ESET MOBILE SECURITY

VOOR ANDROID

Gebruikershandleiding

(bedoeld voor productversie 3.0 en hoger)

Klik hier om de meest recente versie van dit document te downloaden

ESET **MOBILE SECURITY**

Klantenservice: www.eset.com/support

REV. 31. 7. 2014

Inhoud

1. Inleiding

ESET Mobile Security is een volledige beveiligingsoplossing die uw apparaat beschermt tegen potentiële bedreigingen en phishingpagina's, ongewenste oproepen en berichten filtert en u in staat stelt op afstand controle over uw apparaat te krijgen als u uw apparaat bent verloren of het apparaat is gestolen.

1.1 Wat is er nieuw

De volgende updates en verbeteringen zijn geïntroduceerd in ESET Mobile Security versie 3:

- Integratie van ESET Antidiefstal op de my.eset.com - webportal
- Locatie volgen: de apparaatlocatie wordt nu op een kaart weergegeven
- Foto's van camera: foto's van de camera aan de voorkant en achterkant worden nu automatisch gemaakt als het apparaat als vermist wordt gemarkeerd
- Schermbericht: u hebt de mogelijkheid een aangepast bericht naar de vinder van het apparaat te sturen
- Automatisch vergrendelen: het apparaat wordt vergrendeld als er verdachte activiteit wordt gedetecteerd of het apparaat als vermist wordt gemarkeerd
- Batterij van apparaat bijna leeg: als de batterij van het apparaat een kritiek laag niveau heeft, stuurt ESET Mobile Security zijn meest recente locatie naar my.eset.com
- Sirene activeren: laat op afstand vanaf my.eset.com een sirene afgaan als u denkt dat uw apparaat in de buurt is
- Beveiligingswachtwoord wijzigen: u hebt de mogelijkheid uw beveiligingswachtwoord te wijzigen op my.eset.com als u dit wachtwoord bent vergeten
- Op afstand wissen: u kunt alle belangrijke gegevens op uw apparaat wissen vanaf my.eset.com
- Genegeerde bedreigingen: een lijst met bedreigingen die worden genegeerd in toekomstige scans
- Scannen tijdens opladen: er wordt automatisch een scan uitgevoerd als het apparaat niet actief is en is aangesloten op een oplader

1.2 Systeemvereisten

Als u ESET Mobile Securitywilt installeren, moet uw Android-apparaat aan de volgende minimale systeemvereisten voldoen:

Besturingssysteem: Android 2.3 (Gingerbread) en later
Resolutie van aanraakscherm: minimaal 240x320 pixels; 320x480 pixels aanbevolen
CPU: 500 MHz (ARM7+)
RAM: 128 MB
Vrije interne opslagruimte: 20 MB
Internetverbinding

OPMERKING: apparaten waarop rooting is toegepast, worden niet ondersteund. Bepaalde functies (bijvoorbeeld Antidiefstal en Sms- en oproepfilter) zijn niet beschikbaar op tablets die geen ondersteuning bieden voor bellen en berichten.

2. Installatie

Gebruik een van de volgende methoden om ESET Mobile Securityte installeren.

OPMERKING: Als u al een actieve gebruikersnaam en wachtwoord of activeringscode hebt die is uitgegeven door ESET, download ESET Mobile Security dan vanaf de ESET-website .

2.1 Installatie vanaf de ESET-website

Download ESET Mobile Security door de QR-code te scannen met uw mobiele apparaat en een toepassing zoals QR Droid of Barcode Scanner:

Of download het APK-installatiebestand voor ESET Mobile Security naar uw computer:

1. Download het bestand op de ESET-website.
2. Kopieer het bestand naar uw apparaat via Bluetooth of USB.
3. Tik op het startpictogram in het startscherm van Android of ga naar **Start** > **Menu** en tik op **Instellingen** > **Toepassingen**. Zorg ervoor dat toepassingen van **Onbekende bronnen** zijn toegestaan op uw apparaat.
4. Ga naar het APK-bestand met een bestandsverkenner zoals ASTRO File Manager of ES File Explorer.
5. Open het bestand en tik op **Installeren**. Tik nadat de toepassing is geïnstalleerd op **Openen**.

2.2 Installatie vanaf Google Play

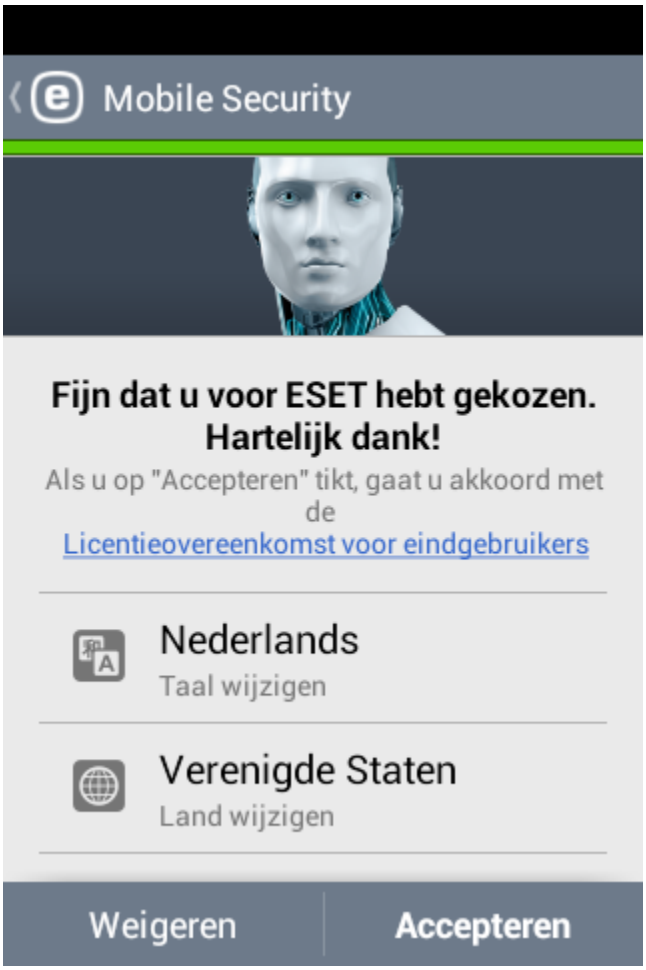
Open Google Play Store op uw Android-apparaat en zoek naar ESET Mobile Security (of alleen naar Eset).

U kunt het programma ook installeren door de onderstaande QR-code te scannen met uw mobiele apparaat en een toepassing zoals QR Droid of Barcode Scanner:

2.3 Installatie vanaf Amazon

Open de Amazon-toepassing op uw Android-apparaat en zoek naar ESET Mobile Security (of alleen Eset).

