

ESET NOD32 Antivirus 4

Gebruikershandleiding

(bedoeld voor productversie 4.2 en hoger)

Microsoft® Windows® 7 / Vista / XP / NT4 / 2000 / 2003 / 2008



ESET NOD32 Antivirus 4

Copyright © 2010 by ESET, spol. s r. o.

ESET NOD32 Antivirus is ontwikkeld door ESET, spol. s r. o.

Ga voor meer informatie naar www.eset.com.

Alle rechten voorbehouden. Niets uit deze documentatie mag worden veeelvoudigd, openbaar gemaakt of overgedragen, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopie, opname, scan of enige andere manier, zonder schriftelijke toestemming van de auteur.

ESET, spol. s r. o. behoudt zich het recht voor de beschreven toepassingssoftware zonder voorafgaande kennisgeving te wijzigen.

Klantenservice wereldwijd: www.eset.eu/support

Klantenservice Noord-Amerika: www.eset.eu/support

REV.20100225-008

Inhoudsopgave

1. ESET NOD32 Antivirus 4	4
1.1 Nieuwe functies	4
1.2 Systeemvereisten	4
2. Installatie	5
2.1 Standaardinstallatie	5
2.2 Aangepaste installatie	6
2.3 Oorspronkelijke instellingen gebruiken	7
2.4 Gebruikersnaam en wachtwoord invoeren	7
2.5 Computerscan op aanvraag	8
3. Handleiding voor beginners	9
3.1 Inleiding tot gebruikersinterfaceontwerp – modi	9
3.1.1 Werking van het systeem controleren	9
3.1.2 Te volgen procedure als het programma niet correct werkt	10
3.2 Update-instellingen	10
3.3 Proxyserver instellen	10
3.4 Instellingen beveiligen	11
4. Werken met ESET NOD32 Antivirus	12
4.1 Antivirus- en antispywarebeveiliging	12
4.1.1 Real-timebeveiliging van bestandssysteem	12
4.1.1.1 Besturingsinstellingen	12
4.1.1.1.1 Te scannen media	12
4.1.1.1.2 Scannen op basis van gebeurtenissen	12
4.1.1.1.3 Aanvullende ThreatSense-parameters voor nieuwe en gewijzigde bestanden	12
4.1.1.1.4 Geavanceerde instellingen	12
4.1.1.2 Opschoonniveaus	12
4.1.1.3 Wanneer moet de configuratie voor real-timebeveiliging worden gewijzigd?	13
4.1.1.4 Real-timebeveiliging controleren	13
4.1.1.5 Te volgen procedure als real-timebeveiliging niet werkt	13
4.1.2 Beveiliging van e-mailclient	13
4.1.2.1 POP3-controle	13
4.1.2.1.1 Compatibiliteit	14
4.1.2.2 Integratie met e-mailclients	14
4.1.2.2.1 Meldingen toevoegen aan de hoofdtekst van een e-mailbericht	14
4.1.2.3 Infiltraties verwijderen	15
4.1.3 Beveiliging van webtoegang	15

4.1.3.1	HTTP, HTTPSs	15	4.8	Extern beheer	30
4.1.3.1.1	Adresbeheer	15	4.9	Licentie	30
4.1.3.1.2	Webbrowsers	15			
4.1.4	Computerscan	16	5. Geavanceerde gebruiker	31	
4.1.4.1	Type scan	16	5.1	Proxyserver instellen	31
4.1.4.1.1	Standaardscan	16	5.2	Instellingen importeren/exporteren	31
4.1.4.1.2	Aangepaste scan	16	5.2.1	Instellingen exporteren	31
4.1.4.2	Scandoelen	17	5.2.2	Instellingen importeren	31
4.1.4.3	Scanprofielen	17	5.3	Opdrachtregel	31
4.1.5	Protocolfiltering	17	5.4	ESET SysInspector	32
4.1.5.1	SSL	17	5.4.1	Gebruikersinterface en gebruik van de toepassing	32
4.1.5.1.1	Vertrouwde certificaten	18	5.4.1.1	Besturingselementen in programma	33
4.1.5.1.2	Uitgesloten certificaten	18	5.4.1.2	Navigeren in ESET SysInspector	33
4.1.6	Parameters voor ThreatSense-engine instellen	18	5.4.1.3	Vergelijken	34
4.1.6.1	Objecten instellen	18	5.4.1.4	SysInspector als onderdeel van ESET NOD32 Antivirus 4	34
4.1.6.2	Opties	18	5.4.1.5	SysInspector als onderdeel van ESET Smart Security 4	35
4.1.6.3	Opschonen	19	5.4.1.5.1	SysInspector als onderdeel van ESET Smart Security 4	35
4.1.6.4	Extensies	19	5.4.1.5.2	De structuur van het servicescript	35
4.1.6.5	Limiet	19	5.4.1.5.3	Servicescripts uitvoeren	36
4.1.6.6	Andere	20	5.5	ESET SysRescue	36
4.1.7	Er is een infiltratie gedetecteerd	20	5.5.1	Minimale vereisten	36
4.2	Het programma bijwerken	20	5.5.2	Een herstel-cd maken	36
4.2.1	Update-instellingen	21	5.5.2.1	Mappen	36
4.2.1.1	Updateprofielen	21	5.5.2.2	ESET Antivirus	37
4.2.1.2	Instellingen voor geavanceerde update	21	5.5.2.3	Geavanceerd	37
4.2.1.2.1	Updatemodus	21	5.5.2.4	Opstartbaar USB-apparaat	37
4.2.1.2.2	Proxyserver	22	5.5.2.5	Branden	37
4.2.1.2.3	Verbinding maken met LAN	22	5.5.3	Werken met ESET SysRescue	37
4.2.1.2.4	Updatekopieën maken – Mirror	23	5.5.3.1	ESET SysRescue in de praktijk	37
4.2.1.2.4.1	Bijwerken vanaf de mirror	23			
4.2.1.2.4.2	Updateproblemen met mirrors oplossen	24	6. Woordenlijst	38	
4.2.2	Updatetaken maken	24	6.1	Typen bedreigingen	38
4.3	Planner	25	6.1.1	Virussen	38
4.3.1	Doel van geplande taken	25	6.1.2	Wormen	38
4.3.2	Nieuwe taken maken	25	6.1.3	Trojaanse paarden	38
4.4	Quarantaine	25	6.1.4	Rootkits	38
4.4.1	Bestanden in quarantaine plaatsen	26	6.1.5	Adware	39
4.4.2	Terugzetten vanuit quarantaine	26	6.1.6	Spyware	39
4.4.3	Bestand verzenden vanuit quarantaine	26	6.1.7	Potentieel onveilige toepassingen	39
4.5	Logbestanden	26	6.1.8	Potentieel ongewenste toepassingen	39
4.5.1	Logbestanden onderhouden	27			
4.6	Gebruikersinterface	27			
4.6.1	Waarschuwingen en meldingen	28			
4.7	ThreatSense.Net	28			
4.7.1	Verdachte bestanden	29			
4.7.2	Statistieken	29			
4.7.3	Verzending	30			

1. ESET NOD32 Antivirus 4

ESET NOD32 Antivirus 4 is de opvolger van het bekroonde product ESET NOD32 Antivirus 2.* Dit pakket maakt gebruik van de scansnelheid en nauwkeurigheid van ESET NOD32 Antivirus, mogelijk gemaakt door de meest recente versie van de ThreatSense®-scanengine.

De geïmplementeerde geavanceerde technieken zijn in staat om op proactieve wijze virussen, spyware, Trojaanse paarden, wormen, adware en rootkits te blokkeren zonder het systeem te vertragen of u lastig te vallen terwijl u werkt of speelt op de computer.

1.1 Nieuwe functies

De lange ervaring op het gebied van ontwikkeling van onze experts heeft geresulteerd in de geheel nieuwe architectuur van het programma ESET NOD32 Antivirus, die garant staat voor maximale detectie en minimale systeemvereisten.

• Antivirus en antispysware

Deze module is gebaseerd op de ThreatSense®-scantechnologie, die voor het eerst is gebruikt in het bekroonde NOD32 Antivirus-systeem. De ThreatSense®-technologie is geoptimaliseerd en verbeterd met de nieuwe ESET NOD32 Antivirus-architectuur.

Functie	Omschrijving
Verbeterd opschoningsproces	Het opschoningsproces van het antivirusstelsel is verbeterd. De meeste gedetecteerde infiltraties kunnen nu worden verwijderd zonder tussenkomst van de gebruiker.
Achtergrond-scanmodus	Computerscans kunnen op de achtergrond worden uitgevoerd zonder dat dit ten koste gaat van de systeemprestaties.
Kleinere update-bestanden	Door kernoptimalisatieprocessen zijn de updatebestanden kleiner dan in versie 2.7. Bovendien zijn de updatebestanden nu beter beveiligd tegen beschadiging.
Beveiliging van veelgebruikte e-mailclients	Inkomende e-mail kan nu niet alleen in MS Outlook worden gescand maar ook in Outlook Express, Windows Mail, Windows Live Mail en Mozilla Thunderbird.
Diverse kleine verbeteringen	<ul style="list-style-type: none">– Hoge snelheid en verwerkingscapaciteit dankzij rechtstreekse toegang tot bestandssystemen– Blokkering van de toegang tot geïnfecteerde bestanden– Optimalisatie voor Windows Beveiligingscentrum, inclusief Vista

• Overige

Functie	Omschrijving
ESET SysRescue	Met ESET SysRescue kan een gebruiker een cd, een dvd of een USB-bestand maken met ESET NOD32 Antivirus. Vervolgens kan het programma onafhankelijk van het besturingssysteem worden uitgevoerd. Dit programma is zeer geschikt om lastig te verwijderen infiltraties te elimineren.
ESET SysInspector	ESET SysInspector is een toepassing waarmee u een grondige inspectie van uw computer kunt uitvoeren. Deze handige toepassing is nu rechtstreeks geïntegreerd in ESET NOD32 Antivirus. Als u via de optie Help en ondersteuning > Verzoek om ondersteuning van klantenservice (aanbevolen) contact opneemt met onze klantenservice, kunt u desgewenst een door ESET SysInspector gemaakte momentopname van de computer meesturen.
Document-bescherming	Deze bescherming houdt in dat Microsoft Office-documenten worden gescand voordat ze worden geopend, evenals bestanden die automatisch worden gedownload door Internet Explorer, zoals Microsoft ActiveX-elementen.
Zelfverdediging	De nieuwe zelfverdedigingstechnologie beschermt onderdelen van ESET NOD32 Antivirus tegen uitschakeling.
Gebruikersinterface	De gebruikersinterface kan nu ook in de tekstmodus worden gebruikt, zodat ESET NOD32 Antivirus kan worden bediend via het toetsenbord. Het voordeel hiervan is dat gebruikers met een visuele handicap die werken met een schermlezer, ESET NOD32 Antivirus optimaal kunnen gebruiken.

1.2 Systeemvereisten

Het systeem moet voldoen aan de volgende hardware- en softwarevereisten om ESET NOD32 Antivirus probleemloos uit te voeren:

ESET NOD32 Antivirus:

Windows NT4 SP6, 2000, XP	400 MHz 32-bits/64-bits (x86/x64) 128 MB RAM systeemgeheugen 130 MB beschikbare schijfruimte Super VGA (800 × 600)
Windows 7, Vista	1 GHz 32-bits/64-bits (x86/x64) 512 MB RAM systeemgeheugen 130 MB beschikbare schijfruimte Super VGA (800 × 600)

ESET NOD32 Antivirus Business Edition:

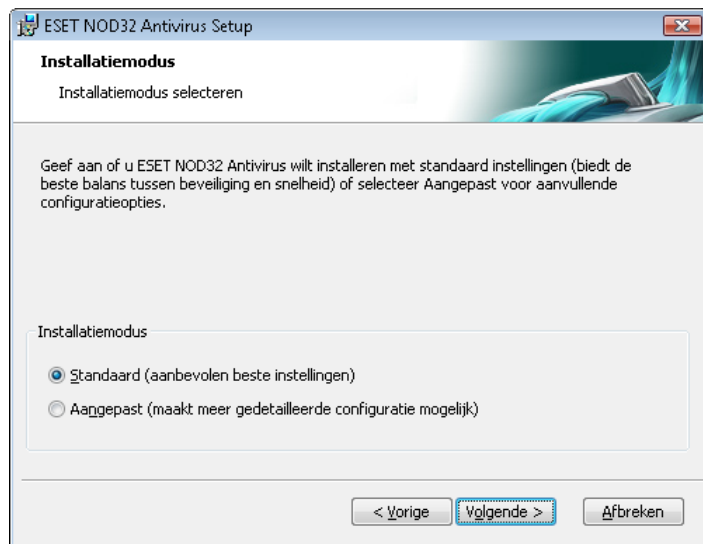
Windows NT4 SP6, 2000, 2000 Server, XP, 2003 Server	400 MHz 32-bits/64-bits (x86/x64) 128 MB RAM systeemgeheugen 130 MB beschikbare schijfruimte Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz 32-bits/64-bits (x86/x64) 512 MB RAM systeemgeheugen 130 MB beschikbare schijfruimte Super VGA (800 × 600)

OPMERKING: Anti Stealth en zelfverdediging zijn niet beschikbaar in Windows NT4 SP6.

2. Installatie

Na aanschaf kunt u het installatieprogramma van ESET NOD32 Antivirus downloaden als MSI-pakket vanaf de website van ESET. Nadat u het installatieprogramma hebt gestart, wordt u met de installatiewizard door de standaardinstallatie geleid. Er zijn twee typen installatie beschikbaar, met verschillende installatieniveaus:

1. Standaardinstallatie
2. Aangepaste installatie



2.1 Standaardinstallatie

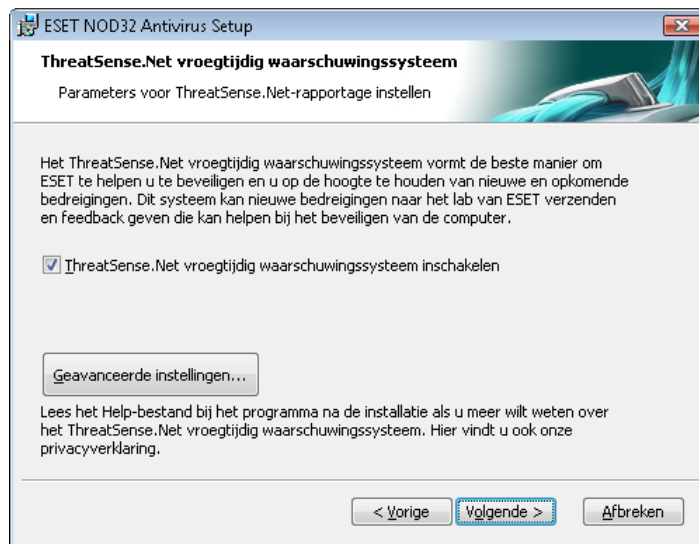
De standaardinstallatie wordt aanbevolen voor gebruikers die ESET NOD32 Antivirus willen installeren met de standaardinstellingen. De standaardinstellingen van het programma bieden het maximale beveiligingsniveau, wat zeer nuttig is voor gebruikers die geen gedetailleerde instellingen willen configureren.

De eerste, uiterst belangrijke, stap is het invoeren van de gebruikersnaam en het wachtwoord voor het automatisch bijwerken van het programma. Dit speelt een belangrijke rol bij het bieden van een constante beveiliging van het systeem.



Typ uw **gebruikersnaam** en **wachtwoord** in de bijbehorende velden. Dit zijn de verificatiegegevens die u hebt ontvangen na de aanschaf of registratie van het product. Als u uw gebruikersnaam en wachtwoord niet bij de hand hebt, selecteert u de optie **Parameters voor de update later instellen**. Verificatiegegevens kunnen op elk gewenst moment later worden ingevoerd, rechtstreeks vanuit het programma.

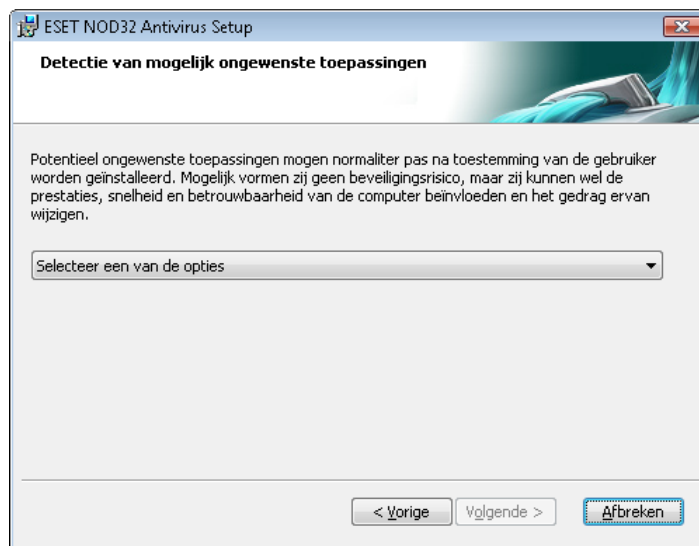
De volgende stap in de installatie is configuratie van het ThreatSense.Net systeem voor vroegtijdige waarschuwing. Het ThreatSense.Net systeem voor vroegtijdige waarschuwing zorgt ervoor dat ESET continu direct wordt geïnformeerd over nieuwe infiltraties om klanten snel bescherming te kunnen bieden. Met het systeem kunnen nieuwe bedreigingen naar het viruslaboratorium van ESET worden verzonden, waar ze worden geanalyseerd, verwerkt en toegevoegd aan de databases met viruskenmerken.



Het selectievakje **ThreatSense.Net systeem voor vroegtijdige waarschuwing inschakelen** is standaard ingeschakeld. Hiermee wordt deze functie geactiveerd. Klik op **Geavanceerde instellingen...** om gedetailleerde instellingen voor het verzenden van verdachte bestanden te wijzigen.

De volgende stap in het installatieproces is het configureren van **Detectie van mogelijk ongewenste toepassingen**. Mogelijk ongewenste toepassingen zijn niet per se schadelijk, maar kunnen het gedrag van het besturingssysteem vaak negatief beïnvloeden.

Deze toepassingen worden vaak meegeleverd met andere programma's en vallen nauwelijks op tijdens de installatie. Hoewel bij deze toepassingen gewoonlijk een melding wordt weergegeven tijdens de installatie, kunnen ze eenvoudig zonder uw toestemming worden geïnstalleerd.



Schakel de optie **Detectie van mogelijk ongewenste toepassingen inschakelen** in om ESET NOD32 Antivirus in staat te stellen dit type bedreiging te detecteren (aanbevolen).

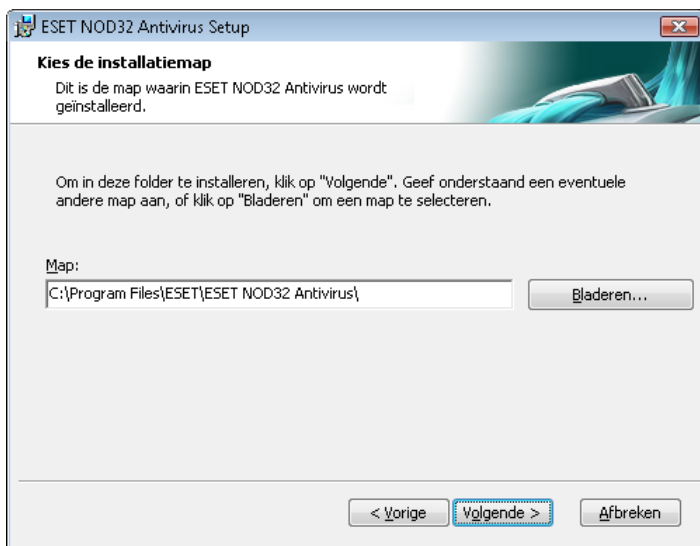
De laatste stap in de modus voor standaardinstallatie is het bevestigen van de installatie door op de knop **Installeren** te klikken.



2.2 Aangepaste installatie

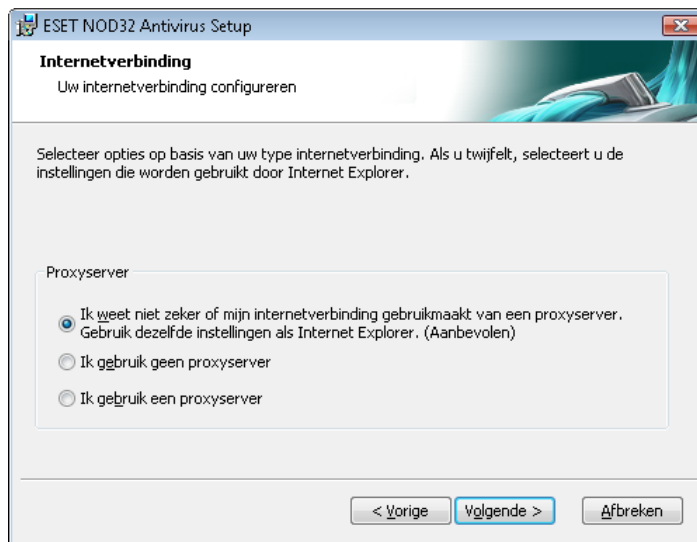
De **aangepaste** installatie is bedoeld voor gebruikers die ervaring hebben met het aanpassen van programma-instellingen en die tijdens de installatie geavanceerde instellingen willen wijzigen.

De eerste stap is het selecteren van de bestemmingslocatie voor de installatie. Standaard wordt het programma geïnstalleerd in de map C:\Program Files\ESET\ESET NOD32 Antivirus\. Klik op **Bladeren...** om de locatie te wijzigen (niet aanbevolen).

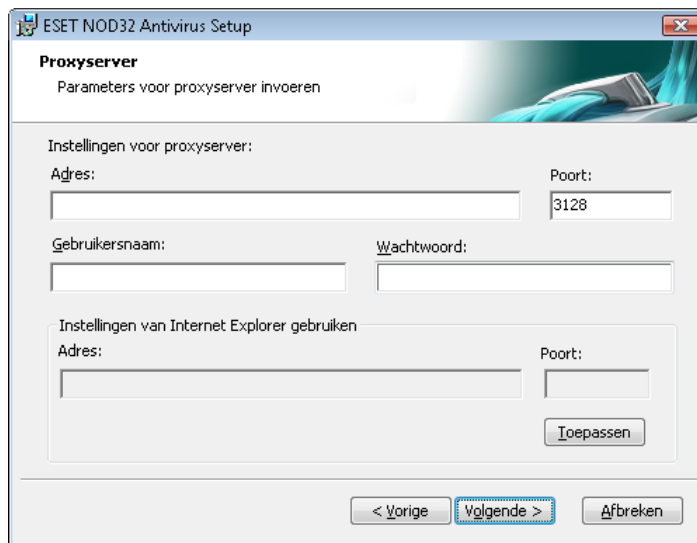


Voer vervolgens uw **gebruikersnaam en wachtwoord** in. Deze stap is hetzelfde als in de standaardinstallatie (zie pagina 5).

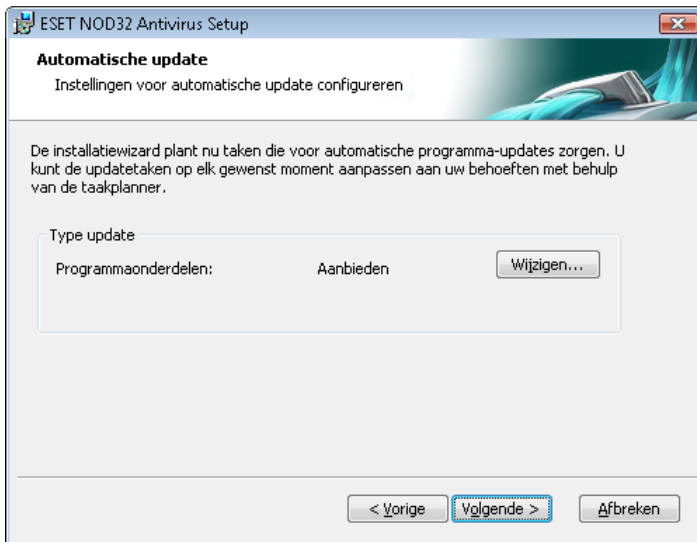
Klik, nadat u uw gebruikersnaam en wachtwoord hebt ingevoerd, op **Volgende** om uw internetverbinding te configureren.



Als u een proxyserver gebruikt, moet deze correct worden geconfigureerd zodat updates van de viruskenmerken naar behoren werken. Als u niet weet of u een proxyserver gebruikt om verbinding met internet te maken, selecteert u **Ik weet niet zeker of mijn internetverbinding gebruikmaakt van een proxyserver. Gebruik dezelfde instellingen als Internet Explorer** en klik op **Volgende**. Als u geen proxyserver gebruikt, selecteert u de bijbehorende optie.

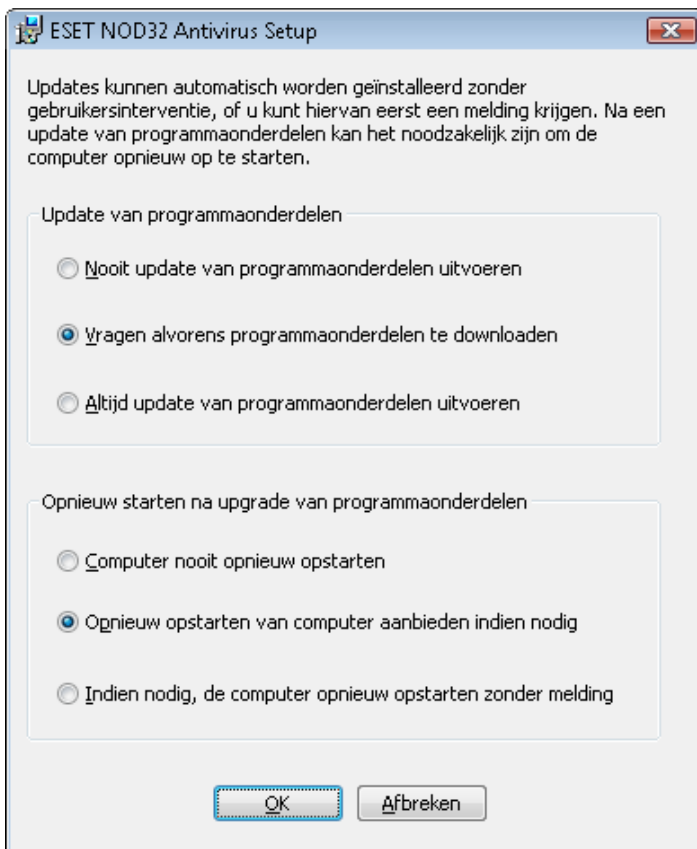


U kunt de instellingen van uw proxyserver configureren door **Ik gebruik een proxyserver** in te schakelen en op **Volgende** te klikken. Geef het IP-adres of de URL van uw proxyserver op in het veld **Adres**. Geef in het veld **Poort** de poort op waarop de proxyserver verbindingen accepteert (standaard is dit 3128). Als de proxyserver verificatie vereist, moet u een geldige gebruikersnaam en een geldig wachtwoord invoeren om toegang tot de proxyserver te verkrijgen. De instellingen voor de proxyserver kunnen desgewenst ook worden gekopieerd vanuit Internet Explorer. Dit kunt u doen door op **Toepassen** te klikken en de selectie te bevestigen.



Klik op **Volgende** om naar het venster **Instellingen voor automatische update configureren** te gaan. Met deze stap kunt u aangeven op welke manier automatische updates van programmaonderdelen op uw systeem moeten worden afgehandeld. Klik op **Wijzigen...** om toegang te verkrijgen tot de geavanceerde instellingen.

Als u niet wilt dat programmaonderdelen worden bijgewerkt, selecteert u **Nooit update van programmaonderdelen uitvoeren**. Als u de optie **Vragen alvorens programmaonderdelen te downloaden** inschakelt, wordt een bevestigingsvenster voor het downloaden van programmaonderdelen weergegeven. U kunt automatische upgrades van programmaonderdelen inschakelen door de optie **Programmaonderdeel bijwerken indien beschikbaar** te selecteren.



OPMERKING: na een upgrade van een programmaonderdeel moet de computer doorgaans opnieuw worden opgestart. De aanbevolen instelling is: **Indien nodig, computer opnieuw opstarten zonder melding**.

De volgende stap van de installatie is het invoeren van een wachtwoord voor het beveiligen van programmaparameters. Kies een wachtwoord waarmee u het programma wilt beveiligen. Typ het wachtwoord opnieuw om het te bevestigen.

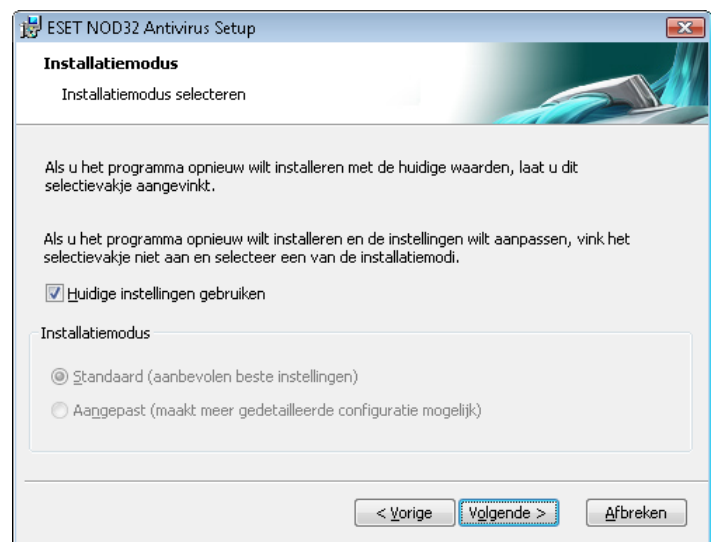


De stappen **Configuratie van het ThreatSense.Net systeem voor vroegtijdige waarschuwing** en **Detectie van mogelijk ongewenste toepassingen** zijn hetzelfde als voor de standaardinstallatie (zie pagina 5).

In de laatste stap wordt een venster weergegeven waarin u toestemming geeft voor de installatie.

