kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 voor Windows

Inhoud

Over Kaspersky Endpoint Security 10 Service Pack 2 voor Windows

In deze sectie worden de functies, de onderdelen en het distributiepakket van Kaspersky Endpoint Security beschreven en vindt u een lijst met hardware- en softwarevereisten voor Kaspersky Endpoint Security.

Nieuwigheden

Kaspersky Endpoint Security 10 Service Pack 2 voor Windows beschikt over de volgende functies en verbeteringen:

1. Programma-opstartcontrole:
    - Ondersteunt besturingssystemen van servers.
    - Controleert downloads van DLL-modules en stuurprogramma's.
    - Beheert de lijst met objecten in de inventarisatietaak (DLL-modules en scriptbestanden)
    - Controleert objecten op basis van een nieuw criterium - door kenmerken van digitale-handtekeningcertificaten.
    - Genereert een rapport over teststarten van geblokkeerde programma's.
    - Ondersteunt twee gebruiksmodi voor Programma-opstartcontrole: 'Black list' en 'White list'.
    - Gebruikt de SHA256-hash voor de controle en de inventarisatie van objecten.
    - Controleert de uitvoer van scripts vanaf de PowerShell interpreter.
    - Gebruikt vertrouwde systeemcertificatenopslag.
2. Het Microsoft BitLocker-beheer maakt de encryptie van harde schijven mogelijk met de hulp van BitLocker-technologie van Microsoft:
    - Beheer de encryptie op afstand.
    - Monitor geëncrypte apparaten.
    - Maak rapporten over de encryptie van apparaten.
    - Herstel de toegang tot geëncrypte apparaten.
3. Kaspersky Disk Encryption:
    - Ondersteunt de invoer van gebruikersgegevens in de preboot-omgeving van Verificatie-agent via een virtueel toetsenbord.
    - Ondersteunt de encryptiemodus waarin alleen de gebruikte ruimte op een apparaat wordt geëncrypt.
    - Ondersteunt encryptie op tablets (MS Surface versie 3 en 4).
4. Controle van programmabevoegdheden:

- Controleert de toegang van programma's tot audio- en video-opnameapparaten.

5. Webcontrole:

   - Configureert de toegangsregels voor webbronnen voor extra categorieën van webbronnen.

6. Apparaatcontrole:

   - Registreert gebeurtenissen die te maken hebben met het verwijderen en opslaan van bestanden op USB-apparaten.
   - Genereert een lijst met vertrouwde Wi-Fi-netwerken op basis van de volgende instellingen: naam, soort encryptie en soort verificatie.
   - Beheert toegangsrechten van gebruikers voor lees- en schrijfbewerkingen voor bestanden op cd's en dvd's.

7. Mail Anti-Virus:

   - Verwijdert en hernoemt specifieke soorten bestanden in archieven die door Mail Anti-Virus worden gescand.

8. Kaspersky Security Network:

   - Geeft KSN weer als reden voor een beslissing over de objectverwerking in rapporten van Kaspersky Endpoint Security en Kaspersky Security Center.
   - Stuurt een verzoek naar KSN om de reputatie van een geselecteerd bestand te achterhalen.
   - Toont de status van de beschikbaarheid van KSN-servers voor clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Software pakket

Het distributiepakket van Kaspersky Endpoint Security bevat de volgende bestanden:

- Benodigde bestanden voor de installatie van het programma via een van de beschikbare methoden:
- Gebruikte updatepakketten tijdens de installatie van het programma.
- Het bestand 'klcfginst.msi' voor de installatie van de Kaspersky Endpoint Security-beheerplug-in via Kaspersky Security Center.
- Het bestand 'ksn_<taalcode>.txt' waarin u de voorwaarden voor de deelname aan Kaspersky Security Network kunt lezen.
- Het bestand 'license.txt' waarin u de Gebruiksrechtovereenkomst kunt lezen.
- Het bestand 'incompatible.txt' dat een lijst met incompatibele software bevat.
- Het bestand 'installer.ini' dat de interne instellingen van het distributiepakket bevat.

> U wordt aanbevolen om de waarden van de instellingen niet te wijzigen. Gebruik het bestand setup.ini als u de installatieopties wilt wijzigen.

U moet het distributiepakket uitpakken om toegang tot de bestanden te krijgen.

Computerbescherming organiseren

Kaspersky Endpoint Security biedt een uitgebreide computerbescherming tegen verschillende soorten bedreigingen en netwerk- en phishingaanvallen.

Elk soort bedreiging wordt door een speciaal onderdeel afgehandeld. Onderdelen kunnen afzonderlijk worden in- of uitgeschakeld en hun instellingen kunnen worden geconfigureerd.

Naast de realtime bescherming van de beschermingsonderdelen raden we aan de computer periodiek te *scannen* op virussen en andere bedreigingen. Zo verkleint u de kans op verspreiding van malware die niet door de beschermingsonderdelen wordt gedetecteerd wegens een laag beschermingsniveau of andere redenen.

Om Kaspersky Endpoint Security up-to-date te houden, moet u de databases en de modules die het programma gebruikt *bijwerken*. Het programma wordt standaard automatisch bijgewerkt maar u kunt indien nodig de databases en de programmamodules handmatig bijwerken.

De volgende programmaonderdelen zijn controle-onderdelen:

- **Programma-opstartcontrole**. Dit onderdeel houdt bij welke programma's de gebruiker probeert te starten en regelt de opstart van programma's.
- **Controle van programmabevoegdheden**. Dit onderdeel registreert de acties van programma's in het besturingssysteem en regelt de programma-activiteit afhankelijk van de vertrouwensgroep van een bepaald programma. Voor elke groep programma's is een reeks regels opgegeven. Deze regels regelen de toegang van programma's tot gebruikersgegevens en tot bronnen van het besturingssysteem. Zulke gegevens zijn onder andere bestanden van de gebruiker (de map 'Documenten', cookies, informatie over gebruikersactiviteit) en bestanden, mappen en registersleutels die instellingen en belangrijke gegevens van de meest gebruikte programma's bevatten.
- **Kwetsbaarheidsbewaking**. Het onderdeel Kwetsbaarheidsbewaking voert een realtime kwetsbaarheidsscan van programma's uit die zijn gestart of actief zijn op de computer van de gebruiker.
- **Apparaatcontrole**. Met dit onderdeel kunt u flexibele beperkingen instellen voor de toegang tot opslagapparaten (zoals harde schijven, verwisselbare schijven, tapestations en cd's/dvd's), apparaten voor gegevensoverdracht (zoals modems), apparaten die gegevens in afgedrukte exemplaren omzetten (zoals printers) of interfaces voor de aansluiting van apparaten op computers (zoals USB, Bluetooth en Infrarood).
- **Webcontrole**. Met dit onderdeel kunt u voor verschillende gebruikersgroepen flexibele beperkingen instellen voor de toegang tot webbronnen.

De werking van controle-onderdelen is op de volgende regels gebaseerd:

- Programma-opstartcontrole gebruikt regels van Programma-opstartcontrole.
- Controle van programmabevoegdheden gebruikt regels voor programmacontrole.
- Apparaatcontrole gebruikt toegangsregels voor apparaten en toegangsregels voor verbindingsbussen.
- Webcontrole gebruikt toegangsregels voor webbronnen.

De volgende programmaonderdelen zijn beschermingsonderdelen:

- **Anti-Virus voor bestanden**. Dit onderdeel beschermt het bestandssysteem van de computer tegen infecties. Anti-Virus voor bestanden wordt samen met Kaspersky Endpoint Security gestart. Het onderdeel blijft voortdurend actief in het computergeheugen en scant alle bestanden die worden geopend, opgeslagen of gestart op de computer en alle aangesloten schijven. Anti-Virus voor bestanden onderschept elke poging om een bestand te openen en scant het bestand op virussen en andere bedreigingen.

- **Systeembewaking**. Dit onderdeel houdt de programma-activiteit op de computer bij en geeft deze informatie aan andere onderdelen om een efficiëntere bescherming van de computer te verzekeren.

- **Mail Anti-Virus**. Dit onderdeel scant inkomende en uitgaande e-mailberichten op virussen en andere bedreigingen.

- **Web Anti-Virus**. Dit onderdeel scant verkeer dat op de computer van de gebruiker terechtkomt via de protocollen HTTP en FTP en controleert of de URL's kwaadaardige of phishingadressen zijn.

- **IM Anti-Virus**. Dit onderdeel scant verkeer dat op de computer terechtkomt via protocollen van instant messengers. Met het onderdeel kunt u veel instant messengers veilig gebruiken.

- **Firewall**. Dit onderdeel beschermt opgeslagen gegevens op de computer en blokkeert de meeste bedreigingen voor het besturingssysteem terwijl de computer verbonden is met het internet of een lokaal netwerk. Het onderdeel filtert alle netwerkactiviteit volgens twee soorten regels: netwerkregels voor programma's en regels voor netwerkpakketten.

- **Netwerkmonitor**. Met dit onderdeel kunt u de netwerkactiviteit van de computer in real time zien.

- **Network Attack Blocker**. Dit onderdeel controleert inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Bij de detectie van een netwerkaanval op uw computer blokkeert Kaspersky Endpoint Security alle netwerkactiviteit van de computer die de aanval uitvoert.

De volgende taken kunt u met Kaspersky Endpoint Security uitvoeren:

- **Volledige Scan**. Kaspersky Endpoint Security scant het besturingssysteem, inclusief RAM, objecten die bij de opstart worden geladen, de back-upopslag van het besturingssysteem en alle harde schijven en verwisselbare schijven.

- **Aangepaste Scan**. Kaspersky Endpoint Security scant de objecten die door de gebruiker worden geselecteerd.

- **Kritieke Gebiedenscan**. Kaspersky Endpoint Security scant objecten die bij de opstart van het besturingssysteem worden geladen, het RAM en objecten die het doelwit van rootkits zijn.

- **Update**. Kaspersky Endpoint Security downloadt bijgewerkte databases en programmamodules. Bijwerken houdt de computer beschermd tegen de nieuwste virussen en andere bedreigingen.

- **Kwetsbaarheidsscan**. Kaspersky Endpoint Security scant het besturingssysteem en geïnstalleerde software op kwetsbaarheden. Door deze scan worden potentiële problemen die indringers kunnen misbruiken tijdig gedetecteerd en verwijderd.

Met de encryptiefunctionaliteit voor bestanden kunt u bestanden en mappen op lokale schijven van de computer encrypten. Met de encryptiefunctionaliteit voor schijven kunt u harde schijven en verwisselbare schijven encrypten.

Extern beheer via Kaspersky Security Center

Via Kaspersky Security Center kunt u Kaspersky Endpoint Security op een clientcomputer op afstand starten en stoppen en programma-instellingen op afstand beheren en configureren.

Onderhoudsfuncties van het programma

Kaspersky Endpoint Security beschikt over een aantal onderhoudsfuncties. Onderhoudsfuncties zijn bedoeld om het programma up-to-date te houden, de functionaliteit van het programma uit te breiden en de gebruiker te helpen bij het gebruik van het programma.

- **Rapporten**. Tijdens de werking houdt het programma een rapport over elk programmaonderdeel en elke taak bij. Het rapport bevat een lijst met gebeurtenissen van Kaspersky Endpoint Security en alle bewerkingen die het programma uitvoert. Bij een eventueel incident kunt u rapporten naar Kaspersky versturen zodat experts van de Technische Support het probleem meer in detail kunnen bestuderen.

- **Gegevensopslag**. Als het programma geïnfecteerde of waarschijnlijk geïnfecteerde bestanden vindt tijdens het scannen van de computer op virussen en andere bedreigingen, blokkeert het die bestanden. Kaspersky Endpoint Security plaatst waarschijnlijk geïnfecteerde bestanden in een speciale opslag genaamd *Quarantaine*. Kaspersky Endpoint Security slaat kopieën van gedesinfecteerde en verwijderde bestanden in *Back-up* op. Kaspersky Endpoint Security plaatst bestanden die om een bepaalde reden niet zijn verwerkt op de *lijst met onverwerkte bestanden*. U kunt bestanden scannen, bestanden in hun originele map terugzetten en de gegevensopslag legen.

- **Service voor meldingen**. De service voor meldingen houdt de gebruiker op de hoogte over de huidige beschermingsstatus van de computer en over de werking van Kaspersky Endpoint Security. Meldingen kunnen op het scherm worden weergegeven of per e-mail worden verstuurd.

- **Kaspersky Security Network**. De deelname van de gebruiker aan Kaspersky Security Network verbetert de doeltreffendheid van de computerbescherming via de realtime verzameling van informatie over de reputatie van bestanden, webbronnen en software van gebruikers wereldwijd.

- **Licentie**. Door de aanschaf van een licentie kunt u de functionaliteit van het programma ontgrendelen, updates voor de programmadatabases en -modules installeren en ondersteuning per telefoon of e-mail krijgen voor problemen met de installatie, de configuratie en het gebruik van het programma.

- **Support**. Alle geregistreerde gebruikers van Kaspersky Endpoint Security kunnen voor assistentie contact opnemen met de experts van Technische Support. U kunt een verzoek vanaf uw My Kaspersky-account op de website van de Technische Support versturen of telefonische assistentie van het ondersteuningspersoneel krijgen.

Als het programma tijdens de werking een fout geeft of crasht, kan het automatisch opnieuw worden gestart.

Als in het programma terugkerende fouten optreden die ervoor zorgen dat het programma crasht, voert het programma de volgende bewerkingen uit:

1. Het schakelt de controle- en beschermingsfuncties uit (de encryptiefunctionaliteit blijft ingeschakeld).

2. Het meldt de gebruiker dat de functies zijn uitgeschakeld.

3. Het probeert het programma te herstellen naar een functionele toestand na het bijwerken van de antivirusdatabases of de programmamodules.

Het programma ontvangt informatie over terugkerende fouten en systeemblokkeringen met speciaal hiervoor ontwikkelde algoritmen van Kaspersky-experts.

Hardware- en softwarevereisten

Uw computer moet aan de volgende vereisten voldoen voor de juiste werking van Kaspersky Endpoint Security:

Minimale algemene vereisten:

- 2 GB beschikbare ruimte op de harde schijf
- Processor met een kloksnelheid van 1 GHz (die SSE2-instructies ondersteunt)
- RAM:
  - 1 GB voor een 32-bits besturingssysteem;
  - 2 GB voor een 64-bits besturingssysteem.

Ondersteunde besturingssystemen voor pc's:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 of hoger;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows 10 raadpleegt u de Knowledge Base van de Technische Support.

Ondersteunde besturingssystemen voor bestandsservers:

- Windows Small Business Server 2008 Standard / Premium (64-bit);
- Windows Small Business Server 2011 Essentials / Standard (64-bit);
- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 of hoger;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 of hoger;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Voor informatie over de ondersteuning voor Microsoft Windows Server 2016 en Microsoft Windows Server 2019 raadpleegt u de Knowledge Base van de Technische Support.

Het programma installeren en verwijderen

In deze sectie leest u meer over de installatie van Kaspersky Endpoint Security op de computer, de voltooiing van de initiële configuratie, de upgrade vanaf een oudere versie van het programma en de verwijdering van het programma.

Het programma installeren

In deze sectie wordt beschreven hoe u Kaspersky Endpoint Security op de computer installeert en de initiële configuratie van het programma voltooit.

Methoden voor de installatie van het programma

Kaspersky Endpoint Security 10 voor Windows kan lokaal worden geïnstalleerd (rechtstreeks op de computer van de gebruiker) of op afstand vanaf het werkstation van de beheerder.

De lokale installatie van Kaspersky Endpoint Security 10 voor Windows kan in een van de volgende modi worden uitgevoerd:

- In de interactieve modus via de Installatiewizard van het programma.

  Bij de interactieve modus is uw assistentie tijdens het installatieproces vereist.

- In de stille modus vanaf de opdrachtregel.

  Nadat de installatie in de stille modus is gestart, is uw assistentie tijdens het installatieproces niet meer vereist.

Het programma kan op afstand vanaf netwerkcomputers worden geïnstalleerd via het volgende:

- De Kaspersky Security Center-softwaresuite (raadpleeg de *Implementatiehandleiding voor Kaspersky Security Center*).

- De Editor voor lokaal groepsbeleid van Microsoft Windows (raadpleeg de Help-bestanden van het besturingssysteem).

- System Center Configuration Manager.

We raden aan dat u alle geopende programma's sluit alvorens u de installatie van Kaspersky Endpoint Security start (inclusief de externe installatie).

Het programma met de Installatiewizard installeren

De interface van de Installatiewizard van het programma bestaat uit een reeks vensters die de installatiestappen van het programma voorstellen. Met de knoppen **Vorige** en **Volgende** kunt u navigeren door de pagina's van de Installatiewizard. Klik op de knop **Beëindigen** om de Installatiewizard te sluiten wanneer die is voltooid. Klik op de knop **Annuleren** om de Installatiewizard op elk gewenst moment te stoppen.

Zo installeert u het programma of upgradet u het programma vanaf een oudere versie via de Installatiewizard:

1. Voer het bestand 'setup.exe' van het distributiepakket uit.

   De Installatiewizard wordt gestart.

2. Volg de instructies van de Installatiewizard.

Wanneer het bestand 'setup.exe' wordt gestart, controleert Kaspersky Endpoint Security de computer op incompatibele software. Als incompatibele software wordt gevonden, wordt de installatie standaard afgebroken en verschijnt op het scherm de lijst met programma's die niet compatibel zijn met Kaspersky Endpoint Security. Verwijder deze programma's van de computer om de installatie voort te zetten.

Stap 1. Controleren of de computer aan de installatievereisten voldoet

Voordat Kaspersky Endpoint Security 10 voor Windows op een computer wordt geïnstalleerd of een oudere versie van het programma wordt bijgewerkt, moet het volgende worden gecontroleerd:

- Of het besturingssysteem en het Service Pack voldoen aan de softwarevereisten voor de installatie van het product.
- Of aan de hardware- en softwarevereisten is voldaan.
- Of de gebruiker over rechten beschikt om het softwareproduct te installeren.

Als niet is voldaan aan een van de eerder vermelde vereisten, wordt een relevante melding op het scherm weergegeven.

Als de computer aan de vermelde vereisten voldoet, zoekt de Installatiewizard naar Kaspersky-programma's die kunnen leiden tot conflicten wanneer ze worden uitgevoerd samen met het programma dat wordt geïnstalleerd. Als zulke programma's worden gevonden, wordt u gevraagd om ze handmatig te verwijderen.

Als oudere versies van Kaspersky Endpoint Security tussen de gevonden programma's staan, worden alle gegevens die kunnen worden gemigreerd (zoals activatiegegevens en programma-instellingen) behouden en gebruikt tijdens de installatie van Kaspersky Endpoint Security 10 Service Pack 2 voor Windows. De vorige versie van het programma wordt automatisch verwijderd. Dit is van toepassing op de volgende programmaversies:

- Kaspersky Anti-Virus 6.0 voor Windows-werkstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 voor Windows-servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 voor Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 voor Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 voor Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 voor Windows

Stap 2. Welkomstpagina van de installatieprocedure

Als aan alle vereisten voor de installatie van het programma is voldaan, ziet u een welkomstpagina nadat u het installatiepakket hebt gestart. De welkomstpagina kondigt het begin van de installatie van Kaspersky Endpoint Security op de computer aan.

Klik op de knop **Volgende** om de Installatiewizard voort te zetten.

Stap 3. Gebruiksrechtovereenkomst bekijken

Tijdens deze stap wordt u aanbevolen om de gebruiksrechtovereenkomst tussen u en Kaspersky te lezen.

Lees de Gebruiksrechtovereenkomst zorgvuldig door en schakel het selectievakje **Ik ga akkoord met de voorwaarden van de Gebruiksrechtovereenkomst** in als u met alle voorwaarden akkoord gaat.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 4. Het installatietype selecteren

Tijdens deze stap kunt u het meest geschikte installatietype voor Kaspersky Endpoint Security selecteren:

- **Basisinstallatie**. Als u dit type installatie kiest, worden de beschermingsonderdelen Controle van programmabevoegdheden en Kwetsbaarheidsbewaking geïnstalleerd op de computer met de instellingen die door experts van Kaspersky zijn aanbevolen.
- **Standaardinstallatie**. Als u dit type installatie kiest, worden de beschermings- en controleonderdelen met instellingen aanbevolen door Kaspersky geïnstalleerd op de computer.
- **Aangepaste installatie**. Als u dit type installatie selecteert, wordt u gevraagd om de te installeren onderdelen te selecteren en om de doelmap van het programma op te geven.

  Met dit type installatie kunt u de onderdelen installeren die niet tot de basis- en standaardinstallaties behoren.

De standaardinstallatie is standaard geselecteerd.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 5. Te installeren programmaonderdelen selecteren

Deze stap wordt uitgevoerd als u de *Aangepaste installatie* van het programma hebt geselecteerd.

Tijdens deze stap kunt u de onderdelen van Kaspersky Endpoint Security selecteren die u wilt installeren. Anti-Virus voor bestanden is verplicht onderdeel tijdens de installatie. U kunt de installatie ervan niet annuleren.

Standaard zijn alle programmaonderdelen voor installatie geselecteerd behalve de volgende:

- BadUSB Attack Prevention.
- Schijfencryptie.
- Bestandsencryptie.
- Microsoft BitLocker Manager.
- KATA Endpoint Sensor.

Microsoft BitLocker Manager voert de volgende functies uit:

- Beheert de BitLocker-encryptie die in het Windows-besturingssysteem is ingebouwd.
- Configureert de instellingen van het encryptiebeleid en controleert de toepasselijkheid ervan voor de beheerder computer.
- Start encryptie- en decryptieprocessen.
- Monitort de encryptiestatus op de beheerde computer.
- Bewaart herstelsleutels op één plaats op de Administration Server van Kaspersky Security Center.

KATA Endpoint Sensor is een onderdeel van het Kaspersky Anti Targeted Attack Platform. Deze oplossing is bedoeld voor de snelle detectie van bedreigingen zoals doelgerichte aanvallen. Het onderdeel monitort voortdurend processen, actieve netwerkverbindingen en bestanden die worden gewijzigd en stuurt deze informatie door naar het Kaspersky Anti Targeted Attack Platform.

Om een onderdeel te selecteren dat u wilt installeren, klikt u op het pictogram naast de naam van het onderdeel om het contextmenu te openen en selecteert u **Onderdeel wordt op de lokale harde schijf geïnstalleerd**. Voor meer informatie over de taken die door het geselecteerde onderdeel worden uitgevoerd en hoeveel schijfruimte u nodig hebt om het onderdeel te installeren, raadpleegt u het gedeelte onder in de huidige pagina van de Installatiewizard.

Als u gedetailleerde informatie over de beschikbare ruimte op de lokale harde schijven wilt zien, klikt u op de knop **Volume**. De informatie wordt in het geopende venster **Beschikbare schijfruimte** weergegeven.

Selecteer in het contextmenu de optie **Deze optie zal niet beschikbaar zijn** om de installatie van het onderdeel te annuleren.

Klik op de knop **Opnieuw instellen** om terug te gaan naar de lijst met onderdelen die standaard worden geïnstalleerd.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 6. Doelmap selecteren

Deze stap is beschikbaar als u de *Aangepaste installatie* van het programma hebt geselecteerd.

Tijdens deze stap kunt u het pad opgeven naar de doelmap waar het programma wordt geïnstalleerd. Klik op de knop **Bladeren** om de doelmap voor het programma te selecteren.

Als u informatie over de beschikbare ruimte op de lokale harde schijven wilt zien, klikt u op de knop **Volume**. In het geopende venster **Vereiste schijfruimte** wordt informatie weergegeven.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 7. Items toevoegen die niet op virussen moeten worden gescand

Deze stap is beschikbaar als u de *Aangepaste installatie* van het programma hebt geselecteerd.

Tijdens deze stap kunt u opgeven welke items niet op virussen moeten worden gescand om ze aan de programma-instellingen toe te voegen.

Met de selectievakjes **Sluit door Microsoft aanbevolen gebieden uit van het virusscanbereik** / **Sluit door Kaspersky aanbevolen gebieden uit van het virusscanbereik** kunt u de gebieden die respectievelijk door Microsoft of Kaspersky zijn aanbevolen al dan niet weglaten uit de vertrouwde zone.

Als een van deze selectievakjes is ingeschakeld, worden de gebieden die respectievelijk door Microsoft of Kaspersky zijn aanbevolen opgenomen in de vertrouwde zone door Kaspersky Endpoint Security. Kaspersky Endpoint Security scant die gebieden niet op virussen of andere bedreigingen.

Het selectievakje **Sluit door Microsoft aanbevolen gebieden uit van het virusscanbereik** is beschikbaar wanneer Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 8. Installatie van programma voorbereiden

U wordt aanbevolen de installatie te beschermen omdat uw computer mogelijk geïnfecteerd is met kwaadaardige programma's die de installatie van Kaspersky Endpoint Security 10 voor Windows kunnen hinderen.

De bescherming van het installatieproces is standaard ingeschakeld.

Als het programma echter niet kan worden geïnstalleerd (bijvoorbeeld wanneer een externe installatie wordt uitgevoerd via Windows Extern bureaublad), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen. In dit geval breekt u de installatie af en start u de Installatiewizard van het programma opnieuw. Schakel bij de stap 'Installatie van programma voorbereiden' het selectievakje **Bescherm het installatieproces** uit.

Het selectievakje **Controleer de compatibiliteit met Citrix PVS** schakelt de functie in of uit die stuurprogramma's in een Citrix PVS-compatibiliteitsmodus installeert.

Schakel dit selectievakje alleen in als u met Citrix Provisioning Services werkt.

Het selectievakje **Voeg het pad naar het bestand avp.com toe aan de systeemvariabele %PATH%** schakelt een optie in of uit waarmee het pad naar het bestand 'avp.com' wordt toegevoegd aan de systeemvariable %PATH%.

Als het selectievakje is ingeschakeld, moet het pad naar het uitvoerbare bestand niet worden ingevoerd voor het starten van Kaspersky Endpoint Security of een taak ervan. Het volstaat om de naam van het uitvoerbare bestand en de opdracht om de specifieke taak te starten in te voeren.

Klik op de knop **Vorige** om naar de vorige stap van de Installatiewizard terug te gaan. Klik op de knop **Installeren** om het programma te installeren. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

De huidige netwerkverbindingen worden mogelijk beëindigd wanneer het programma op de computer wordt geïnstalleerd. De meeste beëindigde netwerkverbindingen worden hersteld nadat de installatie van het programma is voltooid.

Stap 9. Het programma installeren

De installatie van het programma kan even duren. Wacht totdat deze is voltooid.

Als u een oude versie van het programma bijwerkt, worden tijdens deze stap ook de instellingen gemigreerd en de oude versie van het programma verwijderd.

Wanneer de installatie van Kaspersky Endpoint Security is voltooid, wordt de wizard Initiële configuratie gestart.

Het programma vanaf de opdrachtregel installeren

U kunt Kaspersky Endpoint Security via de opdrachtregel installeren in een van de volgende modi:

- In de interactieve modus via de Installatiewizard van het programma.
- In de stille modus. Nadat de installatie in de stille modus is gestart, is uw assistentie tijdens het installatieproces niet meer vereist. Gebruik de sleutels `/s` en `/qn` om het programma in de stille modus te installeren.