2.4 Wizard Opstarten

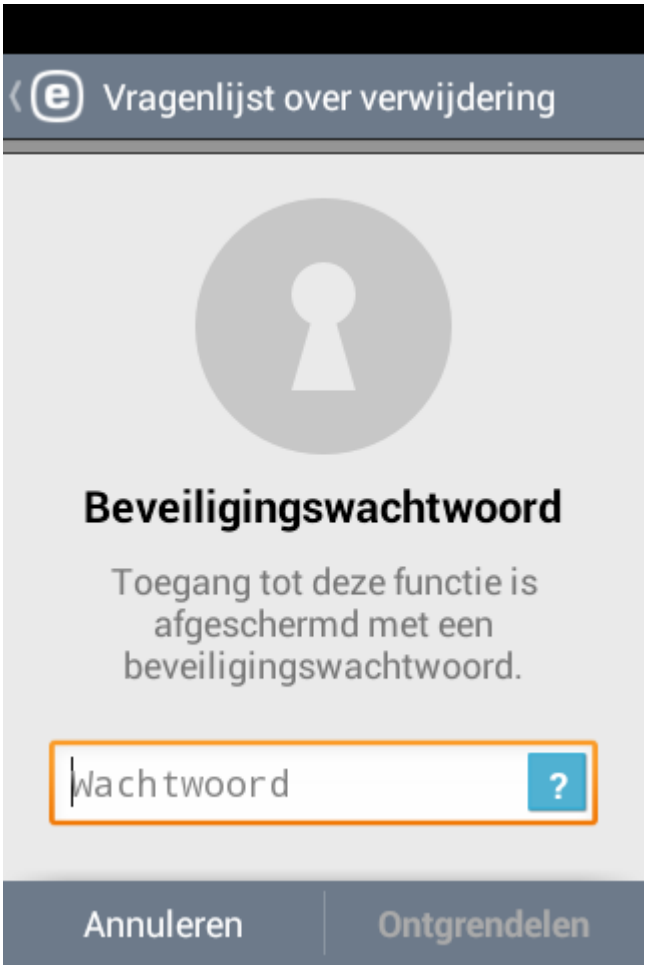


Als de toepassing op uw apparaat is geïnstalleerd, volgt u de aanwijzingen van de wizard Opstarten:

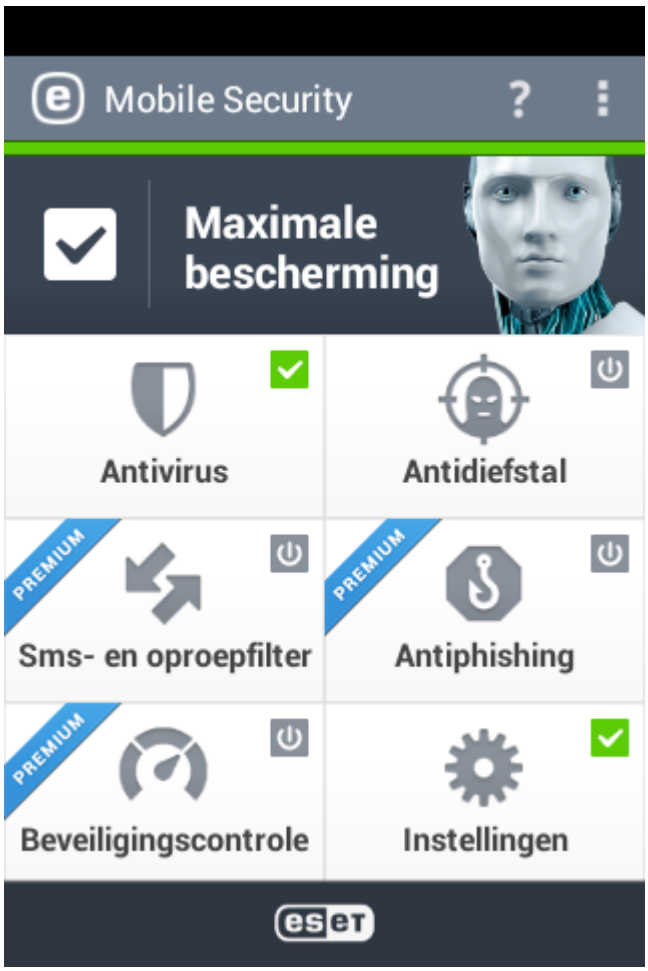
1. Selecteer de taal die u wilt gebruiken in ESET Mobile Security.
2. Selecteer het land waarin u woonachtig bent.
3. Als u wilt helpen met het verbeteren van ESET-producten door anoniem gegevens over het gebruik van toepassingen te verzenden, schakel dan de desbetreffende optie in.
4. Tik op **Accepteren**. Door hierop te tikken, gaat u akkoord met de licentieovereenkomst voor eindgebruikers.
5. Kies of u wilt deelnemen aan ESET Live Grid. Voor meer informatie over ESET Live Gridverwijzen wij u naar deze sectie 9.
6. Tik op **Volgende**.
7. Kies of u wilt dat ESET Mobile Security potentieel ongewenste toepassingen detecteert. Meer informatie over dergelijke toepassingen kunt u vinden in deze sectie 9.
8. Tik op **Volgende**.
9. Tik op **Voltooien**.

2.5 Verwijderen

Als u ESET Mobile Securitywilt verwijderen, gebruik dan de wizard Verwijderen in het hoofdmenu van ESET Mobile Security onder **Instellingen** > **Verwijderen**. Als u bescherming tegen verwijderen hebt ingeschakeld, wordt u gevraagd om uw beveiligingswachtwoord op te geven.



3. Licentie



Na een geslaagde installatie moet ESET Mobile Security worden geactiveerd. Als u de sectie **Licentie** wilt openen, tikt u op het pictogram Menu in het hoofdvenster van ESET Mobile Security (of drukt u op de knop **MENU** op uw apparaat) en tikt u op **Licentie**.

Activeringsmethoden zijn afhankelijk van of u ESET Mobile Security hebt gedownload vanaf de website van ESET, Amazon of Google Play.

- **Gratis proefversie** - selecteer deze optie als u geen licentie hebt en u ESET Mobile Security wilt evalueren voordat u overgaat tot aanschaf van het product. Voer uw **E-mailadres** in om ESET Mobile Security voor een beperkte periode te activeren. U ontvangt een bevestigingsbericht nadat het product is geactiveerd. U kunt een proeflicentie slechts eenmaal per apparaat activeren.
- **Toepassing activeren met uw gebruikersnaam en wachtwoord** - als u uw product hebt gekocht bij een ESET-distributeur, hebt u een gebruikersnaam en wachtwoord bij uw aankoop ontvangen. Voer de informatie die u hebt ontvangen in de velden **Gebruikersnaam** en**Wachtwoord** in.
- **Toepassing activeren met uw activeringscode** - indien u uw programma hebt ontvangen bij een nieuw apparaat (of een versie in de detailhandel hebt aangeschaft), hebt u een activeringscode bij uw aankoop ontvangen. Voer de informatie die u hebt ontvangen in het veld **Activeringscode** in en uw huidige contactadres in het veld **E-mailadres**. Uw nieuwe verificatiegegevens (gebruikersnaam en wachtwoord) zullen automatisch de activeringscode vervangen en zullen naar het door u opgegeven e-mailadres worden verzonden.
- **Licentie aanschaffen** - selecteer deze optie als u geen licentie hebt en deze wilt aanschaffen. U wordt doorgestuurd naar de webpagina van uw lokale ESET-distributeur.

Elke licentie is geldig voor een vaste periode. Nadat de licentie is verlopen, wordt u gevraagd of u deze wilt verlengen (het programma meldt u dit vooraf).

OPMERKING: tijdens de activering, moet het apparaat met internet zijn verbonden. Er wordt dan een kleine hoeveelheid gegevens gedownload.