2.3 Oorspronkelijke instellingen gebruiken

Als u ESET NOD32 Antivirus opnieuw installeert, wordt de optie **Huidige instellingen gebruiken** weergegeven. Schakel deze optie in om instellingsparameters van de oorspronkelijke installatie over te dragen naar de nieuwe.



2.4 Gebruikersnaam en wachtwoord invoeren

Voor een optimale werking is het van belang dat het programma automatisch wordt bijgewerkt. Dit is alleen mogelijk als de juiste gebruikersnaam en wachtwoord worden ingevoerd in de update-instellingen.

Als u uw gebruikersnaam en wachtwoord niet hebt ingevoerd tijdens de installatie, kunt u dit nu doen. Klik in het hoofdvenster van het programma op **Update** en vervolgens op **Gebruikersnaam en wachtwoord invoeren...** Typ de gegevens die u hebt ontvangen bij uw productlicentie in het venster **Licentiedetails**.



2.5 Computerscan op aanvraag

Nadat ESET NOD32 Antivirus is geïnstalleerd, moet een computerscan worden uitgevoerd om te controleren op de aanwezigheid van schadelijke code. U kunt snel beginnen met scannen door **Computerscan** te selecteren in het hoofdmenu en vervolgens **Standaardscan** te selecteren in het hoofdvenster van het programma. Zie het hoofdstuk "Computerscan" voor meer informatie over de functie Computerscan.



3. Handleiding voor beginners

Dit hoofdstuk biedt een eerste overzicht van ESET NOD32 Antivirus en de basisinstellingen van het programma.

3.1 Inleiding tot gebruikersinterfaceontwerp – modi

Het hoofdvenster van ESET NOD32 Antivirus is onderverdeeld in twee hoofdgedeelten. De kolom aan de linkerkant biedt toegang tot het gebruikersvriendelijke hoofdmenu. Het hoofdvenster van het programma aan de rechterkant dient voor het weergeven van informatie over de optie die is geselecteerd in het hoofdmenu.

Hieronder volgt een beschrijving van de knoppen binnen het hoofdmenu:

Beveiligingsstatus – In een gebruikersvriendelijke vorm wordt hier informatie verstrekt over de beveiligingsstatus van ESET NOD32 Antivirus. Als de geavanceerde modus is geactiveerd, wordt de status van alle beveiligingsmodules weergegeven. Klik op een module om de huidige status hiervan te bekijken.

Computerscan – In dit gedeelte kan de gebruiker de computerscan op aanvraag configureren en starten.

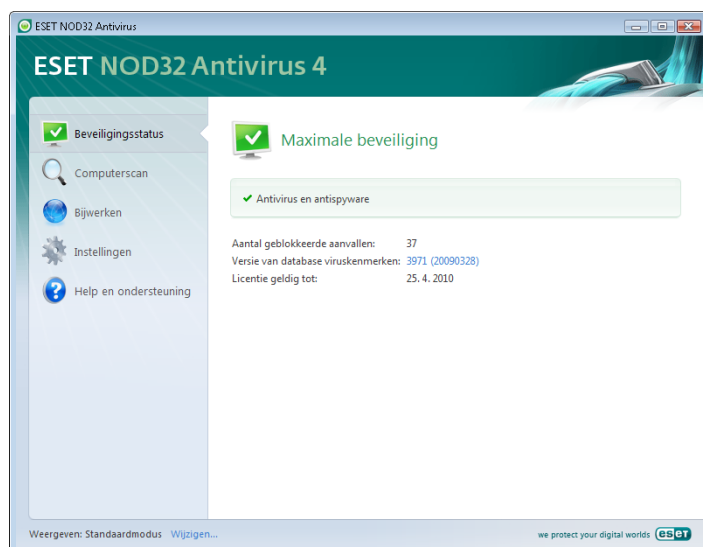
Update – Selecteer deze optie om toegang te krijgen tot de updatemodule waarmee updates van de database met viruskenmerken worden beheerd.

Instellingen – Selecteer deze optie om het beveiligingsniveau van uw computer aan te passen. Als de geavanceerde modus is geactiveerd, worden de submenu's van de module voor antivirus- en antispywarebeveiliging weergegeven.

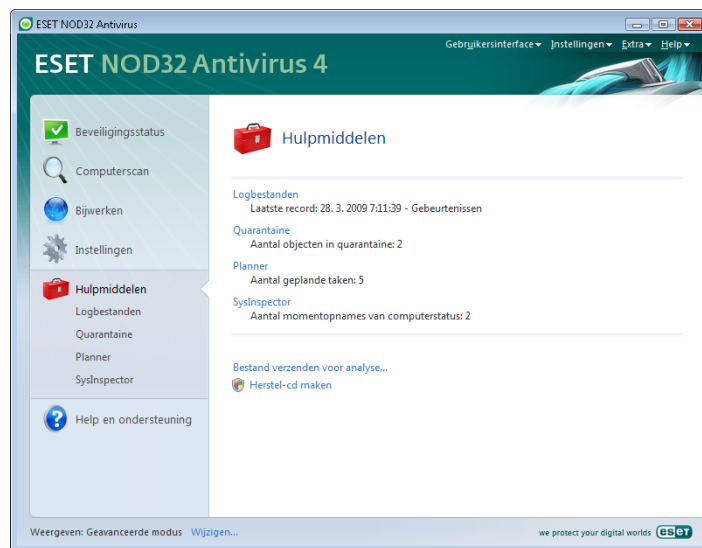
Hulpmiddelen – Deze optie is alleen beschikbaar in de geavanceerde modus. Biedt toegang tot Logbestanden, Quarantaine en de Planner.

Help en ondersteuning – Selecteer deze optie om toegang te krijgen tot Help-bestanden, de ESET-knowledgebase en de website van ESET en om een verzoek om technische ondersteuning te verzenden.

De gebruikersinterface van ESET NOD32 Antivirus stelt gebruikers in staat te schakelen tussen de modi Standaard en Geavanceerd. Als u wilt schakelen tussen modi, klikt u op de koppeling **Weergave** in de linkerbenedenhoek van het hoofdvenster van ESET NOD32 Antivirus. Klik op deze knop om de gewenste weergavemodus te selecteren.



De standaardmodus biedt toegang tot functies die zijn vereist voor veelgebruikte bewerkingen. Er worden geen geavanceerde opties weergegeven.

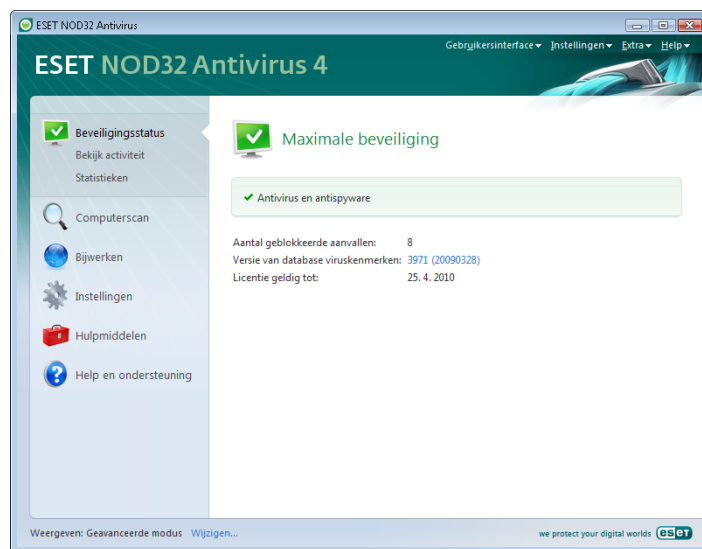


Als u schakelt naar de geavanceerde modus, wordt de optie **Hulpmiddelen** toegevoegd aan het hoofdmenu. Met de optie Hulpmiddelen heeft de gebruiker toegang tot de Planner en Quarantaine, en kan de gebruiker logbestanden van ESET NOD32 Antivirus bekijken.

OPMERKING: alle verdere instructies in deze handleiding worden uitgevoerd in de geavanceerde modus.

3.1.1 Werking van het systeem controleren

U kunt de **beveiligingsstatus** bekijken door op deze optie boven aan het hoofdmenu te klikken. Het submenu **Antivirus en antispyware** wordt hieronder weergegeven en een statusoverzicht van de werking van ESET NOD32 Antivirus wordt weergegeven in het hoofdvenster van het programma. Klik op Antivirus en antispyware in het hoofdvenster van het programma om de status van de individuele beveiligingsmodules te bekijken.



Als de ingeschakelde modules correct werken, zijn ze voorzien van een groen vinkje. Als dit niet het geval is, wordt een rood uitroepteken of een oranje waarschuwpictogram weergegeven en wordt aanvullende informatie over de module weergegeven in het bovenste deel van het venster. Tevens ziet u hier mogelijke oplossingen voor het probleem met de module. U kunt de status van individuele modules wijzigen door op **Instellingen** in het hoofdmenu te klikken en op de gewenste module te klikken.

3.1.2 Te volgen procedure als het programma niet correct werkt

Als ESET NOD32 Antivirus een probleem met een van de beveiligingsmodules detecteert, wordt dit gemeld in het venster **Beveiligingsstatus**. Ook wordt hier een mogelijke oplossing voor het probleem aangeboden.

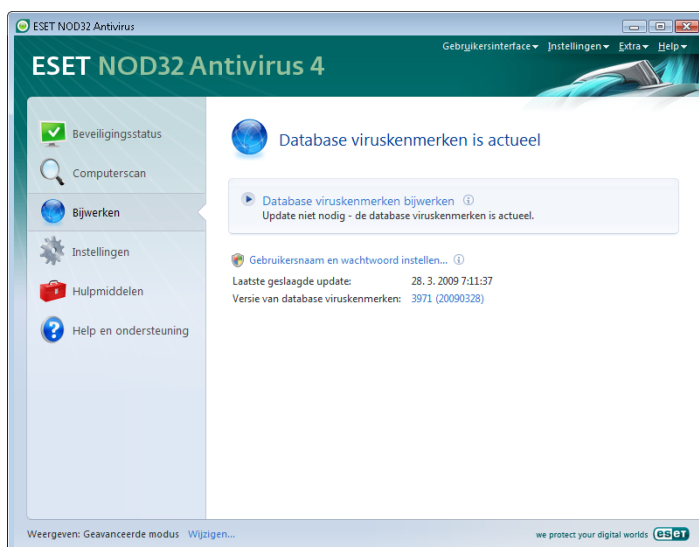


Als het niet mogelijk is om het probleem op te lossen door middel van de lijst met bekende problemen en oplossingen, klikt u op **Help en ondersteuning** om toegang te krijgen tot de Help-bestanden of om de knowledgebase te doorzoeken. Als u nog steeds geen oplossing kunt vinden, verstuurt u een verzoek om ondersteuning naar de klantenservice van ESET. Op basis van deze feedback kunnen onze specialisten snel reageren op uw vragen en u op effectieve wijze van advies ten aanzien van het probleem voorzien.

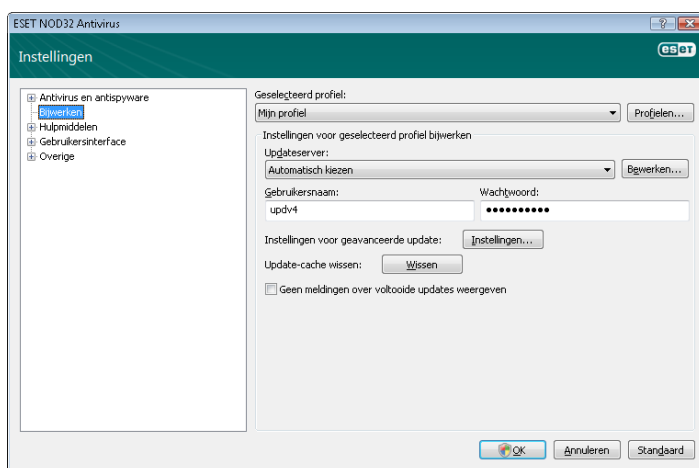
3.2 Update-instellingen

Het uitvoeren van updates voor de database met viruskenmerken en voor programmaonderdelen vormt een belangrijk onderdeel van de complete beveiliging tegen schadelijke code. Besteed speciale aandacht aan de configuratie en werking van het updateproces. Selecteer **Update** in het hoofdmenu en klik vervolgens op **Database viruskenmerken bijwerken** in het hoofdvenster van het programma om direct te controleren of een nieuwe update voor de database beschikbaar is. Klik op **Gebruikersnaam en wachtwoord instellen...** om een dialoogvenster weer te geven waarin u de gebruikersnaam en het wachtwoord invoert die u bij aanschaf hebt ontvangen.

Als de gebruikersnaam en het wachtwoord zijn ingevoerd tijdens de installatie van ESET NOD32 Antivirus, wordt u er hier niet om gevraagd.

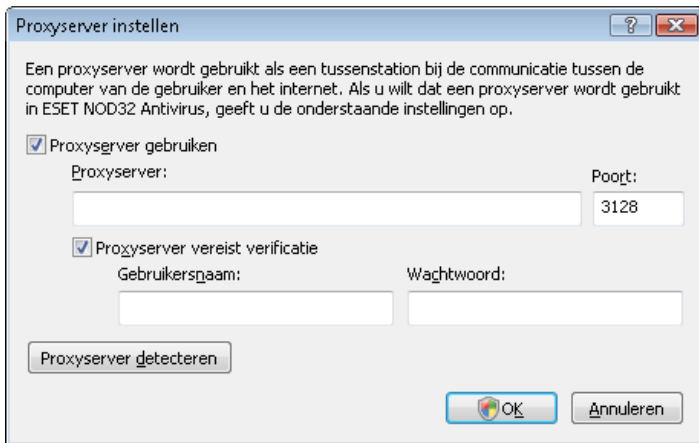


Het venster **Geavanceerde instellingen** (dat kan worden geopend door op F5 te drukken) bevat andere gedetailleerde updateopties. De vervolgkeuzelijst **Updateserver:** moet worden ingesteld op **Automatisch kiezen**. U kunt geavanceerde updateopties configureren, zoals de updatemodus, proxyservertoegang, toegang tot updates op een lokale server en het maken van kopieën van viruskenmerken (in ESET NOD32 Antivirus Business Edition) door op de knop **Instellingen...** te klikken.



3.3 Proxyserver instellen

Als u een proxyserver gebruikt om verbinding te maken met internet op een systeem met ESET NOD32 Antivirus, moet dit in Geavanceerde instellingen (F5) worden opgegeven. U kunt het configuratievenster **Proxyserver** openen door in Geavanceerde instellingen op **Overige > Proxyserver** te klikken. Schakel het selectievakje **Proxyserver** in en voer het IP-adres en de poort van de proxyserver in, samen met de verificatiegegevens.



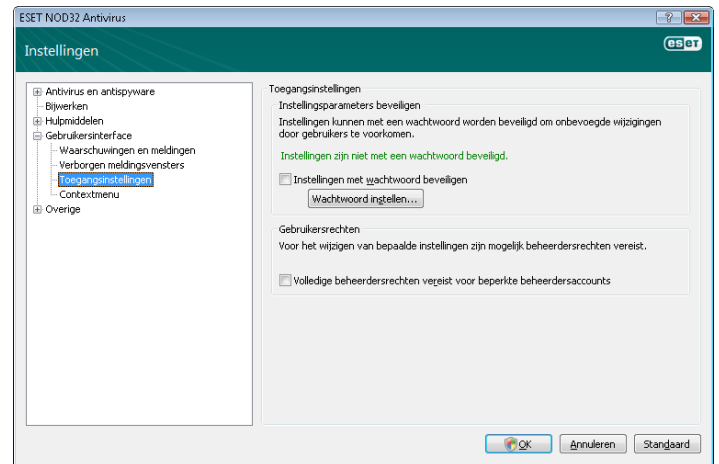
Als deze informatie niet beschikbaar is, kunt u de instellingen van de proxyserver voor ESET NOD32 Antivirus automatisch laten detecteren. Klik hiervoor op de knop **Proxyserver detecteren**.

OPMERKING: proxyserveropties voor verschillende updateprofielen kunnen verschillen. Als dit het geval is, configureert u de proxyserver in de instellingen voor geavanceerde update.

3.4 Instellingen beveiligen

De instellingen van ESET NOD32 Antivirus kunnen zeer belangrijk zijn met betrekking tot het beveiligingsbeleid binnen uw organisatie. Onbevoegde wijzigingen kunnen de stabiliteit en beveiliging van uw systeem in gevaar brengen. U kunt de instellingsparameters met een wachtwoord beveiligen door naar het hoofdmenu te gaan en op **Instellingen > Volledige structuur voor geavanceerde instellingen invoeren... > Gebruikersinterface > Instellingsbeveiliging** te klikken en vervolgens op de knop **Wachtwoord invoeren...** te klikken.

Voer een wachtwoord in, bevestig dit door het opnieuw te typen en klik op **OK**. Dit wachtwoord is vereist voor alle toekomstige wijzigingen in de instellingen van ESET NOD32 Antivirus.



4. Werken met ESET NOD32 Antivirus

4.1 Antivirus- en antispywarebeveiliging

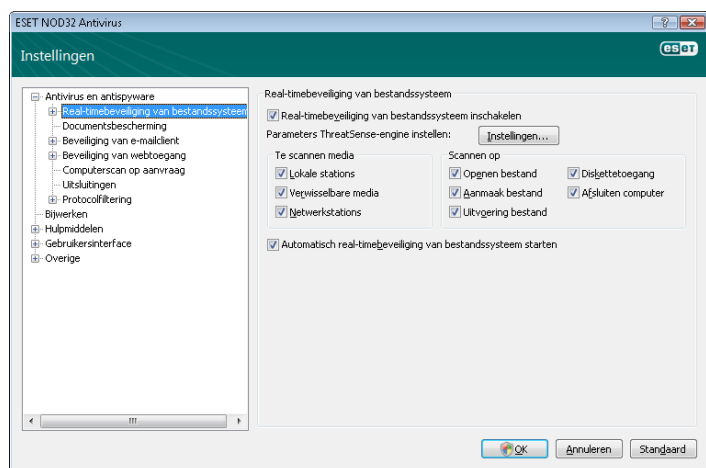
Antivirusbeveiliging biedt bescherming tegen kwaadwillende systeemaanvallen door middel van controle over bestanden, e-mail en internetcommunicatie. Als een bedreiging via schadelijke code wordt gedetecteerd, kan de antivirusmodule deze onschadelijk maken door de code eerst te blokkeren en deze vervolgens op te schonen, te verwijderen of in quarantaine te plaatsen.

4.1.1 Real-timebeveiliging van bestandssysteem

Met real-timebeveiliging van bestandssysteem worden alle gebeurtenissen met betrekking tot antivirusbeveiliging in het systeem gecontroleerd. Alle bestanden worden gescand op schadelijke code op het moment dat ze op de computer worden geopend, gemaakt of uitgevoerd. Real-timebeveiliging van bestandssysteem wordt uitgevoerd bij het opstarten van het systeem.

4.1.1.1 Besturingsinstellingen

Met de real-timebestandssysteembeveiliging worden alle typen media gecontroleerd. De besturing wordt geactiveerd door verschillende gebeurtenissen. Bij de besturing wordt gebruikgemaakt van de detectiemethoden van de ThreatSense-technologie (zoals beschreven in Parameters voor ThreatSense-engine instellen). Het besturingsgedrag kan verschillen voor nieuwe bestanden en bestaande bestanden. Voor nieuwe bestanden is het mogelijk een hoger besturingsniveau in te stellen.



4.1.1.1.1 Te scannen media

Standaard worden alle typen media gescand op mogelijke bedreigingen.

Lokale stations – Hiermee worden alle vaste-schijfstations van het systeem bestuurd.

Verwisselbare media – Diskettes, USB-opslagapparaten, enzovoort.

Netwerkstations – Hiermee worden alle gekoppelde stations gescand.

Wij adviseren u de standaardinstellingen te handhaven en deze alleen in specifieke gevallen te wijzigen, bijvoorbeeld als het scannen van bepaalde media tot aanzienlijke vertragingen in de gegevensoverdracht leidt.

4.1.1.1.2 Scannen op basis van gebeurtenissen

Standaard worden alle bestanden gescand op het moment dat ze worden geopend, uitgevoerd of gemaakt. Wij adviseren u de standaardinstellingen te handhaven aangezien deze het hoogste niveau van real-timebeveiliging voor uw computer bieden.

De optie **Diskettetoegang** biedt controle over de opstartsector van de diskette als dit station wordt geactiveerd. De optie **Afsluiten computer** biedt controle over de opstartsectoren van de vaste schijf tijdens het afsluiten van de computer. Hoewel opstartvirussen vandaag de dag nog maar weinig voorkomen, adviseren wij deze opties ingeschakeld te houden, aangezien de kans op infectie door een opstartvirus uit andere bronnen blijft bestaan.

4.1.1.1.3 Aanvullende ThreatSense-parameters voor nieuwe en gewijzigde bestanden

De waarschijnlijkheid van infectie is bij nieuwe bestanden in verhouding hoger dan bij bestaande bestanden. Daarom controleert het programma deze bestanden met aanvullende scanparameters. Behalve algemene, op viruskenmerken gebaseerde scanmethoden wordt ook geavanceerde heuristiek gebruikt, waardoor de detectiepercentages sterk verbeteren. Behalve nieuwe bestanden worden ook zelfuitpakkende bestanden (SFX) en programma's voor runtime-compressie (intern gecompriëerde uitvoerbare bestanden) gescand. Archieven worden standaard tot maximaal tien niveaus gescand en worden gecontroleerd ongeacht hun grootte. Schakel de optie **Standaardinstellingen voor archieven scannen** uit om de scaninstellingen voor archieven te wijzigen.

4.1.1.1.4 Geavanceerde instellingen

Teneinde het systeem minimaal te belasten bij gebruik van real-timebeveiliging, worden bestanden die reeds zijn gescand, niet opnieuw gescand (tenzij ze zijn gewijzigd). Bestanden worden direct na elke update van de database met viruskenmerken opnieuw gescand. Dit gedrag kan worden geconfigureerd via de optie **Geoptimaliseerd scannen**. Als deze optie is uitgeschakeld, worden alle bestanden gescand wanneer ze worden geopend.

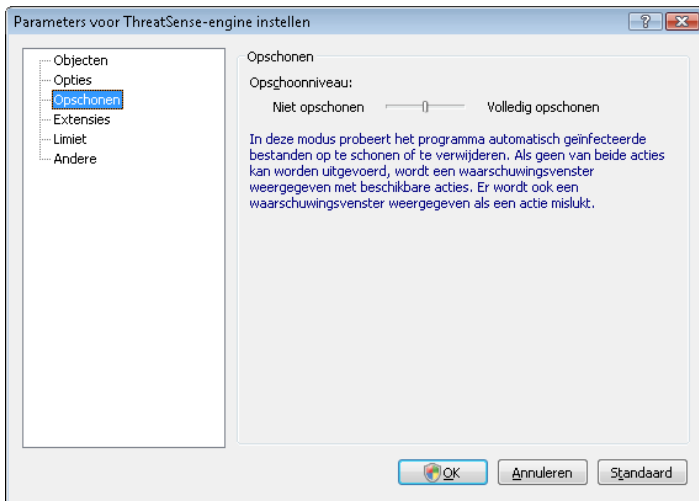
Real-timebeveiliging wordt standaard gestart bij het opstarten van het besturingssysteem, waardoor ononderbroken scannen mogelijk is. In speciale gevallen (zoals bij conflicten met een andere real-timescanner), kan de real-timebeveiliging worden beëindigd door de optie **Automatisch real-timebeveiliging van bestandssysteem starten** uit te schakelen.

Standaard wordt tijdens het uitvoeren van bestanden geen gebruik gemaakt van geavanceerde heuristiek. In bepaalde gevallen kan het echter nodig zijn om deze optie in te schakelen (door de optie **Geavanceerde heuristiek voor uitvoeren bestanden** in te schakelen). Houd er rekening mee dat sommige programma's mogelijk trager worden uitgevoerd door geavanceerde heuristiek vanwege de extra belasting van het systeem.

4.1.1.2 Opschoonniveaus

De real-timebeveiliging heeft drie opschoonniveaus (u opent deze door op de knop **Instellingen...** in de sectie **Real-timebeveiliging van bestandssysteem** te klikken en vervolgens op **Opschonen** te klikken).

- Bij het eerste niveau wordt een waarschuwingsvenster met beschikbare opties weergegeven voor elke gevonden infiltratie. De gebruiker moet een actie kiezen voor elke afzonderlijke infiltratie. Dit niveau is bedoeld voor geavanceerde gebruikers die weten wat ze moeten doen met elk type infiltratie.
- Bij het middelste niveau wordt automatisch een vooraf gedefinieerde actie gekozen en uitgevoerd (afhankelijk van het type infiltratie). Het detecteren en verwijderen van een geïnfecteerd bestand wordt aangegeven via een informatiebericht in de rechterbenedenhoek van het scherm. Er wordt echter geen automatische actie uitgevoerd als de infiltratie zich binnen een archief bevindt dat tevens schone bestanden bevat of als voor object geen vooraf gedefinieerde actie beschikbaar is.
- Het derde niveau is het meest "agressieve": alle geïnfecteerde objecten worden opgeschoond. Aangezien dit niveau kan resulteren in het verlies van geldige bestanden, adviseren wij dit alleen in specifieke situaties te gebruiken.



4.1.1.3 Wanneer moet de configuratie voor real-timebeveiliging worden gewijzigd?

Real-timebeveiliging vormt het meest essentiële onderdeel van het onderhouden van een veilig systeem. Wees daarom voorzichtig bij het wijzigen van de bijbehorende parameters. Wij adviseren u de parameters alleen te wijzigen in specifieke situaties. Als er bijvoorbeeld een conflict is met een bepaalde toepassing of real-timescanner van een ander antivirusprogramma.

Na installatie van ESET NOD32 Antivirus zijn alle instellingen geoptimaliseerd om gebruikers een zo hoog mogelijk niveau van systeembeveiliging te bieden. U kunt de standaardinstellingen herstellen door op de knop **Standaard** in de rechterbenedenhoek van het venster **Real-timebeveiliging van bestandssysteem (Geavanceerde instellingen > Antivirus en antispyware > Real-timebeveiliging van bestandssysteem)** te klikken.

4.1.1.4 Real-timebeveiliging controleren

U kunt controleren of real-timebeveiliging werkt en virussen worden gedetecteerd door middel van een testbestand van eicar.com. Dit testbestand is een speciaal onschadelijk bestand dat door alle antivirusprogramma's kan worden gedetecteerd. Het bestand is gemaakt door het bedrijf EICAR (European Institute for Computer Antivirus Research) om de werking van antivirusprogramma's te testen. Het bestand eicar.com kan worden gedownload van <http://www.eicar.org/download/eicar.com>

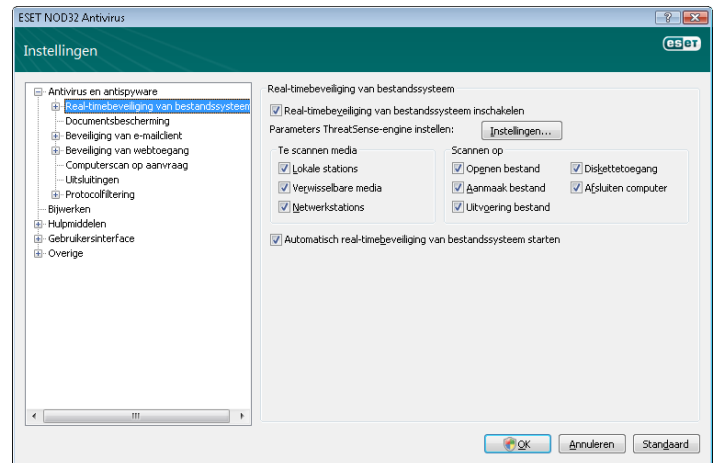
4.1.1.5 Te volgen procedure als real-timebeveiliging niet werkt

In het volgende hoofdstuk worden probleemsituaties beschreven die zich kunnen voordoen bij het gebruik van real-timebeveiliging en enkele oplossingen hiervoor.

Real-timebeveiliging is uitgeschakeld

Als real-timebeveiliging per ongeluk door de gebruiker is uitgeschakeld, moet deze opnieuw worden geactiveerd. U kunt real-timebeveiliging opnieuw activeren door naar **Instellingen > Antivirus en antispyware** te gaan en op **Inschakelen** te klikken in de sectie **Real-timebeveiliging van bestandssysteem** van het hoofdvenster van het programma.

Als real-timebeveiliging niet wordt gestart bij het opstarten van het systeem, komt dit waarschijnlijk doordat de optie **Automatisch real-timebeveiliging van bestandssysteem starten** is uitgeschakeld. U kunt deze optie inschakelen door naar **Geavanceerde instellingen (F5)** te gaan en op **Real-timebeveiliging van bestandssysteem** te klikken in Geavanceerde instellingen. Controleer in de sectie **Geavanceerde instellingen** onder in het venster of het selectievakje **Automatisch real-timebeveiliging van bestandssysteem starten** is ingeschakeld.



Real-timebeveiliging detecteert geen infiltraties en schoont deze niet op

Controleer of er andere antivirusprogramma's zijn geïnstalleerd op de computer. Als twee programma's voor real-timebeveiliging tegelijkertijd zijn geactiveerd, kunnen deze conflicteren. Wij adviseren u alle andere antivirusprogramma's van uw systeem te verwijderen.

Real-timebeveiliging wordt niet gestart

Als real-timebeveiliging niet wordt gestart bij het opstarten van het systeem (en de optie **Automatisch real-timebeveiliging van bestandssysteem starten** is ingeschakeld), is er mogelijk een conflict met een ander programma opgetreden. Als dit het geval is, raadpleegt u de specialisten van de klantenservice van ESET.