Zo installeert u het programma installeren of upgradet u de programmaversie:

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.
2. Ga naar de map waar het distributiepakket van Kaspersky Endpoint Security is opgeslagen.
3. Voer de volgende opdracht uit:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<onderdeel>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<gebruikersnaam> /pKLPASSWD=<wachtwoord> /pKLPASSWDAREA=<wachtwoordbereik>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracingniveau>] /s
   ```

   of

   ```
   msiexec /i <naam van distributiepakket> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<onderdeel>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<gebruikersnaam> KLPASSWD=<wachtwoord> KLPASSWDAREA=<wachtwoordbereik>] [ENABLETRACES=1|0 TRACESLEVEL=<tracingniveau>] /qn
   ```

`EULA`	Aanvaarding of weigering van de voorwaarden van de Gebruiksrechtovereenkomst. Beschikbare waarden: • `1` – Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst. • `0` – Weigering van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het distributiepakket van Kaspersky Endpoint Security. U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.
`PRIVACYPOLICY`	Aanvaarding of weigering van het Privacybeleid. Beschikbare waarden: • `1` – Aanvaarding van het Privacybeleid. • `0` – Weigering van het Privacybeleid.

	De tekst van het Privacybeleid wordt bij het distributiepakket van Kaspersky Endpoint Security meegeleverd. U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.
KSN	Aanvaarding of weigering van deelname aan Kaspersky Security Network (KSN). Als geen waarde voor deze parameter is ingesteld, wordt u door Kaspersky Endpoint Security gevraagd of u al dan niet wilt deelnemen aan KSN wanneer Kaspersky Endpoint Security voor het eerst wordt gestart. Beschikbare waarden: • `1` – Aanvaarding van de deelname aan KSN. • `0` – Weigering van de deelname aan KSN (standaardwaarde). Het distributiepakket van Kaspersky Endpoint Security is geoptimaliseerd voor gebruik met Kaspersky Security Network. Als u ervoor hebt gekozen om niet deel te nemen aan Kaspersky Security Network, moet u Kaspersky Endpoint Security meteen na de installatie bijwerken.
ALLOWREBOOT	Computer automatisch opnieuw opstarten, indien nodig na de installatie of upgrade van het programma. Beschikbare waarden: • `1` – Computer automatisch opnieuw opstarten, indien nodig. • `0` – Computer niet automatisch opnieuw opstarten (standaardwaarde). Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. Opnieuw opstarten is alleen nodig als u incompatibele programma's moet verwijderen alvorens u de installatie kunt starten. De computer opnieuw opstarten is mogelijk ook vereist wanneer u de programmaversie updatet.
ADDLOCAL	Selecteer extra onderdelen die u wilt installeren. Standaard zijn alle programmaonderdelen voor installatie geselecteerd behalve de volgende: BadUSB Attack Prevention, File Level Encryption, Full Disk Encryption, Beheer van BitLocker en KATA Endpoint Sensor. Beschikbare waarden: • `MSBitLockerFeature`. Het onderdeel BitLocker Manager wordt geïnstalleerd. • `AntiAPTFeature`. Het onderdeel KATA Endpoint Sensor wordt geïnstalleerd.
SKIPPRODUCTCHECK	Controleer op incompatibele software. De lijst met incompatibele software vindt u in het bestand incompatible.txt in het distributiepakket. Beschikbare waarden: • `1` – De controle op incompatibele software is ingeschakeld (standaardwaarde). • `0` – De controle op incompatibele software is uitgeschakeld.
SKIPPRODUCTUNINSTALL	Verwijder automatisch gevonden incompatibele software. Beschikbare waarden: • `1` – Kaspersky Endpoint Security probeert incompatibele software te verwijderen (standaardwaarde).

	• `0` – De automatische verwijdering van incompatibele software is niet toegestaan.
`KLLOGIN`	Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel Wachtwoordbeveiliging). De gebruikersnaam wordt samen met de parameters `KLPASSWD` en `KLPASSWDAREA`.ingesteld. De standaard gebruikersnaam is KLAdmin.
`KLPASSWD`	Geef een wachtwoord op voor de toegang tot functies en instellingen van Kaspersky Endpoint Security (het wachtwoord wordt samen de parameters `KLLOGIN` en `KLPASSWDAREA` opgegeven). Als u wel een wachtwoord hebt opgegeven maar geen gebruikersnaam bij de parameter `KLLOGIN`, wordt de gebruikersnaam 'KLAdmin' standaard gebruikt.
`KLPASSWDAREA`	Geef het bereik van het wachtwoord op voor toegang tot functies en instellingen van Kaspersky Endpoint Security. Wanneer een gebruiker een actie uit dit bereik probeert uit te voeren, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om de accountgegevens in te voeren (de parameters `KLLOGIN` en `KLPASSWD`). Gebruik het teken '`;`' om meerdere waarden op te geven. Beschikbare waarden: • `SET` – voor het wijzigen van de programma-instellingen. • `EXIT` – voor het afsluiten van het programma. • `DISPROTECT` – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken. • `DISPOLICY` – voor het uitschakelen van het Kaspersky Security Center-beleid. • `UNINST` – voor het verwijderen van het programma op de computer. • `DISCTRL` – voor het uitschakelen van de controle-onderdelen. • `REMOVELIC` – voor het verwijderen van de licentie. • `REPORTS` – voor het bekijken van rapporten.
`ENABLETRACES`	Programmatraces inschakelen of uitschakelen. Nadat Kaspersky Endpoint Security is gestart, worden de tracebestanden opgeslagen in de map %ProgramData%/Kaspersky Lab. Beschikbare waarden: • `1` – traces zijn ingeschakeld. • `0` – traces zijn uitgeschakeld (standaardwaarde).
`TRACESLEVEL`	Detailniveau van tracing. Beschikbare waarden: • `100` (kritiek). Alleen berichten over kritieke fouten. • `200` (hoog). Berichten over alle fouten, inclusief onherstelbare fouten. • `300` (diagnostisch). Berichten over alle fouten en een selectie van berichten met waarschuwingen.

- `400` (belangrijk). Alle waarschuwingen en berichten over normale en kritieke fouten en een selectie van berichten met aanvullende informatie.
- `500` (normaal). Alle waarschuwingen en berichten over normale en kritieke fouten en ook berichten met gedetailleerde informatie over de werking van het programma in de normale modus (standaardwaarde).
- `600` (laag). Alle mogelijke berichten.

Voorbeeld:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Wachtwoord
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Na de installatie van het programma activeert Kaspersky Endpoint Security de evaluatielicentie tenzij u een activatiecode in het bestand setup.ini hebt opgegeven. Een evaluatielicentie heeft doorgaans een korte gebruiksduur. Wanneer de evaluatielicentie verloopt, worden alle functies van Kaspersky Endpoint Security uitgeschakeld. Als u het programma verder wilt gebruiken, moet u een commerciële licentie activeren.

Tijdens de installatie van het programma of de upgrade van de programmaversie in de stille modus is het gebruik van de volgende bestanden ondersteund:

- setup.ini – algemene instellingen voor de installatie van het programma;
- install.cfg – lokale instellingen van Kaspersky Endpoint Security;
- setup.reg – registersleutels.

  Registersleutels uit het bestand 'setup.reg' worden alleen naar het register geschreven als de waarde `setup.reg` is ingesteld voor de parameter `SetupReg` in het bestand 'setup.ini'. Het bestand 'setup.reg' is door experts van Kaspersky gegenereerd. U wordt aanbevolen om de inhoud van dit bestand niet te wijzigen.

Als u de instellingen uit de bestanden setup.ini, install.cfg en setup.reg wilt toepassen, plaatst u deze bestanden in de map met het distributiepakket van Kaspersky Endpoint Security.

Het programma op afstand installeren via System Center Configuration Manager

Deze instructies zijn van toepassing op System Center Configuration Manager 2012 R2.

Zo installeert u het programma op afstand via System Center Configuration Manager:

1. Open de console Configuratiebeheer.

2. Selecteer in het gedeelte **Appbeheer** rechts in de console de optie **Pakketten**.

3. Klik boven in de console van het configuratiescherm op de knop **Pakket maken**.

   Hiermee start u de *wizard Nieuw pakket en programma*.

4. In de wizard Nieuw pakket en programma:

   a. In het gedeelte **Pakket**:

   - Voer in het veld **Naam** de naam van het installatiepakket in.
   - Geef in het veld **Bronmap** het pad op naar de map met het distributiepakket van Kaspersky Endpoint Security.

   b. Selecteer in het gedeelte **Type programma** de optie **Standaardprogramma**.

   c. In het gedeelte **Standaardprogramma**:

   - Voer in het veld **Naam** de unieke naam voor het installatiepakket in (bijvoorbeeld de naam van het programma met de versie).
   - Geef in het veld **Opdrachtregel** de installatieopties van Kaspersky Endpoint Security op vanaf de opdrachtregel.
   - Klik op de knop **Bladeren** om het pad naar het uitvoerbare bestand van het programma op te geven.
   - Zorg ervoor dat in de lijst **Uitvoeringsmodus** de optie **Als administrator uitvoeren** is ingeschakeld.

   d. In het gedeelte **Vereisten**:

   - Schakel het selectievakje **Start een ander programma eerst** in als u een ander programma wilt starten voordat u Kaspersky Endpoint Security installeert.

     Selecteer het programma in de vervolgkeuzelijst **Programma** of geef het pad naar het uitvoerbare bestand van dit programma op door te klikken op de knop **Bladeren**.

   - Selecteer de optie **Dit programma mag alleen worden gestart op de opgegeven platformen** in het gedeelte **Platformvereisten** als u wilt dat het programma alleen in de opgegeven besturingssystemen wordt geïnstalleerd.

     Schakel in de onderstaande lijst de selectievakjes in naast de besturingssystemen waarin Kaspersky Endpoint Security mag worden geïnstalleerd.

   Deze stap is optioneel.

   e. Controleer in het gedeelte **Samenvatting** alle ingevoerde waarden van de instellingen en klik op **Volgende**.

   Het gemaakte installatiepakket verschijnt in het gedeelte **Pakketten** in de lijst met beschikbare installatiepakketten.

5. Selecteer in het contextmenu van het installatiepakket de optie **Implementeren**.

   Hiermee start u de *wizard Implementatie*.

6. In de wizard Implementatie:

   a. In het gedeelte **Algemeen**:

- Voer in het veld **Software** de unieke naam van het installatiepakket in of selecteer het installatiepakket uit de lijst door te klikken op de knop **Bladeren**.

- Voer in het veld **Verzameling** de naam van de verzameling van computers in waarop het programma zal worden geïnstalleerd of selecteer de verzameling door te klikken op de knop **Bladeren**.

b. Voeg in het gedeelte **Bevat** verdeelpunten toe (voor meer gedetailleerde informatie raadpleegt u de Help-documentatie van System Center Configuration Manager).

c. Geef indien nodig de waarden van andere instellingen in de wizard Implementatie op. Deze instellingen zijn optioneel voor de installatie van Kaspersky Endpoint Security op afstand.

d. Controleer in het gedeelte **Samenvatting** alle ingevoerde waarden van de instellingen en klik op **Volgende**.

Wanneer de wizard Implementatie is voltooid, wordt een taak gemaakt voor de installatie van Kaspersky Endpoint Security op afstand.

Beschrijving van de installatie-instellingen in het bestand ‘setup.ini’

Het bestand ‘setup.ini’ wordt gebruikt wanneer het programma wordt geïnstalleerd via de opdrachtregel of met de Editor voor lokaal groepsbeleid van Microsoft Windows. Als u de instellingen uit de bestanden 'setup.ini' wilt toepassen, plaatst u dit bestand in de map met het distributiepakket van Kaspersky Endpoint Security.

Het bestand 'setup.ini' bestaat uit de volgende onderdelen:

- `[Setup]` - algemene opties voor de installatie van het programma.

- `[Components]` – selectie van programmaonderdelen die u wilt installeren. Als geen onderdelen zijn opgegeven, worden alle beschikbare onderdelen voor het besturingssysteem geïnstalleerd. Anti-Virus voor bestanden is een verplicht onderdeel en wordt op de computer geïnstalleerd ongeacht de geconfigureerde instellingen in dit gedeelte.

- `[Tasks]` – selectie van taken die aan de lijst met taken van Kaspersky Endpoint Security moeten worden toegevoegd. Als geen taak is opgegeven, worden alle taken aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.

De alternatieven voor de waarde `1` zijn de waarden `yes`, `on`, `enable` en `enabled`.

De alternatieven voor de waarde `0` zijn de waarden `no`, `off`, `disable` en `disabled`.

Instellingen van het bestand 'setup.ini'

Gedeelte	Parameter	Beschrijving
`[Setup]`	`InstallDir`	Pad naar installatiemap van programma.
	`ActivationCode`	Activatiecode van Kaspersky Endpoint Security.
	`Eula`	Aanvaarding of weigering van de voorwaarden van de Gebruiksrechtovereenkomst. Beschikbare waarden: • `1` – Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst.

		• `0` – Weigering van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het distributiepakket van Kaspersky Endpoint Security. U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.
	`PrivacyPolicy`	Aanvaarding of weigering van het Privacybeleid. Beschikbare waarden: • `1` – Aanvaarding van het Privacybeleid. • `0` – Weigering van het Privacybeleid. De tekst van het Privacybeleid wordt bij het distributiepakket van Kaspersky Endpoint Security meegeleverd. U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.
	`KSN`	Aanvaarding of weigering van deelname aan Kaspersky Security Network (KSN). Als geen waarde voor deze parameter is ingesteld, wordt u door Kaspersky Endpoint Security gevraagd of u al dan niet wilt deelnemen aan KSN wanneer Kaspersky Endpoint Security voor het eerst wordt gestart. Beschikbare waarden: • `1` – Aanvaarding van de deelname aan KSN. • `0` – Weigering van de deelname aan KSN (standaardwaarde). Het distributiepakket van Kaspersky Endpoint Security is geoptimaliseerd voor gebruik met Kaspersky Security Network. Als u ervoor hebt gekozen om niet deel te nemen aan Kaspersky Security Network, moet u Kaspersky Endpoint Security meteen na de installatie bijwerken.
	`Login`	Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel Wachtwoordbeveiliging). De gebruikersnaam wordt samen met de parameters `Password` en `PasswordArea` ingesteld. De standaard gebruikersnaam is KLAdmin.
	`Password`	Geef een wachtwoord op voor de toegang tot functies en instellingen van Kaspersky Endpoint Security (het wachtwoord wordt samen de parameters `Login` en `PasswordArea` opgegeven). Als u wel een wachtwoord hebt opgegeven maar geen gebruikersnaam bij de parameter `Gebruikersnaam`, wordt de gebruikersnaam 'KLAdmin' standaard gebruikt.

	`PasswordArea`	Geef het bereik van het wachtwoord op voor toegang tot functies en instellingen van Kaspersky Endpoint Security. Wanneer een gebruiker een actie uit dit bereik probeert uit te voeren, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om de accountgegevens in te voeren (de parameters `Login` en `Password`). Gebruik het teken '`;`' om meerdere waarden op te geven. Beschikbare waarden: • `SET` – voor het wijzigen van de programma-instellingen. • `EXIT` – voor het afsluiten van het programma. • `DISPROTECT` – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken. • `DISPOLICY` – voor het uitschakelen van het Kaspersky Security Center-beleid. • `UNINST` – voor het verwijderen van het programma op de computer. • `DISCTRL` – voor het uitschakelen van de controle-onderdelen. • `REMOVELIC` – voor het verwijderen van de licentie. • `REPORTS` – voor het bekijken van rapporten.
	`SelfProtection`	Schakel het beschermingsmechanisme voor de installatie van het programma in of uit. Beschikbare waarden: • `1` – Het beschermingsmechanisme voor de installatie van het programma is ingeschakeld. • `0` – Het beschermingsmechanisme voor de installatie van het programma is uitgeschakeld. U kunt de bescherming van de installatie uitschakelen. De bescherming van de installatie voorkomt de vervalsing van het distributiepakket door malware, blokkeert de toegang tot de installatiemap van Kaspersky Endpoint Security en blokkeert de toegang tot het systeemregister met de programmasleutels. Als het programma echter niet kan worden geïnstalleerd (bijvoorbeeld wanneer een externe installatie wordt uitgevoerd via Windows Extern bureaublad), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen.
	`Reboot=1`	Computer automatisch opnieuw opstarten, indien nodig na de installatie of upgrade van het programma. Als er geen waarde is ingesteld voor deze parameter,

		wordt het automatisch herstarten van de computer geblokkeerd. Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. Opnieuw opstarten is alleen nodig als u incompatibele programma's moet verwijderen alvorens u de installatie kunt starten. De computer opnieuw opstarten is mogelijk ook vereist wanneer u de programmaversie updatet.
	`AddEnvironment`	Vervolledig de systeemvariabele %PATH% met het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden. Beschikbare waarden: • `1` – De systeemvariabele %PATH% wordt toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden. • `0` – De systeemvariabele %PATH% wordt niet toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden.
	`AMPPL`	Schakel de bescherming van de Kaspersky Endpoint Security-service met AM-PPL-technologie (Antimalware Protected Process Light) in of uit. Beschikbare waarden: • `1` – Bescherming van de Kaspersky Endpoint Security-service met AM-PPL-technologie is ingeschakeld. • `0` – Bescherming van de Kaspersky Endpoint Security-service met AM-PPL-technologie is uitgeschakeld.
	`SetupReg`	Schakel het schrijven van registersleutels vanuit het bestand 'setup.reg' naar het register in. Waarde van de parameter `SetupReg: setup.reg`.
	`EnableTraces`	Tracing voor het geïnstalleerde programma inschakelen of uitschakelen. Kaspersky Endpoint Security slaat tracebestanden op in de map %ProgramData%/Kaspersky Lab. Beschikbare waarden: • `1` – De tracing voor het geïnstalleerde programma is ingeschakeld. • `0` – De tracing voor het geïnstalleerde programma is uitgeschakeld (standaardwaarde).
	`TracesLevel`	Detailniveau van tracing. Beschikbare waarden: • `100` (kritiek). Alleen berichten over kritieke fouten. • `200` (hoog). Berichten over alle fouten, inclusief onherstelbare fouten.

		• `300` (diagnostisch). Berichten over alle fouten en een selectie van berichten met waarschuwingen. • `400` (belangrijk). Alle waarschuwingen en berichten over normale en kritieke fouten en een selectie van berichten met aanvullende informatie. • `500` (normaal). Alle waarschuwingen en berichten over normale en kritieke fouten en ook berichten met gedetailleerde informatie over de werking van het programma in de normale modus (standaardwaarde). • `600` (laag). Alle mogelijke berichten.
`[Components]`	`ALL`	Installeer alle onderdelen. Als parameterwaarde `1` is opgegeven, worden alle onderdelen geïnstalleerd ongeacht de installatie-instellingen van individuele onderdelen.
	`MailAntiVirus`	Mail Anti-Virus.
	`IMAntiVirus`	IM Anti-Virus.
	`WebAntiVirus`	Web Anti-Virus.
	`ApplicationPrivilegeControl`	Controle van programmabevoegdheden.
	`SystemWatcher`	Systeembewaking.
	`Firewall`	Firewall.
	`NetworkAttackBlocker`	Network Attack Blocker.
	`WebControl`	Webcontrole.
	`DeviceControl`	Apparaatcontrole.
	`ApplicationStartupControl`	Programma-opstartcontrole.
	`FileEncryption`	File Level Encryption-bibliotheken.
	`DiskEncryption`	Full Disk Encryption-bibliotheken.
	`VulnerabilityAssessment`	Kwetsbaarheidsbewaking.
	`KeyboardAuthorization`	BadUSB Attack Prevention.
	`AntiAPT`	KATA Endpoint Sensor.
	`MSBitLocker`	Microsoft BitLocker Manager.
	`AdminKitConnector`	Network Agent Connector voor het externe beheer van het programma via Kaspersky Security Center. Beschikbare waarden: • `1` – Network Agent Connector wordt geïnstalleerd. • `0` – Network Agent Connector wordt niet geïnstalleerd.
`[Tasks]`	`ScanMyComputer`	Volledige Scan. Beschikbare waarden:

		• `1` – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd. • `0` – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.
	`ScanCritical`	Kritieke Gebiedenscan. Beschikbare waarden: • `1` – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd. • `0` – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.
	`Updater`	Updatetaak. Beschikbare waarden: • `1` – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd. • `0` – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.

De wizard Initiële configuratie

De wizard Initiële configuratie van Kaspersky Endpoint Security wordt gestart wanneer de installatie van het programma is voltooid. Met de wizard Initiële configuratie kunt u het programma activeren en informatie over de geïnstalleerde programma's in het besturingssysteem verzamelen. Deze programma's worden aan de lijst met vertrouwde programma's toegevoegd en de acties van de programma's in het besturingssysteem mogen onbeperkt plaatsvinden.

De interface van de wizard Initiële configuratie bestaat uit een aantal pagina's (stappen). Met de knoppen **Vorige** en **Volgende** kunt u navigeren door de pagina's van de wizard Initiële configuratie. Klik op de knop **Beëindigen** om de wizard Initiële configuratie te voltooien. Klik op **Annuleren** om de wizard Initiële configuratie op elk gewenst moment te stoppen.

Als de wizard Initiële configuratie om een willekeurige reden wordt gestopt, worden de al opgegeven instellingen niet opgeslagen. De volgende keer dat u het programma probeert te gebruiken, wordt de wizard Initiële configuratie opnieuw gestart en moet u de instellingen vanaf het begin configureren.

Programma activeren

Het programma moet op een computer met de actuele systeemdatum en -tijd worden geactiveerd. Als de systeemdatum en -tijd na de activatie van het programma worden gewijzigd, wordt de code onbruikbaar. Het programma schakelt dan over naar een gebruiksmodus zonder updates en Kaspersky Security Network is niet beschikbaar. De code kan alleen door het besturingssysteem opnieuw te installeren weer worden gebruikt.

Selecteer bij deze stap een van de volgende opties voor de activatie van Kaspersky Endpoint Security:

- **Activeren met een activatiecode**. Selecteer deze optie en voer een activatiecode in om het programma met een activatiecode te activeren.
- **Activeren met een licentiebestand**. Selecteer deze optie om het programma met een licentiebestand te activeren.
- **Evaluatieversie activeren**. Selecteer deze optie om de evaluatieversie van het programma te activeren. De gebruiker kan de volledig functionele versie van het programma gebruiken gedurende de beperkte periode die door de licentie voor de evaluatieversie van het programma is ingesteld. Na het verlopen van de licentie wordt de functionaliteit van het programma geactiveerd en kunt u de evaluatieversie niet opnieuw activeren.
- **Later activeren**. Selecteer deze optie als u de activatie van Kaspersky Endpoint Security wilt overslaan. De gebruiker kan dan alleen met de onderdelen Anti-Virus voor bestanden en Firewall werken. De gebruiker kan de antivirusdatabases en de modules van Kaspersky Endpoint Security pas bijwerken na de installatie. De optie **Later activeren** is pas beschikbaar na de eerste start van de wizard Initiële configuratie, net na de installatie van het programma.

U hebt een internetverbinding nodig om de evaluatieversie van het programma te activeren of om het programma met een activatiecode te activeren.

Selecteer een optie voor de activatie en klik op de knop **Volgende** om de wizard Initiële configuratie voort te zetten. Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

Activeren met een activatiecode

Deze stap is alleen beschikbaar wanneer u het programma met een activatiecode activeert. Deze stap wordt overgeslagen wanneer u de evaluatieversie van het programma activeert of wanneer u het programma met een licentiebestand activeert.

Tijdens deze stap stuurt Kaspersky Endpoint Security gegevens naar de activatieserver om de ingevoerde activatiecode te verifiëren:

- Als de verificatie van de activatiecode met succes wordt voltooid, gaat de wizard Initiële configuratie automatisch door naar het volgende venster.
- Als de verificatie van de activatiecode mislukt, wordt een desbetreffend bericht weergegeven. In dit geval moet u advies vragen aan de softwareleverancier die u de licentie voor Kaspersky Endpoint Security heeft verkocht.
- Als het aantal activaties met de activatiecode wordt overschreden, wordt een desbetreffende melding weergegeven. De wizard Initiële configuratie wordt onderbroken en het programma stelt voor dat u contact opneemt met de Technische Support van Kaspersky.

Klik op de knop **Vorige** om naar de vorige stap van de wizard Initiële configuratie terug te gaan. Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

Activeren met een licentiebestand

Deze stap is alleen beschikbaar wanneer u het programma met een licentiebestand activeert.

Geef tijdens deze stap het pad naar het licentiebestand op. Klik hiervoor op de knop **Bladeren** en selecteer een licentiebestand met de structuur `<Bestands-ID>.key`.

Wanneer u een licentiebestand hebt geselecteerd, ziet u de volgende informatie onder in het venster:

- Code
- Soort licentie (commercieel of evaluatie) en het aantal computers die door deze licentie worden gedekt
- Datum van de activatie van het programma op de computer
- Verloopdatum van licentie
- Beschikbare functionaliteit met de licentie
- Meldingen over eventuele problemen met de code. Bijvoorbeeld, *Blacklist van codes beschadigd*.

Klik op de knop **Vorige** om naar de vorige stap van de wizard Initiële configuratie terug te gaan. Klik op de knop **Volgende** om de wizard Initiële configuratie voort te zetten. Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

De te activeren functies selecteren

Deze stap is alleen beschikbaar wanneer u de evaluatieversie van het programma activeert.

Tijdens deze stap kunt u de functionaliteit selecteren die na de activatie van het programma beschikbaar wordt:

- **Basisinstallatie**. Als deze optie wordt geselecteerd, zijn na de activatie van het programma alleen de beschermingsonderdelen, Controle van programmabevoegdheden en Kwetsbaarheidsbewaking beschikbaar.
- **Standaardinstallatie**. Als deze optie wordt geselecteerd, zijn na de activatie alleen de beschermings- en controle-onderdelen van het programma beschikbaar.
- **Volledige installatie**. Als deze optie wordt geselecteerd, zijn na de activatie van het programma alle geïnstalleerde programmaonderdelen beschikbaar, inclusief de functionaliteit voor de gegevensencryptie.

Als u tijdens de installatie meer onderdelen hebt geselecteerd dan toegestaan door de verkregen licentie, worden na de activatie van het programma de onderdelen die niet beschikbaar zijn met deze licentie geïnstalleerd maar zullen ze niet werken. Als de aangeschafte licentie toestaat dat u meer onderdelen kunt gebruiken dan deze die momenteel zijn geïnstalleerd, ziet u na de activatie van het programma de niet-geïnstalleerde onderdelen in een lijst in het gedeelte **Licentiebeheer**.

De standaardinstallatie is standaard geselecteerd.

Klik op de knop **Vorige** om naar de vorige stap van de wizard Initiële configuratie terug te gaan. Klik op de knop **Volgende** om de wizard Initiële configuratie voort te zetten. Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

Activatie voltooien