4. Antivirus

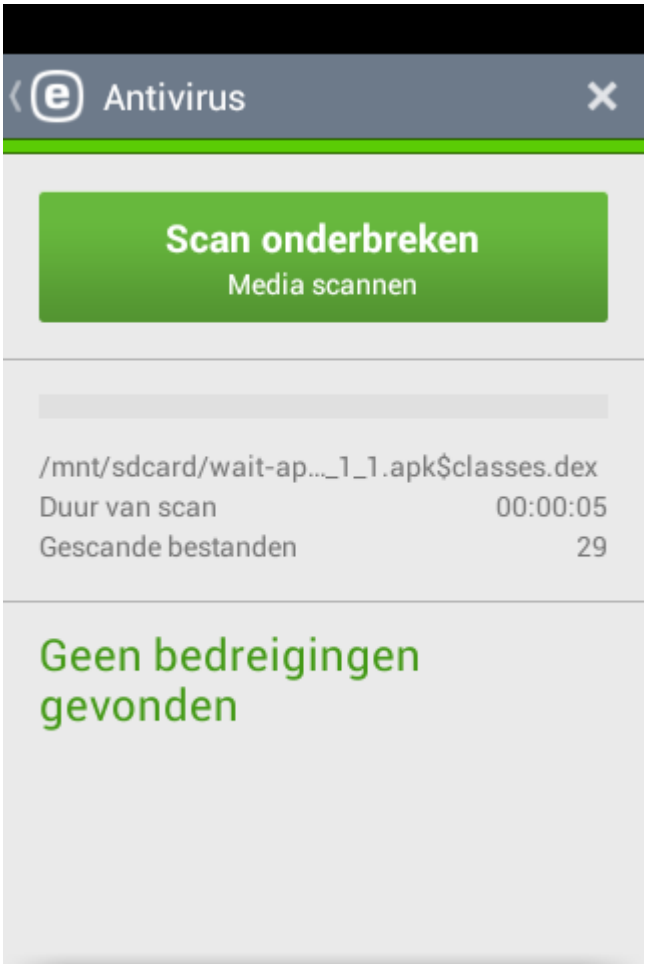
De module Antivirus beschermt uw apparaat tegen schadelijke code door bedreigingen te blokkeren en deze vervolgens op te schonen of in quarantaine te plaatsen.

Apparaat scannen

Apparaat scannen kan worden gebruikt om uw apparaat te controleren op infiltraties.

Bepaalde vooraf gedefinieerde bestandstypen worden standaard gescand. Tijdens een volledige apparaatscan worden het geheugen, actieve processen en hun afhankelijke DLL's (Dynamic Link Libraries), evenals bestanden die onderdeel zijn van de interne en verwisselbare opslag gecontroleerd. Een korte samenvatting van de scan wordt als logbestand opgeslagen in de sectie **Scanlogboeken** .

Als u een scan die wordt uitgevoerd wilt afbreken, tikt u op het pictogram .



Scantype

Er zijn 3 verschillende scanniveaus waaruit u kunt kiezen:

- **Snel** - Als u dit selecteert, scant ESET Mobile Security alleen geïnstalleerde toepassingen, DEX-bestanden (uitvoerbare bestanden voor het Android-besturingssysteem), SO-bestanden (bibliotheken) en ZIP-bestanden met een maximale scandiepte van 3 geneste archieven.
- **Slim** - Met Slimme scan wordt de inhoud van SD-kaarten gescand, afgezien van de bestandstypen die met de snelle scan worden gescand.
- **Diep** - Alle bestandstypen, ongeacht hun extensie worden gescand in zowel het interne geheugen als op de SD-kaart .

Automatisch scannen

Afgezien van Apparaatscan (op aanvraag) biedt ESET Mobile Security ook automatische scans. Als u wilt weten hoe u Scannen tijdens opladen en Geplande scan gebruikt, verwijzen wij u naar deze sectie 8.

Quarantaine

Het hoofddoel van de quarantaine is het veilig opslaan van geïnfecteerde bestanden. Zie de sectie Quarantaine 8 voor meer informatie.

Genegeerde bedreigingen

Voor meer informatie over deze functie, verwijzen wij u naar deze sectie 8.

Scanlogboeken

Met de optie **Scanlogboeken** beschikt u over uitvoerige gegevens over voltooide scans in de vorm van logboekbestanden. Meer informatie vindt u in dit hoofdstuk 8 .

Database met viruskenmerken bijwerken

ESET Mobile Security beschikt standaard over een updatetaak, zodat het programma regelmatig wordt bijgewerkt. Als u het programma handmatig wilt bijwerken, tikt u op **Database met viruskenmerken bijwerken**.

OPMERKING: om onnodig bandbreedteverbruik te voorkomen, worden updates uitgegeven wanneer ze nodig zijn als er een nieuwe bedreiging is toegevoegd. Hoewel updates gratis zijn bij uw actieve licentie, kunnen de kosten voor gegevensoverdracht door uw mobiele provider worden doorberekend.

Uitvoerige beschrijvingen van de **Geavanceerde instellingen** van Antivirus vindt u in de sectie Geavanceerde instellingen 8 .

4.1 Automatisch scannen

Scanniveau

Er zijn 3 verschillende scanniveaus waaruit u kunt kiezen. Deze instelling is van toepassing op Scannen tijdens opladen en Geplande scan:

- **Snel** - Als u deze optie selecteert, scant ESET Mobile Security alleen geïnstalleerde toepassingen, DEX-bestanden (uitvoerbare bestanden voor het Android-besturingssysteem), SO-bestanden (bibliotheken) en ZIP-bestanden met een maximale scandiepte van 3 geneste archieven.
- **Slim** - Met Slimme scan wordt de inhoud van de SD-kaart gescand, afgezien van de bestandstypen die met de snelle scan worden gescand.
- **Diep** - Alle bestandstypen, ongeacht hun extensie, worden gescand in zowel het interne geheugen als op de SD-kaart .

Scannen tijdens opladen

Als dit is geselecteerd,wordt het scannen automatisch gestart wanneer het apparaat niet actief is, volledig is opgeladen en op een oplader is aangesloten.

Geplande scan

Geplande scan is een functie waarmee u Apparaatscan automatisch op een vooraf ingesteld tijdstip kunt laten starten. Als u een scan wilt plannen, tikt u op de knop naast **Geplande scan** en geeft u de datums en tijden op waarop de scan moet worden gestart. Standaard zijn alle dagen van de week geselecteerd.

4.2 Quarantaine

Bestanden moeten in quarantaine worden geplaatst als ze niet kunnen worden opgeschoond, als het niet veilig of raadzaam is om ze te verwijderen, of als ze ten onrechte door ESET Mobile Security zijn gedetecteerd.

Bestanden die in quarantaine zijn geplaatst, kunnen worden bekeken in een logboek waarin de naam en de oorspronkelijke locatie van het geïnfecteerde bestand samen met de datum en tijd van in quarantaine plaatsen worden weergegeven.

Als u een bestand in quarantaine naar de oorspronkelijke locatie wilt terugzetten, tikt u op het bestand en op het pictogram . Wij raden u af om regelmatig bestanden die in quarantaine zijn geplaatst, terug te zetten.

Als u een bestand in quarantaine definitief uit uw apparaat wilt verwijderen, tikt u op het bestand en op het pictogram .

OPMERKING: als u een verdachte toepassing in quarantaine plaatst, maar deze later wilt installeren, wordt de toepassing automatisch uit de quarantaine verwijderd.