4.1.2 Beveiliging van e-mailclient

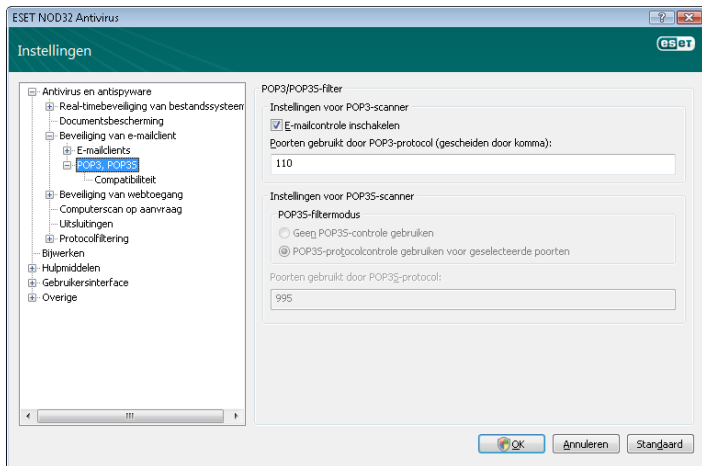
E-mailbeveiliging biedt controle over e-mailcommunicatie die wordt ontvangen via het POP3-protocol. Met behulp van het invoegtoepassingsprogramma voor Microsoft Outlook biedt ESET NOD32 Antivirus controle over alle communicatie via de e-mailclient (POP3, MAPI, IMAP, HTTP). Bij het onderzoeken van binnenkomende berichten maakt het programma gebruik van alle geavanceerde scanmethoden die beschikbaar zijn via de ThreatSense-engine. Dit betekent dat schadelijke programma's worden gedetecteerd nog voordat deze worden vergeleken met de database met viruskenmerken. Het scannen van communicatie via het POP3-protocol gebeurt onafhankelijk van de gebruikte e-mailclient.

4.1.2.1 POP3-controle

Het POP3-protocol is het meest gebruikte protocol voor het ontvangen van e-mailcommunicatie in een e-mailclienttoepassing. ESET NOD32 Antivirus biedt beveiliging van dit protocol ongeacht de gebruikte e-mailclient.

De module die deze controle verzorgt, wordt automatisch gestart bij het opstarten van het besturingssysteem en is vervolgens actief in het geheugen. De module werkt alleen goed als deze is ingeschakeld. POP3-controle wordt automatisch uitgevoerd zonder dat de e-mailclient opnieuw hoeft te worden geconfigureerd. Standaard wordt alle communicatie op poort 110 gescand, maar andere communicatiepoorten kunnen zo nodig worden toegevoegd. Poortnummers moeten van elkaar worden gescheiden door een komma.

Gecodeerde communicatie wordt niet gecontroleerd.



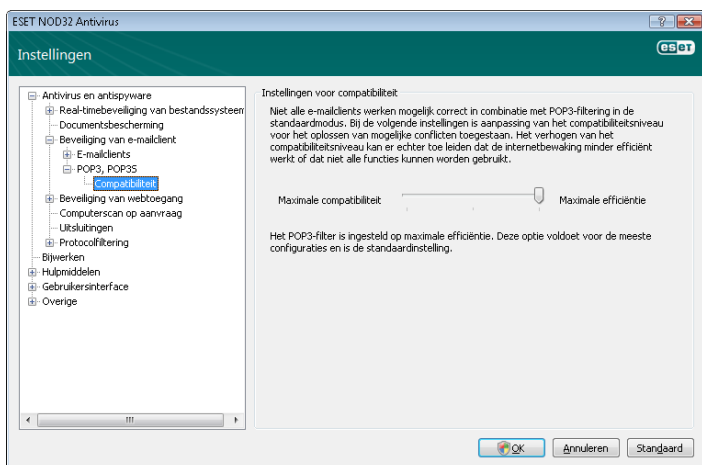
4.1.2.1.1 Compatibiliteit

Bij bepaalde e-mailprogramma's kunt u problemen ondervinden met POP3-filtering (bij het ontvangen van berichten via een trage internetverbinding kunnen bijvoorbeeld time-outs optreden vanwege controles). In dat geval wijzigt u de manier waarop de controle plaatsvindt. Het verlagen van het controleniveau kan de snelheid van het opschoonproces bevorderen. U kunt het controleniveau van POP3-filtering aanpassen door naar **Antivirus en antispysware > E-mailbeveiliging > POP3 > Compatibiliteit** te gaan.

Als **Maximale efficiëntie** is ingeschakeld, worden infiltraties uit geïnfecteerde bestanden verwijderd en wordt informatie over de infiltratie ingevoegd vóór het oorspronkelijke onderwerp van het e-mailbericht (de optie **Verwijderen** of **Opschonen** moet zijn geactiveerd, of **Volledig opschonen** of **Standaard opschonen** moet zijn ingeschakeld).

Gemiddelde compatibiliteit wijzigt de manier waarop berichten worden ontvangen. Berichten worden geleidelijk naar de e-mailclient verzonden en nadat het laatste deel van het bericht is overgedragen, wordt het bericht gescand op infiltraties. Het risico van infectie neemt echter toe bij dit controleniveau. Het opschoonniveau en de afhandeling van meldingen (waarschuwingsberichten die worden toegevoegd aan de onderwerpregel en de hoofdtekst van e-mailberichten) is gelijk aan de instelling voor maximale efficiëntie.

Met het niveau **Maximale compatibiliteit** wordt de gebruiker via een waarschuwingsvenster op de hoogte gebracht van de ontvangst van een geïnfecteerd bericht. Er wordt geen informatie over geïnfecteerde bestanden toegevoegd aan de onderwerpregel of aan de hoofdtekst van afgeleverde e-mailberichten en infiltraties worden niet automatisch verwijderd. Het verwijderen van infiltraties moet worden uitgevoerd door de gebruiker vanaf de e-mailclient.

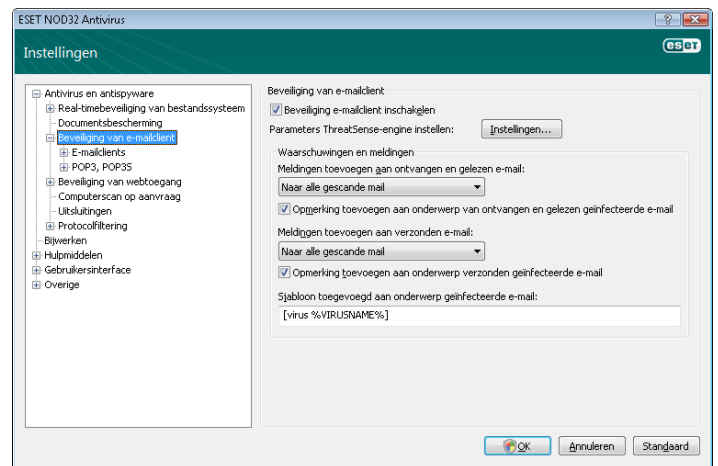


4.1.2.2 Integratie met e-mailclients

Door integratie van ESET NOD32 Antivirus met e-mailclients neemt het niveau van actieve beveiliging tegen schadelijke code in e-mailberichten toe. Als uw e-mailclient wordt ondersteund, kan deze integratie worden ingeschakeld in ESET NOD32 Antivirus. Als integratie is geactiveerd, wordt de werkbalk van ESET NOD32 Antivirus rechtstreeks in de e-mailclient ingevoegd, waardoor een efficiëntere e-mailbeveiliging mogelijk is. De integratie-instellingen zijn beschikbaar via **Instellingen > Volledige structuur voor geavanceerde instellingen invoeren... > Overige > Integratie met e-mailclients**. In dit dialoogvenster kunt u integratie met de ondersteunde e-mailclients activeren. Enkele e-mailclients die momenteel worden ondersteund zijn Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail en Mozilla Thunderbird.

Schakel de optie **Controle bij wijziging inhoud Postvak IN uitschakelen** in als het systeem trager wordt tijdens het werken met de e-mailclient. Dit kan bijvoorbeeld gebeuren wanneer u e-mailberichten downloadt uit het archief Kerio Outlook Connector.

U kunt e-mailbeveiliging starten door het selectievakje **E-mailbeveiliging inschakelen** bij **Geavanceerde instellingen (F5) > Antivirus en antispysware > E-mailbeveiliging** in te schakelen.



4.1.2.2.1 Meldingen toevoegen aan de hoofdtekst van een e-mailbericht

Elk e-mailbericht dat door ESET NOD32 Antivirus wordt gecontroleerd, kan worden gemarkeerd door een melding aan het onderwerp of de hoofdtekst van het e-mailbericht toe te voegen. Door deze functie neemt de geloofwaardigheid voor de geadresseerde toe en als een infiltratie wordt gedetecteerd, wordt waardevolle informatie verstrekt over het bedreigingsniveau van een specifiek e-mailbericht of een bepaalde afzender.

De opties voor deze functionaliteit zijn te vinden in de sectie **Geavanceerde instellingen > Antivirus en antispysware > Beveiliging van e-mailclient**. Het programma kan **meldingen toevoegen aan ontvangen en gelezen e-mail**, en **meldingen toevoegen aan verzonden e-mail**. Gebruikers hebben bovendien de mogelijkheid om te kiezen of meldingen moeten worden toegevoegd aan alle e-mailberichten, alleen aan geïnfecteerde e-mailberichten of aan helemaal geen e-mailberichten.

ESET NOD32 Antivirus stelt de gebruiker tevens in staat meldingen toe te voegen aan het oorspronkelijke onderwerp van geïnfecteerde berichten. Als u meldingen wilt toevoegen aan het onderwerp, schakelt u de opties **Opmerking toevoegen aan onderwerp van ontvangen en gelezen geïnfecteerde e-mail** en **Opmerking toevoegen aan onderwerp verzonden geïnfecteerde e-mail** in.

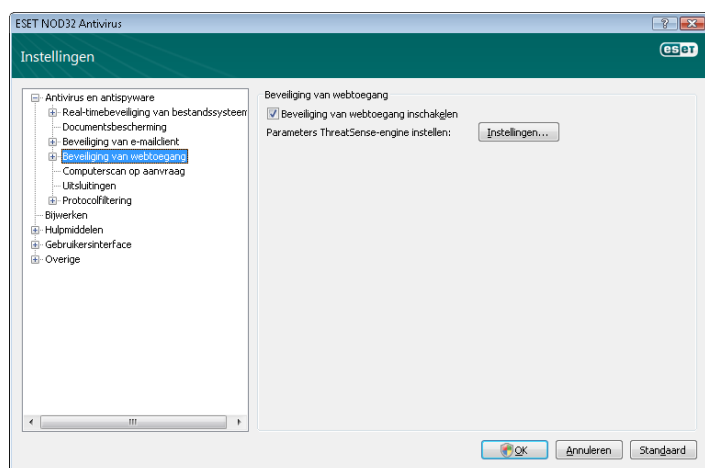
De inhoud van de meldingen kan worden gewijzigd in het veld Sjabloon dat is toegevoegd aan het onderwerp van geïnfecteerde e-mailberichten. De bovengenoemde wijzigingen kunnen helpen bij het automatiseren van het filteren van geïnfecteerde e-mail, aangezien u hiermee e-mailberichten met een bepaald onderwerp kunt filteren (indien ondersteund door uw e-mailclient) en deze in een aparte map kunt opnemen.

4.1.2.3 Infiltraties verwijderen

Als een geïnfecteerd e-mailbericht wordt ontvangen, wordt een waarschuwingsvenster weergegeven. In dit waarschuwingsvenster worden de naam van de afzender, de e-mail en de naam van de infiltratie weergegeven. In het onderste deel van het venster vindt u de opties **Opschonen**, **Verwijderen** en **Verlaten** voor het gedetecteerde object. In vrijwel alle gevallen adviseren wij u **Opschonen** of **Verwijderen** te selecteren. In speciale gevallen, als u het geïnfecteerde bestand wilt ontvangen, selecteert u **Verlaten**. Als **Volledig opschonen** is ingeschakeld, wordt een informatievenster zonder selecteerbare opties voor geïnfecteerde objecten weergegeven.

4.1.3 Beveiliging van webtoegang

Toegang tot internet is een standaardfunctie op een pc. Helaas is internet uitgegroeid tot het belangrijkste medium voor de overdracht van schadelijke code. Hierdoor is het van essentieel belang dat u de nodige aandacht besteedt aan de beveiliging van uw webtoegang. Wij adviseren u dringend om ervoor te zorgen dat de optie **Beveiliging van webtoegang inschakelen** is geactiveerd. U vindt deze optie in **Geavanceerde instellingen (F5) > Antivirus en antispyware > Beveiliging van webtoegang**.



4.1.3.1 HTTP, HTTPS

De toegangsbeveiliging van websites wordt geregeld door de communicatie tussen internetbrowsers en externe servers te controleren. Hierbij worden de regels voor HTTP (Hypertext Transfer Protocol) en HTTPS (HTTP met gecodeerde communicatie) gehanteerd. ESET NOD32 Antivirus is standaard geconfigureerd voor het gebruik van de standaarden van de meeste internetbrowsers. De instellopties voor HTTP-controle kunnen echter worden gewijzigd in **Beveiliging van webtoegang > HTTP, HTTPS**. In het hoofdvenster met instellingen voor het HTTP-filter kunt u de optie **HTTP-controle inschakelen** in- of uitschakelen. U kunt ook de poortnummers opgeven die mogen worden gebruikt voor HTTP-communicatie. Standaard zijn de poortnummers 80, 8080 en 3128 vooraf gedefinieerd. HTTPS-controle kan in de volgende modi worden uitgevoerd:

Geen HTTPS-protocolcontrole gebruiken

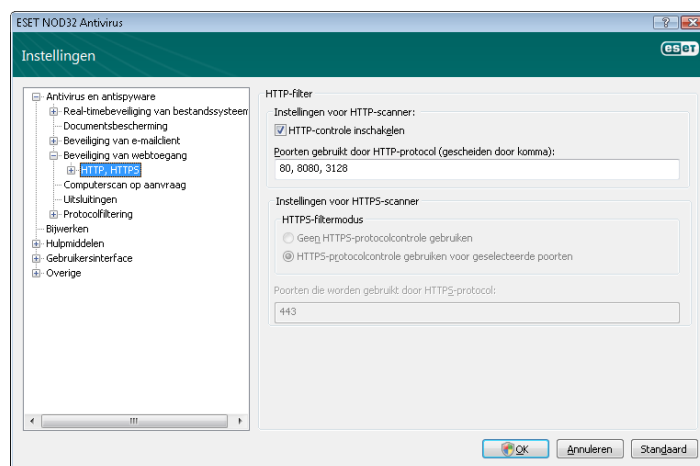
Gecodeerde communicatie wordt niet gecontroleerd.

HTTPS-protocolcontrole gebruiken voor geselecteerde poorten

HTTPS-controle alleen inschakelen voor poorten die zijn gedefinieerd bij Poorten gebruikt door HTTPS-protocol.

HTTPS-protocolcontrole gebruiken voor toepassingen die zijn gemarkeerd als internetbrowsers en die geselecteerde poorten gebruiken

Alleen toepassingen controleren die zijn opgegeven in de sectie Browsers en die poorten gebruiken die zijn gedefinieerd in **Poorten gebruikt door HTTPS-protocol**.

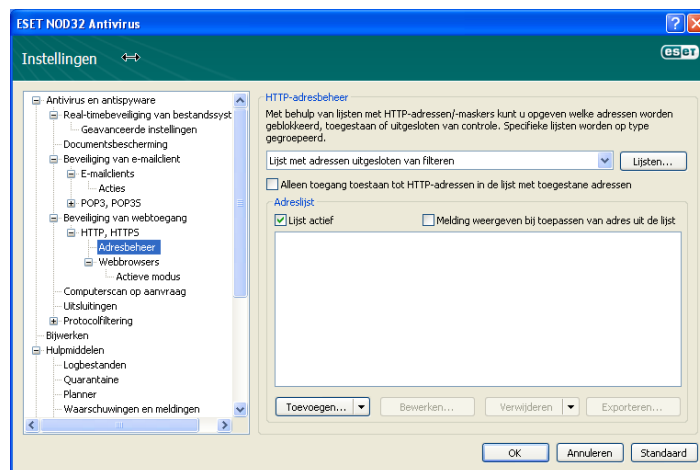


4.1.3.1.1 Adresbeheer

Gebruik deze sectie om HTTP-adressen op te geven die u wilt blokkeren, toestaan of uitsluiten van controle.

De knoppen **Toevoegen**, **Wijzigen**, **Verwijderen** en **Exporteren** kunt u gebruiken om de lijsten met adressen te beheren. Websites in de lijst met geblokkeerde adressen zijn niet toegankelijk. Websites in de lijst met uitgesloten adressen zijn toegankelijk zonder dat er wordt gecontroleerd op schadelijke code. Als u de optie **Alleen toegang toestaan tot HTTP-adressen in de lijst met toegestane adressen** inschakelt, zijn alleen adressen in de lijst met toegestane adressen toegankelijk en worden alle andere HTTP-adressen geblokkeerd.

In alle lijsten kunnen de speciale symbolen * (sterretje) en ? (vraagteken) worden gebruikt. Het sterretje vervangt elke willekeurige tekenreeks, terwijl het vraagteken elk willekeurig symbool vervangt. Wees met name voorzichtig bij het opgeven van uitgesloten adressen omdat deze lijst alleen vertrouwde en veilige adressen zou moeten bevatten. Ga tevens zorgvuldig om met de symbolen * en ? en zorg ervoor dat deze correct worden gebruikt in deze lijst. Als u een lijst wilt activeren, selecteert u de optie **Lijst actief**. Als u een melding wilt zien wanneer u een adres uit de huidige lijst invoert, selecteert u **Melding weergeven bij toepassen van adres uit de lijst**.

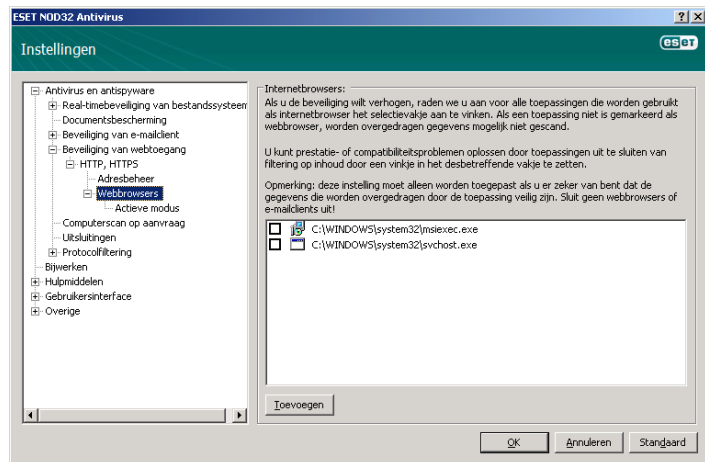


4.1.3.1.2 Webrowsers

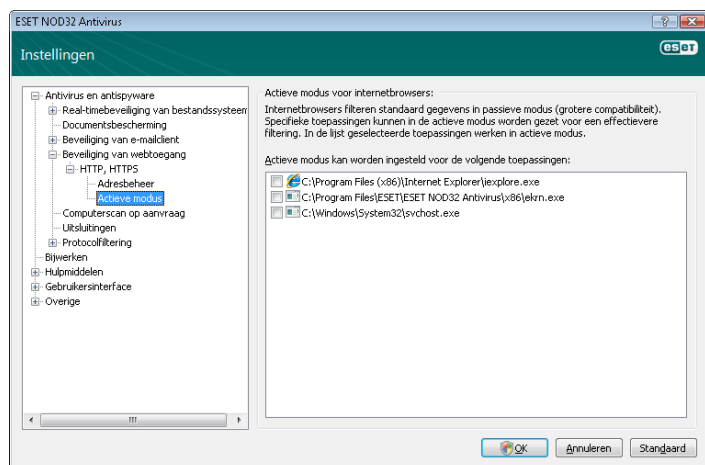
ESET Smart Security bevat tevens de functie **Webrowsers**, waarmee de gebruiker kan definiëren of het desbetreffende programma een browser is of niet. Als een toepassing door de gebruiker is gemarkeerd als een browser, wordt alle communicatie via deze toepassing gecontroleerd ongeacht de poortnummers die zijn betrokken bij de communicatie.

De functie Webrowsers geldt als aanvulling op de functie voor HTTP-controle, aangezien HTTP-controle alleen plaatsvindt op

vooraf gedefinieerde poorten. Veel internetservices maken echter gebruik van dynamisch veranderende of onbekende poortnummers. Daarom kan de functie Webbrowser de controle verwerven over alle poortcommunicatie ongeacht de verbidingsparameters.



De lijst met toepassingen die zijn gemarkeerd als browsers is direct toegankelijk vanuit het submenu **Webrowsers** onder **HTTP**. Deze sectie bevat tevens het submenu **Actieve modus**, waarin de controlemodus voor internetbrowsers wordt gedefinieerd. De optie **Actieve modus** is nuttig omdat hiermee overgedragen gegevens in hun geheel worden onderzocht. Als deze optie niet is ingeschakeld, wordt de communicatie van toepassingen geleidelijk aan, in batches, gecontroleerd. Hierdoor neemt de effectiviteit van het proces van gegevensverificatie af, maar wordt wel een grotere compatibiliteit met de toepassingen in de lijst geboden. Als er geen problemen optreden bij het gebruik ervan, adviseren wij u de actieve controlemodus te activeren door het selectievakje naast de gewenste toepassing in te schakelen.



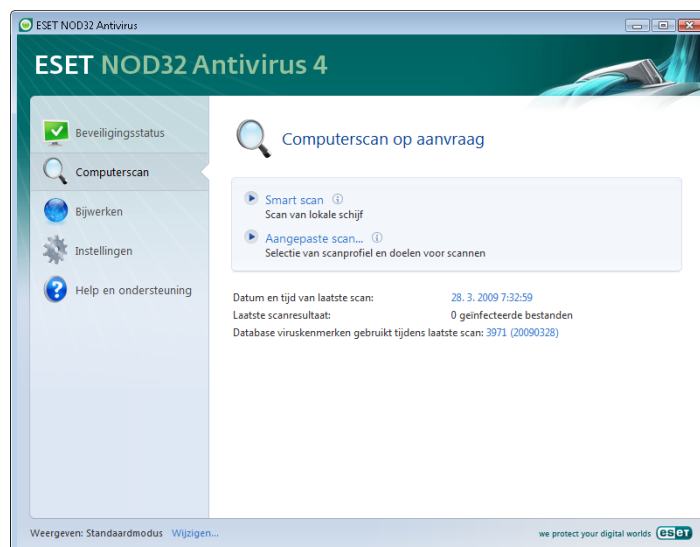
4.1.4 Computerscan

Als u vermoedt dat de computer is geïnfecteerd (deze gedraagt zich abnormaal), voert u een computerscan op aanvraag uit om uw computer te onderzoeken op infiltraties. Vanuit beveiligingsoogpunt is het van essentieel belang dat computerscans niet alleen worden uitgevoerd als infecties worden vermoed, maar regelmatig als onderdeel van routinematige beveiligingsmaatregelen. Regelmatig scannen biedt detectie van infiltraties die niet zijn gedetecteerd door de real-timescanner op het moment van opslag op de schijf. Dit kan gebeuren als de real-timescanner was uitgeschakeld op het moment van infectie of de database met viruskenmerken verouderd was.

Wij adviseren u minimaal een- of tweemaal per maand een scan op aanvraag uit te voeren. Scannen kan worden geconfigureerd als een geplande taak in **Hulpmiddelen > Planner**.

4.1.4.1 Type scan

Er zijn twee typen beschikbaar. De **standaardscan** scant snel het systeem zonder verdere configuratie van de scanparameters. De **aangepaste scan...** stelt de gebruiker in staat een van de vooraf gedefinieerde scanprofielen te selecteren en scanobjecten te kiezen uit de boomstructuur.



4.1.4.1.1 Standaardscan

Standaardscan is een gebruikersvriendelijke methode die de gebruiker in staat stelt snel een computerscan te starten en geïnfecteerde bestanden op te schonen zonder dat er gebruikersinterventie is vereist. Het belangrijkste voordeel is de eenvoudige werking zonder gedetailleerde scanconfiguratie. Standaardscan controleert alle bestanden op lokale stations en schoont automatisch gedetecteerde infiltraties op of verwijdert deze. Het opschoonniveau wordt automatisch ingesteld op de standaardwaarde. Zie Opschonen (pagina 18) voor nadere informatie over typen opschoonbewerkingen.

Het standaardscanprofiel is ontworpen voor gebruikers die snel en eenvoudig hun computers willen scannen. Het biedt een effectieve oplossing voor scannen en opschonen zonder dat een uitgebreid configuratieproces is vereist.

4.1.4.1.2 Aangepaste scan

Aangepaste scan is een optimale oplossing als u scanparameters wilt opgeven, zoals scandoelen en scanmethoden. Het voordeel van Aangepaste scan is de mogelijkheid om de parameters in detail te configureren. De configuraties kunnen worden opgeslagen in door de gebruiker gedefinieerde scanprofielen. Deze profielen zijn met name handig als het scannen herhaaldelijk plaatsvindt met dezelfde parameters.

U kunt scandoelen selecteren door gebruik te maken van de vervolgkeuzelijst van de functie voor het snel kiezen van doelen of door doelen te selecteren uit de boomstructuur met alle apparaten die beschikbaar zijn op de computer. Bovendien kunt u een keuze maken uit drie opschoonniveaus door op **Instellingen... > Opschonen** te klikken. Als u alleen bent geïnteresseerd in het scannen van het systeem en geen extra acties wilt uitvoeren, schakelt u het selectievakje **Scannen zonder opschonen** in.

Het uitvoeren van computerscans via de modus Aangepaste scan is geschikt voor gevorderde gebruikers met ervaring in het gebruik van antivirusprogramma's.

4.1.4.2 Scandoelen

In de vervolgkeuzelijst Scandoelen kunt u bestanden, mappen en apparaten (schijven) selecteren die moeten worden gescand op virussen.

Via de menuoptie Snel scandoelen kiezen kunt u de volgende doelen selecteren:

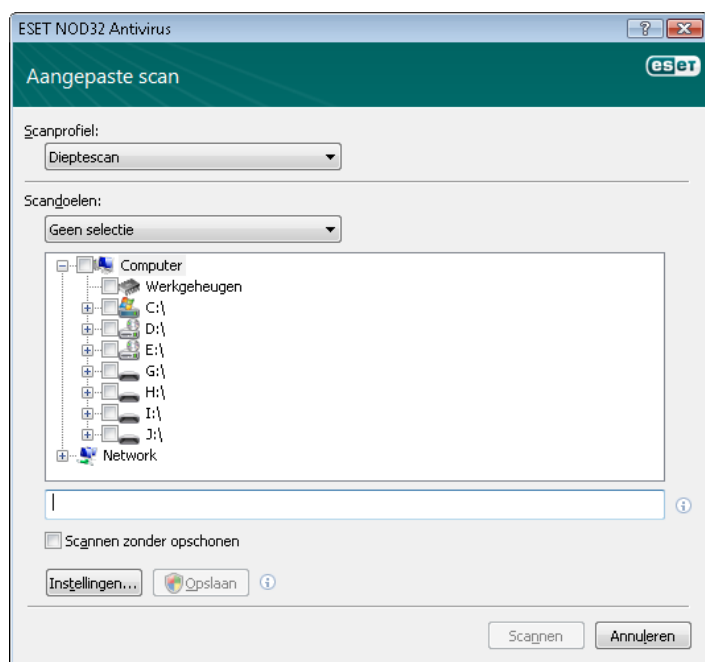
Op profielinstellingen – Hiermee worden doelen gecontroleerd die zijn ingesteld in het geselecteerde scanprofiel.

Verwisselbare media – Diskettes, USB-opslagapparaten, cd/dvd

Lokale stations – Hiermee worden alle vaste schijfstations van het systeem gecontroleerd.

Netwerkstations – Alle gekoppelde stations.

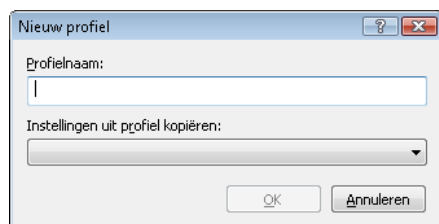
Geen selectie – Hiermee worden alle selecties geannuleerd.



Een scandoel kan tevens nader worden gespecificeerd door het pad naar de map met het bestand of de bestanden die u wilt opnemen in de scan in te voeren. Selecteer doelen uit de boomstructuur met alle apparaten die beschikbaar zijn op de computer.

4.1.4.3 Scanprofielen

De geprefereerde computerscanparameters kunnen worden opgeslagen in profielen. Het voordeel van het maken van scanprofielen is dat zij regelmatig kunnen worden gebruikt voor toekomstige scans. Wij adviseren u zoveel profielen (met verschillende scandoelen, scanmethoden en andere parameters) te maken als de gebruiker regelmatig gebruikt.



U kunt een nieuw profiel maken dat herhaaldelijk kan worden gebruikt voor toekomstige scans door naar **Geavanceerde instellingen (F5) > Computerscan op aanvraag** te navigeren. Klik op de knop **Profielen...** aan de rechterkant om de lijst met bestaande scanprofielen en de optie voor het maken van een nieuw profiel weer te geven. In het volgende gedeelte **Parameters ThreatSense-engine instellen** wordt elke parameter van de scaninstellingen beschreven. Dit helpt u bij het maken van een scanprofiel dat is aangepast aan uw behoeften.

Voorbeeld:

stel dat u uw eigen scanprofiel wilt maken en de configuratie die is toegewezen aan het profiel **Smart Scan** is gedeeltelijk geschikt Maar u wilt geen programma's voor runtime-compressie of potentieel onveilige toepassingen scannen en u wilt ook **Volledig opschonen** toepassen. Ga naar het venster **Configuratieprofielen** en klik op de knop **Toevoegen...** Geef de naam van uw nieuwe profiel op in het veld **Profielnaam** en selecteer **Smart Scan** in de vervolgkeuzelijst **Instellingen uit profiel kopiëren**: Pas daarna de resterende parameters aan uw vereisten aan.

