werk:
  - a. Voer een **Wiscode** in. De wiscode moet uit minstens 8 tekens bestaan. Bewaar deze code op een veilige plek.
  - b. Schakel **Wissen op afstand** in.

Wanneer het apparaat wordt gewist, worden alle gegevens op het apparaat verwijderd.

### Uw apparaat op afstand vergrendelen of wissen:

Stuur het volgende sms-bericht naar uw apparaat.

- Om het apparaat te vergrendelen, verstuurt u:  
#LOCK#<vergrendelingscode> (Bijvoorbeeld: #LOCK#abcd1234)
- Om het apparaat leeg te maken, verstuurt u:  
#WIPE#<wiscode> (Bijvoorbeeld: #WIPE#abcd1234)
- Om het apparaat te lokaliseren, verstuurt u:  
#LOCATE#<vergrendelings code> (Bijvoorbeeld:  
#LOCATE#abcd1234)



*Anti-Theft slaat geen locatiegegevens op. De enige locatiegegevens staan in het sms-bericht dat naar u wordt verstuurd.*

## 5. Internetbrowsen beveiligen

Browsing protection beschermt u tegen websites die persoonlijke gegevens, zoals creditcardnummers, gebruikersaccountgegevens en wachtwoorden van u kunnen stelen.

Browsing protection controleert websites die u via de standaardbrowser van uw apparaat bezoekt. Als u een browser van derden gebruikt, biedt Browsing protection geen bescherming tijdens het browsen op internet.



*Schakel de internetbrowser uit en maak de cache leeg voordat u Browsing protection gebruikt.*

### Browsing protection inschakelen:

1. Blader naar **Instellingen** en druk op de selectietoets.
2. Selecteer **Browsing protection** in de selectielijst met instellingen.
3. Zet **Browsing protection** aan.
4. In **Te gebruiken netwerk** selecteert u of u Browsing protection altijd wilt gebruiken, of alleen als u via het netwerk van uw eigen provider gebruikmaakt van internet:
  - Selecteer **Alleen mijn provider** om Browsing protection alleen te gebruiken als u het netwerk van uw eigen provider gebruikt.
  - Selecteer de instelling **Alle providers** op de bescherming aan te laten staan als u zich buiten het bereik van het netwerk van uw eigen provider bevindt.

### Privacy-modus

Browsing protection kan informatie over websites die schadelijk materiaal bevatten, automatisch naar de analyse sturen om de kwaliteit van de service te behouden. U kunt kiezen welke informatie u naar de analyse wilt versturen.

### De privacymodus wijzigen:

1. Blader naar **Instellingen** en druk op de selectietoets.
2. Selecteer **Overige instellingen** in de selectielijst met instellingen.
3. In de Privacymodus selecteert u
  - **Alleen statistieken** om alleen de statistieken van Browsing protection en gegevens over de serververbinding te versturen.
  - **Alles toestaan** om statistieken en informatie over websites te versturen die niet zijn geanalyseerd of schadelijk materiaal bevatten.



*Voor de beste service, raden wij u aan de privacymodus in de stand **Alles toestaan** te laten staan.*

## Privacy-verklaring

Door informatie te versturen, wordt uw privacy niet in gevaar gebracht.

Hoewel de verzonden informatie in sommige rechtsgebieden als persoonsgegevens kan worden beschouwd, wordt uw privacy tijdens het proces beschermd. Wij versturen de informatie op beveiligde wijze, verwijderen overbodige persoonsgegevens en verwerken de informatie anoniem in een bulkbestand. Hierdoor kan de informatie op geen enkele wijze met u in verband worden gebracht. In de informatie die u verstuurt, zijn geen gebruikersaccountgegevens, IP-adressen of licentiegegevens opgenomen. Wij beschermen uw privacy bovendien door bij het verzenden van de informatie gebruik te maken van codering.

De verstuurde informatie wordt gebruikt om de beschermingsmogelijkheden van onze diensten en producten te verbeteren.

## 6. Het product up-to-date houden

### Automatische updates

F-Secure Mobile Security bevat een service voor automatische updates. Hiermee wordt de virusdefinitiedatabase in de toepassing regelmatig bijgewerkt. Het apparaat is alleen beveiligd tegen de nieuwste virussen als de virusdefinitiedatabase up-to-date is. Automatische updates worden ingeschakeld nadat u het product hebt geactiveerd.

Voor updates is een actieve verbinding met internet nodig. Als er een internetverbinding is, wordt er gecontroleerd wanneer de virusdefinitiedatabase voor het laatst is bijgewerkt. Vervolgens worden zo nodig nieuwe updates gedownload.

### Handmatige updates

#### **De toepassing handmatig bijwerken:**

1. Blader naar [Virusbeveiliging](#) en druk op de selectietoets.
2. Selecteer **Nu bijwerken**.
3. Selecteer het internettoegangspunt voor verbinding met de updateserver. De nieuwste virusdefinitiedatabase wordt gedownload en direct gebruikt.
4. Als de update is voltooid, drukt u op **Ja** om het apparaat te scannen op virussen als dit wordt gevraagd. Zie het gedeelte [Scannen op virussen](#) hierboven.

### Versie-updates

Als er een nieuwe versie van F-Secure Mobile Security beschikbaar is, wordt u gevraagd deze te downloaden. Zodra de update is voltooid, start de toepassing automatisch opnieuw op.

## Technische ondersteuning

In het hoofdvenster van de gebruikersinterface wordt het beveiligingsoverzicht en de huidige status weergegeven.

Als wordt aangegeven dat uw apparaat niet is beschermd, doet u het volgende:

1. Blader naar **Beveiligingsoverzicht** en druk op de selectietoets.
2. Selecteer het item met een rood of geel statuspictogram en druk op de selectietoets om het probleem op te lossen.

Download de *F-Secure Mobile Security for S60 User's Guide* (beschikbaar in het Engels) op <http://mobile.f-secure.com/> voor meer informatie.

Als u vragen hebt over de toepassing die niet worden besproken in de handleidingen of de online services, kunt u rechtstreeks contact opnemen met de plaatselijke F-Secure-distributeur of met F-Secure Corporation.

---

### VRIJWARINGSVERKLARING

"F-Secure" en het driehoekige symbool zijn gedeponeerde handelsmerken van F-Secure Corporation en productnamen en symbolen/logo's van F-Secure zijn handelsmerken of gedeponeerde handelsmerken van F-Secure Corporation. Alle productnamen waarnaar in dit document wordt verwezen zijn handelsmerken of gedeponeerde handelsmerken van hun respectieve eigenaren. F-Secure Corporation maakt geen aanspraak op eigendomsrechten van de merken en namen van anderen. Hoewel F-Secure Corporation er alles aan doet om ervoor te zorgen dat deze informatie nauwkeurig is, is F-Secure Corporation niet aansprakelijk voor fouten of de weglating van feiten in dit document. F-Secure Corporation behoudt zich het recht voor specificaties te wijzigen die in dit document worden genoemd, zonder voorafgaande kennisgeving.

Bedrijven, namen en gegevens die in voorbeelden in dit document worden gebruikt, zijn fictief tenzij anders vermeld. Geen enkel gedeelte van dit document mag, in welke vorm of op welke manier dan ook, worden gereproduceerd of overgedragen, elektronisch of mechanisch, voor welk doel dan ook, zonder de uitdrukkelijke schriftelijke toestemming van F-Secure Corporation.

Op dit product rusten één of meer patenten van F-Secure, waaronder de volgende:

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

Copyright © 2009 F-Secure Corporation. Alle rechten voorbehouden