4.3 Genegeerde bedreigingen

Tijdens het scannen kunt u een nieuwe bedreiging aan de witte lijst toevoegen. Die bedreiging wordt dan bij toekomstige scans genegeerd.

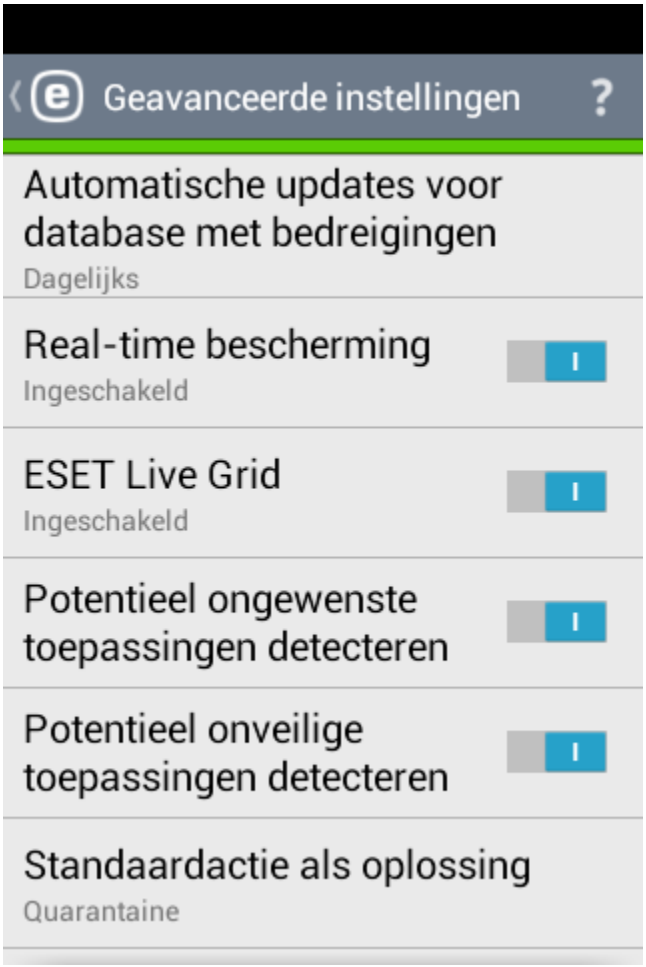
4.4 Scanlogboeken

Scanlogboeken worden gemaakt na elke geplande scan of na een handmatig geactiveerde apparaatscan.

Elk logboek bevat:

- datum en tijd van de gebeurtenis
- duur van de scan
- aantal gescande bestanden
- scanresultaat of fouten die tijdens de scan zijn ontdekt

4.5 Geavanceerde instellingen



Automatische updates voor de database met viruskenmerken.
Met deze optie kunt u het tijdsinterval instellen op basis waarvan updates voor de database met bedreigingen automatisch worden gedownload. Deze updates worden uitgegeven als dat nodig is wanneer er een nieuwe bedreiging aan de database is toegevoegd. Het wordt aangeraden deze instelling op de standaardwaarde te laten staan (dagelijks).

Real-time bescherming
Met deze optie kunt u de Real-time scanner in- en uitschakelen. Deze scanner wordt automatisch gestart als het systeem wordt gestart en scant bestanden die u gebruikt. De map *Downloads*, *.apk-installatiebestanden* en alle bestanden op de SD-kaart worden automatisch gescand nadat de SD-kaart is gekoppeld.

ESET Live Grid
is gebaseerd op het geavanceerde vroegtijdige waarschuwingssysteem ThreatSense.Net. **ESET Live Grid** is ontworpen om uw apparaat het hoogst mogelijke beveiligingsniveau te bieden. Hiermee worden de programma's en processen die op uw systeem worden uitgevoerd, continu gecontroleerd aan de hand van de nieuwste informatie van miljoenen ESET-gebruikers wereldwijd. Verder worden uw scans sneller en nauwkeuriger verwerkt naarmate de ESET Live Grid-database in de loop van de tijd steeds verder wordt uitgebreid. Hierdoor kunnen wij alle ESET-gebruikers betere proactieve bescherming en een hogere scansnelheid bieden. Wij raden aan dat u deze functie activeert. Hartelijk dank voor uw steun.

Potentieel ongewenste toepassingen detecteren
Een ongewenst programma is een programma waarin adware is opgenomen, dat een werkbalk installeert, uw zoekresultaten volgt of andere onduidelijke doelstellingen heeft. Er zijn bepaalde situaties denkbaar waarin u misschien van mening bent dat de voordelen van de ongewenste toepassing zwaarder wegen dan de risico's. Om deze reden kent ESET dergelijke toepassingen een lagere risicocategorie toe dan andere typen schadelijke software.

Potentieel onveilige toepassingen detecteren
Er zijn veel legitieme programma's die alleen zijn bedoeld om netwerkapparaten te beheren. Als zij echter in verkeerde handen zijn, kunnen ze voor schadelijke doelen worden misbruikt. Met de optie **Potentieel onveilige toepassingen detecteren** kunt u dergelijke bedreigingen opsporen. “Potentieel onveilige toepassingen” is de classificatie die wordt gebruikt voor commerciële, legitieme software. Deze classificatie omvat onder andere hulpprogramma's voor externe toegang, toepassingen voor het kraken van wachtwoorden en keyloggers.

Standaardactie als oplossing
Met deze instelling wordt bepaald welke actie wordt uitgevoerd nadat de scan is voltooid en er bedreigingen zijn gevonden. Als u **Verwijderen**selecteert, wordt het geïnfecteerde bestand verwijderd. Als u **Quarantaine**selecteert, wordt het geïnfecteerde bestand verplaatst naar de map Quarantaine 8.

Updateserver
Met deze optie kunt u kiezen of u de database met bedreigingen wilt bijwerken vanaf de **pre-releaseserver**. Pre-release updates zijn intern grondig getest en komen binnenkort voor het algemene publiek beschikbaar. U kunt voordeel hebben van de pre-release updates doordat u hiermee toegang hebt tot de meest recente detectiemethoden en oplossingen. Pre-release updates zijn echter mogelijk niet in alle gevallen stabiel genoeg. De lijst met huidige modules vindt u in de sectie Info: tik op het pictogram Menu  in het hoofdscherm van ESET Mobile Security (of druk op de knop **MENU** op uw apparaat) en tik op **Info** > **Toepassingsversie**. Het wordt aangeraden dat basisgebruikers de optie **Releaseserver** standaard ingeschakeld laten.

5. Antidiefstal

Met de functie Antidiefstal beschermt u uw mobiele apparaat tegen niet-geautoriseerde toegang.

Als u uw apparaat verliest of iemand steelt het en vervangt uw simkaart door een nieuwe (niet-vertrouwde) simkaart, dan wordt het apparaat automatisch vergrendeld door ESET Mobile Security en wordt er een waarschuwing ge-sms't naar een of meer door de gebruiker opgegeven telefoonnummers. In dit bericht wordt het telefoonnummer van de op dat moment geplaatste simkaart, het IMSI-nummer (International Mobile Subscriber Identity) en het IMEI-nummer (International Mobile Equipment Identity) van de telefoon vermeld. De niet-geautoriseerde gebruiker merkt niet dat dit bericht is verzonden omdat het automatisch wordt verwijderd uit de berichtenthreads van het apparaat. U kunt ook de GPS-coördinaten van uw verloren mobiele apparaat opvragen of op afstand alle opgeslagen gegevens van het apparaat wissen.