4.1.5 Protocolfiltering

De antivirusbeveiliging voor de toepassingsprotocollen POP3 en HTTP wordt geleverd door de ThreatSense-scanengine, waarin alle geavanceerde malware-scantechnieken naadloos zijn geïntegreerd. De controle werkt automatisch, ongeacht de gebruikte internetbrowsers of e-mailclient. De volgende opties zijn beschikbaar voor protocolfiltering (als de optie **Filter toepassingsprotocol inschakelen** is ingeschakeld):

HTTP- en POP3-poorten – Hiermee wordt het scannen van communicatie beperkt tot bekende HTTP- en POP3-poorten.

Toepassingen die zijn gemarkeerd als internetbrowsers en e-mailclients – Schakel deze optie in als u alleen communicatie van toepassingen wilt filteren die zijn gemarkeerd als browser (Beveiliging van webtoegang > HTTP, HTTPS > Webrowsers) en e-mailclient (Beveiliging van e-mailclient > POP3, POP3S > E-mailclients).

Poorten en toepassingen die zijn gemarkeerd als internetbrowsers en e-mailclients – Zowel poorten als browsers worden gecontroleerd op malware.

Opmerking:

Vanaf Windows Vista Service Pack 1 en Windows Server 2008 wordt een nieuwe communicatiefilter gebruikt. Als gevolg daarvan is de sectie Protocolfiltering niet beschikbaar.

4.1.5.1 SSL

Met ESET NOD32 Antivirus 4 kunt u protocollen controleren die in het SSL-protocol zijn ingesloten. U kunt verschillende scanmodi gebruiken voor met SSL beveiligde communicaties met behulp van vertrouwde certificaten, onbekende certificaten of certificaten die zijn uitgesloten van controle met door SSL beveiligde communicatie.

Altijd SSL-protocol scannen (uitgesloten en vertrouwde certificaten blijven geldig)

– Selecteer deze optie als u alle door SSL beveiligde communicaties wilt scannen, behalve communicaties die worden beveiligd door certificaten die voor controle zijn uitgezonderd. Als een nieuwe communicatie tot stand wordt gebracht met een onbekend, ondertekend certificaat, wordt de gebruiker daarvoor niet gewaarschuwd en wordt de communicatie automatisch gefilterd. Als de gebruiker toegang krijgt tot een server met een niet-vertrouwd certificaat dat door de gebruiker als vertrouwd is gemarkeerd (is toegevoegd aan de lijst met vertrouwde certificaten), is communicatie naar de server toegestaan en wordt de inhoud van het communicatiekanaal gefilterd.

Vragen stellen over niet-bezochte sites (onbekende certificaten)

– Als u een nieuwe, met SSL beveiligde site invoert (met een onbekend certificaat), wordt een actieselectievenster weergegeven. Met deze modus kunt u een lijst met SSL-certificaten maken die van het scannen worden uitgesloten.

SSL-protocol niet scannen – Als deze optie is geselecteerd, wordt communicatie via SSL niet gescand door het programma.

Als het certificaat niet kan worden gecontroleerd met het TRCA-certificaatarchief (Trusted Root Certification Authorities)

Vragen stellen over geldigheid certificaat – De gebruiker wordt gevraagd een actie uit te voeren.

Communicatie die gebruikmaakt van het certificaat blokkeren – De verbinding met de site die het certificaat gebruikt, wordt beëindigd.

Als het certificaat ongeldig of beschadigd is

Vragen stellen over geldigheid certificaat – De gebruiker wordt gevraagd een actie uit te voeren.

Communicatie die gebruikmaakt van het certificaat blokkeren – De verbinding met de site die het certificaat gebruikt, wordt beëindigd.

4.1.5.1.1 Vertrouwde certificaten

Naast het TRCA-certificaatarchief (Trusted Root Certification Authorities), waar ESET NOD32 Antivirus 4 vertrouwde certificaten opslaat, kunt u een aangepaste lijst met vertrouwde certificaten maken die u kunt bekijken in **Instellingen (F5) > Protocolfiltering > SSL > Vertrouwde certificaten**.

4.1.5.1.2 Uitgesloten certificaten

De sectie Uitgesloten certificaten bevat certificaten die als veilig zijn beoordeeld. De inhoud van gecodeerde communicatie wordt niet gecontroleerd aan de hand van de certificaten in deze lijst. Het is raadzaam alleen webcertificaten te installeren waarvan u zeker weet dat ze veilig zijn en waarvoor het niet nodig is de inhoud te filteren.

4.1.6 Parameters voor ThreatSense-engine instellen

ThreatSense is de naam van de technologie die een aantal complexe methoden voor bedreigingsdetectie omvat. Deze technologie is proactief. Dit betekent dat tevens beveiliging wordt geboden tijdens de eerste uren van de verspreiding van een nieuwe bedreiging. Er wordt gebruikgemaakt van een combinatie van verschillende methoden (code-analyse, code-emulatie, generieke kenmerken, viruskenmerken) die samenwerken om de systeembeveiliging aanzienlijk te verbeteren. De scanengine is in staat verschillende gegevensstromen tegelijk te besturen voor een maximale efficiëntie en een zo hoog mogelijk detectiepercentage. ThreatSense-technologie zorgt tevens voor de verwijdering van rootkits.

De instellopties voor de ThreatSense-technologie stellen de gebruiker in staat verschillende scanparameters op te geven:

- Bestandstypen en extensies die moeten worden gescand
- De combinatie van verschillende detectiemethoden
- Opschoonniveaus, enz.

U kunt het instellingsvenster openen door op de knop **Instellingen...** te klikken in het instellingsvenster van een willekeurige module die gebruikmaakt van ThreatSense-technologie (zie beneden). Verschillende beveiligingsszenario's vereisen mogelijk verschillende configuraties. ThreatSense is individueel configureerbaar voor de volgende beveiligingsmodules:

- Real-timebeveiliging van bestandssysteem
- Controle opstartbestanden van systeem
- E-mailbeveiliging
- Beveiliging van webtoegang
- Computerscan op aanvraag

De ThreatSense-parameters zijn in hoge mate geoptimaliseerd voor elke module en wijziging hiervan kan een aanzienlijke invloed hebben op de werking van het systeem. Als bijvoorbeeld parameters voor het altijd scannen van programma's voor runtime-compressie worden gewijzigd of als geavanceerde heuristiek wordt ingeschakeld in de module voor real-timebeveiliging van het bestandssysteem, zou dit kunnen resulteren in een vertraging van het systeem (normaliter worden alleen nieuwe bestanden gescand via deze methoden). Daarom adviseren wij de standaard ThreatSense-parameters ongewijzigd te laten voor alle modules met uitzondering van Computerscan.

4.1.6.1 Objecten instellen

In de sectie **Objecten** kunt u definiëren welke computeronderdelen en bestanden worden gescand op infiltraties.

Werkgeheugen – Scant op bedreigingen die het werkgeheugen van het systeem aanvallen.

Opstartsectoren – Scant opstartsectoren op de aanwezigheid van virussen in de hoofdopstartrecord.

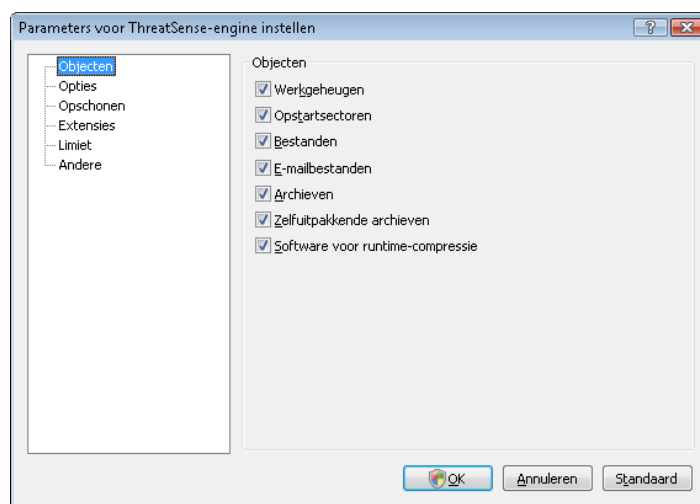
Bestanden – Biedt scanfuncties voor alle veelgebruikte bestandstypen (programma's, afbeeldingen, audio, videobestanden, databasebestanden, enz.)

E-mailbestanden – Scant speciale bestanden waarin e-mailberichten zijn opgenomen.

Archieven – Biedt scanfuncties voor bestanden die zijn gecomprimeerd in archieven (.RAR, .ZIP, .ARJ, .TAR, enz.)

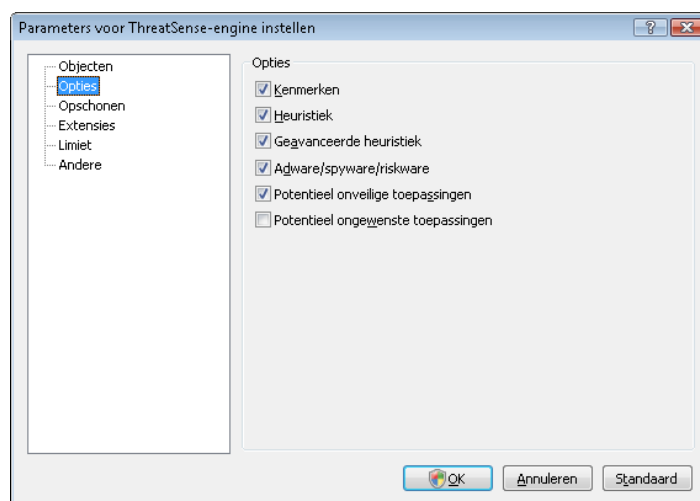
Zelfuitpakkende archieven – Scant bestanden die deel uitmaken van zelfuitpakkende archiefbestanden, maar die gewoonlijk de extensie .EXE hebben.

Programma's voor runtime-compressie – Programma's voor runtime-compressie decomprimeren in het geheugen (in tegenstelling tot standaardarchieftypen), naast standaardprogramma's voor statische compressie (zoals UPX, yoda, ASPack, FGS, enz.)



4.1.6.2 Opties

In de sectie **Opties** kan de gebruiker de methoden selecteren die moeten worden gebruikt bij het scannen van het systeem op infiltraties. De volgende opties zijn beschikbaar:



Kenmerken – Kenmerken kunnen infiltraties op exacte en betrouwbare wijze detecteren en identificeren met behulp van viruskenmerken.

Heuristiek – Heuristiek is een algoritme dat de (schadelijke) activiteit van programma's analyseert. Het voornaamste voordeel van heuristiek is het vermogen om schadelijke software te identificeren die nog niet bestond of niet bekend was in de lijst met bekende virussen (database met viruskenmerken).

Geavanceerde heuristiek – Geavanceerde heuristiek bestaat uit een uniek heuristisch algoritme dat door ESET is ontwikkeld en is geoptimaliseerd voor het detecteren van computerwormen en Trojaanse paarden. Dit algoritme is geschreven in programmeertalen van hoog niveau. De geavanceerde heuristiek breidt de detectie-intelligentie van het programma aanzienlijk uit.

Adware/spyware/riskware – Deze categorie omvat software waarmee allerlei vertrouwelijke gegevens over gebruikers worden verzameld zonder dat zij dit weten en zonder dat zij hiervoor toestemming hebben gegeven. Deze categorie omvat tevens software waarmee reclamemateriaal wordt weergegeven.

Potentieel onveilige toepassingen – Potentieel onveilige toepassingen is de classificatie voor commerciële, legitieme software. Het omvat programma's zoals hulpmiddelen voor externe toegang. Dat is de reden waarom deze optie standaard is uitgeschakeld.

Potentieel ongewenste toepassingen – Potentieel ongewenste toepassingen zijn niet per se schadelijk maar kunnen de prestaties van uw computer aantasten. Voor de installatie van dergelijke toepassingen moet doorgaans expliciet toestemming worden gegeven. Deze toepassingen veranderen de manier waarop uw computer werkt (vergeleken met de status van de computer voorafgaand aan de installatie). De meest ingrijpende wijzigingen omvatten ongewenste pop-upvensters, activering en uitvoering van verborgen processen, toegenomen gebruik van systeembronnen, wijzigingen in zoekresultaten en programma's die communiceren met externe servers.

4.1.6.3 Opschonen

De opschooninstellingen bepalen het gedrag van de scanner tijdens het opschonen van geïnfecteerde bestanden. Er zijn 3 opschoonniveaus:

Niet opschonen

Geïnfecteerde bestanden worden niet automatisch opgeschoond. Er wordt een waarschuwingvenster weergegeven en de gebruiker kan een actie kiezen.

Standaardniveau

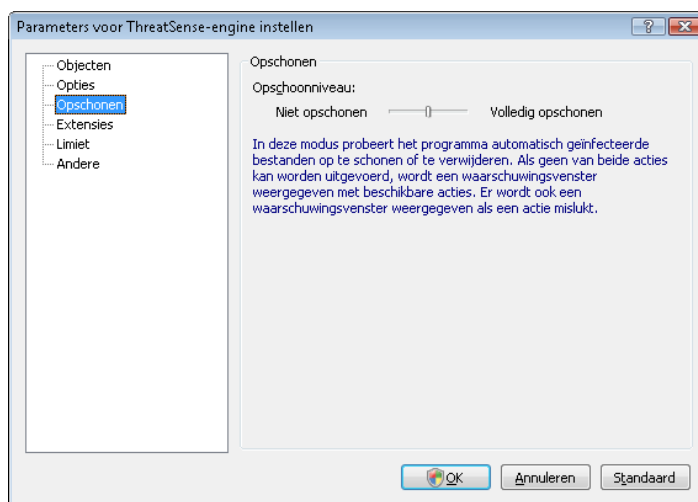
Er wordt automatisch geprobeerd een geïnfecteerd bestand op te schonen of te verwijderen. Als het niet mogelijk is de juiste actie automatisch te selecteren, wordt een selectie van vervolgacties aangeboden. De beschikbare vervolgacties worden tevens weergegeven als een vooraf gedefinieerde actie niet kon worden voltooid.

Volledig opschonen

Alle geïnfecteerde bestanden (inclusief archieven) worden opgeschoond of verwijderd. De enige uitzonderingen zijn systeembestanden. Als deze niet kunnen worden opgeschoond, wordt een waarschuwingvenster geopend waarin de gebruiker een actie kan selecteren.

Waarschuwing:

In de standaardmodus wordt het hele archiefbestand alleen verwijderd als alle bestanden in het archief geïnfecteerd zijn. Als het archief ook legitieme bestanden bevat, wordt het niet verwijderd. Als een geïnfecteerd archiefbestand wordt gedetecteerd in de modus Volledig opschonen, wordt het hele archief verwijderd, zelfs als er schone bestanden aanwezig zijn.



4.1.6.4 Extensies

Een extensie maakt deel uit van de bestandsnaam en wordt afgebakend door een punt. De extensie definieert het type en de inhoud van het bestand. In dit gedeelte van de instellingen voor ThreatSense-parameters kunt u de typen bestanden definiëren die u wilt scannen.

Standaard worden alle bestanden gescand, ongeacht hun extensie. Elke extensie kan worden toegevoegd aan de lijst met bestanden die zijn uitgesloten van scannen. Als het selectievakje **Alle bestanden scannen** is uitgeschakeld, worden in de lijst alle extensies van momenteel gescande bestanden weergegeven. Met de knoppen **Toevoegen** en **Verwijderen** kunt u het scannen van gewenste extensies inschakelen of verbieden.

U kunt het scannen van bestanden zonder extensie activeren door de optie **Bestanden zonder extensie scannen** te selecteren.

Het uitsluiten van bestanden van scannen is nuttig als het scannen van bepaalde bestandstypen een onjuiste werking veroorzaakt van het programma dat de extensies gebruikt. Zo kan het raadzaam zijn de extensies .EDB, .EML en .TMP uit te sluiten als gebruik wordt gemaakt van de MS Exchange-server.

4.1.6.5 Limiet

Gebruik de sectie Limiet om de maximale grootte op te geven van objecten die moeten worden gescand, evenals het maximale niveau voor het scannen van geneste archieven:

Maximale objectgrootte (bytes)

De maximale grootte van objecten die moeten worden gescand. De antivirusmodule scant dan alleen objecten die kleiner zijn dan de opgegeven grootte. Het is in de meeste gevallen niet nodig de standaardwaarde te wijzigen. De waarde mag alleen worden gewijzigd door gevorderde gebruikers die een specifieke reden hebben om grotere objecten niet te scannen.

Maximale scantijd voor object (sec.)

De maximale tijd voor het scannen van een object. Als hier een waarde is ingevoerd, wordt het scannen van een object beëindigd wanneer die tijd is verstreken, ongeacht of de scan is voltooid.

Nestingsniveau voor archieven

Het maximum aantal niveaus waarop archieven moeten worden gescand. Het is in de meeste gevallen niet nodig de standaardwaarde van 10 te wijzigen. Als het scannen voortijdig wordt afgebroken omdat archieven dieper dan 10 niveaus zijn genest, worden archieven op lagere niveaus niet gecontroleerd.

Maximale grootte van bestanden in archief (bytes)

Gebruik deze optie om de maximale bestandsgrootte op te geven voor bestanden in archieven (als deze worden uitgepakt) die moeten worden gescand. Als het scannen van een archief om deze reden voortijdig wordt afgebroken, blijft het archief ongecontroleerd.

4.1.6.6 Andere

Alternatieve gegevensstromen (ADS) scannen

Alternatieve gegevensstromen (ADS) die worden gebruikt door het NTFS-bestandssysteem zijn bestands- en mapkoppelingen die onzichtbaar zijn voor normale scantechnieken. Veel infiltraties proberen detectie te vermijden door zichzelf te vermommen als alternatieve gegevensstromen.

Achtergrondscans uitvoeren met lage prioriteit

Elke scanprocedure neemt een bepaalde hoeveelheid systeembronnen in beslag. Als u werkt met programma's waarbij de systeembronnen zwaar worden belast, kunt u achtergrondscans met lage prioriteit inschakelen en zo bronnen besparen voor uw toepassingen.

Alle objecten in logbestand opnemen

Als deze optie wordt geselecteerd, worden alle gescande bestanden, zelfs de niet-geïnfecteerde, in het logbestand vermeld.

Tijdstempel laatste toegang bewaren

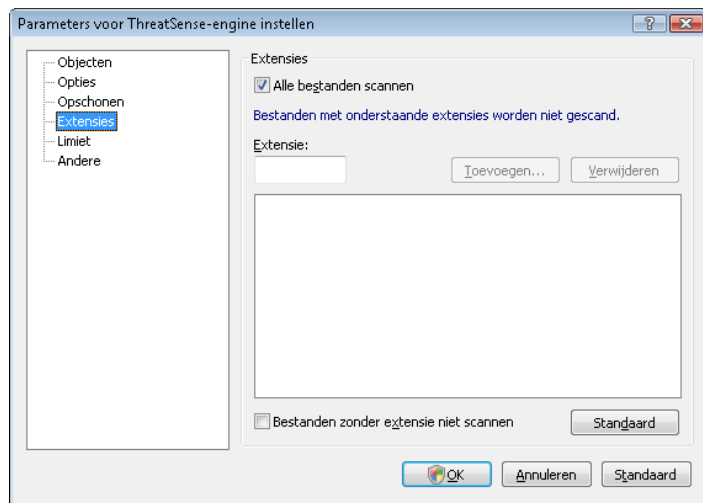
Selecteer deze optie om de oorspronkelijke toegangstijd van gescande bestanden te handhaven in plaats van deze bij te werken (bijvoorbeeld voor gebruik met back-upsystemen).

Scanlogboek doorbladeren

Met deze optie kunt u het doorbladeren van het logboek in- of uitschakelen. Als u deze optie selecteert, wordt de informatie in het venster omhoog geschoven.

Melding over voltooiing van scan weergeven in afzonderlijk venster

Informatie over de scanresultaten wordt in een afzonderlijk venster weergegeven.



4.1.7 Er is een infiltratie gedetecteerd

Infiltraties kunnen het systeem bereiken vanaf verschillende toegangspunten: webpagina's, gedeelde mappen, via e-mail of via verwisselbare computermedia (USB, externe schijven, cd's, dvd's, diskettes, enz.).

Als de computer tekenen van infectie door malware vertoont, bijvoorbeeld trager is, vaak vastloopt, enz., adviseren wij u het volgende te doen:

- Open ESET NOD32 Antivirus en klik op **Computerscan**.
- Klik op de knop **Standaardscan** (zie Standaardscan voor meer informatie).
- Nadat de scan is voltooid, controleert u in het logbestand het aantal gescande, geïnfecteerde en opgeschoonde bestanden.

Als u alleen een bepaald gedeelte van uw schijf wilt scannen, klikt u op **Aangepaste scan** en selecteert u doelen die u wilt scannen op virussen.

Als algemeen voorbeeld van hoe infiltraties worden afgehandeld in ESET NOD32 Antivirus, gaan we ervan uit dat een infiltratie is gedetecteerd door de real-timebestandssysteembewaking, die gebruikmaakt van

het standaardopschoonniveau. Deze zal proberen om het bestand op te schonen of te verwijderen. Als er geen vooraf gedefinieerde actie is die de module voor real-timebeveiliging kan uitvoeren, wordt u via een waarschuwingsvenster gevraagd om een optie te selecteren. Gewoonlijk zijn de opties **Opschonen**, **Verwijderen** en **Verlaten** beschikbaar. Het wordt niet aanbevolen **Verlaten** te selecteren aangezien de geïnfecteerde bestanden dan ongemoeid zouden worden gelaten. De enige uitzondering is wanneer u er zeker van bent dat het bestand onschadelijk is en per vergissing is gedetecteerd.



Opschonen en verwijderen

Pas opschonen toe als een schoon bestand is aangevallen door een virus dat schadelijke code aan het opgeschoonde bestand heeft toegevoegd. Als dit het geval is, probeert u eerst het geïnfecteerde bestand op te schonen zodat het in de oorspronkelijke staat kan worden hersteld. Als het bestand uitsluitend uit schadelijke code bestaat, wordt het verwijderd.

Als een geïnfecteerd bestand is vergrendeld of wordt gebruikt door een systeemproces, wordt het gewoonlijk pas verwijderd nadat het is vrijgegeven (gewoonlijk na een herstart van het systeem).

Bestanden in archieven verwijderen

In de modus Standaard opschonen wordt het volledige archief alleen verwijderd als dit uitsluitend geïnfecteerde en geen schone bestanden bevat. Met andere woorden, archieven worden niet verwijderd als zij ook onschadelijke, schone bestanden bevatten. Wees echter voorzichtig bij het gebruik van een scan in de modus Volledig opschonen: hierbij wordt het archief verwijderd als het minimaal één geïnfecteerd bestand bevat, ongeacht de status van andere bestanden in het archief.

4.2 Het programma bijwerken

Het regelmatig bijwerken van het systeem geldt als basisvereiste voor een maximaal beveiligingsniveau via ESET NOD32 Antivirus. De module Update waarborgt dat het programma altijd actueel is. Dit gebeurt op twee manieren: door het bijwerken van de database met viruskenmerken en door het bijwerken van alle systeemonderdelen.

U kunt informatie over de huidige updatestatus, inclusief de huidige versie van de database met viruskenmerken en of er een update is vereist, bekijken door op **Update** te klikken. Tegelijkertijd is de optie voor het direct activeren van het updateproces, **Database viruskenmerken bijwerken**, beschikbaar, alsmede basisinstellingsopties voor update, zoals de gebruikersnaam en het wachtwoord om toegang te krijgen tot de updateservers van ESET.

Het informatievenster bevat tevens details zoals de datum en het tijdstip van de laatste succesvolle update en het nummer van de database met viruskenmerken. Deze numerieke aanduiding vormt een actieve koppeling naar de website van ESET, met een lijst met alle kenmerken die in de desbetreffende update zijn toegevoegd.

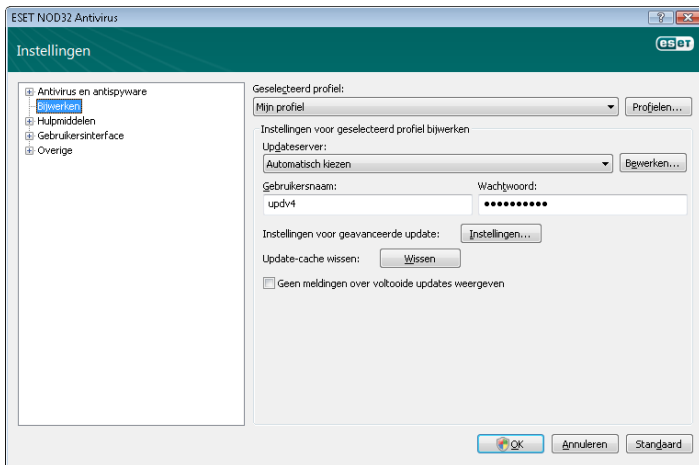
Met de koppeling **Registreren** kunt u het registratieformulier openen voor de registratie van uw nieuwe licentie bij ESET, waarna uw verificatiegegevens naar uw e-mailadres worden gestuurd.



OPMERKING: de gebruikersnaam en het wachtwoord worden door ESET verstrekt na aanschaf van ESET NOD32 Antivirus.

4.2.1 Update-instellingen

In het gedeelte met instellingen voor update wordt de broninformatie voor de update, zoals de updateservers en verificatiegegevens voor deze servers, opgegeven. Het veld **Updateserver:** is standaard ingesteld op **Automatisch kiezen**. Deze waarde zorgt ervoor dat updatebestanden automatisch worden gedownload van de servers van ESET met de laagste netwerkbelasting. De instellingen voor de update zijn beschikbaar in de sectie Geavanceerde instellingen (F5) onder **Update**.



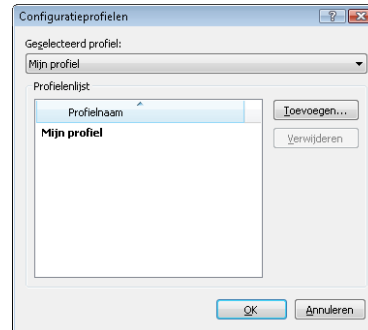
De lijst met huidige bestaande updateservers is toegankelijk via de vervolgkeuzelijst **Updateserver:**. U kunt een nieuwe updateserver toevoegen door op **Bewerken...** te klikken in de sectie **Instellingen voor geselecteerd profiel bijwerken** en vervolgens op de knop **Toevoegen** te klikken.

Verificatie voor updateservers vindt plaats op basis van de **gebruikersnaam** en het **wachtwoord**, die zijn gegenereerd en door ESET naar de gebruiker gezonden nadat deze de productlicentie heeft aangeschaft.

4.2.1.1 Updateprofielen

Voor verschillende updateconfiguraties kunnen door de gebruiker gedefinieerde updateprofielen worden gemaakt die kunnen worden gebruikt voor een specifieke updatetaak. Het maken van verschillende updateprofielen is met name handig voor mobiele gebruikers, aangezien de eigenschappen van de internetverbinding regelmatig veranderen. Door de updatetaak te wijzigen, kunnen mobiele gebruikers opgeven dat, als het niet mogelijk is het programma bij te werken via de configuratie die is opgegeven in **Mijn profiel**, de update wordt uitgevoerd met een alternatief profiel.

In de vervolgkeuzelijst **Geselecteerd profiel** wordt het huidige geselecteerde profiel weergegeven. Standaard is deze vermelding ingesteld op **Mijn profiel**. U kunt een nieuw profiel maken door op de knop **Profielen...** te klikken en vervolgens op **Toevoegen...** te klikken en uw eigen **profielnaam** in te voeren. Bij het maken van een nieuw profiel kunt u instellingen kopiëren van een bestaand profiel door dit profiel te selecteren in de vervolgkeuzelijst **Instellingen uit profiel kopiëren**:



Binnen de profielinstellingen kunt u de updateserver opgeven waarmee het programma verbinding maakt en waarvan updates worden gedownload. Elke server in de lijst met beschikbare servers kan worden gebruikt of er kan een nieuwe server worden toegevoegd. De lijst met bestaande updateservers is toegankelijk via de vervolgkeuzelijst **Updateserver:** U kunt een nieuwe updateserver toevoegen door op **Bewerken...** te klikken in de sectie **Instellingen voor geselecteerd profiel bijwerken** en vervolgens op de knop **Toevoegen** te klikken.

4.2.1.2 Instellingen voor geavanceerde update

U kunt de **Instellingen voor geavanceerde update** bekijken door op de knop **Instellingen...** te klikken. De instellingen voor geavanceerde update omvatten configuratie van **Updatemodus**, **HTTP-proxy**, **LAN** en **Mirror**.

4.2.1.2.1 Updatemodus

Het tabblad **Updatemodus** bevat opties met betrekking tot de update van programmaonderdelen.

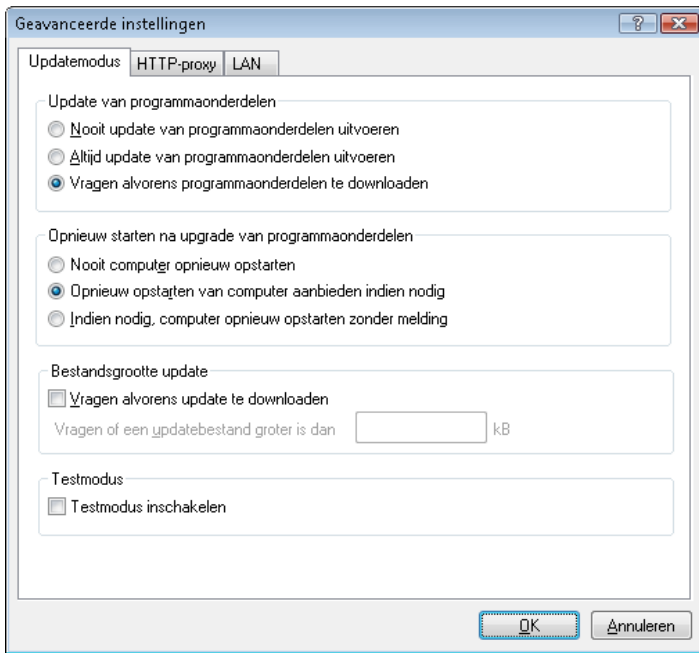
In de sectie **Update van programmaonderdelen** zijn drie opties beschikbaar:

- **Nooit update van programmaonderdelen uitvoeren**
- **Altijd update van programmaonderdelen uitvoeren**
- **Vragen alvorens programmaonderdelen te downloaden**

Door de optie **Nooit update van programmaonderdelen uitvoeren** te selecteren, zorgt u ervoor dat een nieuwe update van programmaonderdelen die is uitgegeven door ESET niet wordt gedownload en dat geen update van programmaonderdelen zal plaatsvinden op het desbetreffende werkstation. De optie **Altijd update van programmaonderdelen uitvoeren** betekent dat updates van programmaonderdelen worden uitgevoerd telkens wanneer een nieuwe update beschikbaar komt op de updateservers van ESET en dat een upgrade van de programmaonderdelen plaatsvindt naar de gedownloade versie.