Tijdens deze stap ziet u in de wizard Initiële configuratie een bericht over de geslaagde activatie van Kaspersky Endpoint Security. De volgende informatie over de licentie wordt verstrekt:

- Soort licentie (commercieel of evaluatie) en het aantal computers die door deze licentie worden gedekt
- Verloopdatum van licentie
- Beschikbare functionaliteit met de licentie

Klik op de knop **Volgende** om de wizard Initiële configuratie voort te zetten. Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

Besturingssysteem analyseren

Tijdens deze stap wordt informatie verzameld over programma's die in het besturingssysteem zijn geïnstalleerd. Deze programma's worden aan de lijst met vertrouwde programma's toegevoegd en de acties van de programma's in het besturingssysteem mogen onbeperkt plaatsvinden.

Andere programma's worden geanalyseerd wanneer ze na de installatie van Kaspersky Endpoint Security voor het eerst worden gestart.

Klik op de knop **Annuleren** om de wizard Initiële configuratie te stoppen.

De initiële configuratie van het programma voltooien

In het venster van de voltooiing van de wizard Initiële configuratie ziet u informatie over de voltooiing van de installatie van Kaspersky Endpoint Security.

Klik op de knop **Voltooien** als u Kaspersky Endpoint Security wilt starten.

Als u de wizard Initiële configuratie wilt sluiten zonder Kaspersky Endpoint Security te starten, schakelt u het selectievakje **Kaspersky Endpoint Security 10 voor Windows starten** uit en klikt u op **Voltooien**.

Verklaring van Kaspersky Security Network

Tijdens deze stap wordt u uitgenodigd om deel te nemen aan Kaspersky Security Network.

Lees de verklaring van het Kaspersky Security Network:

- Als u akkoord gaat met alle voorwaarden, selecteert u de optie **Ik ga akkoord met de voorwaarden voor deelname aan Kaspersky Security Network** in het venster van de wizard Initiële configuratie.
- Als u niet akkoord gaat met de voorwaarden voor deelname aan Kaspersky Security Network, selecteert u de optie **Ik ga niet akkoord met de voorwaarden voor deelname aan Kaspersky Security Network** in het venster van de wizard Initiële configuratie.

Klik op **OK** om de wizard Initiële configuratie voort te zetten.

Methoden om een oude programmaversie te upgraden

Als u een eerdere versie van het programma wilt upgraden naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, decrypt u alle geëncrypte harde schijven.

U kunt de volgende programma's upgraden naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows:

- Kaspersky Anti-Virus 6.0 voor Windows Workstations MP4 CF1 (build 6.0.4.1424) / MP4 CF2 (build 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 voor Windows Servers MP4 (build 6.0.4.1424) / MP4 CF2 (build 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 voor Windows (build 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 voor Windows (build 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 voor Windows (build 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 voor Windows (build 10.2.5.3201).

Wanneer een van de hierboven vermelde programma's wordt geüpgraded naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, wordt de inhoud van Quarantaine en Back-up niet overgezet.

U kunt de oude versie van het programma als volgt upgraden:

- Lokaal in de interactieve modus via de Installatiewizard van het programma.
- Lokaal in de niet-interactieve modus, vanaf de opdrachtregel
- Op afstand met de Kaspersky Security Center-softwaresuite (raadpleeg de *Implementatiehandleiding voor Kaspersky Security Center*)
- Op afstand via de Editor voor lokaal groepsbeleid van Microsoft Windows (raadpleeg de Help-bestanden van het besturingssysteem)

Wanneer u een eerdere versie van het programma upgradet naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, hoeft u de vorige versie van het programma niet te verwijderen. We raden aan dat u alle geopende programma's afsluit alvorens u de programmaversie upgradet.

Het programma verwijderen

In deze sectie wordt beschreven hoe u Kaspersky Endpoint Security van de computer verwijdert.

Methoden voor de verwijdering van het programma

Door de verwijdering van Kaspersky Endpoint Security zijn de computer en de gegevens van de gebruiker niet meer beschermd tegen bedreigingen.

Kaspersky Endpoint Security kan op verschillende manieren worden verwijderd van de computer:

- Lokaal in interactieve modus, met de Installatiewizard
- Lokaal in de niet-interactieve modus, vanaf de opdrachtregel
- Op afstand met de Kaspersky Security Center-softwaresuite (raadpleeg de *Implementatiehandleiding voor Kaspersky Security Center* voor informatie)
- Op afstand via de Editor voor lokaal groepsbeleid van Microsoft Windows (raadpleeg de Help-bestanden van het besturingssysteem)

Het programma met de Installatiewizard verwijderen

Zo verwijdert u Kaspersky Endpoint Security met de Installatiewizard:

1. Selecteer in het menu **Start** achtereenvolgens **Apps** → **Kaspersky Endpoint Security 10 voor Windows** → **Wijzigen, herstellen of verwijderen**.

   De Installatiewizard wordt gestart.

2. Klik in het venster **Programma wijzigen, herstellen of verwijderen** van de Installatiewizard op de knop **Verwijderen**.

3. Volg de instructies van de Installatiewizard.

Stap 1. Gegevens van het programma opslaan voor later gebruik

Tijdens deze stap kunt u opgeven welke gegevens van het programma u wilt bewaren voor later gebruik tijdens de volgende installatie van het programma (bijvoorbeeld wanneer u een nieuwere versie installeert). Als u geen gegevens kiest, wordt het programma volledig verwijderd.

Als u gegevens van het programma voor later gebruik wilt opslaan,

schakelt u de selectievakjes in naast de gegevenstypen die u wilt opslaan:

- **Activatiegegevens**: gegevens die ervoor zorgen dat het programma dat u later installeert niet meer hoeft te activeren. Het wordt automatisch geactiveerd met de huidige licentie zolang deze licentie niet verlopen is op het moment van de installatie.
- **Back-upbestanden en bestanden in Quarantaine**: bestanden die door het programma zijn gescand en in Back-up of Quarantaine zijn geplaatst.

Bestanden van Back-up en Quarantaine die na de verwijdering van het programma worden behouden, kunnen alleen vanuit dezelfde versie van het programma worden geopend als de versie die is gebruikt om deze bestanden op te slaan.

Als u van plan bent om na de verwijdering van het programma objecten uit Back-up en Quarantaine te gebruiken, moet u die objecten vanuit hun opslag terugzetten alvorens het programma te verwijderen. Experts van Kaspersky raden wel af dat u bestanden uit Back-up en Quarantaine terugzet omdat deze bestanden de computer mogelijk schade toebrengen.

- **Instellingen van de programmawerking**: waarden van programma-instellingen die tijdens de configuratie van het programma zijn geselecteerd.
- **Lokale opslag van encryptiesleutels**: gegevens die rechtstreeks toegang geven tot bestanden en apparaten die vóór de verwijdering van het programma waren geëncrypt. Geëncrypte bestanden en schijven kunnen rechtstreeks worden geopend als het programma opnieuw wordt geïnstalleerd met encryptiefunctionaliteit.

  Dit selectievakje is standaard ingeschakeld.

Klik op de knop **Volgende** om de Installatiewizard voort te zetten. Klik op de knop **Annuleren** om de Installatiewizard te stoppen.

Stap 2. Verwijdering van het programma bevestigen

Aangezien de verwijdering van het programma de veiligheid van de computer op het spel zet, wordt u gevraagd de verwijdering van het programma te bevestigen. Klik hiervoor op de knop **Verwijderen**.

Als u de verwijdering van het programma wilt stoppen, kunt u deze bewerking annuleren door op de knop **Annuleren** te klikken.

Stap 3. Het programma verwijderen. Verwijderen voltooien

Tijdens deze stap verwijdert de Installatiewizard het programma van de computer. Wacht tot de verwijdering van het programma is voltooid.

Tijdens de verwijdering van het programma moet het besturingssysteem mogelijk opnieuw worden opgestart. Als u beslist om niet onmiddellijk opnieuw op te starten, wordt de verwijdering van het programma pas voltooid wanneer het besturingssysteem opnieuw wordt opgestart of wanneer de computer wordt uitgeschakeld en opnieuw wordt ingeschakeld.

Het programma vanaf de opdrachtregel verwijderen

U kunt de verwijdering van het programma starten vanaf de opdrachtregel. De verwijdering wordt in de interactieve of stille modus uitgevoerd (zonder de Installatiewizard van het programma te starten).

Om de verwijdering van het programma in de interactieve modus te starten,

typt u op de opdrachtregel `setup.exe /x` of `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

De Installatiewizard wordt gestart. Volg de instructies van de Installatiewizard.

Om de verwijdering van het programma in de stille modus te starten,

typt u op de opdrachtregel `setup.exe /s /x` of `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Hiermee start u de verwijdering van het programma in de stille modus (zonder de Installatiewizard te starten).

Als de verwijdering van het programma met een wachtwoord beveiligd is, moet de gebruikersnaam en het bijbehorende wachtwoord in de opdrachtregel worden ingevoerd.

Zo verwijdert u het programma vanaf de opdrachtregel in de interactieve modus wanneer de gebruikersnaam en het wachtwoord voor de verificatie van de verwijdering, wijziging of reparatie van Kaspersky Endpoint Security zijn ingesteld:

Typ op de opdrachtregel `setup.exe /pKLLOGIN=<gebruikersnaam> /pKLPASSWD=***** /x` of

`msiexec.exe KLLOGIN=<gebruikersnaam> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

De Installatiewizard wordt gestart. Volg de instructies van de Installatiewizard.

Zo verwijdert u het programma vanaf de opdrachtregel in de stille modus wanneer de gebruikersnaam en het wachtwoord voor de verificatie van de verwijdering, wijziging of reparatie van Kaspersky Endpoint Security zijn ingesteld:

Typ op de opdrachtregel `setup.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /s /x` of

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<gebruikersnaam> KLPASSWD=***** /qn`.

Resterende objecten en gegevens verwijderen na de test van Verificatie-agent

Als Kaspersky Endpoint Security objecten en gegevens vindt die na de test van Verificatie-agent zijn achtergebleven op de harde schijf van het systeem, wordt de verwijdering van het programma onderbroken en kan de verwijdering pas worden voortgezet wanneer die objecten en gegevens zijn verwijderd.

Alleen in uitzonderlijke gevallen kunnen er na de geteste werking van Verificatie-agent objecten en gegevens achterblijven op de harde schijf van het systeem. Dit kan bijvoorbeeld gebeuren als de computer niet opnieuw is opgestart nadat een Kaspersky Security Center-beleid met encryptie-instellingen werd toegepast of als het programma niet kan worden gestart nadat de werking van Verificatie-agent is getest.

U kunt objecten en gegevens die na de geteste werking van Verificatie-agent zijn achtergebleven op de harde schijf van het systeem op twee manieren verwijderen:

- Met het Kaspersky Security Center-beleid.
- Met de Herstelvoorziening.

Zo gebruikt u een Kaspersky Security Center-beleid om objecten en gegevens te verwijderen die na de geteste werking van Verificatie-agent zijn blijven staan:

1. Pas een Kaspersky Security Center-beleid op de computer toe dat instellingen heeft die zijn geconfigureerd om alle harde schijven van de computer te decrypten.

2. Start Kaspersky Endpoint Security.

Zo gebruikt u de Herstelvoorziening om objecten en gegevens te verwijderen die na de geteste werking van Verificatie-agent zijn blijven staan:

1. Start Herstelvoorziening door het uitvoerbare bestand 'fdert.exe', dat is gemaakt met Kaspersky Endpoint Security, uit te voeren op de computer met de aangesloten systeemschijf waarop de objecten en de gegevens na de geteste werking van Verificatie-agent zijn blijven staan.

2. Selecteer in de vervolgkeuzelijst **Apparaat selecteren** in het venster van Herstelvoorziening de harde schijf van het systeem waarop de objecten en de gegevens staan die u wilt verwijderen.

3. Klik op de knop **Scannen**.

4. Klik op de knop **AA-objecten en -gegevens verwijderen**.

   Hiermee start u de verwijdering van de objecten en de gegevens die na de geteste werking van Verificatie-agent zijn blijven staan.

Na de verwijdering van de objecten en de gegevens die na de geteste werking van Verificatie-agent zijn blijven staan moet u mogelijk ook informatie over de incompatibiliteit van het programma met Verificatie-agent verwijderen.

Om informatie over de incompatibiliteit van het programma met Verificatie-agent te verwijderen,

typt u de opdracht `avp pbatestreset` op de opdrachtregel.

De encryptie-onderdelen moeten geïnstalleerd zijn opdat de opdracht `avp pbatestreset` kan worden uitgevoerd.

Programma-interface

In deze sectie worden de belangrijkste elementen van de programma-interface beschreven.

Programmapictogram in het systeemvak van de taakbalk

Net na de installatie van Kaspersky Endpoint Security verschijnt het pictogram van het programma in het systeemvak van de taakbalk in Microsoft Windows.

Het pictogram heeft de volgende functies:

- Het geeft de programma-activiteit aan.
- Het werkt als een snelkoppeling naar het contextmenu en het hoofdvenster van het programma.

Indicatie van programma-activiteit

Het pictogram van het programma werkt als een indicator voor de programma-activiteit:

- Het pictogram betekent dat alle beschermingsonderdelen van het programma zijn ingeschakeld.
- Het pictogram betekent dat er tijdens de werking van Kaspersky Endpoint Security zich belangrijke gebeurtenissen voordeden die uw aandacht vereisen. Bijvoorbeeld: Anti-Virus voor bestanden is uitgeschakeld of de programmadatabases zijn verouderd.
- Het pictogram betekent dat er tijdens de werking van Kaspersky Endpoint Security zich kritieke gebeurtenissen voordeden die uw aandacht vereisen. Bijvoorbeeld: een fout in de werking van een onderdeel of de beschadiging van de programmadatabases.

Contextmenu van het programmapictogram

Het contextmenu van het programmapictogram bevat de volgende opties:

- **Kaspersky Endpoint Security 10 voor Windows**. Opent het tabblad **Bescherming en controle** in het hoofdvenster van het programma. Op het tabblad **Bescherming en controle** kunt u de werking van programmaonderdelen en -taken aanpassen en kunt u de statistieken over verwerkte bestanden en gedetecteerde bedreigingen bekijken.
- **Instellingen**. Opent het tabblad **Instellingen** in het hoofdvenster van het programma. Op het tabblad **Instellingen** kunt u de standaard programma-instellingen wijzigen.
- **Bescherming en controle pauzeren** / **Bescherming en controle hervatten**. Pauzeert tijdelijk / hervat de werking van de beschermings- en controle-onderdelen. Deze optie van het contextmenu is niet van invloed op de update- en scantaken en is alleen beschikbaar als het Kaspersky Security Center-beleid uitgeschakeld is.
- **Beleid uitschakelen** / **Beleid inschakelen**. Schakelt het Kaspersky Security Center-beleid in of uit. Deze optie in het contextmenu is beschikbaar als Kaspersky Endpoint Security met een beleid werkt en als er een wachtwoord voor de uitschakeling van het Kaspersky Security Center-beleid is ingesteld.

- **Over**. Deze optie opent een venster met informatie over het programma.
- **Afsluiten**. Deze optie sluit Kaspersky Endpoint Security af. Met een klik op deze optie van het contextmenu wordt het programma uit het RAM van de computer gehaald.

Contextmenu van het programmapictogram

U kunt het contextmenu van het programmapictogram openen door de muisaanwijzer op het programmapictogram in het systeemvak van de taakbalk in Microsoft Windows te plaatsen en met de rechtermuisknop te klikken.

Het hoofdvenster van het programma

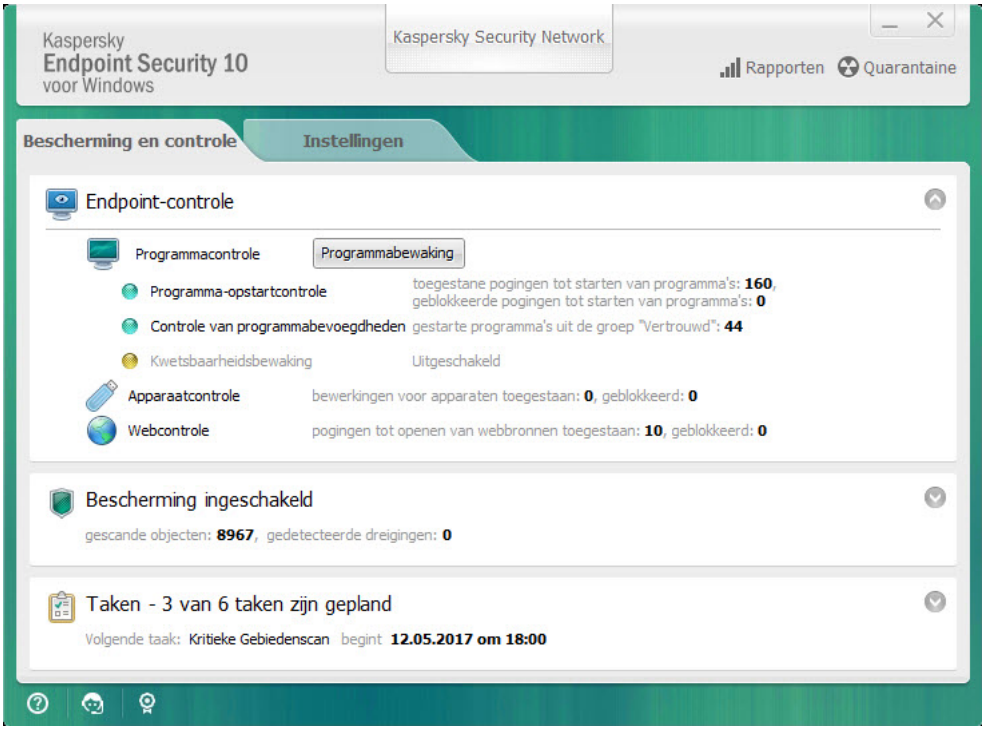
Het hoofdvenster van Kaspersky Endpoint Security bevat interface-elementen die toegang geven tot de belangrijkste functies van het programma.

Het hoofdvenster van het programma heeft vier delen (zie onderstaande afbeelding):

- Het bovenste deel van het venster bevat interface-elementen waarmee u de volgende informatie kunt bekijken:
  - Informatie over het programma
  - Statistieken van Kaspersky Security Network
  - Lijst met onverwerkte bestanden
  - Lijst met gevonden kwetsbaarheden
  - Lijst met bestanden die in Quarantaine zijn geplaatst
  - Opslag van kopieën van geïnfecteerde bestanden die het programma heeft verwijderd
  - Rapporten over gebeurtenissen die zich tijdens de werking van het programma of de aparte onderdelen voordeden, of tijdens de uitvoering van taken
- Op het tabblad **Bescherming en controle** kunt u de werking van programmaonderdelen en de voltooiing van taken aanpassen. U ziet het tabblad **Bescherming en controle** wanneer u het hoofdvenster van het programma opent.
- Op het tabblad **Instellingen** kunt u de standaard programma-instellingen bewerken.
- Onder in het venster vindt u de volgende elementen:
  - **Knop** . Met een klik op deze knop gaat u naar het Help-systeem van Kaspersky Endpoint Security.
  - **Knop** . Met een klik op deze knop opent u het venster **Support** waarin u informatie over het besturingssysteem, de huidige versie van Kaspersky Endpoint Security en koppelingen naar informatiebronnen van Kaspersky vindt.
  - **Knop** / . Met een klik op deze knop opent u het venster **Licentiebeheer** waarin u informatie over de huidige licentie vindt.

- **Knop** / / Met een klik op deze knop opent u het venster **Gebeurtenissen** waarin u informatie over beschikbare updates en verzoeken voor toegang tot geëncrypte bestanden en apparaten ziet.

  De knop is alleen beschikbaar als er toegangsaanvragen of niet-geïnstalleerde updates zijn.



Het hoofdvenster van het programma

Voer een van de volgende acties uit om het hoofdvenster van Kaspersky Endpoint Security te openen:

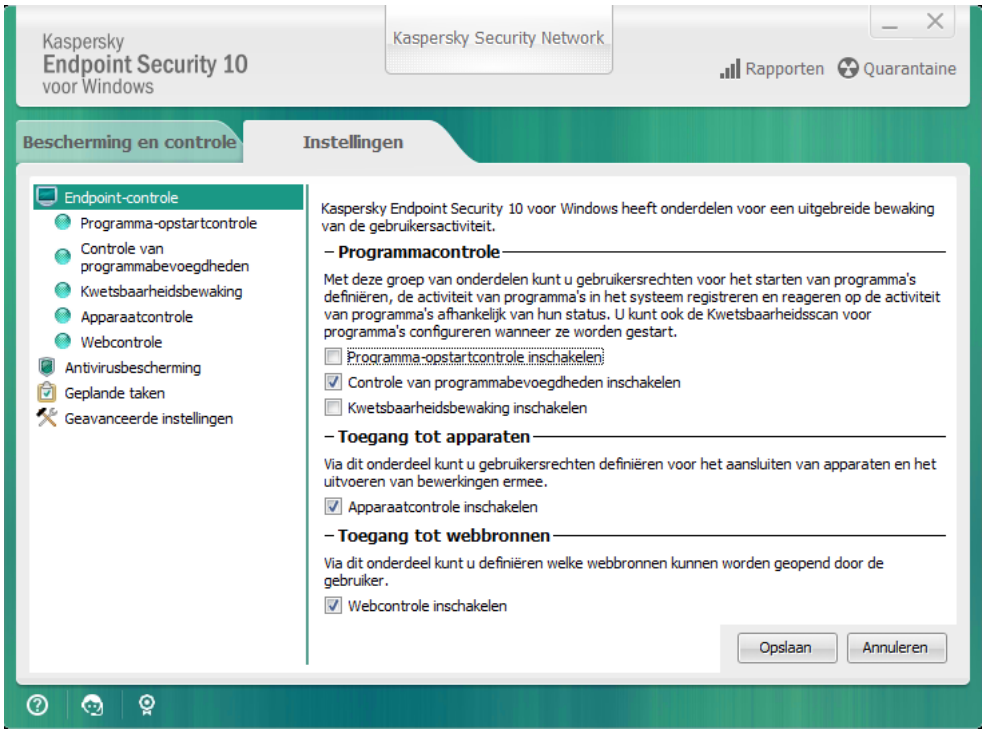
- Klik op het programmapictogram in het systeemvak van de taakbalk in Microsoft Windows.
- Selecteer **Kaspersky Endpoint Security 10 voor Windows** in het contextmenu van het programmapictogram.

Het tabblad Programma-instellingen configureren

Op het tabblad met instellingen van Kaspersky Endpoint Security kunt u algemene programma-instellingen, individuele onderdelen, rapporten en opslag, scantaken, updatetaken, kwetsbaarheidsscans en de communicatie met Kaspersky Security Network-servers configureren.

Het tabblad met programma-instellingen heeft twee delen (zie onderstaande afbeelding):

- Het linkerdeel bevat programmaonderdelen, taken en een gedeelte met geavanceerde instellingen dat verschillende subgedeelten heeft.
- Het rechterdeel bevat controle-onderdelen die u kunt gebruiken voor de configuratie van de instellingen van het geselecteerde onderdeel of de geselecteerde taak links in het venster, alsook voor geavanceerde instellingen.



Het tabblad Programma-instellingen configureren

Voer een van de volgende acties uit om het tabblad met de programma-instellingen te openen:

- Selecteer in het hoofdvenster van het programma het tabblad **Instellingen**.
- Selecteer in het contextmenu van het programmapictogram de optie **Instellingen**.

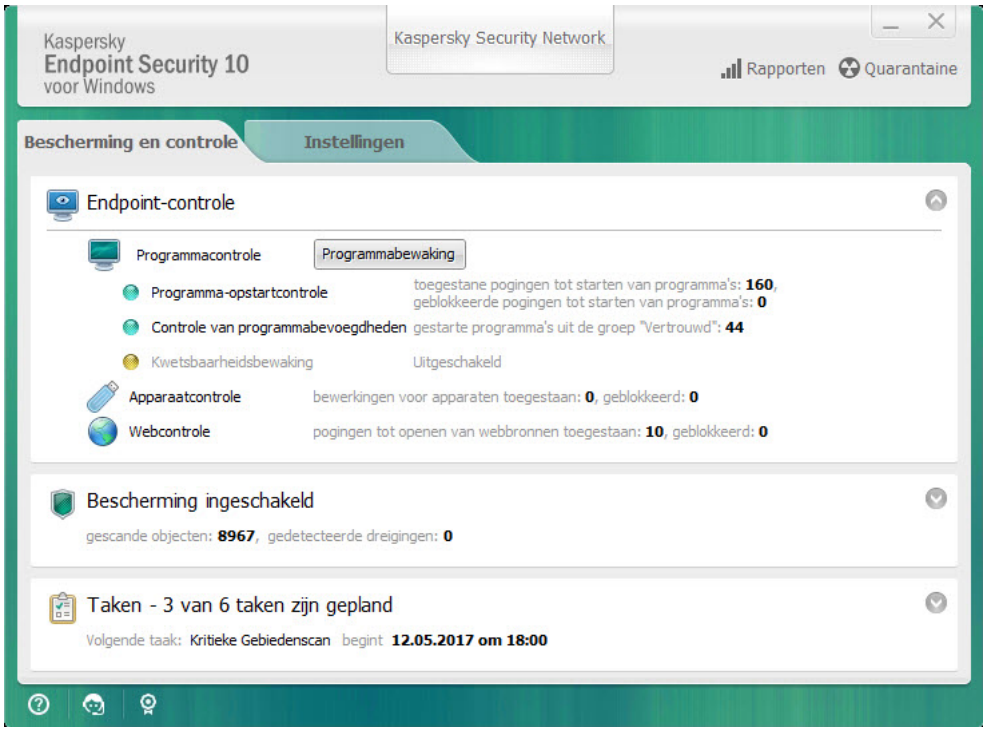
Het tabblad Bescherming en controle van het programma

Het tabblad Bescherming en controle van Kaspersky Endpoint Security is bedoeld om algemene informatie over de prestaties van alle taken en de werking van alle programmaonderdelen te geven. Op dit tabblad kunt u ook de werking van onderdelen en de prestaties van taken beheren.

Het tabblad Bescherming en controle heeft drie delen (zie onderstaande afbeelding):

- Het gedeelte **Endpoint-controle** bevat een lijst met controle-onderdelen.
- Het gedeelte **Bescherming beheren** bevat een lijst met onderdelen van de antivirusbescherming.
- Het gedeelte **Taken** bevat een lijst met lokale taken die op de computer worden uitgevoerd.

Elk gedeelte bevat bedieningselementen die u kunt gebruiken om de werking van een onderdeel in of uit te schakelen, om naar de instellingen van het geselecteerde onderdeel of de geselecteerde taak te gaan en om statistieken over het geselecteerde onderdeel of de geselecteerde taak te bekijken.



Het tabblad Bescherming en controle van het programma

Voer een van de volgende acties uit om het tabblad Bescherming en controle te openen:

- Selecteer in het hoofdvenster van het programma het tabblad **Bescherming en controle**.
- Klik op het programmapictogram in het systeemvak van de taakbalk in Microsoft Windows.
- Selecteer **Kaspersky Endpoint Security 10 voor Windows** in het contextmenu van het programmapictogram.

Licentie van het programma activeren

In deze sectie vindt u algemene informatie over het licentiebeheer van het programma.

Over de Gebruiksrechtovereenkomst

De *Gebruiksrechtovereenkomst* is een bindende overeenkomst tussen u en AO Kaspersky Lab waarin de voorwaarden voor het gebruik van het programma zijn vastgelegd.

We raden aan dat u de voorwaarden van de Gebruiksrechtovereenkomst zorgvuldig doorleest alvorens u het programma gebruikt.

U kunt de voorwaarden van Gebruiksrechtovereenkomst bekijken:

- Wanneer u Kaspersky Endpoint Security in de interactieve modus installeert.
- Door het bestand 'license.txt' te lezen. Dit document is een onderdeel van het distributiepakket van het programma.

Door tijdens de installatie van het programma te bevestigen dat u akkoord gaat met de Gebruiksrechtovereenkomst geeft u aan dat u de voorwaarden van Gebruiksrechtovereenkomst aanvaardt. Als u niet akkoord gaat met de voorwaarden van de Gebruiksrechtovereenkomst, moet u de installatie afbreken.

Over de licentie

Een *licentie* is een recht dat onder de Gebruiksrechtovereenkomst is verleend om het programma gedurende een bepaalde tijd te gebruiken.

Een geldige licentie geeft u recht op de volgende soorten diensten:

- Gebruik van het programma overeenkomstig de voorwaarden van de Gebruiksrechtovereenkomst
- Technische Support

De diensten en de gebruiksduur van het programma hangen af van de soort licentie waarmee het programma is geactiveerd.

De volgende soorten licenties zijn er:

- *Evaluatie* – een gratis licentie om het programma uit te proberen.

  Een evaluatielicentie heeft doorgaans een korte gebruiksduur. Wanneer de evaluatielicentie verloopt, worden alle functies van Kaspersky Endpoint Security uitgeschakeld. Als u het programma verder wilt gebruiken, moet u een commerciële licentie aanschaffen.

- *Commercieel* – een betaalde licentie die u ontvangt wanneer u Kaspersky Endpoint Security aanschaft.

  De beschikbare functionaliteit van het programma met een commerciële licentie hangt af van het gekozen product. Het geselecteerde product wordt in het licentiecertificaat aangegeven. Informatie over verkrijgbare producten vindt u op de website van Kaspersky.

Wanneer de commerciële licentie verloopt, blijft het programma werken in de modus met beperkte functionaliteit. U kunt beschermings- en controle-onderdelen gebruiken en een virusscan starten met de programmadatabases die waren geïnstalleerd voordat de licentie is verlopen. Het programma encrypt ook nog bestanden die zijn gewijzigd en geëncrypt vóór het verlopen van de licentie maar encrypt geen nieuwe bestanden. Kaspersky Security Network kan niet worden gebruikt.

De beperkingen in de functionaliteit van Kaspersky Endpoint Security kunnen worden opgeheven door de commerciële licentie te verlengen of door een nieuwe licentie aan te schaffen.

We raden aan dat u de licentie verlengt voordat u die verloopt om ervoor te zorgen dat de computer volledig beschermd blijft tegen bedreigingen.

Over het licentiecertificaat

Een *licentiecertificaat* is een document dat samen met een licentiebestand of een activatiecode wordt gegeven aan de gebruiker.

Het licentiecertificaat bevat de volgende licentie-informatie:

- Bestelnummer
- Gegevens van de gebruiker aan wie de licentie is verleend
- Gegevens van het programma dat met de licentie kan worden geactiveerd
- Beperking in het aantal activaties van de licentie (bijvoorbeeld het aantal apparaten waarop het programma met de licentie kan worden gebruikt)
- Begindatum van de licentie
- Verloopdatum van de licentie of geldigheidsduur van de licentie
- Type licentie

Over het abonnement

Een *abonnement voor Kaspersky Endpoint Security* is een inkooporder voor het programma met specifieke parameters (verloopdatum van het abonnement, aantal beschermde apparaten). U kunt een abonnement voor Kaspersky Endpoint Security bestellen bij uw serviceprovider (zoals uw internetprovider). Een abonnement kan handmatig of automatisch worden verlengd. U kunt het ook annuleren. U kunt uw abonnement op de website van de serviceprovider beheren.

Het abonnement kan een beperkte duur (bijvoorbeeld één jaar) of een onbeperkte duur (zonder verloopdatum) hebben. Als u Kaspersky Endpoint Security na het verlopen van het abonnement met beperkte duur verder wilt gebruiken, moet u het abonnement verlengen. Een abonnement met onbeperkte duur wordt automatisch verlengd als de diensten van de leverancier tijdig op voorhand zijn betaald.

Bij een abonnement met beperkte duur krijgt u mogelijk een respijtperiode aangeboden om het abonnement te verlengen. Tijdens deze periode wordt de functionaliteit van het programma behouden. De serviceprovider beslist zelf of een respijtperiode wordt verleend en bepaalt dan ook de duur van de eventuele respijtperiode.

Om Kaspersky Endpoint Security met een abonnement te gebruiken, moet u de activatiecode toepassen die u van de serviceprovider hebt gekregen. Wanneer de activatiecode is toegepast, is de actieve code geïnstalleerd. De actieve code definieert de licentie voor het gebruik van het programma met een abonnement. Een extra code kan alleen met een activatiecode worden geïnstalleerd en kan niet met een licentiebestand of met een abonnement worden geïnstalleerd.

De beschikbare functionaliteit van het programma met een abonnement kan overeenkomen de functionaliteit van het programma voor de volgende soorten commerciële licenties: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Deze soorten licenties zijn ontworpen voor de bescherming van bestandsservers, werkstations en mobiele apparaten en ondersteunen het gebruik van controle-onderdelen op werkstations en mobiele apparaten.

De mogelijke opties voor het beheer van het abonnement kunnen verschillen naargelang de serviceprovider. Mogelijk biedt de serviceprovider geen respijtperiode voor de verlenging van het abonnement aan (tijdens deze periode wordt de functionaliteit van het programma behouden).

Aangeschafte activatiecodes voor abonnementen kunnen niet worden gebruikt om oudere versies van Kaspersky Endpoint Security te activeren.

Over de activatiecode

Een *activatiecode* is een unieke alfanumerieke reeks van twintig Latijnse letters en cijfers die u ontvangt wanneer u een commerciële licentie voor Kaspersky Endpoint Security aanschaft.

Om het programma met een activatiecode te activeren, hebt u een internetverbinding nodig om verbinding te maken met de activatieservers van Kaspersky.