OPMERKING: Bepaalde functies van Antidiefstal (Simbescherming, Vertrouwde vrienden en Sms-tekstopdrachten) zijn niet beschikbaar op tablets die geen ondersteuning bieden voor berichtenuitwisseling.

Versie 3 van ESET Mobile Security kan via my.eset.com volledig in ESET Antidiefstal worden geïntegreerd. Hierdoor kunt u uw apparaat bewaken vanuit de webportal van ESET Antidiefstal, het apparaat vergrendelen, aangepaste berichten verzenden naar de vinder van het apparaat, een harde sirene activeren en gegevens op het apparaat op afstand wissen.

Tik op **Antidiefstal** in het hoofdmenu van het programma als u uw apparaat met Antidiefstal wilt beschermen. Een overzichtelijke wizard begeleidt u bij het instellen van een beveiligingswachtwoord, bij het instellen van bescherming tegen verwijdering, bij het toevoegen van uw simkaart als vertrouwde simkaart, bij het toevoegen van een vertrouwde vriend, het opgeven van contactgegevens en het inschakelen van sms-opdrachten. Nadat deze stappen zijn voltooid, kunt u uw apparaat koppelen aan uw my.eset.com-account.

5.1 my.eset.com

Als u al een my.eset.com-account hebt, tikt u op **Hebt u al een account?** en voert u uw e-mailadres en wachtwoord in om u aan te melden.

Als u geen my.eset.com-account hebt, tikt u op **Registreren** en vult u het registratieformulier in. Ga in uw postvak naar het bevestigingsbericht en klik op de koppeling om uw account te activeren. U kunt nu de beveiligingsfuncties van Antidiefstal gebruiken die u vanuit my.eset.com beheert.

Voor meer advies over het gebruik van Antidiefstal op my.eset.com verwijzen wij u naar de online-Help. Klik op **Help** rechtsboven in het scherm.

5.2 Optimalisatie

ESET Antidiefstal-optimalisatie is een meetbare technische beoordeling van de beveiligingsstatus van uw apparaat. ESET Antidiefstal onderzoekt uw systeem op de volgende problemen:

- Locatieservices uitgeschakeld
- GPS-satellieten niet gebruikt
- Schermvergrendeling niet beveiligd
- Mobiele gegevens niet ingeschakeld
- Google Play-services niet aanwezig

Voor elk beveiligingsprobleem kunt u tikken op **Instellingen wijzigen** om naar het scherm te gaan waar u dat specifieke probleem kunt oplossen. Als u niet wilt dat ESET Mobile Security een gebeurtenis als probleem rapporteert, tikt u op **Dit probleem negeren**.

5.3 Simbescherming

In de sectie **Simbescherming** staat de lijst met vertrouwde simkaarten die door ESET Mobile Security worden geaccepteerd. Als u een simkaart plaatst die niet in de lijst staat, wordt het scherm vergrendeld en wordt er via sms een waarschuwingsbericht verzonden naar uw **Vertrouwde vrienden**.

Als u een nieuwe simkaart wilt toevoegen, tikt u op het pictogram ➕. Zie deze sectie 10 voor meer informatie.

Als u een simkaart uit de lijst wilt verwijderen, raakt u de vermelding aan, houdt u deze vast en tikt u op het pictogram 🗑.

OPMERKING: Simbescherming is niet beschikbaar op bepaalde mobiele apparaten van het type CDMA en WCDMA.

5.3.1 Een nieuwe vertrouwde sim toevoegen

Geef een **naam voor de simkaart** op (bijv. Thuis, Werk) en het bijbehorende **IMSI**-nummer (International Mobile Subscriber Identity). IMSI wordt doorgaans aangegeven met een 15-cijferig lang nummer dat op uw simkaart is gedrukt. In bepaalde gevallen is het getal korter.

5.4 Vertrouwde vrienden

In de lijst **Vertrouwde vrienden** kunt u de telefoonnummers toevoegen en verwijderen die via sms een waarschuwingsbericht ontvangen als er een niet-vertrouwde simkaart in uw apparaat wordt geplaatst. Als u een nieuwe vertrouwde vriend wilt toevoegen, tikt u op **Toevoegen vanuit Contacten** en selecteert u een contact in uw lijst met contacten.

Als een persoon niet in uw lijst met contacten staat, tikt u op het pictogram ➕. Zie deze sectie 11 voor meer informatie.

Als u een contact uit de lijst wilt verwijderen, raakt u de contactvermelding in de lijst aan, houdt u deze vast en tikt u op

het pictogram  .

OPMERKING: als u zich in het buitenland bevindt, moeten alle telefoonnummers die aan de lijst worden toegevoegd de internationale toegangscode bevatten, gevolgd door het feitelijke nummer (bijvoorbeeld +1610100100).

5.4.1 Een nieuwe vertrouwde vriend toevoegen

Geef de naam van de vriend(in) op en zijn/haar telefoonnummer. Als het contact meerdere telefoonnummers heeft, wordt het waarschuwingsbericht naar alle bijbehorende nummers verzonden. Als u wilt toestaan dat deze vriend uw wachtwoord opnieuw kan instellen als u uw wachtwoord bent vergeten, selecteer dan de optie **Op afstand opnieuw instellen van wachtwoord toestaan** in.

5.5 Sms-tekstopdrachten

Sms-opdrachten op afstand (vergrendelen, sirene, zoeken en wissen) werken alleen als **Sms-tekstopdrachten** is ingeschakeld.

Als u uw apparaat verliest en het wilt vergrendelen, kunt u vanaf elk mobiel apparaat in deze indeling een sms-bericht voor vergrendelen op afstand naar uw telefoonnummer verzenden:
eset lock wachtwoord
Vervang *wachtwoord* door uw beveiligingswachtwoord. Nadat uw apparaat is vergrendeld, moet een niet-geautoriseerde gebruiker uw wachtwoord opgeven om het apparaat te kunnen ontgrendelen.

Als u uw apparaat wilt vergrendelen en een sirene wilt activeren, moet u een sms-bericht in de volgende indeling naar uw mobiele nummer sturen:
eset siren wachtwoord
De sirene wordt zelfs geactiveerd als het geluid van uw apparaat is gedempt.

Als u de GPS-coördinaten van uw mobiele apparaat wilt opvragen, stuurt u een sms-bericht in de volgende indeling naar uw mobiele nummer of het mobiele nummer van de niet-geautoriseerde gebruiker (als de simkaart al is vervangen):
eset find wachtwoord
U ontvangt een sms-bericht met de GPS-coördinaten van uw verdwenen apparaat, en een koppeling naar die locatie op Google Maps.

Als u alle gegevens wilt wissen die zijn opgeslagen op uw apparaat en alle geplaatste verwisselbare media, stuurt u een sms-bericht om op afstand te wissen in de volgende indeling naar uw apparaat:
eset wipe wachtwoord
Alle contacten, berichten, e-mails, geïnstalleerde toepassingen, uw Google-account en de inhoud van de SD-kaart worden definitief van uw apparaat gewist. Indien ESET Mobile Security niet is ingesteld als de apparaatbeheerder, worden alleen de contacten, berichten en de inhoud van de SD-kaart gewist.