Selecteer de derde optie, **Vragen alvorens programmaonderdelen te downloaden**, om ervoor te zorgen dat het programma de gebruiker zal vragen om het downloaden van updates van programmaonderdelen te bevestigen op het moment dat dergelijke updates beschikbaar komen. In dat geval wordt een dialoogvenster weergegeven met informatie over de beschikbare updates voor programmaonderdelen, met de optie om te bevestigen of te weigeren. Bij bevestiging worden updates gedownload en worden nieuwe programmaonderdelen geïnstalleerd.

De standaardoptie voor een update van programmaonderdelen is **Vragen alvorens programmaonderdelen te downloaden**.



Na installatie van een update van programmaonderdelen, moet het systeem opnieuw worden opgestart, zodat alle modules de volledige functionaliteit kunnen bieden. De sectie **Opnieuw starten na upgrade van programmaonderdelen** stelt de gebruiker in staat een van de volgende drie opties te selecteren:

- **Computer nooit opnieuw opstarten**
- **Herstart computer aanbieden indien nodig**
- **Indien nodig, computer opnieuw opstarten zonder melding**

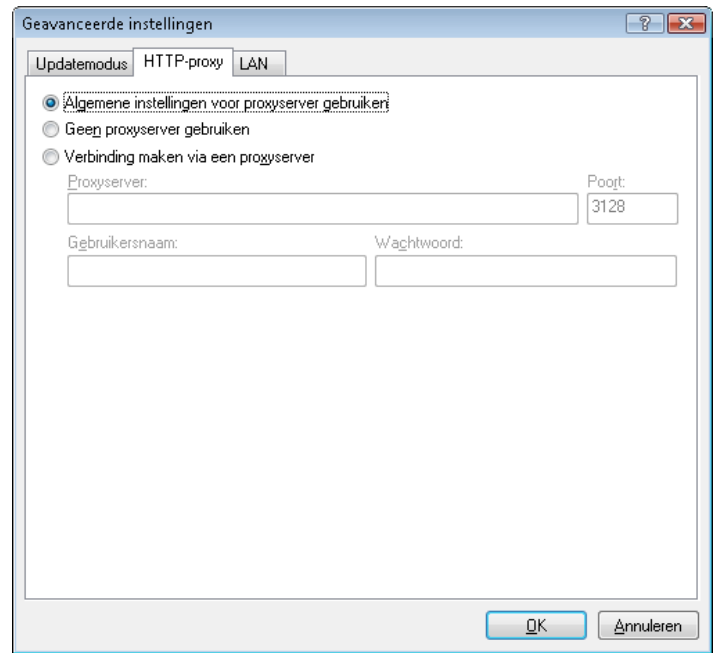
De standaardoptie voor opnieuw opstarten is **Herstart computer aanbieden indien nodig**. De selectie van de meest geschikte opties voor updates van programmaonderdelen op het tabblad **Updatemodus** kan voor elk individueel werkstation weer anders zijn, omdat dit de plek is waar deze instellingen moeten worden toegepast. Houd er rekening mee dat er verschillen bestaan tussen werkstations en servers. Zo kan het automatisch opnieuw opstarten van de server na een programma-upgrade ernstige schade veroorzaken.

4.2.1.2.2 Proxyserver

U kunt als volgt toegang krijgen tot de instellingsopties voor proxy servers voor een bepaald updateprofiel: Klik op **Update** in de menustructuur van Geavanceerde instellingen (F5) en klik vervolgens op de knop **Instellingen...** rechts van **Instellingen voor geavanceerde update**. Klik op de tab **HTTP-proxy** en selecteer een van de drie volgende opties:

- **Algemene instellingen voor proxyserver gebruiken**
- **Geen proxyserver gebruiken**
- **Verbinding maken via een proxyserver** (verbinding gedefinieerd door de verbindingseigenschappen)

Als u de optie **Algemene instellingen voor proxyserver gebruiken** selecteert, wordt gebruikgemaakt van alle opties voor configuratie van de proxyserver die al zijn opgegeven binnen de tak **Overige > Proxyserver** van de structuur voor geavanceerde instellingen.



Selecteer de optie **Geen proxyserver gebruiken** om expliciet te definiëren dat geen proxyserver zal worden gebruikt voor het bijwerken van ESET NOD32 Antivirus.

De optie **Verbinding maken via een proxyserver** kan worden gekozen als wel een proxyserver moet worden gebruikt voor het bijwerken van ESET NOD32 Antivirus en deze afwijkt van de proxyserver die is opgegeven in de algemene instellingen (**Overige > Proxyserver**). Als dat het geval is, moeten de instellingen hier worden opgegeven: **proxyserveradres**, communicatie**poort**, plus **gebruikersnaam** en **wachtwoord** voor de proxyserver, indien vereist.

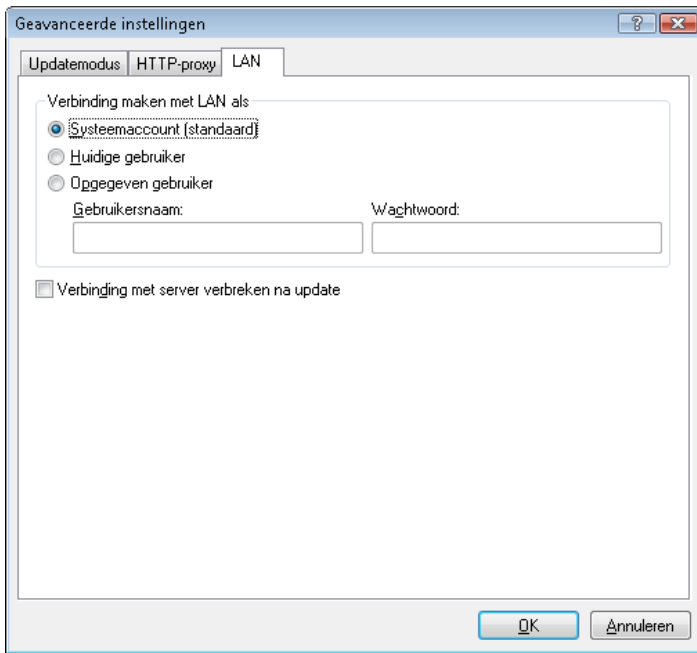
Deze optie moet tevens worden geselecteerd als de instellingen voor de proxyserver niet algemeen zijn ingesteld, maar ESET NOD32 Antivirus wel verbinding maakt met een proxyserver voor updates.

De standaardinstelling voor de proxyserver is **Algemene instellingen voor proxyserver gebruiken**.

4.2.1.2.3 Verbinding maken met LAN

Bij het bijwerken vanaf een lokale server waarop een op NT gebaseerd besturingssysteem wordt uitgevoerd, is standaardverificatie vereist voor elke netwerkverbinding. In de meeste gevallen beschikt een lokale systeemaccount niet over voldoende toegangsrechten voor de mirror-map (de mirror-map bevat kopieën van updatebestanden). Als dit het geval is, geeft u de gebruikersnaam en het wachtwoord op in de sectie voor instellingen voor update of geeft u een bestaande account op waarmee het programma toegang verkrijgt tot de updateserver (Mirror).

U kunt een dergelijke account configureren door op de tab **LAN** te klikken. De sectie **Verbinding maken met LAN als** biedt de opties **Systeemaccount (standaard)**, **Huidige gebruiker** en **Opgegeven gebruiker**.



Selecteer de optie **Systeemaccount** om de systeemaccount te gebruiken voor verificatie. Normaliter vindt geen verificatieproces plaats als er geen verificatiegegevens beschikbaar worden gesteld in het hoofdgedeelte voor instellingen voor update.

U kunt ervoor zorgen dat het programma zichzelf autoriseert via een momenteel aangemelde gebruikersaccount door **Huidige gebruiker** te selecteren. Het nadeel van deze oplossing is dat het programma geen verbinding kan maken met de updateserver als momenteel geen gebruiker is aangemeld.

Selecteer **Opgegeven gebruiker** als u wilt dat het programma een specifieke gebruikersaccount gebruikt voor verificatie.

De standaardoptie voor LAN-verbinding is **Systeemaccount**.

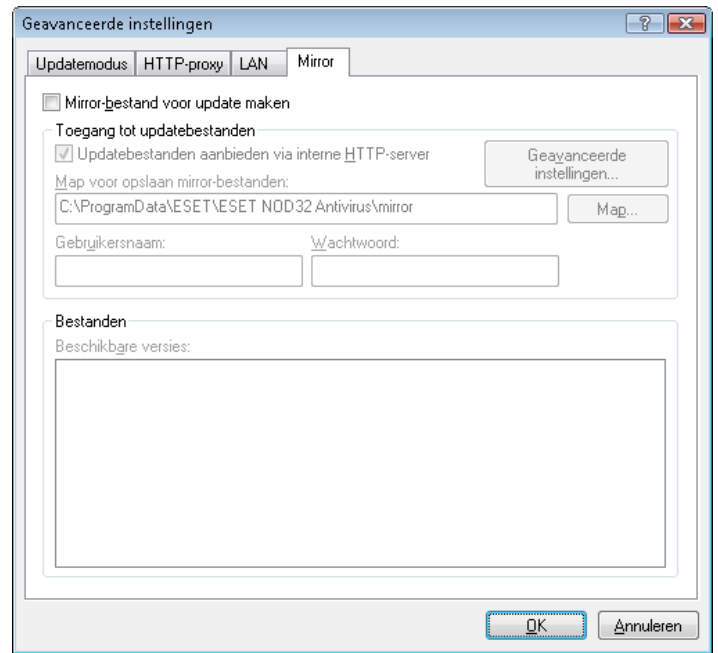
Waarschuwing:

Als **Huidige gebruiker** of **Opgegeven gebruiker** is ingeschakeld, kan er een fout optreden bij het wijzigen van de identiteit van het programma naar de gewenste gebruiker. Daarom adviseren wij de LAN-verificatiegegevens op te nemen in het hoofdgedeelte van de instellingen voor update. In dit gedeelte van de instellingen voor update moeten de verificatiegegevens als volgt worden ingevoerd: domeinnaam\gebruiker (als het een werkgroep betreft, voert u werkgroepnaam\naam in) en het wachtwoord van de gebruiker. Bij het bijwerken vanaf de HTTP-versie van de lokale server is geen verificatie vereist.

4.2.1.2.4 Updatekopieën maken – Mirror

In ESET NOD32 Antivirus Business Edition kan de gebruiker kopieën maken van updatebestanden, die kunnen worden gebruikt voor het bijwerken van andere werkstations in het netwerk. Als clientwerkstations worden bijgewerkt op basis van een mirror wordt de netwerkbelasting gelijkmatig verdeeld en wordt bandbreedte voor uw internetverbinding bespaard.

Configuratieopties voor de lokale server Mirror zijn toegankelijk (nadat u een geldige licentiesleutel hebt ingevoerd in licentiebeheer, die zich in de sectie Geavanceerde instellingen van ESET NOD32 Antivirus Business Edition bevindt) in de sectie **Instellingen voor geavanceerde update:** (u kunt toegang tot deze sectie krijgen door op F5 te drukken en op **Update** te klikken in de menustructuur van Geavanceerde instellingen. Klik op de knop **Instellingen...** naast **Instellingen voor geavanceerde update:** en selecteer het tabblad **Mirror**).



De eerste stap bij het configureren van de mirror is het inschakelen van het selectievakje **Update mirror maken**. Als deze optie wordt geselecteerd, worden andere configuratieopties voor mirrors, zoals de manier waarop updatebestanden worden geopend en het updatepad naar de mirror-bestanden, ingeschakeld.

De methoden voor mirror-activering worden beschreven in het volgende hoofdstuk, "Varianten van het openen van de mirror". Nu beperken we ons tot de opmerking dat er twee basisvarianten voor het openen van de mirror zijn. De map met updatebestanden kan namelijk worden gepresenteerd als een gedeelde netwerkmap of als een HTTP-server.

De map die specifiek is bestemd voor het opslaan van updatebestanden voor de mirror wordt gedefinieerd in de sectie **Map voor opslaan mirror-bestanden**. Klik op **Map...** om te bladeren naar een gewenste map op de lokale computer of naar een gedeelde netwerkmap. Als verificatie voor de opgegeven map is vereist, moeten verificatiegegevens worden ingevoerd in de velden **Gebruikersnaam** en **Wachtwoord**. De gebruikersnaam en het wachtwoord moeten worden ingevoerd in de notatie *Domein/Gebruiker* of *Werkgroep/Gebruiker*. Geef ook de bijbehorende wachtwoorden op.

Bij het opgeven van een gedetailleerde mirror-configuratie kunt u tevens de taalversie specificeren waarvoor updatekopieën moeten worden gedownload. De instellingen voor de taalversie kunnen worden uitgevoerd in de sectie **Bestanden – Beschikbare versies:**

4.2.1.2.4.1 Bijwerken vanaf de mirror

Er zijn twee basismethoden voor het configureren van de mirror. De map met updatebestanden kan namelijk worden gepresenteerd als een gedeelde netwerkmap of als een HTTP-server.

Toegang tot de mirror verkrijgen via een interne HTTP-server

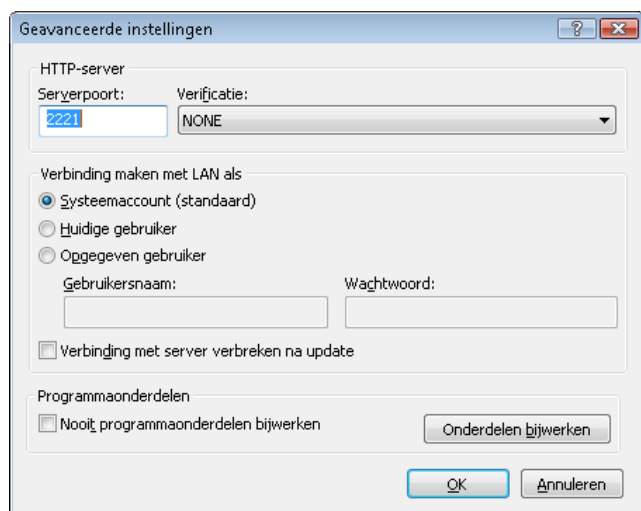
Deze configuratie is de standaardmethode, die is geconfigureerd in de vooraf gedefinieerde configuratie van het programma. U kunt toegang tot de mirror bieden via de HTTP-server door naar **Instellingen voor geavanceerde update** (het tabblad **Mirror**) te navigeren en de optie **Update mirror maken** te selecteren.

In de sectie **Geavanceerde instellingen** van het tabblad **Mirror** kunt u de **serverpoort** opgeven waarop de HTTP-server zal luisteren alsmede het type **verificatie** dat wordt gebruikt door de HTTP-server. Standaard is de serverpoort ingesteld op de waarde **2221**. De optie **Verificatie** definieert de verificatiemethode die wordt gebruikt voor toegang tot de updatebestanden. De volgende opties zijn beschikbaar: **GEEN**, **Standaard** en **NTLM**. Selecteer **Standaard** om de base64-codering met standaardverificatie van gebruikersnaam

en wachtwoord te gebruiken. De optie **NTLM** biedt codering via een veilige coderingsmethode. Voor verificatie wordt gebruikgemaakt van de gebruiker die is gemaakt op het werkstation dat de updatebestand deelt. De standaardinstelling is **GEEN**, waarbij toegang tot de updatebestanden wordt geboden zonder dat verificatie is vereist.

Waarschuwing:

Als u toegang tot de updatebestanden wilt bieden via de HTTP-server, moet de mirror-map zich op dezelfde computer bevinden als de instantie van ESET NOD32 Antivirus deze map maakt.



Nadat de configuratie van de mirror is voltooid, gaat u naar de werkstations en voegt u een nieuwe updateserver toe in de notatie **http://IP-adres_van_uw_server:2221**. Dit kunt u doen door de onderstaande stappen uit te voeren:

- Open **Geavanceerde instellingen van ESET NOD32 Antivirus** en klik op **Update**.
- Klik op **Bewerken...** rechts van de vervolgkeuzelijst **Updateserver** en voeg een nieuwe server toe in de volgende notatie: **http://IP-adres_van_uw_server:2221**
- Selecteer deze nieuw toegevoegde server in de lijst met updateservers.

De mirror openen via systeemshares

Als eerste moet een gedeelde map worden gemaakt op een lokaal of een netwerkapparaat. Bij het maken van de map voor de mirror is het noodzakelijk om de gebruiker die bestanden zal opslaan in de map 'schrijftoegang' te verlenen en alle gebruikers die ESET NOD32 Antivirus zullen bijwerken vanuit de mirror-map 'leestoegang' te geven.

Ga vervolgens verder met de configuratie van de toegang tot de mirror in de sectie **Instellingen voor geavanceerde update** (het tabblad **Mirror**) door de optie **Updatebestanden leveren via interne HTTP-server** uit te schakelen. Deze optie is standaard ingeschakeld in het installatiepakket van het programma.

Als de gedeelde map zich op een andere computer in het netwerk bevindt, moet u verificatiegegevens voor het verkrijgen van toegang tot de andere computer opgeven. U kunt verificatiegegevens opgeven door Geavanceerde instellingen van ESET NOD32 Antivirus (F5) te openen en op **Update** te klikken. Klik op de knop **Instellingen...** en klik vervolgens op de tab **LAN**. Deze instelling is hetzelfde als bij bijwerken, zoals beschreven in het hoofdstuk "Verbinding maken met LAN".

Nadat de mirror-configuratie is voltooid, gaat u naar de werkstations en stelt u **\\UNC\PAD** in als de updateserver. Deze bewerking kan als volgt worden uitgevoerd:

- Open Geavanceerde instellingen van ESET NOD32 Antivirus en klik op **Update**

- Klik op **Bewerken...** naast de updateserver en voeg een nieuwe server toe in de notatie **\\UNC\PAD**.
- Selecteer deze nieuw toegevoegde server in de lijst met updateservers.

OPMERKING: voor een juiste werking moet het pad naar de mirror-map worden gespecificeerd als een UNC-pad. Updates vanaf toegewezen stations werken mogelijk niet.

4.2.1.2.4.2 Updateproblemen met mirrors oplossen

Afhankelijk van de methode voor het openen van de mirror-map, kunnen zich verschillende typen problemen voordoen. In de meeste gevallen worden problemen tijdens een update vanaf een mirror-server veroorzaakt door het volgende: onjuiste specificatie van de opties voor de mirror-map, onjuiste verificatiegegevens voor de mirror-map, onjuiste configuratie op lokale werkstations die proberen updatebestanden te downloaden van de mirror, of een combinatie van bovengenoemde redenen. Hier geven wij een overzicht van de meestvoorkomende problemen die zich kunnen voordoen bij een update vanaf de mirror:

- **ESET NOD32 Antivirus meldt een fout bij het maken van een verbinding met de mirror-server** – waarschijnlijk veroorzaakt door een onjuiste specificatie van de updateserver (netwerkpad naar de mirror-map) van waar lokale werkstations updates downloaden. U kunt de map controleren door op het Windows-menu **Start** te klikken, op **Uitvoeren** te klikken, de mapnaam in te voeren en op **OK** te klikken. De inhoud van de map zou nu moeten worden weergegeven.
- **ESET NOD32 Antivirus vereist een gebruikersnaam en wachtwoord** – waarschijnlijk veroorzaakt door de onjuiste invoer van verificatiegegevens (gebruikersnaam en wachtwoord) in het updategedeelte. De gebruikersnaam en het wachtwoord worden gebruikt om toegang te verlenen tot de updateserver, van waar het programma zichzelf bijwerkt. Controleer of de verificatiegegevens juist zijn en zijn ingevoerd in de juiste notatie. Bijvoorbeeld *Domein/Gebruikersnaam* of *Werkgroep/Gebruikersnaam*, plus de bijbehorende wachtwoorden. Als de mirror-server toegankelijk is voor "Iedereen", moet u zich realiseren dat dit niet betekent dat elke gebruiker zomaar toegang kan krijgen. "Iedereen" betekent niet elke onbevoegde gebruiker, maar alleen dat de map toegankelijk is voor alle domeingebruikers. Het resultaat is dat, ook als de map toegankelijk is voor "Iedereen", nog steeds een domeingebruikersnaam en wachtwoord moet worden ingevoerd in het gedeelte voor het instellen van de update.

- **ESET NOD32 Antivirus rapporteert een fout bij het tot stand brengen van een verbinding met de mirror-server** – de communicatie op de poort die is gedefinieerd voor toegang tot de HTTP-versie van de mirror is geblokkeerd.

4.2.2 Updatetaken maken

Updates kunnen handmatig worden geactiveerd, door de optie **Database viruskenmerken bijwerken** te selecteren in het informatievenster dat wordt weergegeven nadat u op **Update** hebt geklikt in het hoofdmenu.

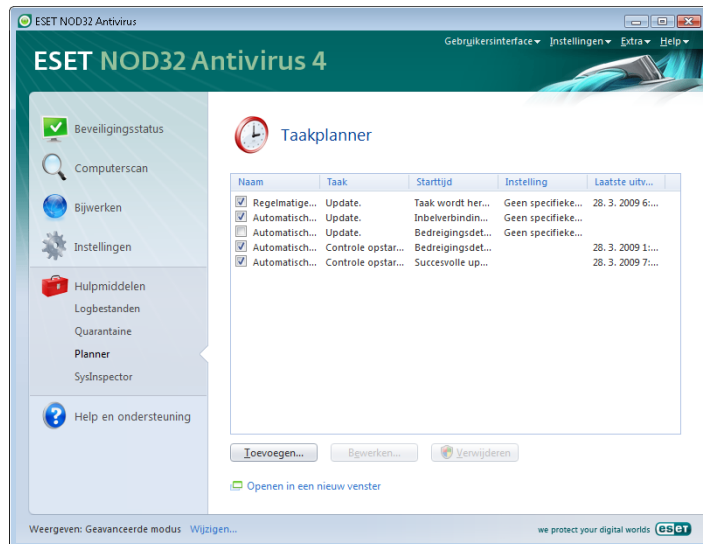
Updates kunnen ook worden uitgevoerd als geplande taken – Configureer een geplande taak door op **Hulpmiddelen > Planner** te klikken. Standaard worden in ESET NOD32 Antivirus de volgende taken geactiveerd:

- **Regelmatige automatische update**
- **Automatisch update uitvoeren na inbelverbinding**
- **Automatische update na aanmelding gebruiker**

Elk van de bovengenoemde updatetaken kan worden gewijzigd om te voldoen aan uw behoeften. Behalve de standaardupdatetaken kunt u ook nieuwe updatetaken maken met een door de gebruiker gedefinieerde configuratie. Zie het hoofdstuk "Planner" voor meer informatie over het maken en configureren van updatetaken.

4.3 Planner

Planner is beschikbaar als de geavanceerde modus in ESET NOD32 Antivirus is geactiveerd. **Planner** is te vinden in het hoofdmenu van ESET NOD32 Antivirus onder **Hulpmiddelen**. Planner bevat een overzichtslijst met alle geplande taken en hun configuratie-eigenschappen, zoals de vooraf gedefinieerde datum en tijd en het gebruikte scanprofiel.



Standaard worden in het programma de volgende geplande taken in **Planner** weergegeven:

- **Regelmatige automatische update**
- **Automatisch update uitvoeren na inbelverbinding**
- **Automatische update na aanmelding gebruiker**
- **Automatisch controle van opstartbestanden uitvoeren na aanmelding gebruiker**
- **Automatisch controle van opstartbestanden uitvoeren na succesvolle update van de database voor viruskenmerken**

U kunt de configuratie van een bestaande geplande taak (zowel standaard als door de gebruiker gedefinieerd) bewerken door met de rechtermuisknop op de taak te klikken en op **Bewerken...** te klikken of door de taak die u wilt wijzigen te selecteren en op de knop **Bewerken...** te klikken.

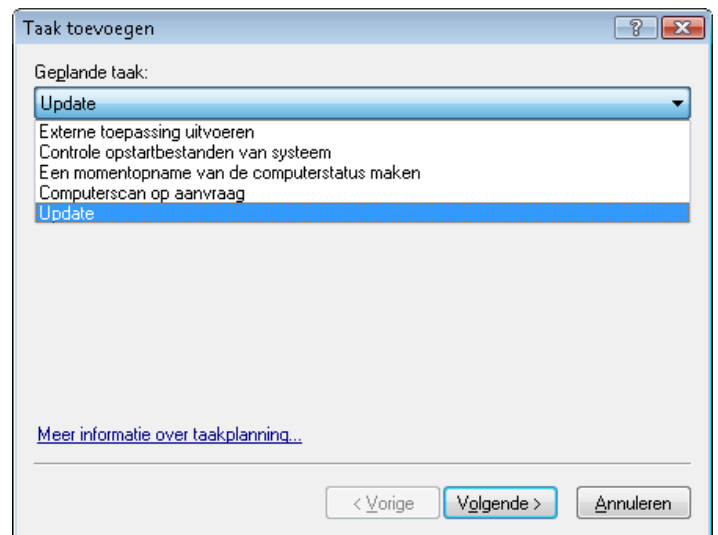
4.3.1 Doel van geplande taken

Planner beheert en start geplande taken met vooraf gedefinieerde configuratie en eigenschappen. De configuratie en eigenschappen bevatten informatie zoals de datum en tijd alsmede opgegeven profielen die moeten worden gebruikt tijdens de uitvoering van de taak.

4.3.2 Nieuwe taken maken

U kunt een nieuwe taak maken in Planner door op de knop **Toevoegen...** te klikken of door met de rechtermuisknop te klikken en **Toevoegen...** te selecteren in het contextmenu. Er zijn vijf typen geplande taken beschikbaar:

- **Externe toepassing uitvoeren**
- **Logbestanden onderhouden**
- **Controle opstartbestanden van systeem**
- **Computerscan op aanvraag**
- **Update**



Aangezien **Computerscan op aanvraag** en **Update** de meest gebruikte geplande taken zijn, leggen wij uit hoe u een nieuwe update taak kunt toevoegen.

Selecteer **Update** in de vervolgkeuzelijst **Geplande taak**: Klik daarna op **Volgende** en geef de naam van de taak op in het veld **Taaknaam**: Selecteer de frequentie van de taak. De volgende opties zijn beschikbaar: **Eenmaal**, **Herhaaldelijk**, **Dagelijks**, **Wekelijks** en **Bij-gebeurtenis**. Op basis van de geselecteerde frequentie wordt u gevraagd om waarden voor verschillende updateparameters in te voeren. Vervolgens definieert u welke actie moet worden ondernomen als de taak niet kan worden uitgevoerd of voltooid op het geplande tijdstip. De volgende drie opties zijn beschikbaar:

- Wachten tot het volgende geplande tijdstip
- Taak zo spoedig mogelijk uitvoeren
- Taak onmiddellijk uitvoeren als laatste uitvoering langer is geleden dan interval (het interval kan onmiddellijk worden gedefinieerd met de optie **Taakinterval**).

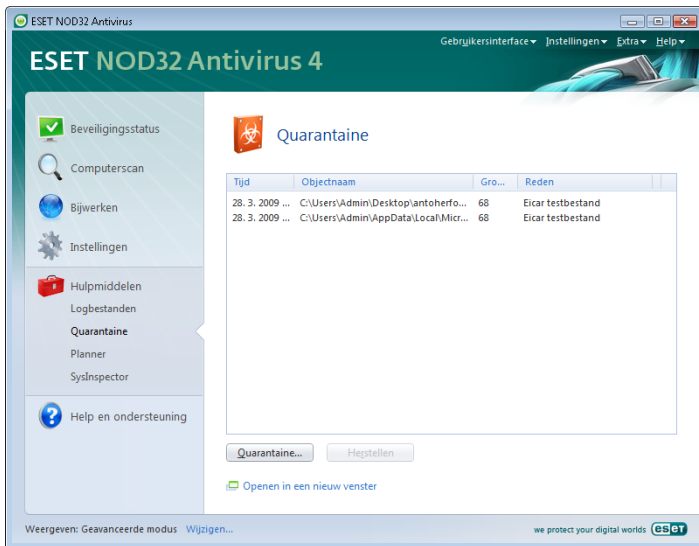
In de volgende stap wordt een overzichtsvenster met informatie over de huidige geplande taak weergegeven. De optie **Taak uitvoeren met specifieke parameters** moet automatisch worden ingeschakeld. Klik op de knop **Voltoeien**.

Een dialoogvenster wordt weergegeven waarin u profielen kunt kiezen voor gebruik bij de geplande taak. Hier kunt u een primair en alternatief profiel opgeven. Dit laatste wordt gebruikt als de taak niet kan worden voltooid met het primaire profiel. Bevestig door op **OK** te klikken in het venster **Updateprofielen**. De nieuw geplande taak wordt toegevoegd aan de lijst met actuele geplande taken.

4.4 Quarantaine

De hoofdtak van de quarantaine is het veilig opslaan van geïnfecteerde bestanden. Bestanden moeten in quarantaine worden geplaatst als zij niet kunnen worden opgeschoond, als het niet veilig of raadzaam is om deze te verwijderen of als zij niet zouden moeten worden gedetecteerd door de ESET NOD32 Antivirus.