De actieve code wordt geïnstalleerd wanneer het programma met een activatiecode wordt geactiveerd. Een extra code kan alleen met een activatiecode worden geïnstalleerd en kan niet met een licentiebestand of met een abonnement worden geïnstalleerd.

Als een activatiecode na de activatie van het programma verloren gaat, kunt u de activatiecode herstellen. Mogelijk hebt u een activatiecode nodig om bijvoorbeeld een Kaspersky CompanyAccount te registreren. Om een activatiecode te herstellen, moet u contact opnemen met de Technische Support van Kaspersky.

Over de code

Een *code* is een unieke alfanumerieke reeks. Met een code kunt u het programma gebruiken aan de voorwaarden die u in het certificaat van de licentie vindt (soort licentie, geldigheidsduur van licentie, beperkingen van licentie).

Bij een code voor een abonnement wordt geen certificaat voor de licentie geleverd.

Een code kan met een activatiecode of een licentiebestand worden toegevoegd aan het programma.

U kunt codes toevoegen, bewerken of verwijderen. De code kan door Kaspersky worden geblokkeerd als de voorwaarden van de Gebruiksrechtovereenkomst worden geschonden. Als code op de blacklist staat, moet u een andere code toevoegen om het programma verder te gebruiken.

Als een code voor een verlopen licentie wordt verwijderd, zijn de functies van het programma niet beschikbaar. U kunt zo'n code niet opnieuw toevoegen nadat die is verwijderd.

Er zijn twee soorten codes: actieve en extra codes.

Een *actieve code* is een code die momenteel wordt gebruikt door het programma. Een evaluatielicentie of commerciële licentie kan als de actieve code worden toegevoegd. Het programma kan maximaal één actieve code hebben.

Een *extra code* is een code die de gebruiker recht geeft op het gebruik van het programma maar momenteel niet wordt gebruikt. Bij het verlopen van de actieve code wordt een extra code automatisch actief. Een extra code kan alleen worden toegevoegd als er al een actieve code is.

Een code voor een evaluatielicentie kan alleen als actieve code worden toegevoegd. Deze kan niet als extra code worden toegevoegd. Een code voor de evaluatielicentie kan de actieve code voor een commerciële licentie niet vervangen.

Als een code op de blacklist wordt geplaatst, blijft de functionaliteit van het programma die is gedefinieerd door de licentie waarmee het programma is geactiveerd beschikbaar gedurende acht dagen. Kaspersky Security Network en de updates voor de databases en programmamodules blijven onbeperkt beschikbaar. Het programma meldt de gebruiker dat de code op de blacklist is geplaatst. Na acht dagen wordt de functionaliteit van het programma beperkt tot de beschikbare functionaliteit na het verlopen van de licentie: het programma werkt zonder updates en Kaspersky Security Network is niet beschikbaar.

Over het licentiebestand

Een *licentiebestand* is een bestand met de extensie .key die u na de aanschaf van Kaspersky Endpoint Security krijgt van Kaspersky. Een licentiebestand dient om een code toe te voegen die het programma activeert.

U hoeft geen verbinding te maken met de activatieservers van Kaspersky om het programma met een licentiebestand te activeren.

U kunt een licentiebestand herstellen als u het per ongeluk hebt verwijderd. Mogelijk hebt u een licentiebestand nodig om een Kaspersky CompanyAccount te registreren.

Doe een van het volgende om een licentiebestand te herstellen:

- Neem contact op met de leverancier van de licentie.
- Krijg op basis van uw bestaande activeringscode een licentiebestand op de Kaspersky-website.

Over de voorziening van gegevens

Met de aanvaarding van de Gebruiksrechtovereenkomst gaat u akkoord met de automatische verzending van informatie over uw gebruik van het product, alsook over het type, de versie en de taalversie van het geïnstalleerde programma, het unieke id van het installatieprogramma en het type van de installatie, en gegevens over actieve en extra codes (inclusief het type licentie, de geldigheidsduur, de datum waarop het programma is geactiveerd en waarop de licentie verloopt, het nummer van de licentie, de huidige status van de licentie, de versie van het protocol voor interactie met de activatieserver).

In het geval dat het programma is geactiveerd met een activatiecode, gaat u voor de verzameling van statistische informatie over de distributie en het gebruik van de producten van de Licentiehouder ermee akkoord om automatisch de volgende informatie te leveren: de versie van het gebruikte programma (inclusief informatie over geïnstalleerde programma-updates, het id van de programma-installatie en informatie over licenties), de versie van het besturingssysteem, en de id's van actieve programma-onderdelen op het moment van de levering van de informatie.

Ontvangen informatie wordt door Kaspersky beschermd overeenkomstig de wettelijke voorschriften en de vereisten en toepasselijke regelgevingen van Kaspersky.

Kaspersky gebruikt de ontvangen informatie volledig anoniem en alleen in de vorm van algemene statistische gegevens. Algemene statistieken worden automatisch gegenereerd op basis van de oorspronkelijk verzamelde informatie en bevatten geen persoonlijke gegevens of andere vertrouwelijke gegevens. De oorspronkelijk verzamelde informatie wordt na verloop van tijd vernietigd (eenmaal per jaar). Algemene statistische gegevens worden voor onbepaalde duur opgeslagen.

Lees de Gebruiksrechtovereenkomst door en bezoek de website van Kaspersky voor meer informatie over de verzameling, verwerking, opslag en vernietiging van informatie over het programmagebruik nadat u akkoord bent gegaan met de Gebruiksrechtovereenkomst en de Verklaring van KSN. De bestanden license.txt en ksn.txt files bevatten de Gebruiksrechtovereenkomst en de Verklaring van KSN en zijn een onderdeel van het distributiepakket van het programma.

Licentie-informatie bekijken

Zo bekijkt u licentie-informatie:

1. Open het hoofdvenster van het programma.
2. Klik op de knop / onder in het hoofdvenster van het programma.

   Het venster **Licentiebeheer** wordt geopend. Informatie over de licentie wordt in het gedeelte boven in het venster **Licentiebeheer** weergegeven.

Een licentie aanschaffen

U kunt na de installatie van het programma een licentie aanschaffen. Bij de aanschaf van een licentie ontvangt u een activatiecode of een licentiebestand om het programma te activeren.

Zo schaft u een licentie aan:

1. Open het hoofdvenster van het programma.
2. Klik op de knop / onder in het hoofdvenster van het programma.

   Het venster **Licentiebeheer** wordt geopend.
3. Doe in het venster **Licentiebeheer** één van het volgende:

- Klik op de knop **Licentie kopen** als geen codes zijn toegevoegd of als een code voor een evaluatielicentie is toegevoegd.
- Klik op de knop **Licentie verlengen** als de code voor een commerciële licentie is toegevoegd.

Een venster met de website van de online shop van Kaspersky wordt geopend. In deze shop kunt u een licentie aanschaffen.

Een licentie verlengen

Als de licentie binnenkort verloopt, kunt u die verlengen. Op deze manier blijft de computer beschermd wanneer de huidige licentie verloopt en totdat u het programma met een nieuwe licentie activeert.

Zo verlengt u een licentie:

1. Krijg een nieuwe activatiecode of een nieuw licentiebestand voor het programma.
2. Voeg een extra code toe met de activatiecode of het licentiebestand dat u hebt ontvangen.

Hierdoor wordt een extra code toegevoegd. Deze wordt actief wanneer de licentie verloopt.

Het kan even duren voordat de code wordt bijgewerkt van extra naar actief wegens de verdeling van de belasting tussen de activatieservers van Kaspersky.

Abonnement verlengen

Wanneer u het programma met een abonnement gebruikt, neemt Kaspersky Endpoint Security automatisch contact op met de activatieserver op specifieke intervallen totdat uw abonnement verloopt.

Als u het programma met een onbeperkt abonnement gebruikt, controleert Kaspersky Endpoint Security de activatieserver automatisch op verlengde codes in de achtergrondmodus. Wanneer een code op de activatieserver beschikbaar is, voegt het programma die toe door de bestaande code te vervangen. Op deze manier wordt het onbeperkte abonnement voor Kaspersky Endpoint Security verlengd zonder dat de gebruiker iets hoeft te doen.

Als u het programma met een beperkt abonnement gebruikt, toont Kaspersky Endpoint Security op de dag dat het abonnement verloopt (of de respijtperiode na het verlopen van de licentie die u kunt gebruiken om het abonnement te verlengen) een melding hierover en probeert het niet meer het abonnement automatisch te verlengen. In dit geval werkt Kaspersky Endpoint Security op dezelfde manier als wanneer een commerciële licentie voor het programma is verlopen: het programma werkt zonder updates en Kaspersky Security Network is niet beschikbaar.

U kunt het abonnement op de website van de serviceprovider verlengen.

U kunt de status van het abonnement handmatig bijwerken in het venster **Licentiebeheer**. Dit is mogelijk vereist als het abonnement na het verlopen van de respijtperiode is verlengd en de status van het programma niet automatisch is bijgewerkt.

De website van de serviceprovider bezoeken

Zo bezoekt u de website van de serviceprovider vanuit de programma-interface:

1. Open het hoofdvenster van het programma.
2. Klik op de knop / onder in het hoofdvenster van het programma.
   Het venster **Licentiebeheer** wordt geopend.
3. Klik in het venster **Licentiebeheer** op **Contact opnemen met abonnementaanbieder**.

Methoden voor de activatie van het programma

De *activatie* is het proces waarbij een licentie wordt geactiveerd om een volledige functionele versie van het programma te gebruiken totdat de licentie verloopt. Voor de activatie van het programma moet u een code toevoegen.

U kunt het programma activeren op één van de volgende manieren:

- Via de wizard Initiële configuratie wanneer u het programma installeert. U kunt de actieve code op deze manier toevoegen.
- Lokaal vanuit de programma-interface door de Activatiewizard te gebruiken. U kunt zowel de actieve code als de extra code op deze manier toevoegen.
- Op afstand met de Kaspersky Security Center-softwaresuite door een taak voor het toevoegen van een code aan te maken en vervolgens te starten. Op deze manier kunt u zowel de actieve code als de extra code toevoegen.
- Op afstand door codes en activatiecodes in de opslag van codes in de Administration Server van Kaspersky Security Center te verdelen tussen clientcomputers (raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie). Op deze manier kunt u zowel de actieve code als de extra code toevoegen.

  De activatiecode die voor een abonnement is aangeschaft wordt als eerste verdeeld.

- Met de opdrachtregel.

Het kan even duren om het programma met een activatiecode te activeren (tijdens de installatie op afstand of niet-interactieve installatie) wegens de verdeling van de belasting tussen de activatieservers van Kaspersky. Als u het programma onmiddellijk wilt activeren, kunt u het actieve activatieproces onderbreken en de activatie met de Activatiewizard starten.

Activatiewizard gebruiken voor de activatie van het programma

Zo activeert u Kaspersky Endpoint Security met de Activatiewizard:

1. Klik op de knop / onder in het hoofdvenster van het programma.

   Het venster **Licentiebeheer** wordt geopend.

2. Klik in het venster **Licentiebeheer** op de knop **Activeer het programma met een nieuwe licentie**.

   De Activatiewizard van het programma wordt gestart.

3. Volg de instructies van de Activatiewizard.

Voor meer gedetailleerde informatie over de activatie van het programma raadpleegt u de sectie over de wizard Initiële configuratie.

Het programma vanaf de opdrachtregel activeren

Om het programma vanaf de opdrachtregel te activeren,

typt u `avp.com license /add <activatiecode of licentiebestand> /password=<wachtwoord>` op de opdrachtregel.

Het programma starten en stoppen

In deze sectie wordt beschreven hoe u de automatische start van het programma kunt configureren, het programma handmatig kunt starten of stoppen en de beschermings- en controle-onderdelen kunt pauzeren of hervatten.

Automatische start van het programma inschakelen en uitschakelen

Onder automatische start verstaan we dat Kaspersky Endpoint Security onmiddellijk wordt gestart na de opstart van het besturingssysteem, zonder enige interventie van de gebruiker. Deze optie voor de start van het programma is standaard ingeschakeld.

Kaspersky Endpoint Security wordt na de installatie voor het eerst automatisch gestart. Daarna wordt het programma automatisch na de opstart van het besturingssysteem gestart.

De download van antivirusdatabases van Kaspersky Endpoint Security na de opstart van het besturingssysteem kan tot wel twee minuten duren afhankelijk van de eigenschappen van de computer. Tijdens deze tijd is de computer minder beschermd. Als de antivirusdatabases worden gedownload wanneer Kaspersky Endpoint Security wordt gestart in een al opgestart besturingssysteem, is de computer niet minder beschermd.

Zo schakelt u de automatische start van het programma in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Voer een van de volgende acties uit:

   - Als u de automatische start van het programma wilt inschakelen, schakelt u het selectievakje **Kaspersky Endpoint Security 10 voor Windows starten bij opstart van computer** in.
   - Als u de automatische start van het programma wilt uitschakelen, schakelt u het selectievakje **Kaspersky Endpoint Security 10 voor Windows starten bij opstart van computer** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het programma handmatig starten en stoppen

Experts van Kaspersky raden af dat u Kaspersky Endpoint Security handmatig stopt omdat u hierdoor de computer en uw persoonlijke gegevens blootstelt aan bedreigingen. U kunt indien nodig de computerbescherming pauzeren zolang u dat wilt zonder het programma te stoppen.

Kaspersky Endpoint Security moet handmatig worden gestart als u de automatische start van het programma eerder hebt uitgeschakeld.

Zo start u het programma handmatig:

Selecteer in het menu **Start** achtereenvolgens **Apps** → **Kaspersky Endpoint Security 10 voor Windows**.

Zo stopt u het programma handmatig:

1. Klik rechts om het contextmenu van het programmapictogram in het systeemvak van de taakbalk te openen.
2. Selecteer in het contextmenu de optie **Afsluiten**.

Bescherming en controle van computer pauzeren en hervatten

Door de pauzering van de bescherming en de controle van de computer schakelt u alle beschermings- en controle-onderdelen van Kaspersky Endpoint Security een bepaalde tijd uit.

De status van het programma wordt via het programmapictogram in het systeemvak van de taakbalk weergegeven.

- Het pictogram geeft aan dat de bescherming en de controle van de computer zijn gepauzeerd.
- Het pictogram geeft aan dat de bescherming en de controle van de computer zijn uitgeschakeld.

Het pauzeren of hervatten van de bescherming en de controle van de computer is niet van invloed op scan- of updatetaken.

Als de netwerkverbindingen al tot stand zijn gebracht wanneer u de bescherming en de controle van de computer pauzeert of hervat, ziet u een melding over de beëindiging van deze netwerkverbindingen.

Zo pauzeert u de bescherming en de controle van de computer:

1. Klik rechts om het contextmenu van het programmapictogram in het systeemvak van de taakbalk te openen.
2. Selecteer in het contextmenu de optie **Bescherming en controle pauzeren**.
   Het venster **Bescherming pauzeren** wordt geopend.
3. Selecteer één van de volgende opties:
   - **Pauzeren gedurende opgegeven tijd** - De bescherming en de controle van de computer worden na de gekozen tijd in de onderstaande vervolgkeuzelijst hervat.
   - **Pauzeren tot herstart** - De bescherming en de controle van de computer worden hervat nadat u het programma hebt gesloten en opnieuw hebt geopend of nadat u het besturingssysteem opnieuw hebt opgestart. De automatisch start van het programma moet ingeschakeld zijn om deze optie te gebruiken.
   - **Pauzeren** - De bescherming en de controle van de computer worden hervat wanneer u beslist die opnieuw in te schakelen.
4. Als u tijdens de vorige stap de optie **Pauzeren gedurende opgegeven tijd** hebt geselecteerd, selecteert u in de vervolgkeuzelijst het noodzakelijke interval.

Zo hervat u de bescherming en de controle van de computer:

1. Klik rechts om het contextmenu van het programmapictogram in het systeemvak van de taakbalk te openen.

2. Selecteer in het contextmenu de optie **Bescherming en controle hervatten**.

U kunt de bescherming en de controle van de computer op elk moment hervatten, ongeacht de optie voor het pauzeren van de bescherming en de controle van de computer die u eerder hebt gekozen.

Bescherming van het bestandssysteem van de computer. Anti-Virus voor bestanden

In deze sectie vindt u informatie over Anti-Virus voor bestanden en leest u hoe u de instellingen van het onderdeel configureert.

Over Anti-Virus voor bestanden

Anti-Virus voor bestanden voorkomt infectie van het bestandssysteem van de computer. Standaard wordt Anti-Virus voor bestanden samen met Kaspersky Endpoint Security gestart. Het onderdeel blijft voortdurend actief in het computergeheugen en scant alle bestanden die worden geopend, opgeslagen of gestart op de computer en alle aangesloten schijven op virussen en andere bedreigingen.

Bij de detectie van een bedreiging in een bestand voert Kaspersky Endpoint Security het volgende uit:

1. Detecteert het type van het gevonden object in het bestand (zoals een *virus* of *Trojan*).
2. Labelt het bestand als *waarschijnlijk geïnfecteerd* als de scan niet kan bepalen of het bestand geïnfecteerd is. Het bestand bevat mogelijk een stuk code dat kenmerkend is voor virussen of andere malware of bevat misschien gewijzigde code van een bekend virus.
3. Het programma geeft een melding over het gevonden kwaadaardige object in het bestand weer (als meldingen zijn geconfigureerd) en verwerkt het bestand door de opgegeven actie in de instellingen van Anti-Virus voor bestanden uit te voeren.

Anti-Virus voor bestanden inschakelen en uitschakelen

Anti-Virus voor bestanden is standaard ingeschakeld en werkt in een modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig Anti-Virus voor bestanden uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Anti-Virus voor bestanden in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.

   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Anti-Virus voor bestanden bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.

5. Voer een van de volgende acties uit:

   - Selecteer **Starten** in het menu om Anti-Virus voor bestanden in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Anti-Virus voor bestanden**, wijzigt in het pictogram .

   - Selecteer **Stoppen** in het menu om Anti-Virus voor bestanden uit te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Anti-Virus voor bestanden**, wijzigt in het pictogram .

Zo schakelt u Anti-Virus voor bestanden in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Anti-Virus voor bestanden inschakelen** in om Anti-Virus voor bestanden in te schakelen.
   - Schakel het selectievakje **Anti-Virus voor bestanden inschakelen** uit om Anti-Virus voor bestanden uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Anti-Virus voor bestanden automatisch pauzeren

U kunt Anti-Virus voor bestanden configureren om automatisch te worden gepauzeerd op een opgegeven tijdstip of wanneer specifieke programma's worden gebruikt.

Anti-Virus voor bestanden pauzeren tijdens conflicten met andere programma's is een noodmaatregel. In het geval van conflicten tijdens de werking van een onderdeel raden we aan dat u contact opneemt met de Technische Support van Kaspersky (https://companyaccount.kaspersky.com). De Support-experts zullen u helpen Anti-Virus voor bestanden zodanig te configureren dat u het tegelijk met andere programma's op uw computer kunt gebruiken.

Zo configureert u het automatisch pauzeren van Anti-Virus voor bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.
4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Extra**.

5. In het gedeelte **Taak pauzeren**:

   - Schakel het selectievakje **Volgens schema** in en klik op de knop **Planning** om het automatisch pauzeren van Anti-Virus voor bestanden op een opgegeven tijdstip te configureren.

     Het venster **Taak pauzeren** wordt geopend.

   - Schakel het selectievakje **Bij opstart van programma** in en klik op de knop **Selecteren** om het automatisch pauzeren van Anti-Virus voor bestanden bij de opstart van specifieke programma's te configureren.

     Het venster **Programma's** wordt geopend.

6. Voer een van de volgende acties uit:

   - Als u het automatisch pauzeren van Anti-Virus voor bestanden op een opgegeven tijdstip configureert, gebruikt u in het venster **Taak pauzeren** de velden **Taak pauzeren om** en **Taak hervatten om** om op te geven wanneer (in de notatie UU:MM) Anti-Virus voor bestanden moet worden gepauzeerd. Klik op **OK**.

   - Als u het automatisch pauzeren van Anti-Virus voor bestanden bij de opstart van specifieke programma's configureert, gebruikt u de knoppen **Toevoegen**, **Bewerken** en **Verwijderen** in het venster **Programma's** om een lijst met programma's te maken die Anti-Virus voor bestanden pauzeren als ze actief zijn. Klik op **OK**.

7. Klik in het venster **Anti-Virus voor bestanden** op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Anti-Virus voor bestanden configureren

U kunt het volgende doen om Anti-Virus voor bestanden te configureren:

- Wijzig het beschermingsniveau.

  U kunt een van de vooraf ingestelde beschermingsniveaus selecteren of instellingen voor een beschermingsniveau handmatig configureren. Als u de instellingen van een beschermingsniveau wijzigt, kunt u altijd de aanbevolen instellingen van het beschermingsniveau herstellen.

- Wijzig de actie die door Anti-Virus voor bestanden wordt uitgevoerd wanneer een geïnfecteerd bestand wordt gevonden.

- Bewerk het beschermd bereik van Anti-Virus voor bestanden.

  U kunt het beschermd bereik vergroten of verkleinen door scanobjecten toe te voegen of te verwijderen of door te wijzigen welke soort bestanden u wilt scannen.

- Configureer de heuristische scanner.

  Anti-Virus voor bestanden gebruikt de techniek genaamd 'Analyse op basis van definities'. Tijdens de analyse op basis van definities controleert Anti-Virus voor bestanden of het gevonden object voorkomt in de antivirusdatabases van het programma. Op aanbeveling van de Kaspersky-experts is de analyse op basis van definities altijd ingeschakeld.

  Om de doeltreffendheid van de bescherming te verhogen, kunt u de heuristische analyse gebruiken. Tijdens de heuristische analyse analyseert Anti-Virus voor bestanden de activiteit van objecten in het besturingssysteem. Met de heuristische analyse vindt u kwaadaardige objecten die momenteel niet voorkomen in de antivirusdatabases van het programma.

- Optimaliseer de scans.

U kunt het scannen van bestanden door Anti-Virus voor bestanden optimaliseren om de duur van de scans in te korten en Kaspersky Endpoint Security sneller te laten werken. Hiertoe scant u gewoon de nieuwe bestanden en de bestanden die sinds de vorige scan zijn gewijzigd. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.

U kunt ook het gebruik van de iChecker- en iSwift-technologie inschakelen. Hiermee optimaliseert u de snelheid van de scans door de bestanden die sinds de laatste scan niet zijn gewijzigd niet te scannen.

- Configureer het scannen van samengestelde bestanden.
- Wijzig de modus voor het scannen van bestanden.

Het beschermingsniveau wijzigen

Anti-Virus voor bestanden past verschillende groepen van instellingen toe om het bestandssysteem van de computer te beschermen. Deze groepen van instellingen worden *beschermingsniveaus* genoemd. Er bestaan drie vooraf ingestelde beschermingsniveaus: **Hoog**, **Aanbevolen** en **Laag**. De instellingen van het beschermingsniveau **Aanbevolen** worden beschouwd als de optimale instellingen die door experts van Kaspersky worden aanbevolen.

Zo wijzigt u een beschermingsniveau:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Doe in het gedeelte **Beschermingsniveau** een van het volgende:
   - Als u een van de vooraf ingestelde beschermingsniveaus wilt instellen (**Hoog**, **Aanbevolen** of **Laag**), selecteert u het niveau met de schuifregelaar.
   - Als u een aangepast beschermingsniveau wilt configureren, klikt u op de knop **Instellingen** en voert u de aangepaste instellingen in het geopende venster **Anti-Virus voor bestanden** in.

     Nadat u een aangepast beschermingsniveau hebt geconfigureerd, wordt de naam van het beschermingsniveau in het gedeelte **Beschermingsniveau** gewijzigd in **Aangepast**.
   - Als u het beschermingsniveau wilt wijzigen in **Aanbevolen**, klikt u op de knop **Standaard**.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De actie wijzigen die Anti-Virus voor bestanden moet uitvoeren op geïnfecteerde bestanden

Zo wijzigt u de actie die Anti-Virus voor bestanden moet uitvoeren op geïnfecteerde bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.

3. Selecteer in het gedeelte **Actie bij detectie van een bedreiging** de vereiste optie:

   - **Actie automatisch selecteren**.
   - **Voer actie uit: Desinfecteren. Verwijderen als desinfectie mislukt**.
   - **Voer actie uit: Desinfecteren**.

     Zelfs als deze optie wordt geselecteerd, past Kaspersky Endpoint Security de actie **Verwijderen** toe op bestanden die tot het Windows Store-programma behoren.

   - **Voer actie uit: Verwijderen**.
   - **Voer actie uit: Blokkeren**.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het beschermd bereik van Anti-Virus voor bestanden bewerken

Het beschermd bereik verwijst naar de objecten die het onderdeel scant wanneer het is ingeschakeld. De beschermde bereiken van de verschillende onderdelen hebben verschillende eigenschappen. De locatie en de soort bestanden die moeten worden gescand zijn eigenschappen van het beschermd bereik van Anti-Virus voor bestanden. Standaard scant Anti-Virus voor bestanden alleen infecteerbare bestanden die op harde schijven, netwerkschijven of verwisselbare media zijn aangesloten.

Zo maakt u het beschermd bereik aan:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.

3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.

4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Algemeen**.
5. Geef in het gedeelte **Bestandstypen** op welke bestanden Anti-Virus voor bestanden moet scannen:

   - Als u alle bestanden wilt scannen, selecteert u **Alle bestanden**.
   - Als u bestanden met indelingen die het meest kwetsbaar zijn voor infecties wilt scannen, selecteert u **Bestanden gescand op indeling**.
   - Als u bestanden met extensies die het meest kwetsbaar zijn voor infecties wilt scannen, selecteert u **Bestanden gescand op extensie**.

   Wanneer u selecteert welke bestanden moeten worden gescand, moet u rekening houden met het volgende:

- Er zijn bepaalde bestandsindelingen (zoals .txt) waarbij het gevaar voor binnendringing van kwaadaardige code en de daaropvolgende activatie vrij klein is. Tegelijkertijd bestaan er ook bestandsindelingen die (mogelijk) uitvoerbare code bevatten (zoals .exe, .dll en .doc). Het risico op binnendringing en de activatie van kwaadaardige code in zulke bestanden is vrij groot.