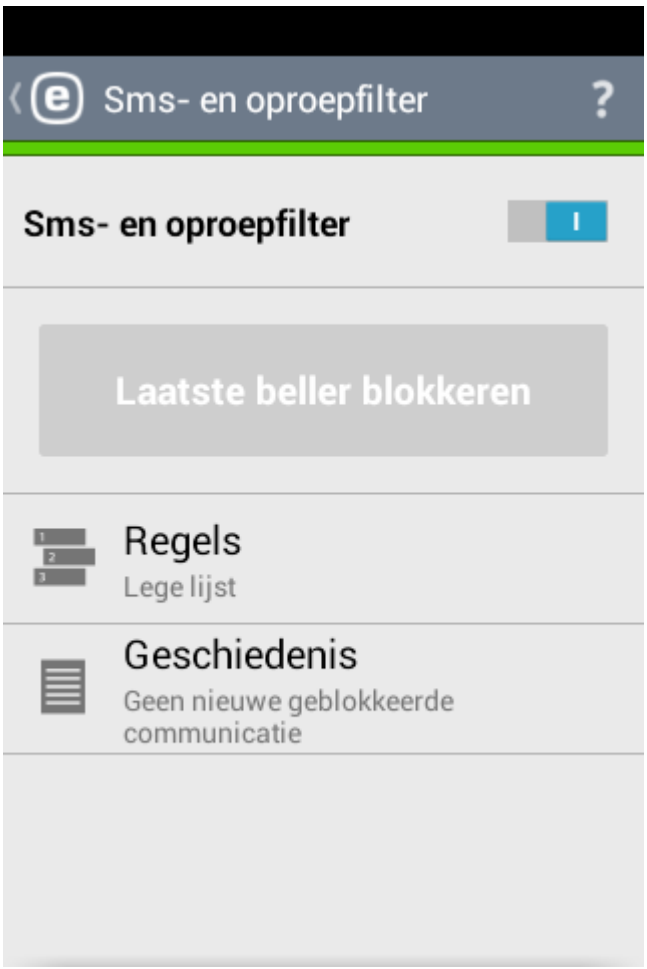
OPMERKING: uw wachtwoord is hoofdlettergevoelig. Het wachtwoord dat u invoert, moet exact overeenkomen met het wachtwoord dat u hebt opgegeven in de installatiewizard Antidiefstal.

5.6 Mijn contactgegevens

Als u uw apparaat als verdwenen markeert op my.eset.com, wordt de informatie van **Mijn contactgegevens** weergegeven op het scherm van uw vergrendelde apparaat, zodat de vinder contact met u kan opnemen.

Geef uw naam, apparaatbeschrijving, alternatief contactnummer (bijvoorbeeld telefoonnummer thuis of op het werk) of uw e-mailadres op.

6. Sms- en oproepfilter



Sms- en oproepfilter blokkeert inkomende sms/mms-berichten en inkomende/uitgaande oproepen op basis van uw regels.

Ongevraagde berichten zijn doorgaans advertenties van providers van mobiele services of berichten van onbekende of niet-opgegeven gebruikers. Het begrip *bericht blokkeren* verwijst naar het automatisch verplaatsen van een inkomend bericht naar het gedeelte **Geschiedenis**. Er wordt geen melding weergegeven wanneer er een inkomend bericht wordt geblokkeerd. Het voordeel hiervan is dat u niet wordt lastig gevallen met ongevraagde informatie, maar altijd de logboeken kunt controleren op berichten die onterecht zijn geblokkeerd.

OPMERKING: Sms- en oproepfilter werkt niet op tablets die geen ondersteuning bieden voor telefoneren en sms'en.

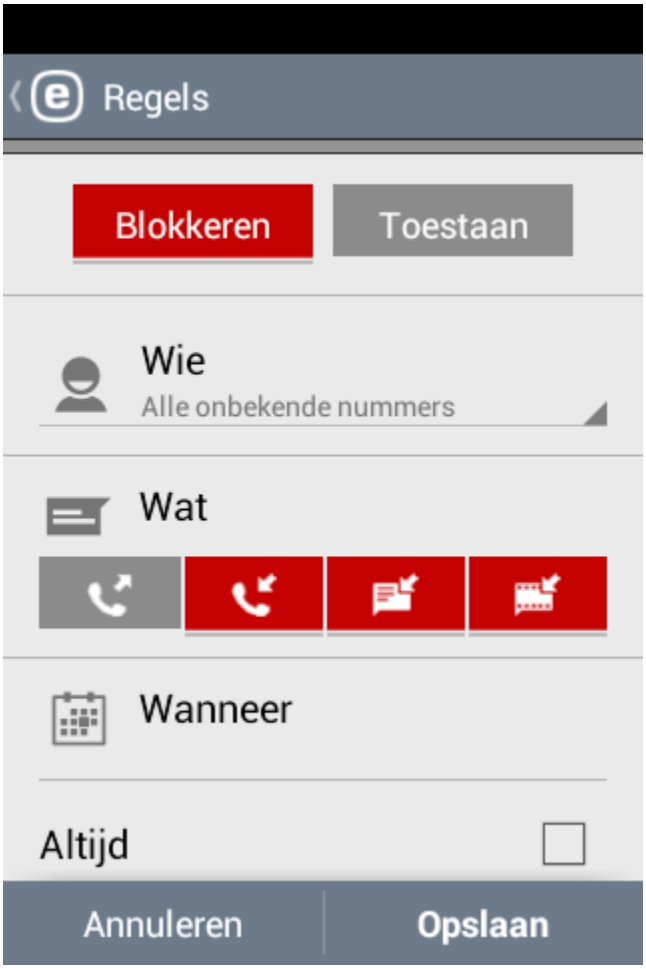
Als u berichten en oproepen van het laatst ontvangen telefoonnummer wilt blokkeren, tik dan op **Laatste beller blokkeren**. Hiermee wordt een nieuwe regel voor Sms- en oproepfilter gemaakt.

6.1 Regels

Als u een nieuwe regel wilt toevoegen, tikt u op het pictogram ➕. Meer informatie over het maken van een nieuwe regel vindt u in deze sectie 12.

Als u een bestaande regelvermelding uit de lijst **Regels** wilt verwijderen, raakt u de vermelding aan, houdt u deze vast en tikt u op het pictogram 🗑.

6.1.1 Een nieuwe regel toevoegen



Geef een groep telefoonnummers of een persoon op. **Alle onbekende nummers** omvat de telefoonnummers die u niet in uw lijst met contacten hebt opgeslagen. U kunt deze optie gebruiken om ongewenste telefoongesprekken te blokkeren (bijvoorbeeld van marketeers) of om te voorkomen dat kinderen onbekende nummers bellen. De optie **Alle bekende nummers** verwijst naar alle telefoonnummers die u in uw lijst met contacten hebt opgeslagen. **Verborgen nummers** heeft betrekking op bellers die hun telefoonnummer met opzet hebben verborgen via Calling Line Identification Restriction (CLIR).

Geef aan wat u wilt laten blokkeren of wat u wilt toestaan:

-  uitgaande oproepen
-  inkomende oproepen
-  inkomende tekstberichten (sms) of
-  inkomende multimediaberichten (mms)

Als u de regel alleen gedurende een bepaalde periode wilt laten gelden, schakel de optie **Altijd** onderaan dan uit en selecteer de datums en tijden waarop u wilt dat de regel van toepassing is. Standaard zijn alle dagen van de week geselecteerd. Deze functionaliteit komt mogelijk van pas als u 's nachts of gedurende het weekend niet gestoord wilt worden.