De gebruiker kan ervoor kiezen elk gewenst bestand in quarantaine te plaatsen. Dit is raadzaam als een bestand zich verdacht gedraagt maar niet wordt gedetecteerd door de antivirusscanner. In quarantaine geplaatste bestanden kunnen voor analyse naar de viruslaboratoria van ESET worden verzonden.



Bestanden die zijn opgeslagen in de quarantainemap kunnen worden bekeken in een tabel waarin de datum en het tijdstip van de quarantaine, het pad naar de oorspronkelijke locatie van het geïnfecteerde bestand, de grootte van het bestand in bytes, de reden (**toegevoegd door gebruiker...**) en het aantal bedreigingen (bijvoorbeeld of het een archief is dat meerdere infiltraties bevat) wordt weergegeven.

4.4.1 Bestanden in quarantaine plaatsen

Het programma plaatst verwijderde bestanden automatisch in quarantaine (als u deze optie niet hebt geannuleerd in het waarschuwingsvenster). Desgewenst kunt u elk willekeurig verdacht bestand handmatig in quarantaine plaatsen door op de knop **Quarantaine...** te klikken. In dat geval wordt het oorspronkelijke bestand niet verwijderd van de oorspronkelijke locatie. Het contextmenu kan eveneens worden gebruikt voor dit doel. Klik met de rechtermuisknop in het quarantainevenster en selecteer **Toevoegen...**

4.4.2 Terugzetten vanuit quarantaine

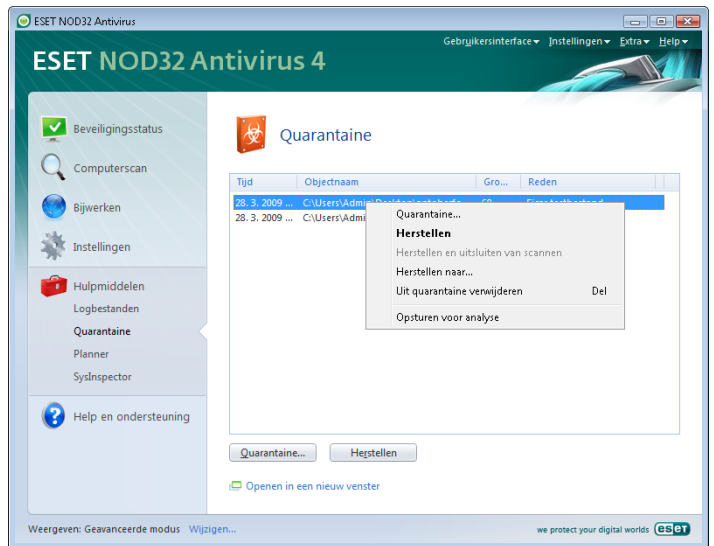
Bestanden die in quarantaine zijn geplaatst kunnen ook worden teruggezet op de oorspronkelijke locatie. Gebruik de functie **Herstellen** voor dit doel. Deze optie is beschikbaar vanuit het contextmenu door met de rechtermuisknop op het desbetreffende bestand in het quarantainevenster te klikken. Het contextmenu biedt tevens de optie **Herstellen naar**, waarmee u bestanden kunt terugzetten naar een andere locatie dan waar deze zijn verwijderd.

OPMERKING:

Als het programma per ongeluk een onschadelijk bestand in quarantaine heeft geplaatst, sluit u het bestand uit van scannen nadat u het hebt teruggezet en stuurt u het naar de klantenservice van ESET.

4.4.3 Bestand verzenden vanuit quarantaine

Als u een verdacht bestand in quarantaine hebt geplaatst dat niet is gedetecteerd door het programma, of als een bestand ten onrechte als geïnfecteerd is beoordeeld (bijvoorbeeld door heuristische analyse van de code) en vervolgens in quarantaine geplaatst, stuurt u het bestand naar het viruslaboratorium van ESET. U kunt een bestand verzenden vanuit quarantaine door met de rechtermuisknop hierop te klikken en **Opsturen voor analyse** te selecteren in het contextmenu.

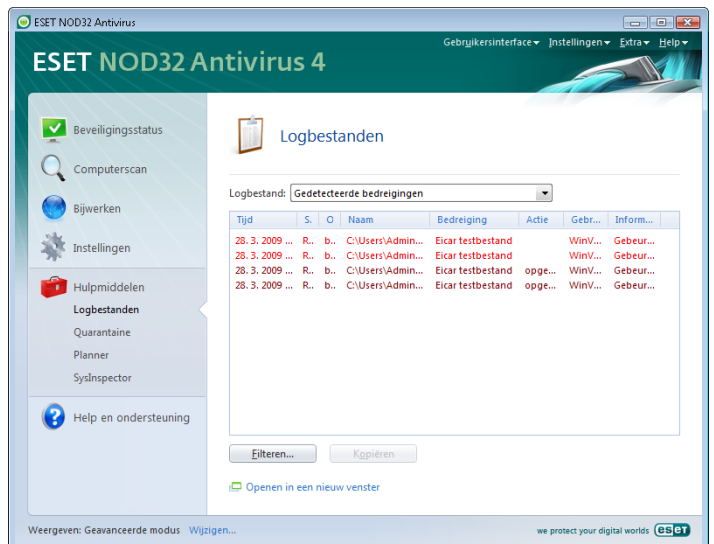


4.5 Logbestanden

De logbestanden bevatten informatie over alle belangrijke programmagebeurtenissen die zich hebben voorgedaan en bieden een overzicht van gedetecteerde bedreigingen. Logboekregistratie vormt een essentieel hulpmiddel bij systeemanalyse, bedreigingsdetectie en probleemoplossing. Logboekregistratie wordt zonder gebruikersinteractie op de achtergrond uitgevoerd. Informatie wordt vastgelegd op basis van de huidige detailinstellingen voor logboekregistratie. U kunt tekstberichten en logboeken rechtstreeks vanuit de ESET NOD32 Antivirus-omgeving weergeven. U kunt de logboeken ook archiveren.

Logbestanden zijn toegankelijk vanuit het hoofdenster van ESET NOD32 Antivirus door op **Hulpmiddelen > Logbestanden** te klikken. Selecteer het gewenste logboektype met de vervolgkeuzelijst **Logbestand**: boven in het venster. De volgende logboeken zijn beschikbaar:

1. **Gedetecteerde bedreigingen** – Gebruik deze optie om alle informatie weer te geven over gebeurtenissen die verband houden met de detectie van bedreigingen.
2. **Gebeurtenissen** – Met deze optie kunnen systeembeheerders en gebruikers problemen oplossen. Alle belangrijke acties die worden uitgevoerd door ESET NOD32 Antivirus worden opgenomen in de gebeurtenislogboeken.
3. **Computerscan op aanvraag** – In dit venster worden de resultaten van alle voltooide scans weergegeven. Dubbelklik op een vermelding om de details van de desbetreffende scan op aanvraag weer te geven.

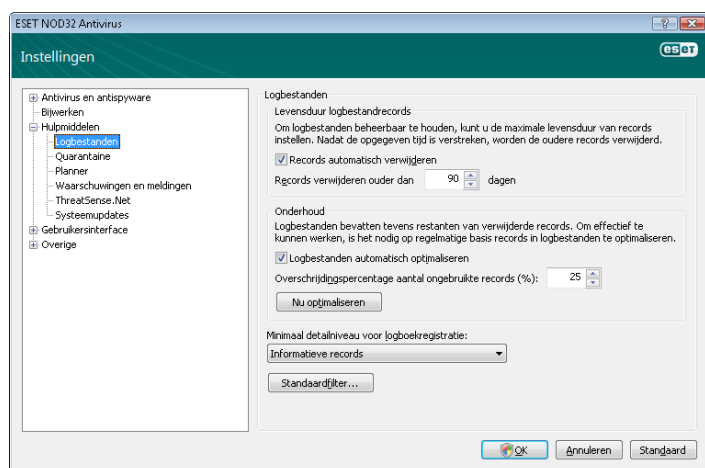


U kunt de informatie in elke sectie rechtstreeks naar het klembord kopiëren door de gewenste vermelding te selecteren en op de knop **Kopiëren** te klikken. Als u meerdere vermeldingen wilt selecteren, gebruikt u de toetsen Ctrl en Shift.

4.5.1 Logbestanden onderhouden

De configuratie van de logbestanden van ESET NOD32 Antivirus is toegankelijk via het hoofdvenster van het programma. Klik op **Instellingen > Volledige structuur voor geavanceerde instellingen invoeren... > Hulpmiddelen > Logbestanden**. U kunt de volgende opties opgeven voor logbestanden:

- **Records automatisch verwijderen:** Vermeldingen die ouder zijn dan het opgegeven aantal dagen, worden automatisch uit het logbestand verwijderd
- **Logbestanden automatisch optimaliseren:** Hiermee wordt automatische defragmentatie van logbestanden ingeschakeld als het opgegeven percentage ongebruikte records is overschreden
- **Minimale detailniveau bij logboekregistratie:** Hiermee wordt het detailniveau van logbestanden opgegeven. Beschikbare opties:
 - **Kritieke fouten** – Alleen kritieke fouten (bijvoorbeeld fouten bij het starten van de antivirusbeveiliging, enz.) worden geregistreerd.
 - **Fouten** – Alleen fouten bij het downloaden van bestanden en kritieke fouten worden vastgelegd.
 - **Waarschuwingen** – Kritieke fouten en waarschuwingsberichten worden vastgelegd.
 - **Informatieve records** – Alle informatieberichten (bijvoorbeeld met betrekking tot geslaagde updates) en alle bovenstaande records worden geregistreerd.
 - **Diagnoserecords** – Alle gegevens die nodig zijn voor het instellen van het programma, en alle bovenstaande records worden geregistreerd.



4.6 Gebruikersinterface

De configuratieopties voor de gebruikersinterface in ESET NOD32 Antivirus kunnen worden gewijzigd zodat u de werkomgeving kunt aanpassen aan uw eigen behoeften. Deze configuratieopties zijn toegankelijk vanuit **Gebruikersinterface** in de structuur voor geavanceerde instellingen van ESET NOD32 Antivirus.

In de sectie **Elementen van gebruikersinterface** kunnen gebruikers overschakelen naar de geavanceerde modus. In de modus Geavanceerd worden meer gedetailleerde instellingen en aanvullende besturingselementen voor ESET NOD32 Antivirus weergegeven.

De optie **Grafische gebruikersinterface** moet worden uitgeschakeld als de grafische elementen de prestaties van de computer negatief beïnvloeden of andere problemen veroorzaken. Ook moet de grafische interface mogelijk worden uitgeschakeld voor gebruikers met een visueel handicap aangezien deze interface mogelijk de werking kan verstoren van speciale toepassingen die worden gebruikt voor het lezen van tekst die wordt weergegeven op het scherm.

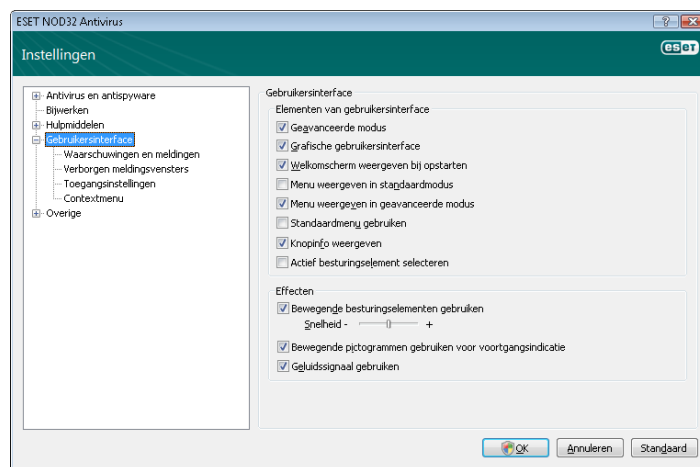
Als u het welkomstscherf van ESET NOD32 Antivirus wilt uitschakelen, schakelt u de optie **Welkomtscherf weergeven bij opstarten** uit.

Boven aan het venster van ESET NOD32 Antivirus bevindt zich een standaardmenu dat kan worden in- of uitgeschakeld op basis van de optie **Standaardmenu gebruiken**.

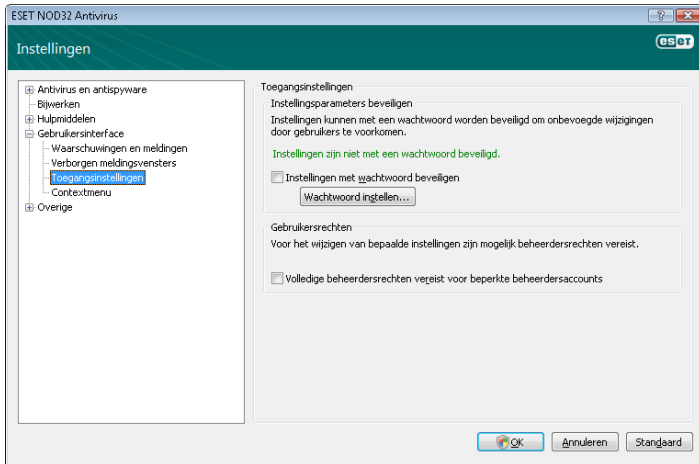
Als de optie **Knopinfo weergeven** is ingeschakeld, wordt een korte beschrijving van elke optie weergegeven als de cursor op de optie wordt geplaatst. De optie **Actief besturingselement selecteren** heeft tot gevolg dat het systeem elk element markeert dat zich momenteel onder het actieve gebied van de muiscursor bevindt. Het gemarkeerde element wordt geactiveerd na een muisklik.

U kunt de snelheid van animatie-effecten verlagen of verhogen door de optie **Bewegende besturingselementen gebruiken** te selecteren en de schuifregelaar voor **Snelheid** naar links of rechts te verplaatsen.

U kunt het gebruik van pictogrammen met animatie inschakelen bij het weergeven van de voortgang van verschillende bewerkingen door het selectievakje **Bewegende pictogrammen gebruiken voor voortgangsindicatie...** in te schakelen. Als u het programma een waarschuwing wilt laten weergeven als een belangrijke gebeurtenis plaatsvindt, selecteert u de optie **Geluidssignaal gebruiken**.



Tot de functies van de **gebruikersinterface** behoort tevens de optie om de instellingen van ESET NOD32 Antivirus met een wachtwoord te beveiligen. Deze optie is te vinden in het submenu **Instellingen beveiligen** onder **Gebruikersinterface**. Om maximale beveiliging voor uw systeem te waarborgen is het van essentieel belang dat het programma correct wordt geconfigureerd. Onbevoegde wijzigingen kunnen resulteren in het verlies van belangrijke gegevens. U kunt een wachtwoord instellen ter beveiliging van de instellingsparameters door op **Wachtwoord invoeren...** te klikken.



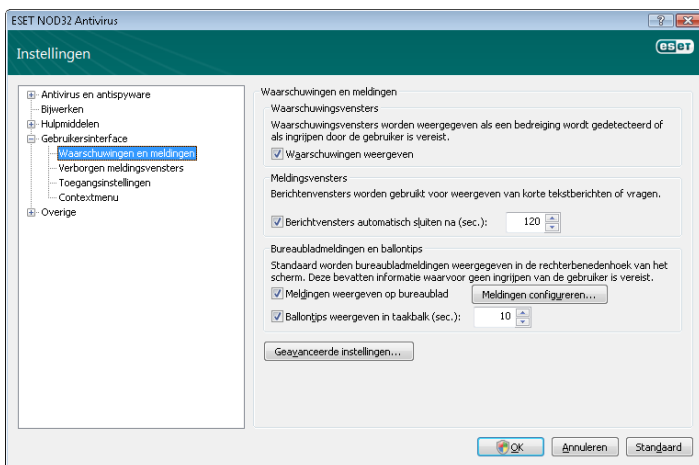
4.6.1 Waarschuwingen en meldingen

In de sectie **Instellingen voor waarschuwingen en meldingen** onder **Gebruikersinterface** kunt u configureren hoe waarschuwingen en systeemmeldingen bij bedreigingen worden afgehandeld in ESET NOD32 Antivirus 4.

De eerste optie is **Waarschuwingen weergeven**. Als u deze optie uitschakelt, worden alle waarschuwingsvensters geannuleerd. Deze optie is alleen geschikt in een beperkt aantal specifieke situaties. Voor de meeste gebruikers adviseren wij de standaardoptie (ingeschakeld) te gebruiken.

U kunt pop-upvensters automatisch na een bepaalde tijd laten sluiten door de optie **Berichtvensters automatisch sluiten na (sec.)** te selecteren. Als waarschuwingsvensters niet handmatig door de gebruiker worden gesloten, gebeurt dit automatisch nadat de opgegeven tijdsperiode is verstreken.

Meldingen op het bureaublad en ballontips zijn informatiemiddelen waarbij geen gebruikersinteractie mogelijk of nodig is. Zij worden weergegeven in het systeemvak in de rechterbenedenhoek van het scherm. Als u het weergeven van meldingen op het bureaublad wilt activeren, schakelt u de optie **Kennisgevingen weergeven op bureaublad** in. Meer gedetailleerde opties, zoals weergavetijd van meldingen en transparantie van het venster, kunnen worden gewijzigd door op de knop **Meldingen configureren...** te klikken. U kunt het gedrag van meldingen vooraf bekijken door op de knop **Voorbeeld** te klikken. U kunt de weergaveduur van ballontips configureren met behulp van de optie **Ballontips weergeven in taakbalk (sec.)**.



Klik op **Geavanceerde instellingen...** om aanvullende opties voor **waarschuwingen en meldingen** in te stellen, inclusief **Alleen meldingen weergeven die gebruikersinteractie vereisen**. Met deze optie kunt u het weergeven van waarschuwingen en meldingen waarvoor geen gebruikersinteractie nodig is in- of uitschakelen. Selecteer **Alleen meldingen weergeven die gebruikersinteractie vereisen** wanneer

toepassingen worden weergegeven in de volledige weergavemodus om alle niet-interactieve meldingen te onderdrukken. In de vervolgkeuzelijst **Minimaal detailniveau voor weergegeven gebeurtenissen** kunt u het begingevaarniveau van weer te geven waarschuwingen en meldingen selecteren.

De laatste functie in dit gedeelte is het opgeven van adressen van meldingen in een omgeving met meerdere gebruikers. In het veld **In systemen met meerdere gebruikers meldingen weergeven op scherm van deze gebruiker**: kan de gebruiker definiëren wie belangrijke meldingen ontvangt van ESET NOD32 Antivirus 4. Normaliter is dit een systeem- of netwerkbeheerder. Deze optie is met name handig voor terminalservers, op voorwaarde dat alle systeemmeldingen naar de beheerder worden verzonden.

4.7 ThreatSense.Net

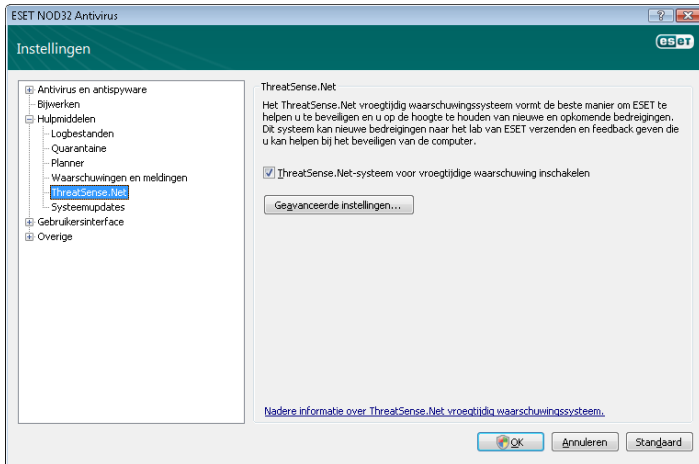
Het ThreatSense.Net systeem voor vroegtijdige waarschuwing is een hulpmiddel dat ervoor zorgt dat ESET onmiddellijk en continu op de hoogte wordt gehouden van nieuwe infiltraties. Het bidirectionele ThreatSense.Net systeem voor vroegtijdige waarschuwing heeft één enkel doel, namelijk de beveiliging verbeteren die wij u kunnen bieden. Dit kunnen we het beste doen door ervoor te zorgen dat we nieuwe bedreigingen zo spoedig mogelijk in de gaten krijgen door deze aan zoveel mogelijk van onze klanten te 'koppelen' en hen te gebruiken als onze 'bedreigingscouts'. Er zijn twee opties:

- U kunt ervoor kiezen om het ThreatSense.Net systeem voor vroegtijdige waarschuwing niet in te schakelen. U verliest geen functionaliteit in de software en geniet nog steeds de best mogelijke beveiliging die wij kunnen bieden.
- U kunt het systeem voor vroegtijdige waarschuwing zodanig configureren dat anonieme informatie over nieuwe bedreigingen en waar de nieuwe bedreiging voorkomt in één enkel bestand wordt verzonden. Dit bestand kan voor gedetailleerde analyse naar ESET worden verzonden. Na bestudering van deze bedreigingen kan ESET haar voorzieningen voor bedreigingsdetectie vervolgens bijwerken. Het ThreatSense.Net systeem voor vroegtijdige waarschuwing verzamelt informatie over uw computer met betrekking tot nieuw gedetecteerde bedreigingen. Deze informatie kan een voorbeeld of kopie bevatten van het bestand waarin de bedreiging voorkwam, het pad naar dat bestand, de bestandsnaam, informatie over datum en tijd, het proces waarbij de bedreiging plaatsvond op uw computer en informatie over het besturingssysteem van uw computer. Sommige van deze gegevens bevatten mogelijk persoonlijke informatie over de gebruiker van de computer, zoals gebruikersnamen in een directorypad, enz. Een voorbeeld van de verzonden bestandsinformatie is hier beschikbaar.

Hoewel de kans bestaat dat het bedreigingslaboratorium van ESET hiermee nu en dan informatie over u of uw computer in bezit krijgt, wordt deze informatie niet gebruikt voor andere doelen dan ons te helpen onmiddellijk te reageren op nieuwe bedreigingen.

Standaard wordt ESET NOD32 Antivirus zodanig geconfigureerd dat u om toestemming wordt gevraagd voordat verdachte bestanden voor gedetailleerde analyse naar het bedreigingslaboratorium van ESET worden verzonden. Houd er rekening mee dat bestanden met bepaalde extensies, zoals .DOC of .XLS altijd worden uitgesloten van verzending als hierin een bedreiging wordt gedetecteerd. U kunt ook andere extensies toevoegen als er specifieke bestanden zijn die u of uw organisatie niet wil laten verzenden.

De instellingen van ThreatSense.Net zijn toegankelijk via de geavanceerde instellingen onder **Hulpmiddelen > ThreatSense.Net**. Schakel het selectievakje **ThreatSense.Net systeem voor vroegtijdige waarschuwing inschakelen** in. Hiermee kunt u de knop **Geavanceerde instellingen...** activeren. Klik vervolgens op deze knop.

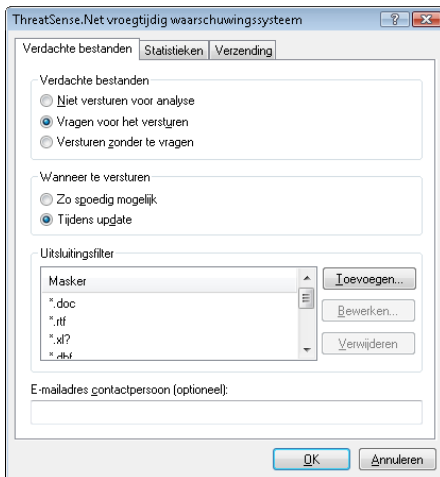


4.7.1 Verdachte bestanden

Op het tabblad **Verdachte bestanden** kunt u de wijze configureren waarop bedreigingen naar het laboratorium van ESET worden verzonden voor analyse.

Als u een verdacht bestand aantreft, kunt u dit naar onze viruslaboratoria versturen voor analyse. Als het bestand een schadelijke toepassing blijkt te zijn, wordt de detectie ervan toegevoegd aan de volgende update van de database met viruskenmerken.

De verzending van bestanden kan automatisch en ongevraagd plaatsvinden. Als deze optie is ingeschakeld, worden verdachte bestanden op de achtergrond verzonden. Als u wilt weten welke bestanden voor analyse zijn verzonden en de verzending wilt bevestigen, selecteert u de optie **Vragen alvorens op te sturen**.



Als u geen bestanden wilt verzenden, selecteert u **Niet opsturen voor analyse**. Houdt u er rekening mee dat het niet opsturen van bestanden voor analyse geen invloed heeft op de verzending van statistische informatie naar ESET. Statistische informatie wordt geconfigureerd in een eigen gedeelte met instellingen, dat in het volgende hoofdstuk wordt beschreven.

Wanneer te versturen

Verdachte bestanden worden zo spoedig mogelijk naar de laboratoria van ESET verzonden voor analyse. Dit wordt aanbevolen als een permanente internetverbinding beschikbaar is en verdachte bestanden zonder vertraging kunnen worden afgeleverd. De andere opties is het versturen van verdachte bestanden **tijdens een update**. Als deze optie is geselecteerd, worden verdachte bestanden verzameld en tijdens een update naar de servers van het systeem voor vroegtijdige waarschuwing geüpload.

Uitsluitingsfilter

Niet alle bestanden hoeven worden opgestuurd voor analyse. Met het uitsluitingsfilter kunt u bepaalde bestanden of mappen uitsluiten van verzending. Het kan bijvoorbeeld handig zijn bestanden uit te sluiten die mogelijk vertrouwelijke informatie bevatten, zoals documenten of spreadsheets. Veelgebruikte bestandstypen worden standaard uitgesloten (Microsoft Office, OpenOffice). De lijst met uitgesloten bestanden kan desgewenst worden uitgebreid.

E-mailadres contactpersoon

Het e-mailadres van de contactpersoon wordt samen met de verdachte bestanden naar ESET verzonden en kan worden gebruikt om contact met u op te nemen als meer informatie over opgestuurde bestanden nodig is voor de analyse. U zult geen antwoord van ESET ontvangen, tenzij nadere informatie nodig is voor de analyse.

4.7.2 Statistieken

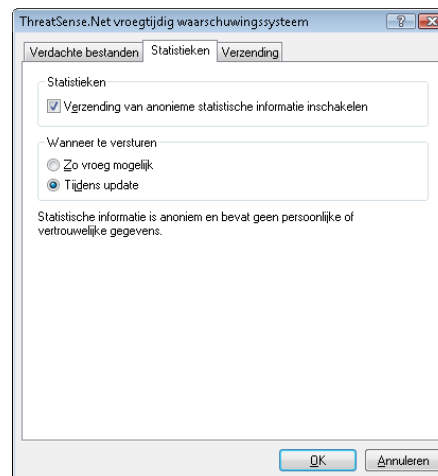
Het ThreatSense.Net systeem voor vroegtijdige waarschuwing verzamelt anonieme informatie over uw computer met betrekking tot nieuw gedetecteerde bedreigingen. Bij deze informatie kan het gaan om de naam van de infiltratie, de datum en het tijdstip waarop deze is gedetecteerd, de versie van ESET NOD32 Antivirus, de versie van het besturingssysteem op uw computer en de locatie-instelling. De statistieken worden normaal gesproken een- of tweemaal per dag naar de servers van ESET verzonden.

Een voorbeeld van een verzonden statistisch pakket:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

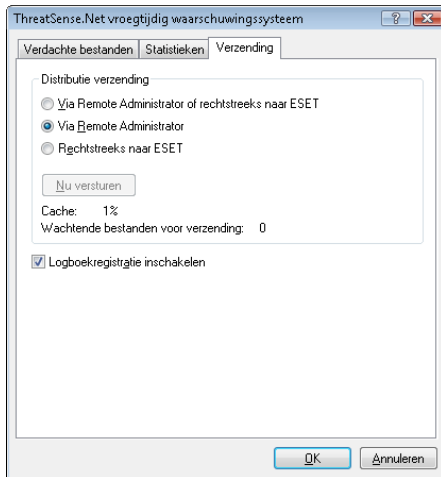
Wanneer te versturen

In de sectie **Wanneer te versturen** kunt u definiëren wanneer de statistische gegevens worden verzonden. Als u kiest voor **Zo spoedig mogelijk**, worden statistische gegevens verzonden onmiddellijk nadat zij zijn aangemaakt. Deze instelling is geschikt als een permanente internetverbinding beschikbaar is. Als **Tijdens update** wordt geselecteerd, worden statistische gegevens bewaard en gezamenlijk verzonden tijdens de volgende update.



4.7.3 Verzending

In dit gedeelte kunt u kiezen of bestanden en statistische gegevens worden verzonden via ESET Remote Administrator of rechtstreeks naar ESET. Als u er zeker van wilt zijn dat verdachte bestanden en statistische gegevens worden afgeleverd bij ESET, selecteert u de optie **Via Remote Administrator of rechtstreeks naar ESET**. Als deze optie is geselecteerd, worden bestanden en statistische gegevens verzonden via alle beschikbare middelen. Bij verzending van verdachte bestanden via Remote Administrator worden bestanden en statistische gegevens naar de externe beheerserver verzonden, die vervolgens zorgdraagt voor verzending naar de viruslaboratoria van ESET. Als de optie **Rechtstreeks naar ESET** wordt geselecteerd, worden alle verdachte bestanden en statistische gegevens rechtstreeks vanuit het programma naar het viruslaboratorium van ESET gezonden.



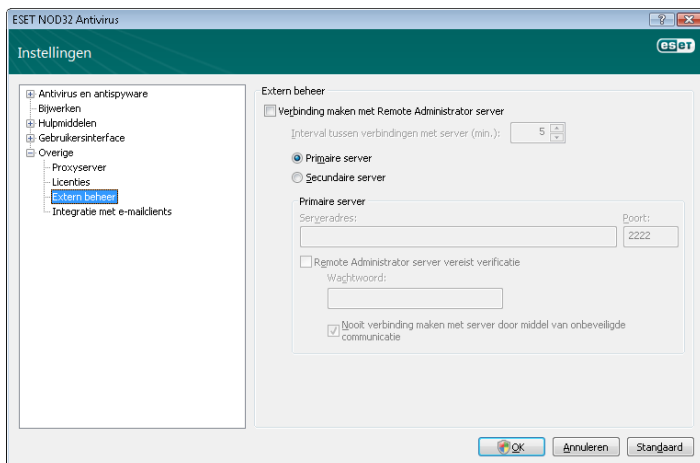
Als er bestanden wachten op verzending, is de knop **Nu versturen** ingeschakeld in dit instellingsvenster. Klik op deze knop als u bestanden en statistische gegevens onmiddellijk wilt verzenden.