- Een indringer kan een virus of een ander kwaadaardig programma naar uw computer sturen in een uitvoerbaar bestand waarvan de extensie in .txt is gewijzigd. Als u ervoor kiest om bestanden op extensie te scannen, wordt zo'n bestand overgeslagen door de scan. Als het scannen van bestanden op indeling is geselecteerd, wordt de bestandsheader door Anti-Virus voor bestanden geanalyseerd, ongeacht de extensie. Deze analyse geeft mogelijk aan dat de eigenlijke indeling van het bestand .exe is. Zo'n bestand wordt grondig gescand op virussen en andere malware.

6. Doe in de lijst **Beschermd bereik** een van het volgende:

   - Als u een nieuw object aan het scanbereik wilt toevoegen, klikt u op de knop **Toevoegen**.

   - Als u de locatie van een object wilt wijzigen, selecteert u het object uit het scanbereik en klikt u op de knop **Bewerken**.

   Het venster **Scanbereik selecteren** wordt geopend.

   - Als u een object wilt verwijderen uit de lijst met objecten die moeten worden gescand, selecteert u er een uit de lijst met te scannen objecten en klikt u op de knop **Verwijderen**.

     Een venster wordt geopend waarin u de verwijdering kunt bevestigen.

7. Voer een van de volgende acties uit:

   - Als u een nieuw object wilt toevoegen of de locatie van een object in de lijst met te scannen objecten wilt wijzigen, selecteert u het object in het venster **Scanbereik selecteren** en klikt u op de knop **Toevoegen**.

     Alle geselecteerde objecten in het venster **Scanbereik selecteren** worden in het venster **Anti-Virus voor bestanden** in de lijst **Beschermd bereik** weergegeven.

     Klik op **OK**.

   - Als u een object wilt verwijderen, klikt u op de knop **Ja** in het venster voor de bevestiging van de verwijdering.

8. Herhaal indien nodig stappen 6-7 voor het toevoegen, verplaatsen of verwijderen van objecten uit de lijst met te scannen objecten.

9. Om een object uit de lijst met te scannen objecten uit te sluiten, schakelt u het selectievakje naast het object in de lijst **Beschermd bereik** uit. Het object blijft wel in de lijst met te scannen objecten staan, hoewel het niet wordt gescand door Anti-Virus voor bestanden.

10. Klik in het venster **Anti-Virus voor bestanden** op **OK**.

11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De heuristische scanner met Anti-Virus voor bestanden gebruiken

Zo configureert u het gebruik van de heuristische scanner in de werking van Anti-Virus voor bestanden:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.

3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.

4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Prestaties**.

5. In het gedeelte **Scanmethoden**:

   - Als u wilt dat Anti-Virus voor bestanden de heuristische analyse gebruikt, schakelt u het selectievakje **Heuristische analyse** in en gebruikt u de schuifregelaar om het niveau van de heuristische analyse in te stellen: **Oppervlakkige scan**, **Gemiddelde scan** of **Gedetailleerde scan**.

   - Als u niet wilt dat Anti-Virus voor bestanden de heuristische analyse gebruikt, schakelt u het selectievakje **Heuristische analyse** uit.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een scantechnologie tijdens de werking van Anti-Virus voor bestanden gebruiken

Zo configureert u het gebruik van scantechnologieën in de werking van Anti-Virus voor bestanden:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.

3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.

4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Extra**.

5. In het gedeelte **Scantechnologieën**:

   - Schakel de selectievakjes in naast de namen van de technologieën die u in de werking van Anti-Virus voor bestanden wilt gebruiken.

   - Schakel de selectievakjes uit naast de namen van de technologieën die u niet in de werking van Anti-Virus voor bestanden wilt gebruiken.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het scannen van bestanden optimaliseren

Zo optimaliseert u het scannen van bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Klik op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.
4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Prestaties**.
5. Schakel in het gedeelte **Scanoptimalisatie** het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** in.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Samengestelde bestanden scannen

Een vaak gebruikte techniek voor het verbergen van virussen en andere malware is de insluiting ervan in samengestelde bestanden zoals archieven of e-maildatabases. Om virussen en andere malware te vinden die op deze manier zijn verborgen, moet het samengestelde bestand worden uitgepakt waardoor het scannen wordt vertraagd. U kunt de reeks samengestelde bestanden die moeten worden gescand beperken om zo de scan sneller te voltooien.

De gebruikte methode voor de verwerking van een geïnfecteerd samengesteld bestand (desinfectie of verwijdering) hangt af van het soort bestand.

Anti-Virus voor bestanden desinfecteert samengestelde bestanden met een RAR-, ARJ-, ZIP-, CAB- en LHA-indeling en verwijdert bestanden met alle andere indelingen (behalve e-maildatabases).

Zo configureert u het scannen van samengestelde bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.

4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Prestaties**.

5. Geef in het gedeelte **Scan van samengestelde bestanden** op welke soorten samengestelde bestanden u wilt scannen: archieven, installatiepakketten of bestanden met Office-indelingen.

6. Om alleen nieuwe en gewijzigde samengestelde bestanden te scannen, schakelt u het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** in.

   Anti-Virus voor bestanden scant dan alleen nieuwe en gewijzigde samengestelde bestanden, ongeacht het type ervan.

7. Klik op de knop **Extra**.

   Het venster **Samengestelde bestanden** wordt geopend.

8. Doe in het gedeelte **Achtergrondscan** een van het volgende:

   - Schakel het selectievakje **Samengestelde bestanden in de achtergrond uitpakken** uit om Anti-Virus voor bestanden geen samengestelde bestanden op de achtergrond te laten uitpakken.

   - Als u Anti-Virus voor bestanden samengestelde bestanden op de achtergrond wilt laten uitpakken, schakelt u het selectievakje **Samengestelde bestanden in de achtergrond uitpakken** in en geeft u de vereiste waarde in het veld **Minimale bestandsgrootte** op.

9. Doe in het gedeelte **Beperking van grootte** een van het volgende:

   - Om Anti-Virus voor bestanden geen grote samengestelde bestanden te laten uitpakken, schakelt u het selectievakje **Grote samengestelde bestanden niet uitpakken** in en geeft u de vereiste waarde in het veld **Maximale bestandsgrootte** op. Anti-Virus voor bestanden pakt geen samengestelde bestanden uit die groter zijn dan de opgegeven grootte.

   - Om Anti-Virus voor bestanden grote samengestelde bestanden te laten uitpakken, schakelt u het selectievakje **Grote samengestelde bestanden niet uitpakken** uit.

     Een bestand wordt als groot beschouwd als het groter is dan de waarde in het veld **Maximale bestandsgrootte**.

   Anti-Virus voor bestanden scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Grote samengestelde bestanden niet uitpakken** is ingeschakeld.

10. Klik op **OK**.

11. Klik in het venster **Anti-Virus voor bestanden** op **OK**.

12. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De scanmodus wijzigen

Onder *scanmodus* verstaan we de toestand waarin Anti-Virus voor bestanden bestanden begint te scannen. Standaard scant Kaspersky Endpoint Security bestanden in de intelligente modus. In deze scanmodus beslist Anti-Virus voor bestanden na de analyse van de bestandsbewerkingen die door de gebruiker, een programma namens de gebruiker (met het account waarmee de gebruiker is aangemeld of een ander gebruikersaccount) of het besturingssysteem zijn uitgevoerd of bestanden al dan niet moeten worden gescand. Wanneer u bijvoorbeeld werkt met een Microsoft Office Word-document, scant Kaspersky Endpoint Security het bestand wanneer het eerst wordt geopend en dan wordt gesloten. Tussentijdse, overschrijvende handelingen zorgen er niet voor dat het bestand wordt gescand.

Zo wijzigt u de scanmodus voor bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Anti-Virus voor bestanden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Anti-Virus voor bestanden.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Anti-Virus voor bestanden** wordt geopend.
4. Selecteer in het venster **Anti-Virus voor bestanden** het tabblad **Extra**.
5. Selecteer in het gedeelte **Scanmodus** de vereiste modus:

   - **Intelligente modus**.
   - **Bij openen en wijzigen**.
   - **Bij openen**.
   - **Bij uitvoeren**.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

E-mailbescherming. Mail Anti-Virus

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Mail Anti-Virus en leest u hoe u de instellingen van het onderdeel configureert.

Over Mail Anti-Virus

Mail Anti-Virus scant inkomende en uitgaande e-mailberichten op virussen en andere bedreigingen. Het onderdeel wordt samen met Kaspersky Endpoint Security gestart, blijft voortdurend actief in het computergeheugen en scant alle berichten die via de protocollen POP3, SMTP, IMAP, MAPI en NNTP worden verstuurd of ontvangen. Als geen bedreigingen worden gevonden in het bericht, wordt het beschikbaar gesteld en/of verwerkt.

Bij de detectie van een bedreiging in een e-mailbericht doet Mail Anti-Virus het volgende:

1. Het identificeert het type van het gevonden object in het e-mailbericht (zoals een *Trojan*).
2. Een e-mailbericht krijgt een van de volgende statussen toegewezen:
   - *Waarschijnlijk geïnfecteerd*. Deze status wordt toegewezen als de scan niet kan bepalen of het e-mailbericht al dan niet is geïnfecteerd. Het e-mailbericht bevat mogelijk een stuk code dat kenmerkend is voor virussen of andere malware of bevat misschien gewijzigde code van een bekend virus.
   - *Geïnfecteerd*. Deze status wordt aan een object toegewezen als tijdens de scan van een e-mailbericht een stuk code van een bekend virus wordt gevonden dat in de antivirusdatabases van Kaspersky Endpoint Security is opgenomen.
   - *Niet gevonden*. Deze status wordt aan een object toegewezen als tijdens de scan van een e-mailbericht geen virussen of andere bedreigingen worden gevonden.

Het programma blokkeert dan het e-mailbericht, geeft een melding over het gevonden object weer (als dit in de instellingen voor meldingen is opgegeven) en voert de actie uit die in de instellingen van Mail Anti-Virus is opgegeven.

Dit onderdeel staat in verbinding met de geïnstalleerde e-mailprogramma's op de computer. Een insluitbare extensie is beschikbaar voor Microsoft Office Outlook® waarmee u de instellingen voor het scannen van berichten precies kunt configureren. De extensie van Mail Anti-Virus wordt tijdens de installatie van Kaspersky Endpoint Security ingesloten in Microsoft Office Outlook.

De werking van Mail Anti-Virus wordt door het pictogram van het programma in het systeemvak van de taakbalk aangegeven. Wanneer Mail Anti-Virus een e-mailbericht scant, wijzigt het pictogram van het programma in

Mail Anti-Virus inschakelen en uitschakelen

Mail Anti-Virus is standaard ingeschakeld en werkt in een modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig Mail Anti-Virus uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Mail Anti-Virus in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.
   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Mail Anti-Virus bevat.
   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:
   - Selecteer **Starten** in het menu om Mail Anti-Virus in te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **Mail Anti-Virus**, wijzigt in het pictogram .
   - Selecteer **Stoppen** in het menu om Mail Anti-Virus uit te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **Mail Anti-Virus**, wijzigt in het pictogram .

Zo schakelt u Mail Anti-Virus in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.
   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **Mail Anti-Virus inschakelen** in om Mail Anti-Virus in te schakelen.
   - Schakel het selectievakje **Mail Anti-Virus inschakelen** uit om Mail Anti-Virus uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Mail Anti-Virus configureren

U kunt het volgende doen om Mail Anti-Virus te configureren:

- Wijzig het beschermingsniveau voor e-mails.
  U kunt een van de vooraf geïnstalleerde beschermingsniveau voor e-mails selecteren of een aangepast beschermingsniveau voor e-mails configureren.
  Als u de instellingen van het beschermingsniveau voor e-mails hebt gewijzigd, kunt u altijd de aanbevolen instellingen van het beschermingsniveau voor e-mails herstellen.

- Wijzig de actie die Kaspersky Endpoint Security uitvoert op geïnfecteerde berichten.
- Bewerk het beschermd bereik van Mail Anti-Virus.
- Configureer het scannen van samengestelde bestanden die als bijlage aan e-mailberichten zijn toegevoegd.

  U kunt het scannen van bijlagen in berichten inschakelen of uitschakelen, de maximale grootte van te scannen bijlagen van berichten beperken en de maximale scanduur voor bijlagen van berichten beperken.
- Configureer een filter voor het type van bijlagen in e-mailberichten.

  Met een filter voor het type van bijlagen in berichten kunt u de opgegeven typen bestanden automatisch hernoemen of verwijderen.
- Configureer de heuristische scanner.

  Om de doeltreffendheid van de bescherming te verhogen, kunt u de heuristische analyse gebruiken. Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van programma's in het besturingssysteem. De heuristische analyse kan bedreigingen in berichten vinden die momenteel niet voorkomen in de databases van Kaspersky Endpoint Security.
- Configureer het scannen van e-mails in Microsoft Office Outlook.

  Een insluitbare extensie is beschikbaar voor Microsoft Office Outlook waarmee u de instellingen voor het scannen van e-mails handig kunt configureren.

  Wanneer u met andere e-mailprogramma's werkt, zoals Microsoft Outlook Express®, Windows Mail of Mozilla™ Thunderbird™, scant Mail Anti-Virus het verkeer van de e-mailprotocollen SMTP, POP3, IMAP en NNTP.

  Als u met Mozilla Thunderbird werkt, worden berichten die zijn verstuurd via het IMAP-protocol niet door Mail Anti-Virus gescand op virussen en andere bedreigingen als u filters gebruikt om berichten vanuit de map **Inbox** te verplaatsen.

Het beschermingsniveau voor e-mails wijzigen

Mail Anti-Virus past verschillende groepen van instellingen toe om e-mails te beschermen. De groepen van instellingen worden *beschermingsniveaus voor e-mails* genoemd. Er bestaan drie vooraf geïnstalleerde beschermingsniveaus voor e-mails: **Hoog**, **Aanbevolen** en **Laag**. Het beschermingsniveau **Aanbevolen** voor bestanden wordt als de optimale groep van instellingen beschouwd en wordt door Kaspersky aanbevolen.

Zo wijzigt u het beschermingsniveau voor e-mails:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Doe in het gedeelte **Beschermingsniveau** een van het volgende:

   - Als u een van de vooraf geïnstalleerde beschermingsniveaus voor e-mails (**Hoog**, **Aanbevolen** of **Laag**) wilt installeren, gebruikt u de schuifregelaar om er een te selecteren.
   - Als u een aangepast beschermingsniveau voor e-mails wilt configureren, klikt u op de knop **Instellingen** en geeft u in het venster **Mail Anti-Virus** instellingen op.

Nadat u een aangepast beschermingsniveau voor e-mails hebt geconfigureerd, wordt de naam van het beschermingsniveau in het gedeelte **Beschermingsniveau** gewijzigd in **Aangepast**.

- Als u het beschermingsniveau voor e-mails wilt wijzigen in **Aanbevolen**, klikt u op de knop **Standaard**.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De uit te voeren actie op geïnfecteerde e-mailberichten wijzigen

Zo wijzigt u de actie die op geïnfecteerde e-mailberichten moet worden uitgevoerd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Selecteer in het gedeelte **Actie bij detectie van een bedreiging** de actie die Kaspersky Endpoint Security moet uitvoeren wanneer een geïnfecteerd bericht wordt gevonden:
   - **Actie automatisch selecteren**.
   - **Voer actie uit: Desinfecteren. Verwijderen als desinfectie mislukt**.
   - **Voer actie uit: Desinfecteren**.
   - **Voer actie uit: Verwijderen**.
   - **Voer actie uit: Blokkeren**.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het beschermd bereik van Mail Anti-Virus bewerken

Onder het beschermd bereik verstaan we de objecten die door het onderdeel worden gescand wanneer het actief is. De beschermde bereiken van de verschillende onderdelen hebben verschillende eigenschappen. De eigenschappen van het beschermd bereik van Mail Anti-Virus omvatten de instellingen voor de integratie van Mail Anti-Virus in e-mailprogramma's en het type e-mailberichten en het verkeer van de e-mailprotocollen die door Mail Anti-Virus worden gescand. Standaard scant Kaspersky Endpoint Security zowel inkomende als uitgaande e-mailberichten en het verkeer van de protocollen POP3, SMTP, NNTP en IMAP. Het is ook geïntegreerd in het e-mailprogramma Microsoft Office Outlook.

Zo maakt u het beschermd bereik van Mail Anti-Virus aan:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Klik op de knop **Instellingen**.

Het venster **Mail Anti-Virus** wordt geopend.

4. Selecteer het tabblad **Algemeen**.

5. Doe in het gedeelte **Beschermd bereik** een van het volgende:

   - Selecteer de optie **Inkomende en uitgaande berichten** als u wilt dat Mail Anti-Virus alle inkomende en uitgaande berichten op de computer scant.

   - Selecteer de optie **Alleen inkomende berichten** als u wilt dat Mail Anti-Virus alleen inkomende berichten op de computer scant.

     Als u ervoor kiest om alleen inkomende berichten te scannen, wordt u aanbevolen om een eenmalige scan van alle uitgaande berichten uit te voeren omdat de computer geïnfecteerd kan zijn met e-mailwormen die zich via e-mail verspreiden. Op deze manier vermijdt u problemen door een niet-gemonitorde, massale verzending van geïnfecteerde berichten vanaf de computer.

6. Doe in het gedeelte **Connectiviteit** het volgende:

   - Schakel het selectievakje **POP3- / SMTP- / NNTP- / IMAP-verkeer** in als u wilt dat Mail Anti-Virus berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP en IMAP scant voordat ze op de computer terechtkomen.

     Schakel het selectievakje **POP3- / SMTP- / NNTP- / IMAP-verkeer** uit als u niet wilt dat Mail Anti-Virus berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP en IMAP scant voordat ze op de computer terechtkomen. In dit geval worden berichten gescand door de extensie van Mail Anti-Virus die in het e-mailprogramma Microsoft Office Outlook is ingebed. Dit gebeurt nadat de berichten door de computer van de gebruiker zijn ontvangen en als het selectievakje **Extra: Microsoft Office Outlook-extensie** is ingeschakeld.

     Als u een ander e-mailprogramma dan Microsoft Office Outlook gebruikt en het selectievakje **POP3- / SMTP- / NNTP- / IMAP-verkeer** is uitgeschakeld, worden berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP en IMAP niet gescand door Mail Anti-Virus.

   - Als u de instellingen van Mail Anti-Virus vanuit Microsoft Office Outlook wilt openen en het scannen van berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP, IMAP en MAPI nadat ze zijn gedownload door de computer wilt inschakelen via de ingebedde extensie in Microsoft Office Outlook, schakelt u het selectievakje **Extra: Microsoft Office Outlook-extensie** in.

     Als u de toegang tot de instellingen van Mail Anti-Virus vanuit Microsoft Office Outlook wilt blokkeren en het scannen van berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP, IMAP en MAPI nadat ze zijn gedownload door de computer wilt uitschakelen via de ingebedde extensie in Microsoft Office Outlook , schakelt u het selectievakje **Extra: Microsoft Office Outlook-extensie** uit.

     De extensie van Mail Anti-Virus wordt tijdens de installatie van Kaspersky Endpoint Security ingesloten in Microsoft Office Outlook.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Samengestelde bestanden die zijn toegevoegd als bijlage aan e-mailberichten scannen

Zo configureert u het scannen van samengestelde bestanden die als bijlage aan e-mailberichten zijn toegevoegd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Klik op de knop **Instellingen**.

   Het venster **Mail Anti-Virus** wordt geopend.
4. Selecteer het tabblad **Algemeen**.
5. Voer het volgende uit in het gedeelte **Scan van samengestelde bestanden**:

   - Als u wilt dat Mail Anti-Virus archieven die zijn toegevoegd aan berichten overslaat, schakelt u het selectievakje **Scan toegevoegde archieven** uit.
   - Als u wilt dat Mail Anti-Virus bijlagen van berichten die groter zijn dan N megabytes overslaat, schakelt u het selectievakje **Scan geen archiefbestanden groter dan N MB** in. Als u dit selectievakje inschakelt, geeft u de maximale grootte voor archieven op in het veld naast de naam van het selectievakje.
   - Als u wilt dat Mail Anti-Virus bijlagen van berichten scant waarvan de scan meer dan N seconden duurt, schakelt u het selectievakje **Scan archieven niet langer dan** N s uit.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bijlagen van e-mailberichten filteren

Kwaadaardige programma's kunnen als bijlagen in e-mailberichten worden verspreid. U kunt een filter op basis van het soort bijlagen van berichten configureren zodat bestanden van het opgegeven type automatisch een andere naam krijgen of worden verwijderd. Door de naam van een bepaald type bijlage te wijzigen kan Kaspersky Endpoint Security de computer beschermen tegen de automatische uitvoering van een kwaadaardig programma.

Zo configureert u een filter voor bijlagen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Mail Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Mail Anti-Virus.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Het venster **Mail Anti-Virus** wordt geopend.

4. Selecteer in het venster **Mail Anti-Virus** het tabblad **Filter voor bijlagen**.

5. Voer een van de volgende acties uit:

   - Selecteer de optie **Filteren uitschakelen** als u niet wilt dat Mail Anti-Virus bijlagen van berichten filtert.

   - Als u wilt dat Mail Anti-Virus de namen van de **opgegeven typen** bijlagen in berichten wijzigt, selecteert u de optie **Naam van opgegeven typen bijlagen wijzigen**.

De werkelijke indeling van een bestand komt mogelijk niet overeen met de bestandsnaamextensie.

Als u een filter inschakelt voor objecten die als bijlage in e-mailberichten zijn toegevoegd, kan Mail Anti-Virus bestanden met de volgende extensies hernoemen of verwijderen:

com – uitvoerbaar bestand van een programma dat maximaal 64 KB groot is

exe – uitvoerbaar bestand of zelfuitpakkend archief

sys – Microsoft Windows-systeembestand

prg – programmatekst voor dBase™, Clipper of Microsoft Visual FoxPro® of een WAVmaker-programma

bin – binair bestand

bat – batchbestand

cmd – opdrachtbestand voor Microsoft Windows NT (vergelijkbaar met een bat-bestand voor DOS), OS/2

dpl – gecomprimeerde Borland Delphi-bibliotheek

dll – dynamic link library

scr – Microsoft Windows-welkomstscherm

cpl – module van Microsoft Windows-configuratiescherm

ocx – Microsoft OLE-object (Object Linking and Embedding)

tsp – programma in gedeelde-tijdmodus

drv – stuurprogramma van apparaat

vxd – virtueel-apparaatstuurprogramma van Microsoft Windows

pif – programma-informatiebestand

lnk – Microsoft Windows-koppelingsbestand

reg – sleutelbestand voor Microsoft Windows-systeemregister

ini – configuratiebestand met configuratiegegevens voor Microsoft Windows, Windows NT en bepaalde programma's

cla – Java-klasse

vbs – Visual Basic®-script

vbe – BIOS-video-extensie

js, jse – JavaScript-brontekst

htm – hypertekstdocument

htt – Microsoft Windows-hypertekstkop

hta – hypertekstprogramma voor Microsoft Internet Explorer®

asp – Active Server Pages-script

chm – gecompileerd HTML-bestand

pht – HTML-bestand met geïntegreerde PHP-scripts

php – script dat in HTML-bestanden is geïntegreerd

wsh – Microsoft Windows Script Host-bestand

wsf – Microsoft Windows-script

the – bestand van Microsoft Windows 95-bureaubladachtergrond

hlp – Win Help-bestand

eml – Microsoft Outlook Express-bericht

nws – nieuw Microsoft Outlook Express-e-mailbericht

msg – Microsoft Mail-e-mailbericht

plg – e-mailbericht

mbx – extensie voor opgeslagen Microsoft Office Outlook-e-mails

doc* – Microsoft Office Word-documenten zoals: doc voor Microsoft Office Word-documenten, docx voor Microsoft Office Word 2007-documenten met XML-ondersteuning en docm voor Microsoft Office Word 2007-documenten met macro-ondersteuning

dot* – Microsoft Office Word-documentsjablonen zoals: dot voor Microsoft Office Word-documentsjablonen, dotx voor Microsoft Office Word 2007-documentsjablonen, dotm voor Microsoft Office Word 2007-documentsjablonen met macro-ondersteuning

fpm – databaseprogramma, Microsoft Visual FoxPro-opstartbestand

rtf – Rich Text Format-document

shs – Windows Shell Scrap Object Handler-fragment

dwg – AutoCAD®-tekeningdatabase

msi – Microsoft Windows Installer-pakket

otm – VBA-project voor Microsoft Office Outlook

pdf – Adobe Acrobat-document

swf – Shockwave® Flash-pakketobject

jpg, jpeg – indeling van gecomprimeerde afbeeldingen

emf – Enhanced Metafile-indelingsbestand. Volgende generatie van Microsoft Windows OS-metabestanden. EMF-bestanden worden niet ondersteund door 16-bits Microsoft Windows-versies.

ico – pictogrambestand van object

ov? – uitvoerbare Microsoft Office Word-bestanden

xl* – Microsoft Office Excel-documenten en bestanden zoals: xla, de extensie voor Microsoft Office Excel, xlc voor diagrammen, xlt voor documentsjablonen, xlsx voor Microsoft Office Excel 2007-werkmappen, xltm voor Microsoft Office Excel 2007-werkmappen met macro-ondersteuning, xlsb voor Microsoft Office Excel 2007-werkboeken in binaire indeling (niet-XML), xltx voor Microsoft Office Excel 2007-sjablonen, xlsm voor Microsoft Office Excel 2007-sjablonen met macro-ondersteuning en xlam voor Microsoft Office Excel 2007-invoegtoepassingen met macro-ondersteuning

pp* – Microsoft Office PowerPoint®-documenten en bestanden zoals: pps voor Microsoft Office PowerPoint-dia's, ppt voor presentaties, pptx voor Microsoft Office PowerPoint 2007-presentaties, pptm voor Microsoft Office PowerPoint 2007-presentaties met macro-ondersteuning, potx voor Microsoft Office PowerPoint 2007-presentatiesjablonen, potm voor Microsoft Office PowerPoint 2007-presentatiesjablonen met macro-ondersteuning, ppsx voor Microsoft Office PowerPoint 2007-diavoorstellingen, ppsm voor Microsoft Office PowerPoint 2007-diavoorstellingen met macro-ondersteuning en ppam voor Microsoft Office PowerPoint 2007-invoegtoepassingen met macro-ondersteuning

md* – Microsoft Office Access®-documenten en -bestanden zoals: mda voor Microsoft Office Access-werkgroepen en mdb voor databases

sldx – een Microsoft PowerPoint 2007-dia

sldm – een Microsoft PowerPoint 2007-dia met macro-ondersteuning

thmx – een Microsoft Office 2007-thema