OPMERKING: als u zich in het buitenland bevindt, moeten alle telefoonnummers die aan de lijst worden toegevoegd de internationale toegangscode bevatten, gevolgd door het feitelijke nummer (bijvoorbeeld +1610100100).

6.2 Geschiedenis

In de sectie **Geschiedenis** kunt u de oproepen en berichten zien die Sms- en oproepfilter heeft geblokkeerd of toegestaan. Elk logboek bevat de naam van de gebeurtenis, het bijbehorende telefoonnummer, en de datum en tijd van de gebeurtenis. In de logboeken met sms- en mms-berichten staan ook de berichtteksten zelf.

Als u een regel voor een geblokkeerd telefoonnummer of contact wilt aanpassen, selecteert u de vermelding in de lijst door erop te tikken en op het pictogram  te tikken.

Als u de vermelding uit de lijst wilt verwijderen, selecteert u deze en tikt u op het pictogram  . Als u meerdere vermeldingen wilt verwijderen, raakt u een van de vermeldingen aan en houdt u deze vast, selecteert u de te verwijderen vermeldingen en tikt u op het pictogram  .

7. Antiphishing

De term *phishing* verwijst naar een criminele activiteit waarbij gebruik wordt gemaakt van 'sociaal engineering'. Hierbij worden gebruikers gemanipuleerd met als doel het verkrijgen van vertrouwelijke informatie. Met phishing wordt vaak geprobeerd toegang te krijgen tot gevoelige gegevens zoals bankrekeningnummers, creditcardnummers, pincodes of gebruikersnamen en wachtwoorden.

U wordt aangeraden **Antiphishing** ingeschakeld te laten. Alle potentiële phishingaanvallen die afkomstig zijn van websites of vanuit domeinen die in de ESET-malwaredatabase staan, worden geblokkeerd en er wordt een waarschuwingsbericht weergegeven waarin u van de aanval op de hoogte wordt gebracht.

Antiphishing kan worden geïntegreerd in alle gangbare browsers die beschikbaar zijn voor het Android-besturingssysteem (bijvoorbeeld Chrome en de standaardwebbrowser van Android).

OPMERKING: Antiphishing biedt geen bescherming als u in privémodus (incognito) surft.

7.1 Geschiedenis

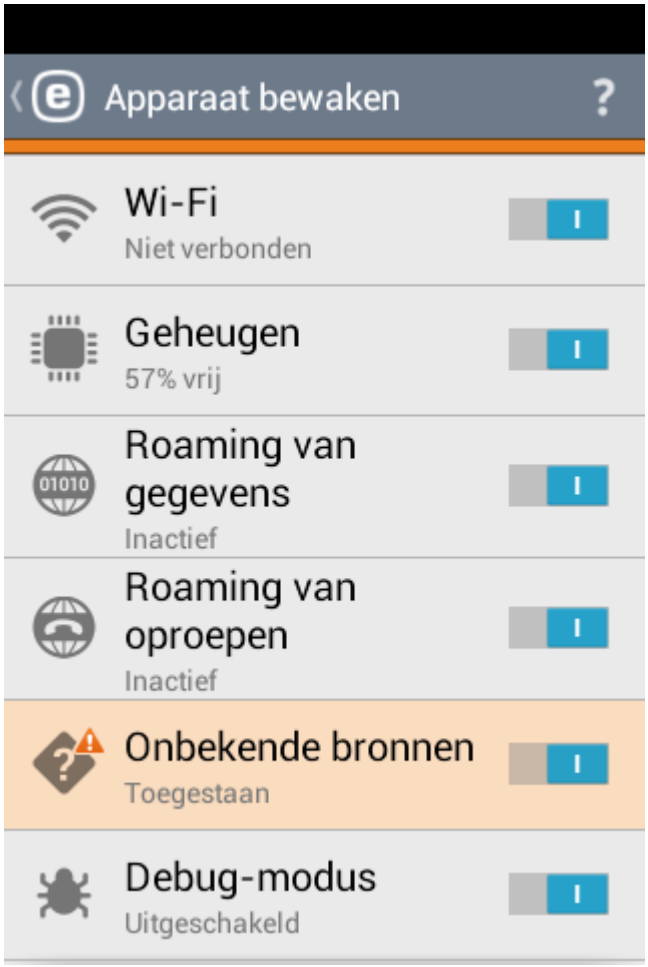
In de sectie **Geschiedenis** kunt u een lijst zien met alle phishingaanvallen die door ESET Mobile Security zijn geblokkeerd.

8. Beveiligingscontrole

Met Beveiligingscontrole kunt u belangrijke apparaatinstellingen en -machtigingen van geïnstalleerde toepassingen bewaken en wijzigen om beveiligingsrisico's te voorkomen.

Gebruik deze knoppen als u Beveiligingscontrole wilt in- of uitschakelen: 

8.1 Apparaatbeheer

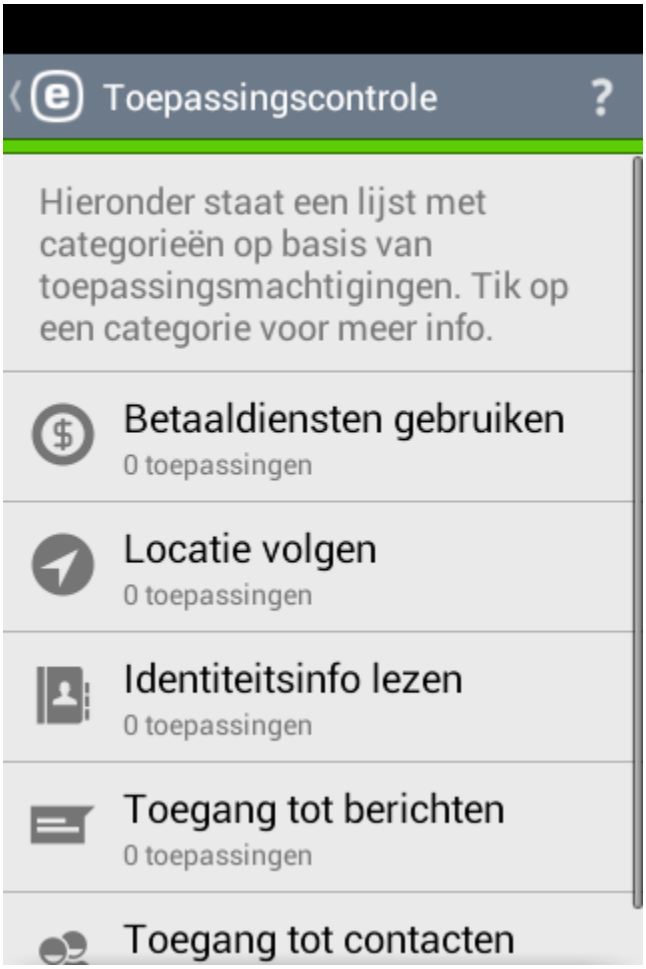


In de sectie **Apparaatbeheer** kunt u opgeven welke apparaatonderdelen moeten worden bewaakt door ESET Mobile Security.