Schakel het selectievakje **Logboekregistratie inschakelen** in om de registratie van bestanden en statistische gegevens in te schakelen. Na elke verzending van een verdacht bestand of van statistische gegevens, wordt een vermelding in het gebeurtenislogboek opgenomen.

4.8 Extern beheer

Extern beheer is een krachtig hulpmiddel voor het onderhouden van beveiligingsbeleid en voor het verkrijgen van een overzicht van het algehele beveiligingsbeheer binnen het netwerk. Het is met name handig bij gebruik in grotere netwerken. Extern beheer leidt niet alleen tot een hoger beveiligingsniveau, maar biedt bovendien extra gebruiksgemak bij het beheer van ESET NOD32 Antivirus op clientwerkstations.

De instellopties voor extern beheer zijn beschikbaar vanuit het hoofdvenster van ESET NOD32 Antivirus. Klik op **Instellingen > Volledige structuur voor geavanceerde instellingen invoeren... > Overige > Extern beheer**.



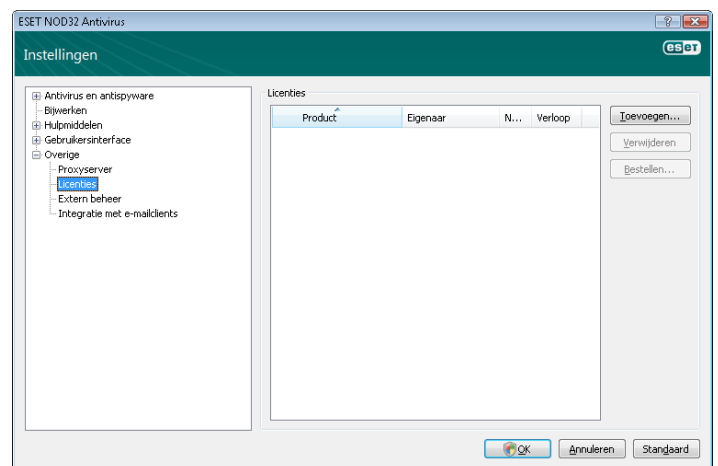
In het instellingsvenster kunt u de modus voor extern beheer activeren door eerst het selectievakje **Verbinding maken met server voor extern beheer** in te schakelen. U kunt vervolgens toegang krijgen tot de overige opties die hieronder worden beschreven:

- **Serveradres** – Netwerkadres van de server waar de server voor extern beheer is geïnstalleerd.
- **Poort** – Dit veld bevat een vooraf gedefinieerde serverpoort die wordt gebruikt om verbinding te maken. Wij adviseren u de vooraf gedefinieerde poortinstelling van 2222 ongewijzigd te laten.
- **Interval tussen verbindingen met server (min.)** – Hiermee wordt aangegeven hoe vaak ESET NOD32 Antivirus verbinding maakt met de ERA-server om de gegevens te verzenden. Met andere woorden, informatie wordt verzonden met de hier gedefinieerde tussenpozen. Als deze waarde is ingesteld op 0, wordt elke 5 seconden informatie verzonden.
- **Server voor extern beheer vereist verificatie** – Hiermee kunt u zo nodig een wachtwoord invoeren voor verbinding met de server voor extern beheer.

Klik op **OK** om wijzigingen te bevestigen en de instellingen toe te passen. ESET NOD32 Antivirus gebruikt deze instellingen om verbinding te maken met de externe server.

4.9 Licentie

Onder **Licentie** kunt u de licentiesleutels voor ESET NOD32 Antivirus en andere ESET-producten beheren. Na aanschaf ontvangt u uw licentiesleutels samen met uw gebruikersnaam en wachtwoord. U kunt een licentiesleutel **toevoegen of verwijderen** door op de bijbehorende knop van het venster voor licentiebeheer te klikken. De functie voor licentiebeheer is bereikbaar via de geavanceerde instellingen onder **Overige > Licenties**.



De licentiesleutel is een tekstbestand met informatie over het aangeschafte product: de eigenaar, het aantal licenties en de vervaldatum.

In het venster voor licentiebeheer kan de gebruiker de inhoud van een licentiesleutel uploaden en bekijken met behulp van de knop **Toevoegen...** De beschikbare informatie wordt weergegeven in licentiebeheer. U kunt licentiebestanden verwijderen uit de lijst door op **Verwijderen** te klikken.

Als een licentiesleutel is verlopen en u wilt verlengen, klikt u op de knop **Bestellen...** – U wordt dan omgeleid naar onze onlinewinkel.

5. Geavanceerde gebruiker

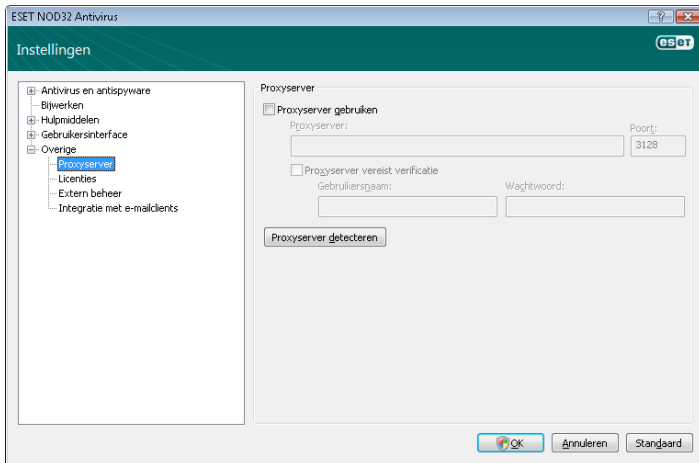
In dit hoofdstuk worden functies van ESET NOD32 Antivirus beschreven die handig kunnen zijn voor meer gevorderde gebruikers. Instellingsopties voor deze functies zijn uitsluitend toegankelijk via de geavanceerde modus. U kunt overschakelen naar de geavanceerde modus door op **Geavanceerde modus in-/uitschakelen** in de linkerbenedenhoek van het hoofdvenster van het programma te klikken of door op Ctrl + M te drukken op uw toetsenbord.

5.1 Proxyserver instellen

In ESET NOD32 Antivirus kunnen proxyserver in twee verschillende secties van de menustructuur voor geavanceerde instellingen worden ingesteld.

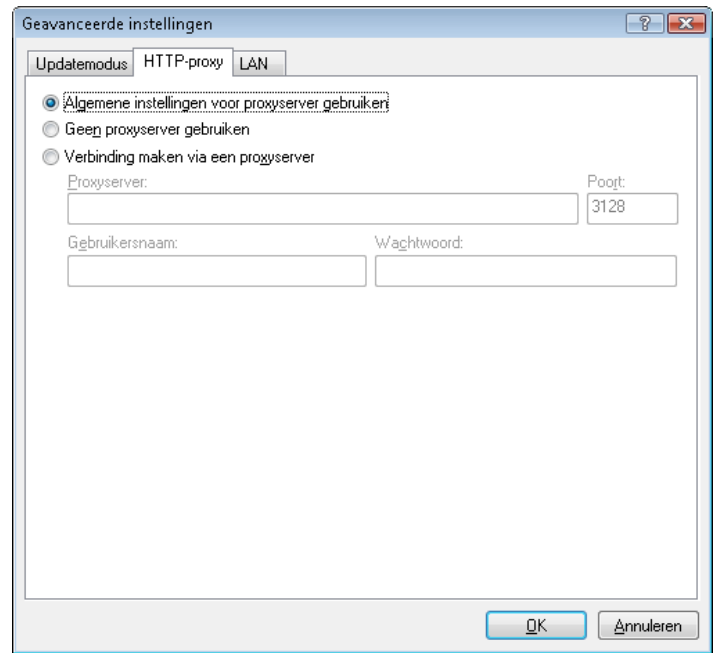
Op de eerste plaats kunnen instellingen voor proxyserver worden geconfigureerd via **Overige > Proxyserver**. Als u de proxyserver op dit niveau opgeeft, worden algemene instellingen voor de proxyserver gedefinieerd voor heel ESET NOD32 Antivirus. Parameters hier worden gebruikt door alle modules die verbinding met internet vereisen.

U kunt instellingen voor de proxyserver op dit niveau opgeven door het selectievakje **Proxyserver gebruiken** in te schakelen en vervolgens het adres van de proxyserver in te voeren in het veld **Proxyserver**: samen met het **poortnummer** van de proxyserver.



Als voor communicatie met de proxyserver verificatie is vereist, schakelt u het selectievakje **Proxyserver vereist verificatie** in en geeft u een geldige **gebruikersnaam** en een geldig **wachtwoord** op in de respectievelijke velden. Klik op de knop **Proxyserver detecteren** om automatisch proxyserverinstellingen te detecteren en in te voegen. De parameters die zijn opgegeven in Internet Explorer worden gekopieerd. Deze functie haalt geen verificatiegegevens (gebruikersnaam en wachtwoord) op. Deze moeten worden ingevoerd door de gebruiker.

Instellingen voor de proxyserver kunnen tevens worden ingesteld in **Instellingen voor geavanceerde update** (optie **Update** van de menustructuur voor geavanceerde instellingen). Deze instelling is van toepassing op het opgegeven updateprofiel en wordt aanbevolen voor laptops, aangezien deze vaak updates van viruskenmerken van verschillende locaties bevatten. Raadpleeg voor meer informatie over deze instelling sectie 4.4, "Het systeem bijwerken".



5.2 Instellingen importeren/exporteren

De huidige configuratie van ESET NOD32 Antivirus kan worden geëxporteerd en geïmporteerd via **Instellingen** in de geavanceerde modus.

Zowel bij exporteren als bij importeren wordt gebruikgemaakt van het bestandstype .XML. Export en importeren zijn handig als u om wat voor reden dan een back-up van de huidige configuratie van ESET NOD32 Antivirus moet maken zodat u dit product later opnieuw kunt gebruiken. De instellingsoptie voor exporteren is tevens handig voor gebruiker die hun favoriete configuratie van ESET NOD32 Antivirus op meerdere systemen willen gebruiken. Zij hoeven alleen hun .XML-bestand te importeren.



5.2.1 Instellingen exporteren

Het exporteren van de configuratie is heel gemakkelijk. Als u de huidige configuratie van ESET NOD32 Antivirus wilt opslaan, klikt u op **Instellingen > Instellingen importeren en exporteren...** Selecteer de optie **Instellingen exporteren** en voer de naam van het configuratiebestand in. Gebruik de browser om een locatie te selecteren op uw computer waar u het configuratiebestand wilt opslaan.

5.2.2 Instellingen importeren

De stappen voor het importeren van een configuratie zijn vergelijkbaar. Selecteer opnieuw **Instellingen importeren en exporteren** en selecteer de optie **Instellingen importeren**. Klik op de knop ... en blader naar het configuratiebestand dat u wilt importeren.

5.3 Oprachtregel

De antivirusmodule van ESET NOD32 Antivirus kan worden gestart via de opdrachtregel, handmatig (met de opdracht "ecls") of via een batchbestand ("bat").

De volgende parameters en schakelopties kunnen worden gebruikt bij het uitvoeren van de scanner op aanvraag vanaf de opdrachtregel:

Algemene opties:

- help help weergeven en afsluiten
- version versiegegevens weergeven en afsluiten
- base-dir = MAP modules laden vanuit MAP
- quar-dir = MAP MAP in quarantaine plaatsen
- aind activiteitindicator weergeven
- auto alle vaste schijven in de modus Opschonen scannen

Doelen:

- files bestanden scannen (standaard)
- no-files bestanden niet scannen
- boots opstartsectoren scannen (standaard)
- no-boots opstartsectoren niet scannen
- arch archieven scannen (standaard)
- no-arch archieven niet scannen
- max-archive-level = NIVEAU maximaal nestingsniveau voor archieven
- scan-timeout = LIMIET archieven scannen gedurende maximaal LIMIET seconden. Als de scantijd deze limiet bereikt, wordt het scannen van het archief gestopt en gaat de scan door naar het volgende bestand
- max-arch-size = GROOTTE alleen de eerste GROOTTE bytes in archieven scannen (standaard 0 = onbeperkt)
- mail e-mailbestanden scannen
- no-mail e-mailbestanden niet scannen
- sfx zelfuitpakkende archieven scannen
- no-sfx zelfuitpakkende archieven niet scannen
- rtp programma's voor runtime-compressie scannen
- no-rtp programma's voor runtime-compressie niet scannen
- exclude = MAP de opgegeven MAP niet scannen
- subdir submappen scannen (standaard)
- no-subdir submappen niet scannen
- max-subdir-level = NIVEAU maximaal nestingsniveau voor submappen (standaard 0 = onbeperkt)
- symlink symbolische koppelingen volgen (standaard)
- no-symlink symbolische koppelingen overslaan
- ext-remove = EXTENSIES EXTENSIES die door dubbele punten zijn gescheiden uitsluiten van scannen
- ext-exclude = EXTENSIES

Methoden:

- adware scannen op adware/spyware/riskware
- no-adware niet scannen op adware/spyware/riskware
- unsafe scannen op potentieel onveilige toepassingen
- no-unsafe niet scannen op mogelijk onveilige toepassingen
- unwanted scannen op mogelijk ongewenste toepassingen
- no-unwanted niet scannen op mogelijk ongewenste toepassingen
- pattern signaturen gebruiken
- no-pattern geen signaturen gebruiken
- heur heuristiek inschakelen
- no-heur heuristiek uitschakelen
- adv-heur geavanceerde heuristiek inschakelen
- no-adv-heur geavanceerde heuristiek uitschakelen

Opschonen:

- action = ACTIE ACTIE uitvoeren op geïnfecteerde objecten. Beschikbare acties: geen, opschonen, vragen
- quarantine geïnfecteerde bestanden naar quarantaine kopiëren (aanvulling op ACTIE)
- no-quarantine geïnfecteerde bestanden niet naar quarantaine kopiëren

Logbestanden:

- log-file = BESTAND uitvoer registreren in BESTAND
- log-rewrite uitvoerbestand overschrijven (standaard - toevoegen)
- log-all ook schone bestanden in logbestand opnemen
- no-log-all schone bestanden niet in logbestand opnemen (standaard)

De mogelijke afsluitcodes van de scan:

- 0 - geen bedreiging gevonden
- 1 - bedreiging gevonden maar niet opgeschoond
- 10 - enkele geïnfecteerde bestanden resteren
- 101 - archieffout
- 102 - toegangsfout
- 103 - interne fout

OPMERKING: Afsluitcodes groter dan 100 betekenen dat het bestand niet is gescand en dus geïnfecteerd kan zijn.

5.4 ESET SysInspector

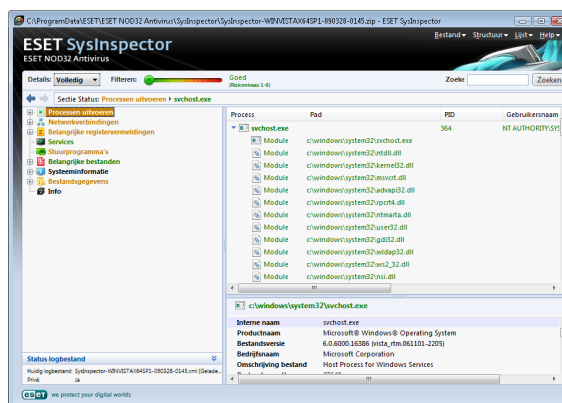
ESET SysInspector is een toepassing waarmee u een uitgebreide inspectie van uw computer kunt uitvoeren om allerlei nuttige gegevens te verzamelen. Informatie zoals geïnstalleerde stuurprogramma's en toepassingen, netwerkverbindingen of belangrijke registervermeldingen, kunnen u helpen mogelijke oorzaken van afwijkend systeemgedrag te elimineren. Het hoeft namelijk niet altijd zo te zijn dat een malware-infectie problemen veroorzaakt. Het is ook mogelijk dat incompatibele software of hardware de oorzaak is.

ESET biedt SysInspector in twee varianten aan. De losse toepassing (SysInspector.exe) kunt u gratis downloaden van de website van ESET. De geïntegreerde variant is opgenomen in ESET NOD32 Antivirus 4. U opent de sectie voor SysInspector door de geavanceerde weergavemodus te activeren in de linkerbenedenhoek en te klikken op **Hulpmiddelen > SysInspector**. Beide varianten hebben dezelfde functionaliteit en dezelfde besturingselementen. Het enige verschil is de manier waarop de uitvoer wordt behandeld. Met de losse toepassing kunt u momentopnamen van het systeem exporteren naar een XML-bestand en dit op schijf opslaan. Dat is ook mogelijk in de geïntegreerde SysInspector. Daarnaast kunt u de momentopnamen van het systeem ook rechtstreeks opslaan in **ESET NOD32 Antivirus 4 > Hulpmiddelen > SysInspector** (zie voor meer informatie [5.4.1.4 SysInspector als onderdeel van ENA](#)).

ESET SysInspector heeft even de tijd nodig om uw computer te scannen. Dat kan variëren van tien seconden tot enkele minuten, afhankelijk van de hardwareconfiguratie, het besturingssysteem en het aantal geïnstalleerde toepassingen op de computer.

5.4.1 Gebruikersinterface en gebruik van de toepassing

Het hoofdvenster is verdeeld in vier gedeelten: de besturingselementen boven aan het hoofdvenster, het navigatievenster aan de linkerkant, het venster Omschrijving aan de rechterkant in het midden en het venster Details aan de rechterkant onderaan.



5.4.1.1 Besturingselementen in programma

Deze sectie bevat een omschrijving van alle besturingselementen die beschikbaar zijn in ESET SysInspector.

Bestand

Klik hierop om een rapport op te slaan voor latere analyse of om een eerder opgeslagen rapport te openen. Als u een rapport wilt publiceren, is het raadzaam de optie Geschikt voor verzenden te kiezen. Vertrouwelijke gegevens worden dan weggelaten uit het rapport.

Opmerking: u kunt eerder opgeslagen rapporten van ESET SysInspector openen door deze naar het hoofdvenster te slepen.

Structuur

Hiermee kunt u alle knooppunten uit- of samenvouwen.

Lijst

Dit menu bevat functies voor een eenvoudige navigatie binnen het programma, evenals verschillende andere functies, zoals voor het zoeken van online informatie.

Belangrijk: rood gemarkeerde items zijn onbekend. Om die reden zijn ze door het programma gemarkeerd als potentieel gevaarlijk. Als een item rood wordt weergegeven, betekent dit niet automatisch dat u het bestand kunt verwijderen. Controleer eerst altijd of het bestand daadwerkelijk gevaarlijk of overbodig is.

Help

Dit menu bevat informatie over de toepassing en de verschillende mogelijkheden.

Details

Hiermee kunt u bepalen wat voor gegevens er worden weergegeven in andere secties van het hoofdvenster, waardoor het werken met het programma zeer eenvoudig is. In de modus Standaard hebt u toegang tot gegevens die nodig zijn voor het vinden van oplossingen voor veelvoorkomende problemen met het systeem. In de modus Gemiddeld zijn er details zichtbaar die minder vaak nodig zijn, terwijl ESET SysInspector in de modus Volledig alle informatie weergeeft die nodig is om zeer specifieke problemen op te lossen.

Items filteren

Deze optie is het meest geschikt voor het zoeken van verdachte bestanden of registervermeldingen in het systeem. Versleep het schuifblokje op de schuifregelaar om items te filteren op risiconiveau. Als u het schuifblokje helemaal links zet (Risiconiveau 1), worden alle items weergegeven. Sleep het schuifblokje naar rechts om alle items uit te filteren die minder riskant zijn dan het huidige risiconiveau. Alleen items die verdacht zijn dan het gekozen niveau worden dan weergegeven. Als u het schuifblokje helemaal rechts zet, worden alleen items weergegeven waarvan bekend is dat ze schadelijk zijn.

Alle items die in het risicobereik 6 – 9 vallen, kunnen een beveiligingsrisico vormen. Als u geen van de beveiligingsoplossingen van ESET gebruikt, is het raadzaam uw systeem te controleren met de ESET Online scanner als het programma een dergelijk item heeft gevonden. De ESET Online scanner is een gratis service die u kunt vinden op <http://www.eset.eu/online-scanner>.

Opmerking: het risiconiveau van een item kan eenvoudig worden bepaald door de kleur van het item te vergelijken met de kleuren op de schuifregelaar Risiconiveau.

Zoeken

Gebruik deze optie om snel een item te vinden door de naam van het item of een deel van de naam in te voeren. De resultaten van de zoekopdracht worden weergegeven in het venster Omschrijving.



Terugkeren

Klik op de pijl-links of de pijl-rechts om terug te keren naar eerder weergegeven informatie in het venster Omschrijving.

Status (sectie)

Hier wordt het huidige knooppunt uit het navigatievenster weergegeven.

5.4.1.2 Navigeren in ESET SysInspector

ESET SysInspector gebruikt basissecties (knooppunten) voor het weergeven van verschillende soorten informatie. Als er aanvullende gegevens beschikbaar zijn, kunt u deze weergeven door een knooppunt uit te vouwen. U kunt een knooppunt uit- of samenvouwen door te dubbelklikken op de naam van het knooppunt. U kunt ook klikken op  of  naast de naam van het knooppunt. Terwijl u in het navigatievenster door de boomstructuur met knooppunten en subknooppunten bladert, kunnen er in het venster Omschrijving verschillende gegevens voor een knooppunt verschijnen. Als u bladert door items in het venster Omschrijving, kunnen er aanvullende gegevens van het item worden weergegeven in het venster Details.

Hieronder volgt een omschrijving van de belangrijkste knooppunten in het navigatievenster. Daarnaast wordt er voor die knooppunten aangegeven welke informatie er kan worden weergegeven in de vensters Omschrijving en Details.

Processen uitvoeren

Dit knooppunt bevat informatie over toepassingen en processen die actief zijn op het moment dat het rapport wordt gegenereerd. In het venster Omschrijving kunnen voor elk proces aanvullende details worden weergegeven, zoals de DLL's (Dynamic Link Libraries) die worden gebruikt door het proces en hun locatie in het systeem, de naam van de leverancier van de toepassing, het risiconiveau van het bestand, enz.

Het venster Details bevat aanvullende informatie over items die zijn geselecteerd in het venster Omschrijving, zoals de bestandsgrootte of de hash-waarde.

Opmerking: een besturingssysteem bestaat uit een aantal belangrijke kernel-onderdelen die continu actief zijn en die eenvoudige maar ook essentiële functies verzorgen voor andere gebruikerstoepassingen. In bepaalde gevallen worden deze processen in ESET SysInspector weergegeven met een bestandspad dat begint met `\\?\\`. Deze symbolen maken het mogelijk dat de processen vóór uitvoering kunnen worden geoptimaliseerd. Het zijn veilige processen voor het systeem en vereisen dus geen verder onderzoek.

Netwerkverbindingen

Het venster Omschrijving bevat een lijst met processen en toepassingen die communiceren over het netwerk met het protocol dat is geselecteerd in het the navigatievenster (TCP of UDP), evenals het externe adres waarmee de toepassing verbinding heeft. U kunt ook de IP-adressen controleren die via DNS zijn toegewezen.

Het venster Details bevat aanvullende informatie over items die zijn geselecteerd in het venster Omschrijving, zoals de bestandsgrootte of de hash-waarde.

Belangrijke registervermeldingen

Deze sectie bevat een lijst met specifieke registervermeldingen, die vaak te maken hebben met verschillende problemen die in het systeem kunnen optreden. Denk hierbij aan problemen met programma's die automatisch moeten worden gestart of BHO's (Browser Helper Objects).

In het venster Omschrijving kunnen bestanden worden weergegeven die gekoppeld zijn aan bepaalde registervermeldingen. Het venster Details kan aanvullende gegevens van de vermeldingen bevatten.

Services

Het venster Omschrijving bevat een lijst met bestanden die zijn geregistreerd als Windows-services. U kunt hier bijvoorbeeld zien op welke manier een service wordt gestart. Het venster Details kan specifieke gegevens van het bestand bevatten.

Stuurprogramma's

Een lijst met de stuurprogramma's die in het systeem zijn geïnstalleerd.

Belangrijke bestanden

Het venster Omschrijving bevat de inhoud van belangrijke bestanden die essentieel zijn voor het besturingssysteem Microsoft Windows.

Systeeminformatie

Deze sectie bevat gedetailleerde informatie over hardware en software, evenals informatie over ingestelde omgevingsvariabelen en gebruikersrechten.

Bestandsgegevens

Een lijst met belangrijke systeembestanden en bestanden in de map Program Files van Windows. De vensters Omschrijving en Details bevatten aanvullende informatie over de bestanden.

Info

Informatie over ESET SysInspector.



5.4.1.3 Vergelijken

Met de functie Vergelijken kan de gebruiker twee bestaande logbestanden vergelijken. Het resultaat is een set items die niet in beide logbestanden voorkomen. Deze functie is handig wanneer u wijzigingen in het systeem wilt bijhouden, bijvoorbeeld om activiteit van schadelijke code op te sporen.









Als u de functie uitvoert, wordt er een nieuw logbestand gemaakt. Dit bestand wordt weergegeven in een nieuw venster. Kies **Bestand -> Logbestand opslaan** om het logbestand op te slaan. U kunt logbestanden later openen en weergeven. Als u een bestaand logbestand wilt openen, kiest u **Bestand -> Logbestand openen**. In het hoofdvenster van ESET SysInspector kan altijd maar één logbestand worden weergegeven.

Als u twee logbestanden vergelijkt, wordt de inhoud van het actieve logbestand vergeleken met een opgeslagen logbestand. Als u twee logbestanden wilt vergelijken, kiest u eerst **Bestand -> Logbestanden vergelijken** en vervolgens **Bestand selecteren**. Het geselecteerde logbestand wordt dan vergeleken met het actieve logbestand in het hoofdvenster van het programma. Het resulterende logbestand (het vergelijkende logbestand) bevat alleen de verschillen tussen de twee logbestanden.

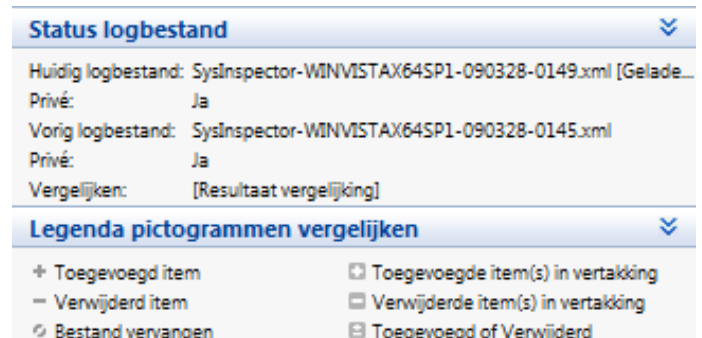
Opmerking: als u twee logbestanden vergelijkt, kiest u Bestand -> Logbestand opslaan en slaat u beide bestanden op in een ZIP-bestand. Als u het ZIP-bestand later opent, worden de logbestanden automatisch vergeleken.

Naast de weergegeven items staan symbolen die de verschillen tussen de vergeleken logbestanden aangeven. Items die zijn gemarkeerd met  zijn alleen aanwezig in het actieve logbestand en niet in het opgeslagen logbestand. Items die worden aangegeven met  zijn alleen gevonden in het opgeslagen logbestand en ontbreken in het actieve logbestand.

Hier volgt een omschrijving van alle symbolen die kunnen worden weergegeven bij een item:

-  nieuwe waarde, niet aanwezig in het vorige logbestand
-  de boomstructuur bevat nieuwe waarden
-  verwijderde waarde, alleen aanwezig in het vorige logbestand
-  de boomstructuur bevat verwijderde waarden
-  waarde/bestand is gewijzigd
-  de boomstructuur bevat gewijzigde waarden/bestanden
-  het risiconiveau is afgenomen / was hoger in het vorige logbestand
-  het risiconiveau is toegenomen / was lager in het vorige logbestand

In de linkerbenedenhoek worden alle symbolen beschreven en ziet u ook de namen van de logbestanden die worden vergeleken.



Een vergelijkend logbestand kunt u opslaan en later opnieuw openen.

Voorbeeld:

Genereer een logbestand met systeeminformatie en sla het bestand op met de naam Vorigbestand.xml. Nadat er wijzigingen zijn aangebracht in het systeem, opent u SysInspector en genereert u een nieuw logbestand. Sla dit logbestand op met de naam Huidigbestand.xml.

Om de verschillen tussen deze twee logbestanden te bepalen, kiest u **Bestand -> Logbestanden vergelijken**. Er wordt een vergelijkend logbestand gemaakt met de verschillen tussen de twee logbestanden.

U kunt dit ook doen door de volgende parameters te gebruiken op de opdrachtregel:

```
SysInspector.exe huidigbestand.xml vorigbestand.xml
```

5.4.1.4 SysInspector als onderdeel van ESET NOD32 Antivirus 4

Als u de sectie SysInspector wilt openen in ESET NOD32 Antivirus 4, klikt u op **Hulpmiddelen > SysInspector**. Het venster SysInspector werkt op ongeveer dezelfde manier als de vensters met logbestanden of geplande taken. Alle bewerkingen met momentopnamen van het systeem (maken, weergeven, vergelijken, verwijderen en exporteren) kunnen met één of twee muisklikken worden uitgevoerd.

Het venster SysInspector bevat basisinformatie over de gemaakte momentopnamen, zoals de aanmaaktijd, een korte omschrijving, de naam van de gebruiker die de momentopname heeft gemaakt en de status van de momentopname.