- Als u wilt dat Mail Anti-Virus de opgegeven typen bijlagen in berichten verwijdert, selecteert u de optie **Opgegeven typen bijlagen verwijderen**.

6. Als u tijdens de vorige stap de opties **Naam van opgegeven typen bijlagen wijzigen** of **Opgegeven typen bijlagen verwijderen** hebt geselecteerd, schakelt u de selectievakjes naast de relevante typen bestanden in.

   U kunt de lijst met bestandstypen wijzigen met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

E-mails in Microsoft Office Outlook scannen

Tijdens de installatie van Kaspersky Endpoint Security wordt de extensie van Mail Anti-Virus ingesloten in Microsoft Office Outlook (hierna ook Outlook genoemd). Hiermee kunt u de instellingen van Mail Anti-Virus vanuit Outlook openen en kunt u opgeven welke e-mailberichten moeten worden gescand op virussen en andere bedreigingen. De extensie van Mail Anti-Virus voor Outlook kan inkomende en uitgaande berichten scannen die via de protocollen POP3, SMTP, NNTP, IMAP en MAPI worden verstuurd en ontvangen.

De instellingen van Mail Anti-Virus kunnen rechtstreeks in Outlook worden geconfigureerd als het selectievakje **Extra: Microsoft Office Outlook-extensie** in de interface van Kaspersky Endpoint Security is ingeschakeld.

In Outlook worden inkomende berichten eerst gescand door Mail Anti-Virus (als het selectievakje **POP3- / SMTP- / NNTP- / IMAP-verkeer** in de interface van Kaspersky Endpoint Security is ingeschakeld) en dan door de extensie van Mail Anti-Virus voor Outlook. Als Mail Anti-Virus een kwaadaardig object in een bericht vindt, geeft het een melding voor deze gebeurtenis weer.

Uw gekozen actie in het venster van de melding bepaalt werk onderdeel de bedreiging in het bericht moet elimineren: Mail Anti-Virus of de extensie van Mail Anti-Virus voor Outlook.

- Als u **Desinfecteren** of **Verwijderen** in het venster van de melding selecteert, elimineert Mail Anti-Virus de bedreiging.
- Als u **Overslaan** in het venster van de melding selecteert, elimineert de extensie van Mail Anti-Virus voor Outlook de bedreiging.

Uitgaande berichten worden eerst gescand door de extensie van Mail Anti-Virus voor Outlook en dan door Mail Anti-Virus.

Het scannen van e-mail configureren in Outlook

Zo configureert u het scannen van e-mail in Outlook 2007:

1. Open het hoofdvenster van Outlook 2007.
2. Selecteer **Service** → **Instellingen** in de menubalk.

   Het venster **Opties** wordt geopend.
3. Selecteer in het venster **Opties** het tabblad **E-mailbeveiliging**.

Zo configureert u het scannen van e-mail in Outlook 2010 / 2013:

1. Open het hoofdvenster van Outlook.

   Selecteer het tabblad **Bestand** in de linkerbovenhoek.
2. Klik op de knop **Opties**.

   Het venster **Opties voor Outlook** wordt geopend.
3. Selecteer het gedeelte **Invoegtoepassingen**.

   Rechts in het venster ziet u de instellingen van plug-ins die in Outlook zijn ingebed.

4. Klik op de knop **Opties invoegtoepassing**.

Het scannen van e-mail configureren via Kaspersky Security Center

Als e-mail wordt gescand met de Mail Anti-Virus-extensie voor Outlook, wordt u aanbevolen de Exchange-modus met cache te gebruiken. Voor meer gedetailleerde informatie over de Exchange-modus met cache en aanbevelingen voor het gebruik ervan, raadpleegt u de Microsoft Knowledge Base: https://technet.microsoft.com/nl-nl/library/cc179175.aspx.

Zo configureert u de modus van de Mail Anti-Virus-extensie voor Outlook via Kaspersky Security Center:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u het scannen van e-mail wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Antivirusbescherming** het subgedeelte **Mail Anti-Virus**.
7. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.
   Het venster **Mail Anti-Virus** wordt geopend.
8. Klik in het gedeelte **Connectiviteit** op de knop **Instellingen**.
   Het venster **E-mailbescherming** wordt geopend.
9. In het venster **E-mailbescherming**:
   - Schakel het selectievakje **Scannen bij ontvangen** in als u wilt dat de Mail Anti-Virus-extensie voor Outlook inkomende berichten scant wanneer ze in het postvak IN belanden.
   - Schakel het selectievakje **Scannen bij lezen** in als u wilt dat de Mail Anti-Virus-extensie voor Outlook inkomende berichten scant wanneer de gebruiker ze opent.
   - Schakel het selectievakje **Scannen bij verzenden** in als u wilt dat de Mail Anti-Virus-extensie voor Outlook uitgaande berichten scant wanneer ze worden verzonden.
10. Klik in het venster **E-mailbescherming** op **OK**.
11. Klik in het venster **Mail Anti-Virus** op **OK**.
12. Pas het beleid toe.

Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Computerbescherming op het internet. Web Anti-Virus

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Web Anti-Virus en leest u hoe u de instellingen van het onderdeel configureert.

Over Web Anti-Virus

Telkens als u online gaat, stelt u informatie op de computer bloot aan virussen en andere malware. Deze kunnen de computer infiltreren wanneer de gebruiker gratis software downloadt of websites bezoekt die criminelen hebben ontwikkeld. Netwerkwormen kunnen zich een weg naar uw computer banen zodra u verbinding maakt met het internet, zelfs voordat als u nog geen webpagina hebt geopend of een bestand hebt gedownload.

Web Anti-Virus beschermt inkomende en uitgaande gegevens die van en naar de computer worden verzonden via de protocollen HTTP en FTP en controleert of URL's voorkomen in de lijst met kwaadaardige of phishingadressen.

Web Anti-Virus onderschept en analyseert alle webpagina's of bestanden die door de gebruiker of een programma via het HTTP- of FTP-protocol worden geopend op virussen en andere bedreigingen. Daarna gebeurt het volgende:

- Als geen kwaadaardige code op de pagina of in het bestand wordt gevonden, krijgt de gebruiker onmiddellijk toegang ertoe.
- Als de gebruiker webpagina's of bestanden opent die kwaadaardige code bevatten, voert het programma de actie uit die in de instellingen van Web Anti-Virus is opgegeven.

Web Anti-Virus inschakelen en uitschakelen

Web Anti-Virus is standaard ingeschakeld en werkt in een modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig Web Anti-Virus uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Web Anti-Virus in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.

   Het gedeelte **Bescherming** wordt geopend.

4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Web Anti-Virus bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.

5. Voer een van de volgende acties uit:

   - Selecteer **Starten** in het menu om Web Anti-Virus in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Web Anti-Virus**, wijzigt in het pictogram .

   - Selecteer **Stoppen** in het menu om Web Anti-Virus uit te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Web Anti-Virus**, wijzigt in het pictogram .

Zo schakelt u Web Anti-Virus in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.

3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Web Anti-Virus inschakelen** in om Web Anti-Virus in te schakelen.
   - Schakel het selectievakje **Web Anti-Virus inschakelen** uit om Web Anti-Virus uit te schakelen.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Web Anti-Virus configureren

U kunt het volgende doen om Web Anti-Virus te configureren:

- Wijzig het beschermingsniveau voor internetverkeer.

  U kunt een van de vooraf geïnstalleerde beschermingsniveaus selecteren voor het internetverkeer dat via de HTTP- en FTP-protocollen wordt verstuurd of u kunt een aangepast beschermingsniveau voor internetverkeer configureren.

  Als u de instellingen van het beschermingsniveau voor het internetverkeer wijzigt, kunt u altijd de aanbevolen instellingen van het beschermingsniveau voor het internetverkeer herstellen.

- Wijzig de actie die Kaspersky Endpoint Security uitvoert op kwaadaardige objecten uit het internetverkeer.

  Als de analyse van een HTTP-object aangeeft dat het kwaadaardige code bevat, hangt het antwoord van Web Anti-Virus af van de actie die u hebt opgegeven.

- Configureer of Web Anti-Virus moet controleren of URL's voorkomen in de databases met phishing- en kwaadaardige webadressen.

- Configureer het gebruik van de heuristische analyse tijdens het scannen van internetverkeer op virussen en andere kwaadaardige programma's.

  Om de doeltreffendheid van de bescherming te verhogen, kunt u de heuristische analyse gebruiken. Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van programma's in het besturingssysteem. De heuristische analyse kan bedreigingen vinden die momenteel niet voorkomen in de databases van Kaspersky Endpoint Security.

- Configureer het gebruik van de heuristische analyse tijdens het scannen van webpagina's op phishingkoppelingen.
- Optimaliseer de scans die Web Anti-Virus uitvoert op het internetverkeer dat via de protocollen HTTP en FTP wordt verstuurd en ontvangen.
- Maak een lijst met vertrouwde URL's.

  U kunt een lijst met URL's maken waarvan u de inhoud vertrouwt. Web Anti-Virus controleert geen gegevens van vertrouwde URL's op virussen of andere bedreigingen. Deze optie kan bijvoorbeeld nuttig zijn wanneer Web Anti-Virus de download van een bestand vanaf een bekende website hindert.

  Een URL kan het adres van een specifieke webpagina of het adres van een website zijn.

Het beschermingsniveau voor internetverkeer wijzigen

Web Anti-Virus past verschillende groepen van instellingen toe om gegevens te beschermen die via de protocollen HTTP en FTP worden ontvangen en verzonden. Deze groepen van instellingen worden *beschermingsniveaus voor internetverkeer* genoemd. Er bestaan drie vooraf geïnstalleerde beschermingsniveaus voor internetverkeer: **Hoog**, **Aanbevolen** en **Laag**. Het beschermingsniveau **Aanbevolen** voor internetverkeer wordt als de optimale groep van instellingen beschouwd en wordt door Kaspersky aanbevolen.

Zo wijzigt u het beschermingsniveau voor internetverkeer:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.
3. Doe in het gedeelte **Beschermingsniveau** een van het volgende:
   - Als u een van de vooraf geïnstalleerde beschermingsniveaus voor internetverkeer (**Hoog**, **Aanbevolen** of **Laag**) wilt installeren, gebruikt u de schuifregelaar om er een te selecteren.
   - Als u een aangepast beschermingsniveau voor internetverkeer wilt configureren, klikt u op de knop **Instellingen** en geeft u in het venster **Web Anti-Virus** instellingen op.

     Wanneer u een aangepast beschermingsniveau voor internetverkeer hebt geconfigureerd, wordt de naam van het beschermingsniveau in het gedeelte **Beschermingsniveau** gewijzigd in **Aangepast**.
   - Als u het beschermingsniveau voor internetverkeer wilt wijzigen in **Aanbevolen**, klikt u op de knop **Standaard**.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De uit te voeren actie op kwaadaardige objecten uit het internetverkeer wijzigen

Zo wijzigt u de actie die op kwaadaardige objecten uit het internetverkeer moet worden uitgevoerd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.
3. Selecteer in het gedeelte **Actie bij detectie van een bedreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op kwaadaardige objecten uit het internetverkeer:
   - **Actie automatisch selecteren**.
   - **Download blokkeren**.
   - **Download toestaan**.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Web Anti-Virus laten controleren of URL's voorkomen in de databases van kwaadaardige en phishingadressen

Door te controleren of koppelingen voorkomen in de lijst met phishingadressen kunt u *phishingaanvallen* vermijden. Een phishingaanval kan bijvoorbeeld vermomd zijn als een e-mailbericht van uw bank met een koppeling naar de officiële website van de bank. Door op de koppeling te klikken gaat u naar een exacte kopie van de website van de bank en kunt u zelfs het echte webadres ervan in de browser zien, hoewel u zich toch op een vervalste website bevindt. Vanaf dit punt worden al uw acties op de website bijgehouden en kunnen die worden gebruikt om uw geld te stelen.

Omdat koppelingen naar phishingwebsites niet alleen via e-mailberichten worden ontvangen maar ook vanaf andere bronnen zoals ICQ-berichten, monitort Web Anti-Virus pogingen tot het openen van een phishingwebsite op het niveau van het internetverkeer en blokkeert het de toegang tot die websites. De lijst met phishing-URL's is een onderdeel van het distributiepakket van Kaspersky Endpoint Security.

Zo configureert u of Web Anti-Virus moet controleren of URL's voorkomen in de databases met phishing- en kwaadaardige webadressen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.
3. Klik op de knop **Instellingen**.

   Het venster **Web Anti-Virus** wordt geopend.
4. Selecteer in het venster **Web Anti-Virus** het tabblad **Algemeen**.
5. Doe het volgende:
   - Als u wilt dat Web Anti-Virus controleert of URL's voorkomen in de databases van kwaadaardige webadressen, schakelt u in het gedeelte **Scanmethoden** het selectievakje **Controleer of koppelingen voorkomen in de database van kwaadaardige koppelingen** in.
   - Als u wilt dat Web Anti-Virus controleert of URL's voorkomen in de databases van phishingadressen, schakelt u in het gedeelte **Instellingen van Anti-Phishing** het selectievakje **Controleer of koppelingen**

voorkomen in de database van phishing-koppelingen in.

U kunt ook controleren of koppelingen voorkomen in de reputatiedatabases van Kaspersky Security Network.

6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De heuristische scanner met Web Anti-Virus gebruiken

Zo configureert u het gebruik van de heuristische analyse:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.
   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.
   Het venster **Web Anti-Virus** wordt geopend.
4. Selecteer het tabblad **Algemeen**.
5. Als u wilt dat Web Anti-Virus de heuristische analyse gebruikt om het internetverkeer op virussen en andere malware te scannen, schakelt u in het gedeelte **Scanmethoden** het selectievakje **Heuristische analyse voor detectie van virussen** in en gebruikt u de schuifregelaar om het niveau van de heuristische analyse in te stellen: **Oppervlakkige scan**, **Gemiddelde scan** of **Gedetailleerde scan**.
6. Als u wilt dat Web Anti-Virus de heuristische analyse gebruikt om webpagina's te scannen op phishingkoppelingen, schakelt u in het gedeelte **Instellingen van Anti-Phishing** het selectievakje **Heuristische analyse voor detectie van phishingkoppelingen** in.
7. Klik op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De lijst met vertrouwde URL's bewerken

Zo maakt u een lijst met vertrouwde URL's:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Web Anti-Virus**.
   Rechts in het venster ziet u de instellingen van het onderdeel Web Anti-Virus.
3. Klik op de knop **Instellingen**.
   Het venster **Web Anti-Virus** wordt geopend.

4. Selecteer het tabblad **Vertrouwde URL's**.

5. Schakel het selectievakje **Scan geen internetverkeer van vertrouwde webadressen** in.

6. Maak een lijst met URL's / webpagina's waarvan u de inhoud vertrouwt. Zo maakt u een lijst aan:

    a. Klik op de knop **Toevoegen**.
    Het venster **Webadres / Webadresmasker** wordt geopend.

    b. Voer het adres van de website / webpagina of het adresmasker van de website / webpagina in.

    c. Klik op **OK**.
    Een nieuwe record wordt in de lijst met vertrouwde URL's weergegeven.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bescherming van chatberichten. IM Anti-Virus

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over IM Anti-Virus en leest u hoe u de instellingen van het onderdeel configureert.

Over IM Anti-Virus

IM Anti-Virus scant het verkeer van chatprogramma's (ook wel *instant messengers* genoemd).

IM Anti-Virus scant geen berichten die via geëncrypte kanalen worden verstuurd.

Berichten die via chatprogramma's worden verstuurd, kunnen de volgende soorten bedreigingen bevatten:

- URL's die proberen om een kwaadaardig programma te downloaden naar de computer
- URL's naar kwaadaardige programma's en websites die indringers gebruiken voor phishingaanvallen

  Phishingaanvallen dienen om de persoonlijke gegevens van gebruikers te stelen, zoals nummers van bankpassen, gegevens van paspoorten, wachtwoorden voor betaalsystemen van banken en andere online diensten (zoals sites van sociale netwerken of e-mailaccounts).

Bestanden kunnen via chatprogramma's worden verstuurd. Bij pogingen tot het opslaan van die bestanden worden ze gescand door het onderdeel Anti-Virus voor bestanden.

IM Anti-Virus onderschept elk bericht dat de gebruiker verstuurt of ontvangt via een chatprogramma en scant het op koppelingen die de beveiliging van de computer kunnen aantasten:

- Als geen gevaarlijke URL's in het bericht worden gevonden, wordt het beschikbaar gemaakt voor de gebruiker.
- Als gevaarlijke koppelingen in het bericht worden gevonden, vervangt IM Anti-Virus het bericht door informatie over de bedreiging in het berichtvenster van het actieve chatprogramma.

IM Anti-Virus inschakelen en uitschakelen

IM Anti-Virus is standaard ingeschakeld en werkt in een modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig IM Anti-Virus uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u IM Anti-Virus in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.
   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts op de regel **IM Anti-Virus** om het contextmenu met acties van het onderdeel te openen.
5. Voer een van de volgende acties uit:
   - Selecteer **Starten** in het menu om IM Anti-Virus in te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **IM Anti-Virus**, wijzigt in het pictogram .
   - Selecteer **Stoppen** in het menu om IM Anti-Virus uit te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **IM Anti-Virus**, wijzigt in het pictogram .

Zo schakelt u IM Anti-Virus in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **IM Anti-Virus**.
   Rechts in het venster ziet u de instellingen van het onderdeel IM Anti-Virus.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **IM Anti-Virus inschakelen** in om IM Anti-Virus in te schakelen.
   - Schakel het selectievakje **IM Anti-Virus inschakelen** uit om IM Anti-Virus uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

IM Anti-Virus configureren

U kunt de volgende acties uitvoeren om IM Anti-Virus te configureren:

- Configureer het beschermd bereik.
  U kunt het beschermd bereik vergroten of verkleinen door te wijzigen welke soort chatberichten moeten worden gescand.
- Configureer of IM Anti-Virus moet controleren of koppelingen in chatberichten voorkomen in de databases van kwaadaardige en phishingadressen.

Het beschermd bereik van IM Anti-Virus aanmaken

Het beschermd bereik verwijst naar de objecten die het onderdeel scant wanneer het is ingeschakeld. De beschermde bereiken van de verschillende onderdelen hebben verschillende eigenschappen. Het type van gescande chatberichten, inkomend of uitgaand, is een eigenschap van het beschermd bereik van IM Anti-Virus. IM Anti-Virus scant standaard zowel inkomende als uitgaande berichten. U kunt het scannen van uitgaand verkeer uitschakelen.

Zo maakt u het beschermd bereik aan:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **IM Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel IM Anti-Virus.
3. Doe in het gedeelte **Beschermd bereik** een van het volgende:
   - Selecteer de optie **Inkomende en uitgaande berichten** als u wilt dat IM Anti-Virus alle inkomende en uitgaande berichten van chatprogramma's scant.
   - Selecteer de optie **Alleen inkomende berichten** als u wilt dat IM Anti-Virus alleen inkomende berichten van chatprogramma's scant.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

IM Anti-Virus laten controleren of URL's voorkomen in de databases van kwaadaardige en phishing-URL's

Zo configureert u of IM Anti-Virus moet controleren of URL's voorkomen in de databases met kwaadaardige en phishingadressen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **IM Anti-Virus**.

   Rechts in het venster ziet u de instellingen van het onderdeel IM Anti-Virus.
3. Selecteer in het gedeelte **Scanmethoden** de methoden die u IM Anti-Virus wilt laten gebruiken:
   - Als u wilt controleren of koppelingen in chatberichten voorkomen in de database van kwaadaardige webadressen, schakelt u het selectievakje **Controleer of koppelingen voorkomen in de database van kwaadaardige koppelingen** in.
   - Als u wilt controleren of koppelingen in chatberichten voorkomen in de database van phishingadressen, schakelt u het selectievakje **Controleer of koppelingen voorkomen in de database van phishingkoppelingen** in.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Systeembewaking

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Systeembewaking en leest u hoe u de instellingen van het onderdeel configureert.

Over Systeembewaking

Systeembewaking verzamelt gegevens over de acties van programma's op de computer en geeft deze informatie door aan andere onderdelen voor een meer betrouwbare bescherming.

Behavior Stream Signatures

Behavior Stream Signatures (BSS) (ook "behavior stream signatures" genoemd) bevat reeksen van programma-acties die als gevaarlijk zijn geclassificeerd door Kaspersky Endpoint Security. Als een programma-activiteit overeenkomt met een behavior stream signature, voert Kaspersky Endpoint Security de opgegeven actie uit. De functionaliteit van Kaspersky Endpoint Security op basis van de behavior stream signatures levert een proactieve bescherming voor de computer.

Als een programma-activiteit overeenkomt met een behavior stream signature, plaatst Systeembewaking standaard het uitvoerbare bestand van dat programma in Quarantaine.

Acties van malware terugdraaien

Op basis van de door Systeembewaking verzamelde informatie kan Kaspersky Endpoint Security tijdens de desinfectie **de acties terugdraaien die door de malware in het besturingssysteem zijn uitgevoerd**.

Wanneer activiteit van malware in het besturingssysteem wordt teruggedraaid, onderneemt Kaspersky Endpoint Security acties voor de volgende soorten activiteit van malware:

- Bestandsactiviteit.

  Kaspersky Endpoint Security verwijdert uitvoerbare bestanden die door een kwaadaardig programma zijn aangemaakt en op alle media behalve netwerkmedia staan.

  Kaspersky Endpoint Security verwijdert uitvoerbare bestanden die zijn aangemaakt door een programma waarin een kwaadaardig programma is binnengedrongen.

  Kaspersky Endpoint Security herstelt geen gewijzigde of verwijderde bestanden.

- Registeractiviteit.

  Kaspersky Endpoint Security verwijdert partities en registersleutels die door malware zijn aangemaakt.

  Kaspersky Endpoint Security herstelt geen gewijzigde of verwijderde partities en registersleutels.

- Systeemactiviteit.

  Kaspersky Endpoint Security beëindigt processen die door een kwaadaardig programma zijn gestart.

  Kaspersky Endpoint Security beëindigt processen waarin een kwaadaardig programma is binnengedrongen.

  Kaspersky Endpoint Security hervat geen processen die door een kwaadaardig programma zijn gestopt.

- Netwerkactiviteit.

  Kaspersky Endpoint Security blokkeert de netwerkactiviteit van kwaadaardige programma's.

  Kaspersky Endpoint Security blokkeert de netwerkactiviteit van processen waarin een kwaadaardig programma is binnengedrongen.

Het terugdraaien van malwareacties kan door Anti-Virus voor bestanden of tijdens een virusscan worden gestart.

Het terugdraaien van malwareacties is van invloed op een specifieke reeks gegevens. Het terugdraaien heeft geen negatieve effecten op het besturingssysteem of de integriteit van uw gegevens op de computer.

Systeembewaking inschakelen en uitschakelen

Systeembewaking is standaard ingeschakeld en werkt in de modus die door Kaspersky is aanbevolen. U kunt indien nodig Systeembewaking uitschakelen.

U wordt afgeraden om Systeembewaking uit te schakelen tenzij dit echt nodig is. De uitschakeling is immers van invloed op de prestaties van de beschermingsonderdelen. De beschermingsonderdelen kunnen de door Systeembewaking verzamelde gegevens opvragen om een gevonden bedreiging beter te identificeren.

Systeembewaking kan op twee manieren worden ingeschakeld of uitgeschakeld:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

*Zo schakelt u Systeembewaking in of uit op het tabblad **Bescherming en controle** van het hoofdvenster van het programma:*

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.

   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Systeembewaking bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:

   - Selecteer **Starten** om Systeembewaking in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Systeembewaking**, wijzigt in het pictogram .
   - Selecteer **Stoppen** om Systeembewaking uit te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Systeembewaking**, wijzigt in het pictogram .

Zo schakelt u Systeembewaking in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Systeembewaking**.

   Rechts in het venster ziet u de instellingen van het onderdeel **Systeembewaking**.
3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Systeembewaking inschakelen** in om Systeembewaking in te schakelen.
   - Schakel het selectievakje **Systeembewaking inschakelen** uit om Systeembewaking uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Systeembewaking configureren

U kunt het volgende doen om Systeembewaking te configureren:

- bescherming tegen exploits inschakelen of uitschakelen;
- actie kiezen bij de detectie van kwaadaardige activiteit in een programma;
- Het terugdraaien van malwareacties tijdens de desinfectie inschakelen of uitschakelen.

Bescherming tegen exploits inschakelen of uitschakelen

Zo schakelt u de bescherming tegen exploits in of uit:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Systeembewaking**.

   Rechts in het venster ziet u de instellingen van het onderdeel **Systeembewaking**.

3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Exploitpreventie inschakelen** in als u wilt dat de bestanden die kwetsbare programma's gebruiken wanneer ze worden gestart worden gemonitord door Kaspersky Endpoint Security.

     Als Kaspersky Endpoint Security detecteert dat een bestand dat wordt gebruikt door een kwetsbaar programma niet is gestart door de gebruiker, zal het handelen naargelang uw keuze uit de pop-uplijst **Actie bij detectie van een bedreiging**.

   - Schakel het selectievakje **Exploitpreventie inschakelen** in als u wilt dat de bestanden die kwetsbare programma's gebruiken wanneer ze worden gestart worden gemonitord door Kaspersky Endpoint Security.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Actie kiezen bij de detectie van kwaadaardige activiteit in een programma

Volg de volgende stappen om te kiezen wat u wilt doen als een programma kwaadaardige activiteit vertoont:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Systeembewaking**.

   Rechts in het venster ziet u de instellingen van het onderdeel **Systeembewaking**.

3. Kies in het gedeelte **Actie bij detectie van een bedreiging** een van de volgende acties in de pop-uplijst **Bij detectie van malware-activiteit**:

   - **Actie automatisch selecteren**.
   - **Bestand in quarantaine plaatsen**.
   - **Kwaadaardig programma beëindigen**.
   - **Overslaan**.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het terugdraaien van malwareacties tijdens de desinfectie inschakelen of uitschakelen