Tik op elke optie om een gedetailleerde beschrijving van de optie en de actuele status ervan weer te geven.

Bepaalde opties zoals **Onbekende bronnen** en **Debug-modus** kunnen worden gewijzigd door te tikken op **Instellingen wijzigen**. Hiermee wordt u doorgestuurd naar het scherm met de instellingen van het Android-besturingssysteem.

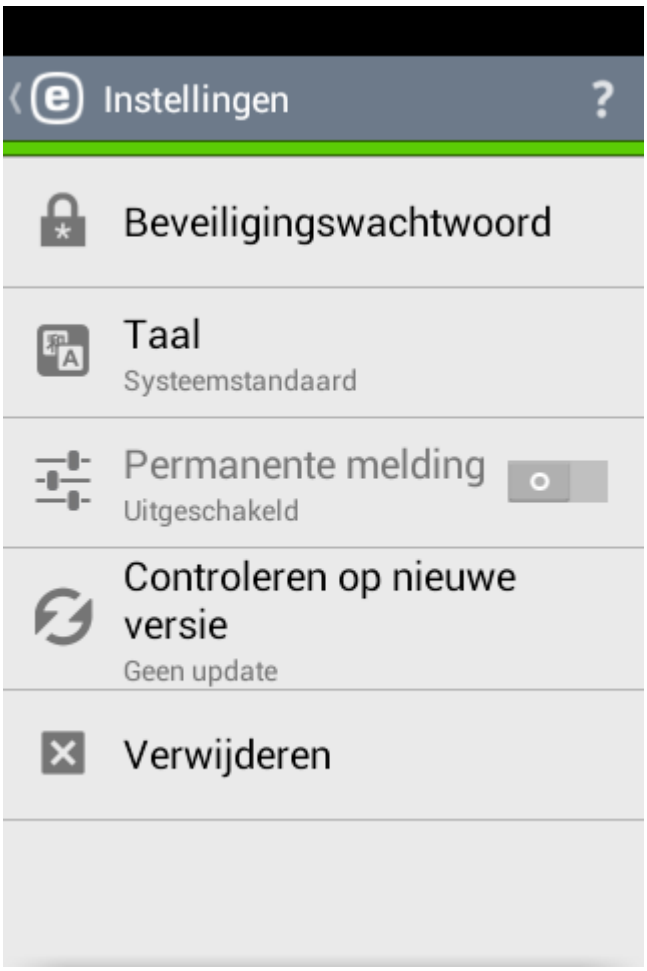
8.2 Toepassingscontrole



Bepaalde toepassingen die op uw apparaat zijn geïnstalleerd, hebben mogelijk toegang tot services die u geld kosten, uw locatie volgen, uw identiteitsgegevens, contacten of tekstberichten lezen. ESET Mobile Security controleert deze toepassingen en geeft een overzicht.

In de sectie **Toepassingscontrole** ziet u een lijst met toepassingen, gesorteerd op categorie. Tik op elke categorie om de uitvoerige beschrijving ervan te zien. U kunt informatie over de machtigingen van de toepassingen zien door op een bepaalde toepassing te tikken.

9. Instellingen



Beveiligingswachtwoord
Met deze optie kunt u een nieuw beveiligingswachtwoord instellen of het bestande wachtwoord wijzigen. Zie de sectie Beveiligingswachtwoord 16.

Taal
ESET Mobile Security wordt standaard geïnstalleerd in de taal die op uw apparaat als landinstelling is ingesteld (in de instellingen voor taal en toetsenbord van het Android-besturingssysteem). Als u de taal van de gebruikersinterface van de toepassing wilt wijzigen, tikt u op **Taal** en selecteert u de taal van uw keuze.

Icoon weergeven

ESET Mobile Security geeft een meldingspictogram weer boven in het venster (Android-statusbalk). Als u niet wilt dat dit pictogram wordt weergegeven, schakelt u deze optie uit: **Pictogram weergeven**.

Controleren op nieuwe versie
Voor maximale bescherming is het belangrijk de nieuwste versie te gebruiken van ESET Mobile Security. Tik op **Controleren op nieuwe versie** om te zien of er een nieuwere versie beschikbaar is om te downloaden.

Verwijderen
Als u ESET Mobile Securitywilt verwijderen, gebruik dan de wizard **Verwijderen** . De mappen van ESET Mobile Security en de quarantainemappen worden dan definitief verwijderd.

9.1 Beveiligingswachtwoord

Uw **beveiligingswachtwoord** is vereist om uw apparaat te ontgrendelen, toegang te krijgen tot functies die met een wachtwoord zijn afgeschermd (bijvoorbeeld Antidiefstal) en voor het verwijderen van ESET Mobile Security. De **herinneringszin** (indien ingesteld) geeft een hint weer om u aan uw wachtwoord te herinneren.

Als u uw wachtwoord bent vergeten, kunt u een sms sturen vanaf het mobiele nummer dat is opgeslagen in uw lijst met vertrouwde vrienden 10 naar uw mobiele nummer. Dit sms-bericht moet de volgende indeling hebben:
eset remote reset
Uw wachtwoord wordt opnieuw ingesteld en u wordt gevraagd een nieuw wachtwoord op te geven.

Als u geen vertrouwde vriend hebt opgegeven voorafgaande aan het vergrendelen van uw apparaat, kunt u een verzoek om het wachtwoord opnieuw in te stellen verzenden. Deze optie wordt actief op uw vergrendelde scherm na 2 mislukte pogingen om uw apparaat te ontgrendelen. U ontvangt een e-mail met een ontgrendelingscode op het e-mailadres van uw Google-account of het e-mailadres dat is opgegeven in **Antidiefstal** > **Mijn contactgegevens**. Geef de ontgrendelingscode op het vergrendelde scherm op. Geef nadat uw apparaat is ontgrendeld een nieuw beveiligingswachtwoord op in **Instellingen** > **Wachtwoord**.

U kunt uw beveiligingswachtwoord ook wijzigen op my.eset.com. Selecteer uw apparaat nadat u zich hebt aangemeld, klik op **Instellingen** en typ een nieuw wachtwoord.

BELANGRIJK: Kies uw wachtwoord met zorg uit. Om de beveiliging te verhogen en ervoor te zorgen dat uw wachtwoord moeilijker voor anderen is te raden, kunt u het beste een combinatie van kleine letters, hoofdletters en cijfers gebruiken.

10. Klantenservice

Medewerkers van de ESET-klantenservice staan klaar om administratieve hulp of technische ondersteuning te bieden met betrekking tot ESET Mobile Security of een ander ESET-product .

Als u rechtstreeks vanaf uw mobiele apparaat een ondersteuningsverzoek wilt versturen, tikt u op het pictogram Menu  in het hoofdscherm van ESET Mobile Security (of druk op de knop **MENU** op uw apparaat) en tik op **Klantenservice** > **Klantenservice**. Vul alle verplichte velden in.

ESET Mobile Security heeft geavanceerde functies voor logboekregistratie waarmee u mogelijke technische problemen kunt onderzoeken. Als u ESET een gedetailleerd toepassingslogboek wilt toesturen, moet u ervoor zorgen dat **Toepassingslogboek** is geselecteerd (standaard). Stuur uw verzoek door te tikken op **Verzenden**. Medewerkers van ESET-klantenservice nemen contact met u op via het e-mailadres dat u hebt opgegeven.