Als u momentopnamen wilt **vergelijken, toevoegen...**, of **verwijderen**, kiest u de betreffende knop onder de lijst met momentopnamen in het venster SysInspector. Deze opties zijn ook beschikbaar in het contextmenu van een momentopname. Als u de geselecteerde momentopname van het systeem wilt bekijken, kiest u **Beeld** in het contextmenu. Om de geselecteerde momentopname te exporteren naar een bestand, klikt u er met de rechtermuisknop op en kiest u **Exporteren...** Er volgt nu een gedetailleerde omschrijving van de beschikbare opties:

Vergelijken – Hiermee kunt u twee bestaande logbestanden vergelijken. Dit is handig als u wilt weten wat de verschillen zijn tussen het huidige logbestand en een ouder logbestand. U kunt deze optie alleen kiezen als er twee momentopnamen zijn geselecteerd om te vergelijken.

Toevoegen – Hiermee kunt u een nieuwe record maken. U moet eerst een korte omschrijving van de record invoeren. In de kolom Status kunt u het voltooiingspercentage zien van een momentopname die op dit moment wordt gemaakt. Alle voltooid momentopnamen hebben de status Gemaakt.

Verwijderen – Hiermee verwijdert u vermeldingen uit de lijst.

Weergeven – Hiermee geeft u de geselecteerde momentopname weer. U kunt dit ook doen door te dubbelklikken op de geselecteerde vermelding.

Exporteren... – Hiermee slaat u de geselecteerde vermelding op in een XML-bestand (ook in een gecomprimeerde versie).

5.4.1.5 SysInspector als onderdeel van ESET Smart Security 4

Servicescript is een hulpmiddel dat rechtstreekse invloed heeft op het besturingssysteem en geïnstalleerde toepassingen. Het stelt gebruikers in staat scripts uit te voeren die problematische onderdelen uit het systeem verwijderen, met inbegrip van virussen, restanten van virussen, geblokkeerde bestanden, records van virussen in het register, enzovoort. Het script wordt opgeslagen in een tekstbestand dat wordt gegenereerd aan de hand van een bestaand .xml-bestand. De gegevens in het .txt-scriptbestand zijn op eenvoudige en leesbare wijze ingedeeld. Het script zal in het begin een neutraal gedrag vertonen. Met andere woorden, in de oorspronkelijke vorm heeft het geen enkele impact op het systeem. De gebruiker moet het script bewerken om een effect te bereiken.

Waarschuwing:

Dit hulpmiddel is alleen bedoeld voor gevorderde gebruikers. Onjuist gebruik kan resulteren in beschadiging van programma's of het besturingssysteem.

5.4.1.5.1 SysInspector als onderdeel van ESET Smart Security 4

U kunt een script genereren door met de rechtermuisknop te klikken op een item in de menustructuur (aan de linkerkant) in het hoofdvenster van SysInspector. In het contextmenu selecteert u de optie **Alle secties naar servicescript exporteren** of de optie **Geselecteerde secties naar servicescript exporteren**.

5.4.1.5.2 De structuur van het servicescript

Op de eerste regel in de kop van het script vindt u informatie over de engine-versie (ev), de GUI-versie (gv) en de versie van het logbestand (lv). Aan de hand van deze gegevens kunt u mogelijke wijzigingen vaststellen in het .xml-bestand aan de hand waarvan het script wordt gegenereerd, en voorkomen dat er bij de uitvoering inconsistenties optreden. Dit gedeelte van het script mag niet worden gewijzigd.

De rest van het bestand is onderverdeeld in secties waarin items kunnen worden bewerkt (om aan te geven welke items door het script zullen worden verwerkt). U geeft aan dat een item moet worden verwerkt door het "-"-teken voor dat item te vervangen door een "+"-teken. De secties in het script zijn van elkaar gescheiden door een lege regel. Iedere sectie heeft een nummer en een titel.

01) Running processes

Deze sectie bevat een lijst met alle processen die in het systeem worden uitgevoerd. Elk proces wordt geïdentificeerd met behulp van het UNC-pad, gevolgd door de CRC16 hash-code tussen sterretjes (*).

Voorbeeld:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In dit voorbeeld is het proces module32.exe geselecteerd (gemarkeerd met een "+"-teken); als het script wordt uitgevoerd, wordt het proces beëindigd.

02) Loaded modules

Deze sectie bevat een lijst met de systeemmodules die momenteel in gebruik zijn.

Voorbeeld:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khibehb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In dit voorbeeld is de module khibehb.dll gemarkeerd met een "+". Als het script wordt uitgevoerd, worden de processen die gebruikmaken van die specifieke module herkend en beëindigd.

03) TCP connections

Deze sectie bevat informatie over bestaande TCP-verbindingen.

Voorbeeld:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 ->
127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 ->
127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 ->
127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe
Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Als het script wordt uitgevoerd, wordt de eigenaar van de socket in de gemarkeerde TCP-verbindingen opgezocht en wordt de socket vrijgegeven, waardoor systeembronnen beschikbaar komen.

04) UDP endpoints

Deze sectie bevat informatie over bestaande UDP-eindpunten.

Voorbeeld:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Als het script wordt uitgevoerd, wordt de eigenaar van de socket bij de aangegeven UDP-eindpunten geïsoleerd en wordt de socket vrijgegeven.

05) DNS server entries

Deze sectie bevat informatie over de huidige configuratie van de DNS-server.

Voorbeeld:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

De gemarkeerde vermeldingen van DNS-servers worden verwijderd als u het script uitvoert.

06) Important registry entries

Deze sectie bevat informatie over belangrijke registervermeldingen.

Voorbeeld:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\
Google\Update\GoogleUpdate.exe" /c

* Category: Internet Explorer (7 items)
HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Als het script wordt uitgevoerd, worden de gemarkeerde vermeldingen verwijderd, teruggedet naar 0-byte waarden of opnieuw ingesteld op de standaardwaarde. De actie die wordt toegepast op een bepaalde vermelding is afhankelijk van de categorie en de sleutelwaarde van de vermelding in het specifieke register.

07) Services

Deze sectie bevat een lijst met services die in het systeem zijn geregistreerd.

Voorbeeld:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\
windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path:
c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path:
c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Als het script wordt uitgevoerd, worden de gemarkeerde services en de ervan afhankelijke services gestopt en verwijderd.

08) Drivers

Deze sectie bevat een lijst met geïnstalleerde stuurprogramma's.

Voorbeeld:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\
system32\drivers\acpi.sys, state: Running, startup:
Boot
- Name: ADI UAA Function Driver for High Definition
Audio Service, exe path: c:\windows\system32\drivers\
adihdaud.sys, state: Running, startup: Manual
[...]
```

Als u het script uitvoert, worden de geselecteerde stuurprogramma's volledig uitgeschakeld en uit het systeem verwijderd.

09) Critical files

Deze sectie bevat informatie over bestanden die essentieel zijn voor een juiste werking van het besturingssysteem.

Voorbeeld:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
```

```
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
```

```
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

De geselecteerde items worden verwijderd of opnieuw ingesteld op de oorspronkelijke waarde.

5.4.1.5.3 Servicescripts uitvoeren

Markeer alle gewenste items, sla het script op en sluit het. U kunt het bewerkte script rechtstreeks vanuit het hoofdvenster van SysInspector uitvoeren door in het menu Bestand de optie **Servicescript uitvoeren** te selecteren. Wanneer u een script opent, wordt een bericht weergegeven met de volgende vraag: **Weet u zeker dat u het servicescript "%Scriptnaam%" wilt uitvoeren?** Nadat u uw selectie hebt bevestigd,

kan er nog een waarschuwing worden weergegeven met de mededeling dat u probeert een servicescript uit te voeren dat niet is ondertekend. Klik op **Uitvoeren** om het script te starten.

De succesvolle uitvoering van het script wordt bevestigd met een dialoogvenster.

Als het script slechts gedeeltelijk kon worden verwerkt, wordt een dialoogvenster weergegeven met het volgende bericht: **Het servicescript is gedeeltelijk uitgevoerd. Wilt u het foutrapport weergeven?** Selecteer **Ja** om een complex foutrapport weer te geven met een overzicht van de bewerkingen die niet zijn uitgevoerd.

Uw script is niet herkend als geldig en zal niet worden uitgevoerd als u het volgende bericht te zien krijgt: **Zijn er problemen met de consistentie van het script (een beschadigde kop of sectietitel, een ontbrekende lege regel tussen secties, enzovoort)?** U kunt het scriptbestand dan opnieuw openen en de fouten in het script corrigeren, of een nieuw servicescript maken.

5.5 ESET SysRescue

ESET Recovery CD (ERCD) is een hulpprogramma waarmee u een opstartschijf kunt maken die ESET NOD32 Antivirus 4 (ENA) bevat. Het belangrijkste voordeel van ESET Recovery CD is dat u ENA onafhankelijk van het besturingssysteem kunt uitvoeren, terwijl het programma toch rechtstreeks toegang heeft tot de schijf en het volledige bestandssysteem. Hierdoor is het mogelijk infiltraties te verwijderen die anders 'ontoegankelijk' zijn, bijvoorbeeld omdat het besturingssysteem actief is.

5.5.1 Minimale vereisten

ESET SysRescue (ESR) werkt in versie 2.x van Microsoft Windows Preinstallation Environment (Windows PE). Deze versie is gebaseerd op Windows Vista. Windows PE maakt deel uit van het gratis pakket Windows Automated Installation Kit (Windows AIK). Dit betekent dat Windows AIK geïnstalleerd moet zijn om een ESR-opstartmedium te kunnen genereren. Vanwege de ondersteuning van de 32-bits versie van Windows PE, kunt u alleen een ESR-opstartmedium maken in de 32-bits versie van ENA/ENA. ESR biedt ondersteuning voor Windows AIK 1.1 en hoger. ESR is beschikbaar in ENA/ENA 4.0 en hoger.

5.5.2 Een herstel-cd maken

Als wordt voldaan aan de minimale vereisten voor het maken van een cd met ESET SysRescue (ESR), is het daadwerkelijk maken van de cd heel eenvoudig. Start de ESR-wizard door te klikken op **Start > Programma's > ESET > ESET NOD32 Antivirus 4 > ESET SysRescue**.

De wizard controleert eerst of Windows AIK is geïnstalleerd en of er een geschikt apparaat is aangesloten voor het maken van het opstartmedium.

In de volgende stap geeft u aan waar u ESR wilt opslaan. U kunt kiezen voor een cd, dvd of USB-apparaat. Daarnaast kunt u de ESR-gegevens ook opslaan in een ISO-bestand. De ISO-afbeelding kunt u dan later op een cd of dvd zetten, of op een andere manier gebruiken (zoals in een virtuele omgeving, bijvoorbeeld VmWare of Virtualbox).

Nadat u alle parameters hebt opgegeven, ziet u in de laatste stap van de ESET SysRescue-wizard een compilatievoorbeeld. Controleer hier de parameters en start vervolgens de compilatie. De volgende opties zijn beschikbaar:

Mappen
ESET Antivirus
Geavanceerd
Opstartbaar USB-apparaat
Branden

5.5.2.1 Mappen

Tijdelijke map is een werkmap voor bestanden die nodig zijn tijdens de ESET SysRescue-compilatie.

ISO-map is een map waarin het resulterende ISO-bestand wordt opgeslagen als de compilatie is voltooid.

De lijst op dit tabblad bevat alle lokale en gekoppelde netwerkschijven, inclusief de beschikbare ruimte. Als bepaalde mappen zich bevinden op een schijf met onvoldoende vrije ruimte, is het raadzaam een schijf te selecteren met meer vrije ruimte. Anders is het namelijk mogelijk dat de compilatie niet kan worden voltooid omdat er onvoldoende ruimte beschikbaar is op de schijf.

Externe toepassingen

Hiermee kunt u aanvullende programma's opgeven die moeten worden uitgevoerd of geïnstalleerd na het opstarten vanaf een SysRescue-medium.

Inclusief externe toepassingen – Hiermee kunt u externe programma's toevoegen aan de SysRescue-compilatie.

Geselecteerde map – Map waarin programma's staan die aan de SysRescue-schijf worden toegevoegd.

5.5.2.2 ESET Antivirus

Als u een ESET SysRescue-cd wilt maken, kunt u kiezen uit twee bronnen voor de ESET-bestanden die door de compiler worden gebruikt.

ENA-map – Bestanden die al in de map staan waarin het ESET-product is geïnstalleerd op de computer.

MSI-bestand – Bestanden die aanwezig zijn in het MSI-installatiepakket worden gebruikt.

Profiel – U kunt een van de volgende twee bronnen gebruiken voor de gebruikersnaam en het wachtwoord:

Geïnstalleerde ENA – De gebruikersnaam en het wachtwoord worden gekopieerd uit de huidige installatie van ESET NOD32 Antivirus 4 of ESET NOD32.

Van gebruiker – De gebruikersnaam en het wachtwoord uit de tekstvakken hieronder worden gebruikt.

Opmerking: *de versie van ESET NOD32 Antivirus 4 of ESET NOD32 Antivirus op de ESET SysRescue-cd wordt bijgewerkt vanaf internet of vanuit de ESET Security-oplossing die is geïnstalleerd op de computer waarop de ESET SysRescue-cd wordt uitgevoerd.*

5.5.2.3 Geavanceerd

Gebruik het tabblad **Geavanceerd** om de ESET SysRescue-cd te optimaliseren voor de grootte van het werkgeheugen van uw computer. Selecteer **512 MB of meer** om de inhoud van de cd naar het werkgeheugen (RAM) te schrijven. Als u **Minder dan 512 MB** selecteert, wordt de herstel-cd permanent gelezen tijdens het uitvoeren van WinPE.

Externe stuurprogramma's – Gebruik deze sectie om stuurprogramma's voor specifieke hardware (meestal een netwerkadapter) toe te voegen. Hoewel WinPE is gebaseerd op Windows Vista SPI en die Windows-versie ondersteuning biedt voor zeer veel hardware, wordt bepaalde hardware soms niet herkend en moet u het betreffende stuurprogramma handmatig toevoegen. Er zijn twee manieren om een stuurprogramma op te nemen in de ESET SysRescue-compilatie: handmatig (via de knop **Toevoegen**) en automatisch (via de knop voor **automatisch zoeken**). In het eerste geval moet u het pad naar het gewenste INI-bestand selecteren (het bijbehorende SYS-bestand moet in dezelfde map staan). Als u de functie voor automatisch zoeken gebruikt, wordt het stuurprogramma automatisch gevonden in het besturingssysteem van de opgegeven computer. Het is raadzaam deze functie alleen te gebruiken als u SysRescue gebruikt op een computer met dezelfde netwerkadapter als de adapter in de computer waarop u de SysRescue-cd maakt. Tijdens het compileren van de cd wordt het stuurprogramma automatisch toegevoegd en hoeft de gebruiker er later niet naar te zoeken.

5.5.2.4 Opstartbaar USB-apparaat

Als u hebt aangegeven dat u een USB-apparaat wilt gebruiken, kunt u op het tabblad Opstartbaar USB-apparaat het gewenste apparaat selecteren als er verschillende USB-apparaten zijn aangesloten.

Waarschuwing: *het geselecteerde USB-apparaat wordt geformatteerd tijdens het voorbereiden van het ESET SysRescue-proces. Dit betekent dat alle gegevens op het apparaat worden verwijderd.*

5.5.2.5 Branden

Als u cd/dvd hebt geselecteerd voor de SysRescue-bestanden, kunt u op het tabblad Branden aanvullende parameters opgeven.

ISO-bestand verwijderen – Selecteer deze optie om ISO-bestanden te verwijderen nadat de herstel-cd van ESET is gebrand.

Verwijderen ingeschakeld – Hiermee kunt u kiezen voor snel wissen en volledig wissen.

Brander – Selecteer het station dat u wilt gebruiken om te branden.

Waarschuwing: *dit is de standaardoptie. Als u een herschrijfbaar cd/dvd gebruikt, worden alle gegevens op de cd/dvd gewist.*

De sectie Medium bevat informatie over het huidige medium dat in het cd/dvd-apparaat is geplaatst.

Brandsnelheid – Selecteer de gewenste brandsnelheid in de vervolgkeuzelijst. Houd hierbij rekening met de mogelijkheden van uw brander en het type cd/dvd dat u gebruikt.

5.5.3 Werken met ESET SysRescue

Een cd, dvd of USB-apparaat met herstel-informatie kan alleen worden gebruikt als de computer wordt opgestart van het opslagmedium dat met ESET SysRescue is gemaakt. De opstartvolgorde kan worden ingesteld in het BIOS. U kunt ook tijdens het opstarten van de computer het opstartmenu oproepen. Hiervoor moet u een toets uit het bereik F9 - F12 indrukken, afhankelijk van de versie van het moederbord/BIOS.

Als het opstarten van de computer is voltooid, wordt ENA/ENA gestart. Aangezien ESET SysRescue alleen in specifieke situaties wordt gebruikt, zijn sommige beveiligingsmodules en programmafuncties van de gewone versie van ENA/ENA niet nodig. Het aantal voorzieningen is dan ook beperkt tot Computerscan, Update en bepaalde secties met instellingen. De mogelijkheid om de database met viruskenmerken bij te werken, is de belangrijkste functie van ESET SysRescue. Het is raadzaam het programma bij te werken voordat u een computerscan start.

5.5.3.1 ESET SysRescue in de praktijk

Stel dat computers in het netwerk zijn geïnfecteerd door een virus dat uitvoerbare bestanden (EXE) aanpast. ENA/ENA kan alle geïnfecteerde bestanden herstellen, behalve Explorer.exe. Dit bestand kan nooit worden hersteld, zelfs niet in de veilige modus.

De reden hiervoor is dat Explorer.exe een van de essentiële processen van Windows is en dus ook in de veilige modus wordt uitgevoerd. ENA/ENA kan dus geen bewerkingen op dit bestand uitvoeren en het bestand blijft dus geïnfecteerd.

In een dergelijk scenario kunt u ESET SysRescue gebruiken om het probleem op te lossen. ESET SysRescue kan namelijk helemaal los van het besturingssysteem worden uitgevoerd. Het programma kan dus elk bestand op de schijf verwerken (opschonen of verwijderen).

6. Woordenlijst

6.1 Typen bedreigingen

Bij infiltratie probeert schadelijke software de computer van een gebruiker binnen te dringen en/of te beschadigen.

6.1.1 Virussen

Een computervirus is een bedreiging die bestaande bestanden op uw computer beschadigt. De naam 'virussen' verwijst naar biologische virussen, omdat ze vergelijkbare methoden gebruiken om zich van computer tot computer te verspreiden.

Computervirussen hebben het voornamelijk voorzien op uitvoerbare bestanden en documenten. Een virus verspreidt zich door zijn code aan het einde van een doelbestand vast te maken. Een computervirus werkt als volgt: nadat het geïnfecteerde bestand is uitgevoerd, activeert het virus zichzelf (vóór de oorspronkelijke toepassing) en wordt de vooraf gedefinieerde taak van het virus uitgevoerd. Pas dan kan de oorspronkelijke toepassing worden uitgevoerd. Een computer kan alleen met een virus worden geïnfecteerd als een gebruiker het schadelijke programma (per ongeluk of opzettelijk) zelf uitvoert of opent.

De activiteiten en het gevaar van computervirussen variëren. Sommige virussen zijn uiterst gevaarlijk omdat ze worden gebruikt om opzettelijk bestanden van een vaste schijf te verwijderen. Andere virussen veroorzaken geen echte schade, maar zijn alleen ontwikkeld om de gebruiker te irriteren en de technische vaardigheden van de ontwikkelaars te laten zien.

Een belangrijke ontwikkeling is dat virussen steeds minder vaak voorkomen (in vergelijking met Trojaanse paarden of spyware) omdat ze niet commercieel interessant zijn voor de makers van schadelijke software. De term 'virus' wordt vaak ten onrechte gebruikt voor alle typen bedreigingen. Hier komt echter langzaam verandering in doordat de nieuwe term 'malware' (malicious software = schadelijke software), die de lading beter dekt, steeds vaker wordt gebruikt.

Als uw computer met een virus is geïnfecteerd, moet u de geïnfecteerde bestanden herstellen door ze op te schonen met een antivirusprogramma.

Voorbeelden van virussen zijn: OneHalf, Tenga en Yankee Doodle.

6.1.2 Wormen

Een computerworm is een programma met schadelijke code dat hostcomputers aanvalt en zich verspreidt via een netwerk. Het belangrijkste verschil tussen een virus en een worm is dat een worm in staat is zichzelf te verspreiden en te verplaatsen. Wormen zijn niet afhankelijk van hostbestanden (of opstartsectoren).

Wormen verspreiden zich via e-mail of netwerkpakketten. Wormen kunnen in twee categorieën worden onderverdeeld:

- **E-mail** – Wormen die zichzelf verspreiden via e-mailadressen in de lijst met contactpersonen van een gebruiker.
- **Netwerk** – Wormen die gebruikmaken van beveiligingsproblemen in verschillende toepassingen.

Wormen zijn daarom veel hardnekkiger dan computervirussen. Door het massale gebruik van het internet kunnen wormen zich enkele uren (soms zelfs enkele minuten) nadat ze in omloop zijn gebracht, over de hele wereld verspreiden. Doordat wormen zich zelfstandig met grote snelheid kunnen verspreiden, zijn ze gevaarlijker dan andere typen malware, zoals virussen.

Als een worm in een systeem wordt geactiveerd, kan dat leiden tot verschillende problemen: de worm kan bestanden verwijderen, de prestaties van het systeem verminderen of zelfs bepaalde programma's deactiveren. Door zijn eigenschappen is de worm geschikt als 'transportmiddel' voor andere typen bedreigingen.

Als uw computer is geïnfecteerd met een computerworm, adviseren wij u de geïnfecteerde bestanden te verwijderen omdat ze waarschijnlijk schadelijke code bevatten.

Voorbeelden van bekende wormen zijn: Lovsan/Blaster, Stration/Warezov, Bagle en Netsky.

6.1.3 Trojaanse paarden

Volgens de traditionele definitie zijn Trojaanse paarden bedreigingen die zichzelf proberen voor te doen als nuttige programma's en die vervolgens door nietsvermoedende gebruikers worden uitgevoerd. Dit gold echter voor Trojaanse paarden in het verleden. Tegenwoordig hoeven Trojaanse paarden hun ware aard niet meer te verbergen. Trojaanse paarden worden gebruikt om zo eenvoudig mogelijk te infiltreren, zodat ze hun schadelijke praktijken kunnen uitvoeren. De term 'Trojaans paard' heeft nu een algemene betekenis en wordt gebruikt voor bedreigingen die niet in een specifieke categorie bedreigingen kunnen worden ingedeeld.

Omdat deze categorie erg breed is, worden Trojaanse paarden vaak verdeeld in een aantal subcategorieën. De bekendste subcategorieën zijn:

- **downloader** – een schadelijk programma waarmee andere bedreigingen van internet kunnen worden gedownload.
- **dropper** – een type Trojaans paard waarmee andere typen malware kunnen worden geïnstalleerd op computers met beveiligingsproblemen.
- **backdoor** – een toepassing die communiceert met externe aanvallers, waardoor zij toegang tot een systeem kunnen krijgen en het systeem kunnen overnemen.
- **keylogger** – (keystroke logger) – een programma waarmee elke toetsaanslag van een gebruiker wordt geregistreerd, waarna de gegevens naar externe aanvallers worden verzonden.
- **dialer** – dialers zijn programma's waarmee automatisch verbinding wordt gemaakt met nummers met hoge tarieven. Het is vrijwel onmogelijk te merken dat er een nieuwe verbinding tot stand is gebracht. Dialers kunnen alleen schade veroorzaken voor gebruikers met inbelmodems, die niet vaak meer worden gebruikt.

Trojaanse paarden zijn meestal uitvoerbare bestanden met de extensie .exe. Als er een Trojaans paard op uw computer wordt gedetecteerd, adviseren wij u het bestand te verwijderen omdat het waarschijnlijk schadelijke code bevat.

Voorbeelden van bekende Trojaanse paarden zijn: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkits

Rootkits zijn schadelijke programma's waarmee internetaanvallers onbeperkte toegang tot een systeem kunnen krijgen, terwijl hun aanwezigheid verborgen blijft. Nadat rootkits zich toegang tot een systeem hebben verschafte (meestal door gebruik te maken van een systeembeveiligingsprobleem), gebruiken ze functies in het besturingssysteem om te voorkomen dat ze worden gedetecteerd met de antivirussoftware: ze verbergen processen, bestanden en Windows-registergegevens. Hierdoor is het vrijwel onmogelijk rootkits te detecteren met de gebruikelijke testmethoden.

Als u preventiemaatregelen tegen rootkits wilt nemen, is het belangrijk onderscheid te maken tussen twee detectieniveaus:

1. Detectie op het moment dat ze toegang tot het systeem proberen te krijgen. Op dat moment zijn ze nog niet aanwezig en dus inactief. Met de meeste antivirussystemen kunnen rootkits op dit niveau worden geëlimineerd (aangenomen dat dergelijke bestanden als geïnfecteerde bestanden worden herkend door het antivirusstelsel).

2. Detectie wanneer ze zijn verborgen en niet met de gebruikelijke testmethoden kunnen worden gedetecteerd. Gebruikers van het ESET-antivirussysteem kunnen gebruikmaken van de Anti-Stealth-technologie, waarmee actieve rootkits kunnen worden gedetecteerd en verwijderd.

6.1.5 Adware

Adware is een afkorting voor door advertenties ondersteunde software. Programma's waarin reclamemateriaal wordt weergegeven vallen onder deze categorie. Adwareprogramma's openen vaak automatisch een nieuw pop-upvenster met reclame in een internetbrowser of wijzigen de startpagina. Adware is vaak opgenomen in freewareprogramma's, waardoor de ontwikkelaars van de freeware de ontwikkelkosten van hun (gewoonlijk nuttige) programma's kunnen terugverdienen.

Adware zelf is niet gevaarlijk. Gebruikers worden alleen lastiggevallen met advertenties. Het gevaar schuilt in het feit dat adware ook traceringsfuncties kan uitvoeren (net als spyware doet).

Als u besluit een freewareproduct te gebruiken, let dan speciaal op het installatieprogramma. Het installatieprogramma waarschuwt u gewoonlijk bij de installatie van een extra adwareprogramma. Vaak kunt u deze annuleren en het programma installeren zonder adware. In sommige gevallen kunnen programma's echter niet worden geïnstalleerd zonder adware of wordt hun functionaliteit beperkt. Dit betekent dat adware vaak op 'legale' wijze toegang heeft tot het systeem, omdat gebruikers hiermee akkoord zijn gegaan. In dat geval is het beter het zekere voor het onzekere te nemen.

Als er een adwarebestand op uw computer wordt gedetecteerd, adviseren wij u het bestand te verwijderen omdat het waarschijnlijk schadelijke code bevat.

6.1.6 Spyware

Deze categorie omvat alle toepassingen waarmee persoonlijke gegevens worden verzonden zonder dat de gebruiker daar toestemming voor heeft gegeven of zonder dat de gebruiker zich ervan bewust is. Deze programma's gebruiken traceerfuncties om verschillende statistische gegevens te verzenden, zoals websites die de gebruiker heeft bezocht, e-mailadressen van de contactpersonen van de gebruiker of toetsaanslagen van de gebruiker.

De makers van spyware beweren dat deze programma's zijn bedoeld om de wensen en interesses van de gebruiker te inventariseren, zodat ze hun reclameboodschappen beter op de gebruiker kunnen afstemmen. Het probleem is echter dat er geen duidelijk onderscheid tussen nuttige en schadelijke toepassingen kan worden gemaakt. Bovendien kan niemand garanderen dat er geen misbruik wordt gemaakt van de gegevens. Voorbeelden van gegevens die kunnen worden verzameld met spywaretoepassingen zijn beveiligingscodes, pincodes of bankrekeningnummers. Spyware wordt vaak door de maker van het programma bij gratis versies van een programma gevoegd om inkomsten te genereren of om de gebruiker ertoe te bewegen de software aan te schaffen. Vaak worden gebruikers tijdens de installatie van een programma geïnformeerd over de aanwezigheid van spyware om hun ertoe te bewegen een betaalde versie zonder spyware aan te schaffen.

Voorbeelden van bekende freewareproducten waarbij spyware wordt meegeleverd, zijn clientprogramma's van P2P-netwerken (peer-to-peer). Spyfalcon of Spy Sheriff (en vele andere programma's) behoren tot een speciale subcategorie spywareprogramma's. Deze programma's doen zich voor als antispywareprogramma's, maar zijn in feite spywareprogramma's.

Als er een spywarebestand op uw computer wordt gedetecteerd, adviseren wij u het bestand te verwijderen omdat het waarschijnlijk schadelijke code bevat.

6.1.7 Potentieel onveilige toepassingen

Er zijn veel legitieme programma's die zijn bedoeld om het beheer van computers in een netwerk te vereenvoudigen. In de verkeerde handen kunnen deze programma's echter worden gebruikt om schadelijke praktijken uit te oefenen. Daarom heeft ESET deze speciale categorie gedefinieerd. Onze klanten kunnen nu kiezen of deze bedreigingen wel of niet moeten worden gedetecteerd met het antivirussysteem.

'Potentieel onveilige programma's' is de classificatie voor commerciële, legitieme software. Deze categorie omvat hulpprogramma's voor externe toegang, programma's voor het kraken van wachtwoorden, keyloggers (programma's die elke toetsaanslag van een gebruiker registreren), enzovoort.

Als u merkt dat er een potentieel onveilige toepassing (die u niet zelf hebt geïnstalleerd) op uw computer actief is, neemt u contact op met de netwerkbeheerder of verwijdert u de toepassing.

6.1.8 Potentieel ongewenste toepassingen

Potentieel ongewenste toepassingen zijn niet per se schadelijk, maar kunnen de prestaties van uw computer aantasten. Voor de installatie van dergelijke toepassingen moet doorgaans expliciet toestemming worden gegeven. Deze toepassingen veranderen de manier waarop uw computer werkt (vergeleken met de status van de computer voorafgaand aan de installatie). De voornaamste wijzigingen zijn:

- Weergave van vensters die u niet eerder hebt gezien
- Activering en uitvoering van verborgen processen
- Verhoogd gebruik van systeembronnen
- Wijzigingen in zoekresultaten
- Communicatie tussen de toepassing en externe servers