Zo schakelt u het terugdraaien van malwareacties tijdens de desinfectie in of uit:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Systeembewaking**.

   Rechts in het venster ziet u de instellingen van het onderdeel **Systeembewaking**.

3. Voer een van de volgende acties uit:

- Als u wilt dat Kaspersky Endpoint Security tijdens de desinfectie de acties terugdraait die door malware in het besturingssysteem zijn uitgevoerd, schakelt u het selectievakje **Malware-acties tijdens desinfectie terugdraaien** in.

- Als u wilt dat Kaspersky Endpoint Security tijdens de desinfectie de acties negeert die door malware in het besturingssysteem zijn uitgevoerd, schakelt u het selectievakje **Malware-acties tijdens desinfectie terugdraaien** uit.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Firewall

In deze sectie vindt u informatie over Firewall en leest u hoe u de instellingen van het onderdeel configureert.

Over Firewall

Als u een computer in een netwerk of met internet gebruikt, wordt die blootgesteld aan virussen, andere malware en talloze soorten aanvallen die kwetsbaarheden in het besturingssysteem en software uitbuiten.

De firewall beschermt persoonlijke gegevens die op de computer van de gebruiker zijn opgeslagen door de meeste bedreigingen voor het besturingssysteem te blokkeren wanneer de computer is verbonden met het internet of een lokaal netwerk. Firewall detecteert alle netwerkverbindingen van de computer van de gebruiker en geeft een lijst met IP-adressen met een aanduiding van de status van de standaard netwerkverbinding.

Het onderdeel Firewall filtert alle netwerkactiviteit volgens netwerkregels. Door netwerkregels te configureren kunt u het gewenste niveau van de computerbescherming instellen, gaande van het blokkeren van de internettoegang voor alle programma's tot het verlenen van onbeperkte toegang.

Firewall inschakelen en uitschakelen

Firewall is standaard ingeschakeld en werkt in de optimale modus. U kunt indien nodig Firewall uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Firewall in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.
   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts op de regel **Firewall** om het contextmenu van Firewall te openen.
5. Voer een van de volgende acties uit:
   - Selecteer in het contextmenu de optie **Starten** om Firewall in te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **Firewall**, wijzigt in het pictogram .
   - Selecteer **Stoppen** in het contextmenu om Firewall uit te schakelen.
     Het statuspictogram van het onderdeel , links in de regel **Firewall**, wijzigt in het pictogram .

Zo schakelt u Firewall in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster de optie **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.

3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Firewall inschakelen** in om Firewall in te schakelen.
   - Schakel het selectievakje **Firewall inschakelen** uit om Firewall uit te schakelen.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Over netwerkregels

Netwerkregels zijn toegestane of geblokkeerde acties die Firewall uitvoert wanneer een poging tot het maken van een netwerkverbinding wordt gedetecteerd.

Firewall biedt bescherming tegen verschillende soorten netwerkaanvallen op twee niveaus: het netwerkniveau en het programmaniveau. De bescherming op netwerkniveau wordt geleverd door regels voor netwerkpakketten toe te passen. De bescherming op programmaniveau wordt geleverd door regels toe te passen waarmee geïnstalleerde programma's toegang tot netwerkbronnen kunnen krijgen.

Op basis van de twee Firewall-beschermingsniveaus kunt u het volgende maken:

- *Regels voor netwerkpakketten*. Regels voor netwerkpakketten leggen beperkingen op aan netwerkpakketten, ongeacht het programma. Zulke regels beperken het inkomende en uitgaande netwerkverkeer via specifieke poorten van het geselecteerde gegevensprotocol. Firewall beschikt standaard over bepaalde regels voor netwerkpakketten.

- *Netwerkregels voor programma's*. Netwerkregels voor programma's leggen beperkingen op aan de netwerkactiviteit van een specifiek programma. Ze houden niet alleen rekening met de kenmerken van het netwerkpakket maar ook met het specifieke programma waarnaar dit netwerkpakket is gestuurd of dat dit netwerkpakket heeft verstuurd. Dankzij zulke regels kan het filteren van netwerkactiviteit precies worden ingesteld: wanneer bijvoorbeeld een bepaald type netwerkverbinding wordt geblokkeerd voor bepaalde programma's maar wordt toegestaan voor andere.

Regels voor netwerkpakketten hebben een hogere prioriteit dan netwerkregels voor programma's. Als zowel regels voor netwerkpakketten als netwerkregels voor programma's zijn opgegeven voor hetzelfde type netwerkactiviteit, wordt de netwerkactiviteit verwerkt volgens de regels voor netwerkpakketten.

U kunt een uitvoeringsprioriteit voor elke regel voor netwerkpakketten en elke netwerkregel voor programma's opgeven.

Regels voor netwerkpakketten hebben een hogere prioriteit dan netwerkregels voor programma's. Als zowel regels voor netwerkpakketten als netwerkregels voor programma's zijn opgegeven voor hetzelfde type netwerkactiviteit, wordt de netwerkactiviteit verwerkt volgens de regels voor netwerkpakketten.

Netwerkregels voor programma's werken als volgt: een netwerkregel voor programma's omvat toegangsregels op basis van de netwerkstatus: *openbaar* , *lokaal* of *vertrouwd*. Programma's in de vertrouwensgroep 'Zeer beperkt' mogen bijvoorbeeld standaard geen netwerkactiviteit uitvoeren in netwerken van alle statussen. Als een netwerkregel is gespecificeerd voor een individueel programma (bovenliggend programma), zullen de onderliggende processen van andere programma's draaien volgens de netwerkregel van het bovenliggende programma. Als er geen netwerkregel voor het programma is, worden de onderliggende processen uitgevoerd volgens de netwerktoegangsregel van de vertrouwensgroep van het programma.

U hebt bijvoorbeeld elke netwerkactiviteit in netwerken met alle statussen voor alle programma's verboden, behalve browser X. Als u de installatie van browser Y (onderliggend proces) start vanuit browser X (bovenliggend programma), krijgt het installatieprogramma van browser Y toegang tot het netwerk en downloadt de nodige bestanden. Na de installatie mag browser Y geen netwerkverbindingen maken op basis van de Firewall-instellingen. Om netwerkactiviteit van het installatieprogramma van browser Y als een onderliggend proces te verbieden, moet u een netwerkregel toevoegen voor het installatieprogramma van browser Y.

Over de status van de netwerkverbinding

Firewall controleert alle netwerkverbindingen op de computer van de gebruiker en wijst automatisch een status aan elke gedetecteerde netwerkverbinding toe.

De netwerkverbinding kan de volgende status hebben:

- **Openbaar netwerk**. Deze status is voor netwerken die niet door antivirusprogramma's, firewalls of filters zijn beveiligd (bijvoorbeeld netwerken van internetcafés). Wanneer de gebruiker een computer gebruikt die met zo'n netwerk is verbonden, blokkeert Firewall de toegang tot bestanden en printers van deze computer. Externe gebruikers hebben ook geen toegang tot gegevens via gedeelde mappen en geen externe toegang tot het bureaublad van deze computer. Firewall filtert de netwerkactiviteit van elk programma volgens de netwerkregels die ervoor zijn ingesteld.

  Firewall wijst standaard de status *Openbaar netwerk* toe aan het internet. U kunt de status van het internet niet wijzigen.

- **Lokaal netwerk**. Deze status is toegewezen aan netwerken waarvan de gebruikers toegang tot bestanden en printers op deze computer hebben (bijvoorbeeld een LAN of thuisnetwerk).

- **Vertrouwd netwerk**. Deze status is bedoeld voor een veilig netwerk waarin de computer niet wordt blootgesteld aan aanvallen of pogingen tot onbevoegde gegevenstoegang. Firewall staat alle netwerkactiviteit in netwerken met deze status toe.

Status van de netwerkverbinding wijzigen

Zo wijzigt u de status van de netwerkverbinding:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Beschikbare netwerken**.

   Het venster **Firewall** wordt geopend.
4. Selecteer de netwerkverbinding waarvan u de status wilt wijzigen.
5. Selecteer in het contextmenu de status van de netwerkverbinding:

   - **Openbaar netwerk**.
   - **Lokaal netwerk**.
   - **Vertrouwd netwerk**.

6. Klik in het venster **Firewall** op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels voor netwerkpakketten beheren

Tijdens het beheer van de regels voor netwerkpakketten kunt u de volgende acties uitvoeren:

- Maak een nieuwe regel voor netwerkpakketten aan.

  U kunt een nieuwe regel voor netwerkpakketten aanmaken door een reeks voorwaarden en acties in te stellen die op netwerkpakketten en gegevensstromen moeten worden toegepast.

- Schakel een regel voor netwerkpakketten in of uit.

  Alle regels voor netwerkpakketten die standaard zijn aangemaakt door Firewall hebben de status *Ingeschakeld*. Als een regel voor netwerkpakketten is ingeschakeld, past Firewall deze regel toe.

  U kunt een geselecteerde regel in de lijst met regels voor netwerkpakketten uitschakelen. Als een regel voor netwerkpakketten is uitgeschakeld, past Firewall deze regel tijdelijk niet toe.

  > Een nieuwe aangepaste regel voor netwerkpakketten wordt standaard met de status *Ingeschakeld* toegevoegd aan de lijst met regels voor netwerkpakketten.

- Bewerk de instellingen van een bestaande regel voor netwerkpakketten.

  Nadat u een nieuwe regel voor netwerkpakketten hebt gemaakt, kunt u altijd teruggaan naar de instellingen ervan en ze naar wens wijzigen.

- Wijzig de actie van Firewall voor een regel voor netwerkpakketten.

  In de lijst met regels voor netwerkpakketten kunt u de actie bewerken die Firewall uitvoert bij de detectie van netwerkactiviteit die overeenkomt met een specifieke regel voor netwerkpakketten.

- Wijzig de prioriteit van een regel voor netwerkpakketten.

  U kunt de prioriteit van een regel voor netwerkpakketten die u hebt geselecteerd in de lijst verhogen of verlagen.

- Verwijder een regel voor netwerkpakketten.

  U kunt een regel voor netwerkpakketten verwijderen om te beletten dat Firewall deze regel toepast bij de detectie van netwerkactiviteit en om te voorkomen dat deze regel in de lijst met regels voor netwerkpakketten wordt weergegeven met de status *Uitgeschakeld*.

Een regel voor netwerkpakketten aanmaken en bewerken

> Wanneer u regels voor netwerkpakketten aanmaakt, moet u onthouden dat deze een hogere prioriteit hebben dan netwerkregels voor programma's.

Zo maakt of bewerkt u een regel voor netwerkpakketten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster de optie **Firewall**.
3. Klik op de knop **Regels voor netwerkpakketten**.
4. Het venster **Firewall** wordt geopend en het tabblad **Regels voor netwerkpakketten** wordt weergegeven.

   Op dit tabblad ziet u een lijst met standaardregels voor netwerkpakketten die door Firewall zijn ingesteld.
5. Voer een van de volgende acties uit:

   - Klik op de knop **Toevoegen** om een nieuwe regel voor netwerkpakketten aan te maken.
   - Om een regel voor netwerkpakketten te bewerken, selecteert u die in de lijst met regels voor netwerkpakketten en klikt u op de knop **Bewerken**.

   Het venster **Netwerkregel** opent.
6. Selecteer in de vervolgkeuzelijst **Actie** de actie die Firewall moet uitvoeren bij de detectie van deze soort netwerkactiviteit:

   - **Toestaan**
   - **Blokkeren**
   - **Volgens programmaregels**.
7. Geef in het veld **Naam** de naam van de netwerkservice op één van de volgende manieren op:

   - Klik op het pictogram rechts van het veld **Naam** en selecteer de naam van de netwerkservice in de vervolgkeuzelijst.

     De vervolgkeuzelijst bevat netwerkservices die de meest gebruikte netwerkverbindingen definiëren.
   - Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
8. Geef het protocol van de gegevensoverdracht op:

   a. Schakel het selectievakje **Protocol** in.

   b. Selecteer in de vervolgkeuzelijst het soort protocol waarvoor de netwerkactiviteit moet worden gemonitord.

   Firewall monitort netwerkverbindingen die de protocollen TCP, UDP, ICMP, ICMPv6, IGMP en GRE gebruiken.

   Als u een netwerkservice uit de vervolgkeuzelijst **Naam** selecteert, wordt het selectievakje **Protocol** automatisch ingeschakeld en bevat de vervolgkeuzelijst naast het selectievakje het soort protocol dat overeenkomt met de geselecteerde netwerkservice. Standaard is het selectievakje **Protocol** uitgeschakeld.
9. Selecteer in de vervolgkeuzelijst **Richting** de richting van de gemonitorde netwerkactiviteit.

   Firewall monitort netwerkverbindingen in de volgende richtingen:

   - **Inkomend (pakket)**.
   - **Inkomend**.
   - **Inkomend/Uitgaand**
   - **Uitgaand (pakket)**.

- **Uitgaand**.

10. Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode opgeven:

    a. Schakel het selectievakje **ICMP-type** in en selecteer het ICMP-pakkettype in de vervolgkeuzelijst.

    b. Schakel het selectievakje **ICMP-code** in en selecteer de ICMP-pakketcode in de vervolgkeuzelijst.

11. Als TCP of UDP als het soort protocol is geselecteerd, kunt u de door komma's gescheiden poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden gemonitord:

    a. Typ de poorten van de externe computer in het veld **Externe poorten**.

    b. Typ de poorten van de lokale computer in het veld **Lokale poorten**.

12. Geef in de tabel **Netwerkadapters** de instellingen op van de netwerkadapters waarmee netwerkpakketten kunnen worden verzonden of ontvangen. Gebruik hiertoe de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

13. Als u de controle van netwerkpakketten wilt beperken op basis van hun actieve duur (Time To Live), schakelt u het selectievakje **TTL** in en geeft u in het veld ernaast het bereik van de Time To Live-waarden op voor inkomende en/of uitgaande netwerkpakketten.

    Een netwerkregel controleert de verzending van netwerkpakketten waarvan de actieve duur niet hoger is dan de opgegeven waarde.

    In het andere geval schakelt u het selectievakje **TTL** uit.

14. Geef de netwerkadressen van externe computers die netwerkpakketten kunnen verzenden en/of ontvangen. Selecteer hiertoe een van de volgende waarden in de vervolgkeuzelijst **Externe adressen**:

    - **Elk adres**. De netwerkregel controleert netwerkpakketten die door externe computers met een willekeurig IP-adres zijn verzonden en/of ontvangen.
    - **Subnetadressen**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door externe computers met IP-adressen die tot het geselecteerde type netwerk behoren: **Vertrouwde netwerken**, **Lokale netwerken** of **Openbare netwerken**.
    - **Adressen uit de lijst**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door externe computers met IP-adressen die in de lijst eronder kunnen worden opgegeven met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

15. Geef de netwerkadressen van computers op waarop Kaspersky Endpoint Security is geïnstalleerd en die netwerkpakketten kunnen verzenden en/of ontvangen. Selecteer hiertoe een van de volgende waarden in de vervolgkeuzelijst **Lokale adressen**:

    - **Elk adres**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door computers waarop Kaspersky Endpoint Security is geïnstalleerd en die een willekeurig IP-adres hebben.
    - **Adressen uit de lijst**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door computers waarop Kaspersky Endpoint Security is geïnstalleerd en die IP-adressen hebben die in de lijst eronder kunnen worden opgegeven met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

    Soms kan geen lokaal adres worden verkregen voor programma's die met netwerkpakketten werken. Als dit het geval is, wordt de waarde van de instelling **Lokale adressen** genegeerd.

16. Als u wilt dat de acties van de netwerkregel worden opgenomen in het rapport, schakelt u het selectievakje **Gebeurtenissen registreren** in.

17. Klik in het venster **Netwerkregel** op **OK**.

    Als u een nieuwe netwerkregel aanmaakt, wordt de regel op het tabblad **Regels voor netwerkpakketten** in het venster **Firewall** weergegeven. Standaard wordt de nieuwe netwerkregel op het einde van de lijst met regels voor netwerkpakketten geplaatst.

18. Klik in het venster **Firewall** op **OK**.

19. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een regel voor netwerkpakketten inschakelen of uitschakelen

Zo schakelt u een regel voor netwerkpakketten in of uit:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.

3. Klik op de knop **Regels voor netwerkpakketten**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor netwerkpakketten** wordt weergegeven.

4. Selecteer in de lijst de noodzakelijke regel voor netwerkpakketten.

5. Voer een van de volgende acties uit:

   - Schakel het selectievakje naast de naam van de regel voor netwerkpakketten in als u de regel wilt inschakelen.

   - Schakel het selectievakje naast de naam van de regel voor netwerkpakketten uit als u de regel wilt uitschakelen.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De actie van Firewall voor een regel voor netwerkpakketten wijzigen

Zo wijzigt u de actie van Firewall die op een regel voor netwerkpakketten wordt toegepast:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.

3. Klik op de knop **Regels voor netwerkpakketten**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor netwerkpakketten** wordt weergegeven.

4. Selecteer in de lijst de regel voor netwerkpakketten waarvan u de actie wilt wijzigen.

5. Klik rechts in de kolom **Machtiging** om het contextmenu te openen en selecteer de actie die u wilt toewijzen:
   - **Toestaan**
   - **Blokkeren**
   - **Overeenkomstig de programmaregel**
   - **Gebeurtenissen registreren**
6. Klik in het venster **Firewall** op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De prioriteit van een regel voor netwerkpakketten wijzigen

De prioriteit van een regel voor netwerkpakketten wordt bepaald volgens de positie ervan in de lijst met regels voor netwerkpakketten. De bovenste regel voor netwerkpakketten in de lijst met regels voor netwerkpakketten heeft de hoogste prioriteit.

Elke handmatig gemaakte regel voor netwerkpakketten wordt op het einde van de lijst met regels voor netwerkpakketten toegevoegd en heeft de laagste prioriteit.

Firewall voert de regels uit in de volgorde waarin ze in de lijst met regels voor netwerkpakketten verschijnen, van boven naar beneden. Naargelang elke verwerkte regel voor netwerkpakketten die van toepassing is op een bepaalde netwerkverbinding staat Firewall al dan niet de toegang tot het adres en de poort toe die in de instellingen van deze netwerkverbinding zijn opgegeven.

Zo wijzigt u de prioriteit van een regel voor netwerkpakketten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Regels voor netwerkpakketten**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor netwerkpakketten** wordt weergegeven.
4. Selecteer in de lijst de regel voor netwerkpakketten waarvan u de prioriteit wilt wijzigen.
5. Gebruik de knoppen **Omhoog** en **Omlaag** om de regel voor netwerkpakketten naar de gewenste plaats in de lijst met regels voor netwerkpakketten te bewegen.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Netwerkregels voor programma's beheren

Standaard groepeert Kaspersky Endpoint Security alle programma's die op de computer zijn geïnstalleerd op naam van de leverancier van de software waarvan het de bestands- of netwerkactiviteit monitort. De programmagroepen worden op hun beurt gecategoriseerd in vertrouwensgroepen. Alle programma's en programmagroepen nemen de eigenschappen van de bovenliggende groep over: regels voor programmacontrole, netwerkregels voor programma's en de prioriteit van uitvoering.

Standaard past het onderdeel Firewall de netwerkregels voor een programmagroep toe wanneer de netwerkactiviteit van alle programma's in de groep wordt gefilterd, net als bij het onderdeel Controle van programmabevoegdheden. De netwerkregels voor programmagroepen definiëren de rechten van programma's in de groep om toegang tot verschillende netwerkverbindingen te krijgen.

Firewall maakt standaard een reeks netwerkregels voor elke programmagroep die door Kaspersky Endpoint Security op de computer wordt gevonden. U kunt de actie van Firewall die wordt toegepast op de standaard gemaakte netwerkregels voor de programmagroepen wijzigen. U kunt wel de prioriteit van de standaard gemaakte netwerkregels voor de programmagroepen niet bewerken, verwijderen, uitschakelen of wijzigen.

U kunt ook een netwerkregel voor een individueel programma aanmaken. Deze regel heeft dan een hoger prioriteit dan de netwerkregel van de groep waartoe het programma behoort.

Tijdens het beheer van de netwerkregels voor programma's kunt u de volgende acties uitvoeren:

- Maak een nieuwe netwerkregel aan.

  U kunt een nieuwe netwerkregel aanmaken die Firewall moet gebruiken om de netwerkactiviteit van het programma of de programma's die tot de geselecteerde groep programma's behoren te regelen.

- Schakel een netwerkregel in of uit.

  Alle netwerkregels worden met de status *Ingeschakeld* toegevoegd aan de lijst met netwerkregels voor programma's. Als een netwerkregel is ingeschakeld, past Firewall deze regel toe.

  U kunt een handmatig gemaakte netwerkregel uitschakelen. Als een netwerkregel is uitgeschakeld, past Firewall deze regel tijdelijk niet toe.

- Wijzig de instellingen van een netwerkregel.

  Nadat u een nieuwe netwerkregel hebt gemaakt, kunt u altijd teruggaan naar de instellingen ervan en ze naar wens wijzigen.

- Wijzig de actie van Firewall voor een netwerkregel.

  In de lijst met netwerkregels kunt u de actie bewerken die Firewall toepast op de netwerkregel bij de detectie van netwerkactiviteit in dit programma of deze programmagroep.

- Wijzig de prioriteit van een netwerkregel.

  U kunt een aangepaste netwerkregel een hogere of lagere prioriteit geven.

- Verwijder een netwerkregel.

  U kunt een aangepaste netwerkregel verwijderen om te voorkomen dat Firewall deze netwerkregel toepast op het geselecteerde programma of de programmagroep bij de detectie van netwerkactiviteit en om deze regel niet langer weer te geven in de lijst met netwerkregels voor programma's.

Een netwerkregel voor programma's aanmaken en bewerken

Zo maakt of bewerkt u een netwerkregel voor een programmagroep:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.
3. Klik op de knop **Netwerkregels voor programma's**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor programmacontrole** wordt weergegeven.
4. Selecteer in de lijst met programma's het programma of de groep van programma's waarvoor u een netwerkregel wilt aanmaken of bewerken.
5. Klik rechts om het contextmenu te openen en selecteer **Programmaregels** of **Groepsregels** afhankelijk van wat u wilt doen.

   Zo opent u het venster **Regels voor programmacontrole** of **Regels voor controle van programmagroepen**.
6. Selecteer in het geopende venster het tabblad **Netwerkregels**.
7. Voer een van de volgende acties uit:

   - Klik op de knop **Toevoegen** om een nieuwe netwerkregel aan te maken.
   - Om een netwerkregel te bewerken, selecteert u die in de lijst met netwerkregels en klikt u op de knop **Bewerken**.

   Het venster **Netwerkregel** opent.
8. Selecteer in de vervolgkeuzelijst **Actie** de actie die Firewall moet uitvoeren bij de detectie van deze soort netwerkactiviteit:

   - **Toestaan**
   - **Blokkeren**
9. Geef in het veld **Naam** de naam van de netwerkservice op één van de volgende manieren op:

   - Klik op het pictogram rechts van het veld **Naam** en selecteer de naam van de netwerkservice in de vervolgkeuzelijst.

     De vervolgkeuzelijst bevat netwerkservices die de meest gebruikte netwerkverbindingen definiëren.
   - Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
10. Geef het protocol van de gegevensoverdracht op:

    a. Schakel het selectievakje **Protocol** in.

    b. Selecteer in de vervolgkeuzelijst het soort protocol waarvoor u de netwerkactiviteit wilt monitoren.

    Firewall monitort netwerkverbindingen die de protocollen TCP, UDP, ICMP, ICMPv6, IGMP en GRE gebruiken.

    Als u een netwerkservice uit de vervolgkeuzelijst **Naam** selecteert, wordt het selectievakje **Protocol** automatisch ingeschakeld en bevat de vervolgkeuzelijst naast het selectievakje het soort protocol dat overeenkomt met de geselecteerde netwerkservice. Standaard is het selectievakje **Protocol** uitgeschakeld.
11. Selecteer in de vervolgkeuzelijst **Richting** de richting van de gemonitorde netwerkactiviteit.

    Firewall monitort netwerkverbindingen in de volgende richtingen:

- **Inkomend**.
- **Inkomend/Uitgaand**.
- **Uitgaand**.

12. Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode opgeven:
    a. Schakel het selectievakje **ICMP-type** in en selecteer het ICMP-pakkettype in de vervolgkeuzelijst.
    b. Schakel het selectievakje **ICMP-code** in en selecteer de ICMP-pakketcode in de vervolgkeuzelijst.
13. Als TCP of UDP als het soort protocol is geselecteerd, kunt u de door komma's gescheiden poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden gemonitord:
    a. Typ de poorten van de externe computer in het veld **Externe poorten**.
    b. Typ de poorten van de lokale computer in het veld **Lokale poorten**.
14. Geef de netwerkadressen van externe computers die netwerkpakketten kunnen verzenden en/of ontvangen. Selecteer hiertoe een van de volgende waarden in de vervolgkeuzelijst **Externe adressen**:
    - **Elk adres**. De netwerkregel controleert netwerkpakketten die door externe computers met een willekeurig IP-adres zijn verzonden en/of ontvangen.
    - **Subnetadressen**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door externe computers met IP-adressen die tot het geselecteerde type netwerk behoren: **Vertrouwde netwerken**, **Lokale netwerken** of **Openbare netwerken**.
    - **Adressen uit de lijst**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door externe computers met IP-adressen die in de lijst eronder kunnen worden opgegeven met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.
15. Geef de netwerkadressen van computers op waarop Kaspersky Endpoint Security is geïnstalleerd en die netwerkpakketten kunnen verzenden en/of ontvangen. Selecteer hiertoe een van de volgende waarden in de vervolgkeuzelijst **Lokale adressen**:
    - **Elk adres**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door computers waarop Kaspersky Endpoint Security is geïnstalleerd en die een willekeurig IP-adres hebben.
    - **Adressen uit de lijst**. De netwerkregel controleert netwerkpakketten die zijn verzonden en/of ontvangen door computers waarop Kaspersky Endpoint Security is geïnstalleerd en die IP-adressen hebben die in de lijst eronder kunnen worden opgegeven met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

    Soms kan geen lokaal adres worden verkregen voor programma's die met netwerkpakketten werken. Als dit het geval is, wordt de waarde van de instelling **Lokale adressen** genegeerd.
16. Als u wilt dat de acties van de netwerkregel worden opgenomen in het rapport, schakelt u het selectievakje **Gebeurtenissen registreren** in.
17. Klik in het venster **Netwerkregel** op **OK**.

    Als u een nieuwe netwerkregel hebt aangemaakt, wordt de regel op het tabblad **Netwerkregels** weergegeven.
18. Klik op **OK** in het venster **Regels voor controle van programmagroepen** als de regel voor een groep programma's bedoeld is of in het venster **Regels voor programmacontrole** als de regel voor een programma

bedoeld is.

19. Klik in het venster **Firewall** op **OK**.
20. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een netwerkregel voor programma's inschakelen en uitschakelen

Zo schakelt u een netwerkregel voor programma's in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Netwerkregels voor programma's**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor programmacontrole** wordt weergegeven.
4. Selecteer in de lijst het programma of de groep van programma's waarvoor u een netwerkregel wilt inschakelen of uitschakelen.
5. Klik rechts om het contextmenu te openen en selecteer **Programmaregels** of **Groepsregels** afhankelijk van wat u wilt doen.

   Zo opent u het venster **Regels voor programmacontrole** of **Regels voor controle van programmagroepen**.
6. Selecteer in het geopende venster het tabblad **Netwerkregels**.
7. Selecteer de relevante netwerkregel in de lijst met netwerkregels voor een programmagroep.
8. Voer een van de volgende acties uit:

   - Schakel het selectievakje naast de naam van de netwerkregel in als u de regel wilt inschakelen.
   - Schakel het selectievakje naast de naam van de netwerkregel uit als u de regel wilt uitschakelen.

   > U kunt een netwerkregel voor een programmagroep die standaard is aangemaakt door Firewall niet uitschakelen.

9. Klik op **OK** in het venster **Regels voor controle van programmagroepen** als de regel voor een groep programma's bedoeld is of in het venster **Regels voor programmacontrole** als de regel voor een programma bedoeld is.
10. Klik in het venster **Firewall** op **OK**.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De actie van Firewall voor een netwerkregel voor programma's wijzigen

U kunt wijzigen welke actie Firewall toepast op alle netwerkregels voor een programma of een programmagroep die standaard zijn aangemaakt. Daarnaast kunt u ook de actie van Firewall voor een enkele aangepaste netwerkregel voor een programma of een programmagroep wijzigen.

Zo wijzigt u de actie van Firewall voor alle netwerkregels voor een programma of een groep van programma's:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Netwerkregels voor programma's**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor programmacontrole** wordt weergegeven.
4. Als u wilt wijzigen welke actie Firewall toepast op alle netwerkregels die standaard zijn aangemaakt, selecteert u een programma of een groep van programma's in de lijst. Handmatig aangemaakte netwerkregels worden ongewijzigd gelaten.
5. Klik rechts in de kolom **Netwerk** om het contextmenu weer te geven en selecteer de actie die u wilt toewijzen:
   - **Overnemen**
   - **Toestaan**
   - **Blokkeren**
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Zo wijzigt u het antwoord van Firewall voor één netwerkregel voor een programma of een programmagroep:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster de optie **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Netwerkregels voor programma's**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor programmacontrole** wordt weergegeven.
4. Selecteer in de lijst het programma of de groep van programma's waarvoor u de actie voor één netwerkregel wilt wijzigen.
5. Klik rechts om het contextmenu te openen en selecteer **Programmaregels** of **Groepsregels** afhankelijk van wat u wilt doen.

   Zo opent u het venster **Regels voor programmacontrole** of **Regels voor controle van programmagroepen**.
6. Selecteer in het geopende venster het tabblad **Netwerkregels**.
7. Selecteer de netwerkregel waarvoor u de actie van Firewall wilt wijzigen.
8. Klik rechts in de kolom **Machtiging** om het contextmenu te openen en selecteer de actie die u wilt toewijzen:
   - **Toestaan**

- **Blokkeren**
- **Gebeurtenissen registreren**

9. Klik op **OK** in het venster **Regels voor controle van programmagroepen** als de regel voor een groep programma's bedoeld is of in het venster **Regels voor programmacontrole** als de regel voor een programma bedoeld is.
10. Klik in het venster **Firewall** op **OK**.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De prioriteit van een netwerkregel voor programma's wijzigen

De prioriteit van een netwerkregel wordt bepaald volgens de positie ervan in de lijst met netwerkregels. Firewall voert de regels uit in de volgorde waarin ze in de lijst met netwerkregels verschijnen, van boven naar beneden. Naargelang elke verwerkte netwerkregel die van toepassing is op een bepaalde netwerkverbinding staat Firewall al dan niet de toegang tot het adres en de poort toe die in de instellingen van deze netwerkverbinding zijn opgegeven.

Handmatig aangemaakte netwerkregels hebben een hogere prioriteit dan standaardnetwerkregels.

U kunt de prioriteit van de standaard gemaakte netwerkregels voor de programmagroepen niet wijzigen.

Zo wijzigt u de prioriteit van een netwerkregel:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Firewall**.

   Rechts in het venster ziet u de instellingen van het onderdeel Firewall.
3. Klik op de knop **Netwerkregels voor programma's**.

   Het venster **Firewall** wordt geopend en het tabblad **Regels voor programmacontrole** wordt weergegeven.
4. Selecteer in de lijst met programma's het programma of de groep van programma's waarvoor u de prioriteit van een netwerkregel wilt wijzigen.
5. Klik rechts om het contextmenu te openen en selecteer **Programmaregels** of **Groepsregels** afhankelijk van wat u wilt doen.

   Zo opent u het venster **Regels voor programmacontrole** of **Regels voor controle van programmagroepen**.
6. Selecteer in het geopende venster het tabblad **Netwerkregels**.
7. Selecteer de netwerkregel waarvan u de prioriteit wilt wijzigen.
8. Gebruik de knoppen **Omhoog** en **Omlaag** om de netwerkregel naar de gewenste plaats in de lijst met netwerkregels te bewegen.
9. Klik op **OK** in het venster **Regels voor controle van programmagroepen** als de regel voor een groep programma's bedoeld is of in het venster **Regels voor programmacontrole** als de regel voor een programma bedoeld is.

10. Klik in het venster **Firewall** op **OK**.

11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Netwerkmonitor

In deze sectie vindt u informatie over Netwerkmonitor en instructies voor het starten van Netwerkmonitor.

Over Netwerkmonitor

Netwerkmonitor is een tool ontworpen voor de realtime weergave van informatie over de netwerkactiviteit van de computer van een gebruiker.

Netwerkmonitor starten

Zo start u Netwerkmonitor:

1. Open het hoofdvenster van het programma.

2. Selecteer het tabblad **Bescherming en controle**.

3. Klik op het gedeelte **Bescherming**.

   Het gedeelte **Bescherming** wordt geopend.

4. Klik rechts op de regel **Firewall** om het contextmenu met Firewall-bewerkingen te openen.

5. Selecteer in het contextmenu de optie **Netwerkmonitor**.

   Het venster **Netwerkmonitor** wordt geopend. In dit venster ziet u informatie over de netwerkactiviteit van de computer op vier tabbladen:

   - Op het tabblad **Netwerkactiviteit** ziet u alle huidige actieve netwerkverbindingen van de computer. Zowel uitgaande als inkomende netwerkverbindingen worden weergegeven.

   - Op het tabblad **Open poorten** ziet u alle open netwerkpoorten van de computer.

   - Op het tabblad **Netwerkverkeer** ziet u het volume van het inkomende en uitgaande netwerkverkeer tussen de computer van de gebruiker en andere computers in het netwerk waarmee de gebruiker momenteel is verbonden.

   - Op het tabblad **Geblokkeerde computers** ziet u de IP-adressen van externe computers waarvan de netwerkactiviteit is geblokkeerd door het onderdeel Network Attack Blocker nadat een netwerkaanval vanaf die IP-adressen is gedetecteerd.

Network Attack Blocker

In deze sectie vindt u informatie over Network Attack Blocker en leest u hoe u de instellingen van het onderdeel configureert.

Over Network Attack Blocker

Network Attack Blocker scant inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Bij de detectie van een netwerkaanval op uw computer blokkeert Kaspersky Endpoint Security alle netwerkactiviteit van de computer die de aanval uitvoert. U ziet dan op uw scherm een waarschuwing met de melding dat iemand een netwerkaanval op uw computer heeft uitgevoerd. De melding bevat informatie over de computer die de aanval heeft uitgevoerd.

Het netwerkverkeer van de aanvallende computer wordt één uur geblokkeerd. U kunt de instellingen voor het blokkeren van een aanvallende computer bewerken.

Beschrijvingen van momenteel bekende soorten netwerkaanvallen en methoden om ze te bestrijden worden via de databases van Kaspersky Endpoint Security geleverd. De lijst met netwerkaanvallen die worden gedetecteerd door het onderdeel Network Attack Blocker wordt bijgewerkt wanneer de databases en de modules van het programma worden bijgewerkt.

Network Attack Blocker inschakelen en uitschakelen

Network Attack Blocker is standaard ingeschakeld en werkt in de optimale modus. U kunt indien nodig Network Attack Blocker uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Network Attack Blocker in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Bescherming**.

   Het gedeelte **Bescherming** wordt geopend.
4. Klik rechts op de regel **Network Attack Blocker** om het contextmenu met acties van Network Attack Blocker weer te geven.
5. Voer een van de volgende acties uit:

   - Selecteer **Starten** in het contextmenu om Network Attack Blocker in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Network Attack Blocker**, wijzigt in het pictogram .

- Selecteer **Stoppen** in het contextmenu om Network Attack Blocker uit te schakelen.

  Het statuspictogram van het onderdeel , links in de regel **Network Attack Blocker**, wijzigt in het pictogram .

Zo schakelt u Network Attack Blocker in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Network Attack Blocker**.

   Rechts in het venster ziet u de instellingen van Network Attack Blocker.
3. Doe het volgende:

   - Schakel het selectievakje **Network Attack Blocker inschakelen** in om Network Attack Blocker in te schakelen.
   - Schakel het selectievakje **Network Attack Blocker inschakelen** uit om Network Attack Blocker uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Instellingen van Network Attack Blocker

U kunt het volgende doen om de instellingen van Network Attack Blocker te configureren:

- Configureer de instellingen voor het blokkeren van een aanvallende computer.
- Genereer een lijst met adressen die u niet wilt blokkeren.

Instellingen voor het blokkeren van een aanvallende computer bewerken

Zo bewerkt u de instellingen voor het blokkeren van een aanvallende computer:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Network Attack Blocker**.

   Rechts in het venster ziet u de instellingen van Network Attack Blocker.
3. Schakel het selectievakje **Voeg de aanvallende computer toe aan de lijst met geblokkeerde computers gedurende** in.

   Als dit selectievakje is ingeschakeld wanneer een netwerkaanval wordt gedetecteerd, blokkeert Network Attack Blocker het netwerkverkeer van de aanvallende computer gedurende de opgegeven tijd. Hiermee beschermt u de computer automatisch tegen mogelijke nieuwe netwerkaanvallen vanaf hetzelfde adres.

   Als dit selectievakje is uitgeschakeld wanneer een netwerkaanval wordt gedetecteerd, schakelt Network Attack Blocker de automatische bescherming tegen mogelijke nieuwe netwerkaanvallen vanaf hetzelfde adres niet in.
4. Wijzig hoelang een aanvallende computer moet worden geblokkeerd in het veld naast het selectievakje **Voeg de aanvallende computer toe aan de lijst met geblokkeerde computers gedurende**.

5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Adressen configureren die niet moeten worden geblokkeerd

Zo configureert u adressen die niet moeten worden geblokkeerd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **Network Attack Blocker**.

   Rechts in het venster ziet u de instellingen van Network Attack Blocker.
3. Klik op de knop **Uitzonderingen**.

   Het venster **Uitzonderingen** wordt geopend.
4. Voer een van de volgende acties uit:

   - Als u een nieuw IP-adres wilt toevoegen, klikt u op de knop **Toevoegen**.
   - Als u een eerder toegevoegd IP-adres wilt bewerken, selecteert u het adres in de lijst met adressen en klikt u op de knop **Bewerken**.

   Het venster **IP-adres** wordt geopend.
5. Voer het IP-adres van de computer dat niet moet worden geblokkeerd als er netwerkaanvallen vanaf dat adres plaatsvinden.
6. Klik in het venster **IP-adres** op **OK**.
7. Klik in het venster **Uitzonderingen** op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

BadUSB Attack Prevention

In deze sectie vindt u informatie over het onderdeel BadUSB Attack Prevention.

Over BadUSB Attack Prevention

Bepaalde virussen passen de firmware van USB-apparaten aan om het besturingssysteem zodanig te misleiden dat het USB-apparaat als een toetsenbord wordt geïdentificeerd.

Het onderdeel BadUSB Attack Prevention voorkomt dat geïnfecteerde USB-apparaten zich voordoen als een toetsenbord wanneer ze op de computer worden aangesloten.

Wanneer een USB-apparaat op de computer wordt aangesloten en door het programma als een toetsenbord wordt geïdentificeerd, wordt de gebruiker door het programma gevraagd om een door het programma gegenereerde numerieke code in te voeren met dit toetsenbord of met Schermtoetsenbord (als dit beschikbaar is). Deze procedure noemen we de toetsenbordautorisatie. Het programma staat het gebruik van een geautoriseerd toetsenbord toe en blokkeert een toetsenbord dat niet is geautoriseerd.

BadUSB Attack Prevention wordt op de achtergrond uitgevoerd zodra dit onderdeel is geïnstalleerd. Als het programma niet door een Kaspersky Security Center-beleid wordt beheerd, kunt u BadUSB Attack Prevention inschakelen of uitschakelen door de bescherming en de controle van de computer tijdelijk te pauzeren en te hervatten.

Het onderdeel BadUSB Attack Prevention installeren

Als u tijdens de installatie van Kaspersky Endpoint Security de basis- of standaardinstallatie hebt geselecteerd, is het onderdeel BadUSB Attack Prevention niet beschikbaar. Om het te installeren, moet u de reeks geïnstalleerde programmaonderdelen aanpassen.

Zo installeert u het onderdeel BadUSB Attack Prevention:

1. Selecteer in het menu **Start** achtereenvolgens **Apps** → **Kaspersky Endpoint Security 10 voor Windows** → **Wijzigen, herstellen of verwijderen**.

   De Installatiewizard wordt gestart.

2. Klik in het venster **Programma wijzigen, herstellen of verwijderen** van de Installatiewizard van het programma op de knop **Wijzigen**.

   Hiermee opent u het venster **Aangepaste installatie** van de Installatiewizard van het programma.

3. Selecteer in het contextmenu van het pictogram naast de naam van het onderdeel **BadUSB Attack Prevention** de optie **Onderdeel wordt op de lokale harde schijf geïnstalleerd**.

4. Klik op de knop **Volgende**.

5. Volg de instructies van de Installatiewizard.

BadUSB Attack Prevention inschakelen en uitschakelen

Zo schakelt u BadUSB Attack Prevention in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **BadUSB Attack Prevention**.

   Rechts in het venster ziet u de instellingen van BadUSB Attack Prevention.
3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **BadUSB Attack Prevention inschakelen** in om BadUSB Attack Prevention in te schakelen.
   - Schakel het selectievakje **BadUSB Attack Prevention inschakelen** uit om BadUSB Attack Prevention uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Het gebruik van Schermtoetsenbord voor autorisaties toestaan en verbieden

Schermtoetsenbord mag alleen worden gebruikt voor de autorisatie van USB-apparaten die de invoer van willekeurige tekens niet ondersteunen (bijvoorbeeld barcodescanners). U wordt afgeraden om Schermtoetsenbord te gebruiken voor de autorisatie van onbekende USB-apparaten.

Zo staat u het gebruik van Schermtoetsenbord voor autorisaties al dan niet toe:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Antivirusbescherming** links in het venster het subgedeelte **BadUSB Attack Prevention**.

   De instellingen van het onderdeel worden rechts in het venster weergegeven.
3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Gebruik van Schermtoetsenbord voor autorisatie verbieden** in om het gebruik van Schermtoetsenbord voor autorisaties te blokkeren.
   - Schakel het selectievakje **Gebruik van Schermtoetsenbord voor autorisatie verbieden** uit om het gebruik van Schermtoetsenbord voor autorisaties toe te staan.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Toetsenbordautorisatie

USB-apparaten die door het besturingssysteem worden geïdentificeerd als toetsenborden en vóór de installatie van het onderdeel BadUSB Attack Prevention op de computer waren aangesloten, worden na de installatie van het onderdeel beschouwd als geautoriseerde toetsenborden.

Alleen als de vraag om autorisatie voor USB-toetsenborden is ingeschakeld, vereist het programma de autorisatie van het aangesloten USB-apparaat dat door het besturingssysteem als een toetsenbord is geïdentificeerd. De gebruiker kan een ongeautoriseerd toetsenbord pas gebruiken wanneer het wordt geautoriseerd.

Als de vraag om autorisatie voor USB-toetsenborden is uitgeschakeld, kan de gebruiker alle aangesloten toetsenborden gebruiken. Net na de inschakeling van de vraag om autorisatie voor USB-toetsenborden toont het programma een vraag om elk aangesloten ongeautoriseerd toetsenbord te autoriseren.

Zo autoriseert u een toetsenbord:

1. Sluit het USB-toetsenbord op een USB-poort aan wanneer de autorisatie voor USB-toetsenborden is ingeschakeld.

   Het venster **Toetsenbordautorisatie - <Naam van toetsenbord>** wordt geopend. In dit venster ziet u de details van het aangesloten toetsenbord en een numerieke code voor de autorisatie ervan.

2. Voer de willekeurig gegenereerde numerieke code in het autorisatievenster in met het aangesloten toetsenbord of Schermtoetsenbord (indien beschikbaar).

3. Klik op **OK**.

   Als de code juist is ingevoerd, slaat het programma de identificatieparameters op (VID/PID van het toetsenbord en het nummer van de poort waarop het is aangesloten) in de lijst met geautoriseerde toetsenborden. U hoeft de autorisatie niet te herhalen wanneer het toetsenbord opnieuw wordt aangesloten of wanneer het besturingssysteem opnieuw wordt opgestart.

   > Wanneer het geautoriseerde toetsenbord op een andere USB-poort van de computer wordt aangesloten, wordt u door het programma gevraagd om dit toetsenbord opnieuw te autoriseren.

   Als de numerieke code onjuist is ingevoerd, genereert het programma een nieuwe code. U hebt drie pogingen om de numerieke code juist in te voeren. Als de numerieke code drie keer na elkaar verkeerd wordt ingevoerd of als het venster **Toetsenbordautorisatie - <Naam van toetsenbord>** wordt gesloten, blokkeert het programma de invoer vanaf dit toetsenbord. Wanneer het programma opnieuw wordt aangesloten of het besturingssysteem opnieuw wordt opgestart, wordt de gebruiker door het programma gevraagd om de toetsenbordautorisatie opnieuw uit te voeren.

Controle van programma-opstart

In deze sectie vindt u informatie over Programma-opstartcontrole en leest u hoe u de instellingen van het onderdeel configureert.

Over Programma-opstartcontrole

Het onderdeel Programma-opstartcontrole monitort pogingen van gebruikers om programma's te starten en regelt het starten van programma's met *regels van Programma-opstartcontrole*.

Het starten van programma's waarvan de instellingen niet voldoen aan de regels van Programma-opstartcontrole wordt geregeld door de geselecteerde modus waarin het onderdeel werkt. De *modus Black list* is standaard geselecteerd. In deze modus kunnen alle gebruikers alle programma's starten.

Alle pogingen van gebruikers om programma's te starten worden in rapporten geregistreerd.

Programma-opstartcontrole inschakelen en uitschakelen

Hoewel Programma-opstartcontrole standaard is uitgeschakeld, kunt u het zo nodig inschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Programma-opstartcontrole in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Endpoint-controle**.

   Het gedeelte **Endpoint-controle** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Programma-opstartcontrole bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:

   - Selecteer **Starten** in het menu om Programma-opstartcontrole in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Programma-opstartcontrole**, wijzigt in het pictogram .
   - Selecteer **Stoppen** in het menu om Programma-opstartcontrole uit te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Programma-opstartcontrole**, wijzigt in het pictogram .

Zo schakelt u Programma-opstartcontrole in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om Programma-opstartcontrole in te schakelen.
   - Schakel het selectievakje **Programma-opstartcontrole inschakelen** uit om Programma-opstartcontrole uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Beperkingen van de functionaliteit van Programma-opstartcontrole

In de volgende gevallen is de werking van het onderdeel Programma-opstartcontrole beperkt:

- Wanneer de versie van het programma wordt geüpgraded, wordt de import van de instellingen van het onderdeel Programma-opstartcontrole niet ondersteund.

  Voor het herstel van de functionaliteit van Programma-opstartcontrole moet u de instellingen van het onderdeel opnieuw configureren.

- Zonder verbinding met KSN-servers krijgt Kaspersky Endpoint Security alleen van de lokale databases informatie over de reputatie van programma's en hun modules. Als de lokale databases geen informatie over het programma bevatten, wordt het programma niet gecategoriseerd in een vertrouwensgroep.

  De categorisering van programma's wanneer er een verbinding met de KSN-servers is kan verschillen van de categorisering wanneer er geen verbinding met KSN is.

- In de Kaspersky Security Center-database kan informatie over 150.000 verwerkte bestanden worden opgeslagen. Zodra dit aantal records is bereikt, worden geen nieuwe bestanden verwerkt. Om de inventarisatie dan te hervatten, moet u de bestanden verwijderen die eerder zijn geïnventariseerd in de Kaspersky Security Center-database vanaf de computer waarop Kaspersky Endpoint Security is geïnstalleerd.

- Het onderdeel controleert de opstart van scripts niet tenzij het script via de opdrachtregel is verstuurd naar de interpreter.

  Als de opstart van een interpreter is toegestaan door de regels van Programma-opstartcontrole, blokkeert het onderdeel de opstart van een script vanaf deze interpreter niet.

- Het onderdeel controleert niet de opstart van scripts vanaf interpreters die niet door Kaspersky Endpoint Security worden ondersteund.

  Kaspersky Endpoint Security ondersteunt de volgende interpreters:

- Java
- PowerShell

De volgende soorten interpreters worden ondersteund:

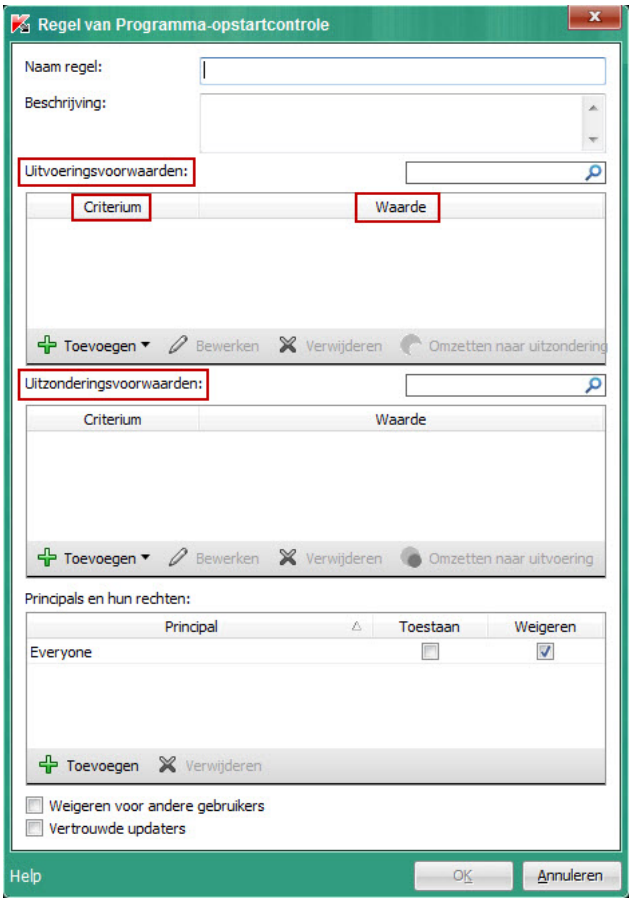
- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Over de regels van Programma-opstartcontrole

Kaspersky Endpoint Security gebruikt regels om de start van programma's door gebruikers te controleren. Een regel van Programma-opstartcontrole bevat de activeringsvoorwaarden en de actie die door Programma-opstartcontrole wordt uitgevoerd wanneer de regel wordt geactiveerd (de start van het programma door gebruikers wordt toegestaan of geblokkeerd).

Voorwaarden voor activatie van regel

Een voorwaarde voor de activatie van de regel heeft de volgende structuur: "type voorwaarde - criterium voorwaarde - waarde voorwaarde" (zie onderstaande afbeelding). Op basis van de voorwaarden voor de activatie van de regel past Kaspersky Endpoint Security (al dan niet) een regel op een programma toe.



Regel van Programma-opstartcontrole. Parameters van voorwaarden voor activatie van regel

Regels gebruiken uitvoerings- en uitzonderingsvoorwaarden:

- *Uitvoeringsvoorwaarden*. Kaspersky Endpoint Security past de regel op het programma toe als het programma aan minstens één van de uitvoeringsvoorwaarden voldoet.

- *Uitzonderingsvoorwaarden*. Kaspersky Endpoint Security past de regel niet op het programma toe als het programma aan minstens één van de uitzonderingsvoorwaarden voldoet en niet aan de uitvoeringsvoorwaarden voldoet.

De voorwaarden voor de activatie van de regel worden met criteria gemaakt. De volgende criteria worden gebruikt om regels in Kaspersky Endpoint Security aan te maken:

- Pad naar de map met het uitvoerbare bestand van het programma of het pad naar het uitvoerbare bestand van het programma.

- Metagegevens: naam van uitvoerbaar bestand van programma, versie van uitvoerbaar bestand van programma, naam van programma, versie van programma, leverancier van programma.

- Hash van het uitvoerbare bestand van het programma.
- Certificaat: verlener, houder, vingerafdruk.
- Opname van het programma in een KL-categorie.
- Locatie van het uitvoerbare bestand van het programma op een verwisselbare schijf.

De waarde van het criterium moet voor elk gebruikt criterium in de voorwaarde worden opgegeven. Als de parameters van het gestarte programma overeenkomen met de opgegeven criteriawaarden in de uitvoeringsvoorwaarde, wordt de regel geactiveerd. In dit geval voert Programma-opstartcontrole de opgegeven actie in de regel uit. Als de parameters van het programma overeenkomen met de opgegeven criteriawaarden in de uitzonderingsvoorwaarde, wordt de start van het programma niet gecontroleerd door Programma-opstartcontrole.

Beslissingen van het onderdeel Programma-opstartcontrole bij de activatie van een regel

Wanneer een regel wordt geactiveerd, worden gebruikers (of groepen van gebruikers) door Programma-opstartcontrole toegestaan om programma's te starten of wordt de start van die programma's geblokkeerd volgens de regel. U kunt individuele gebruikers of groepen van gebruikers selecteren die al dan niet programma's mogen starten die een regel activeren.

Als in een regel niet is opgegeven welke gebruikers programma's mogen starten die aan de regel voldoen, wordt deze regel een *Blokkeren*-regel genoemd.

Als voor een regel geen gebruikers zijn opgegeven die geen programma's mogen starten die aan de regel voldoen, wordt deze regel een *Toestaan*-regel genoemd.

De prioriteit van een Blokkeren-regel is hoger dan die van een Toestaan-regel. Als bijvoorbeeld een Toestaan-regel van Programma-opstartcontrole is opgegeven voor een gebruikersgroep terwijl een Blokkeren-regel van Programma-opstartcontrole is opgegeven voor één gebruiker in deze gebruikersgroep, kan deze gebruiker het programma niet starten.

Status van werking van regel

Regels van Programma-opstartcontrole kunnen een van twee mogelijke statussen voor hun werking hebben:

- **Aan.**

  Deze regelstatus betekent dat de regel is ingeschakeld.

- **Uit.**

  Deze regelstatus betekent dat de regel is uitgeschakeld.

Standaardregels van Programma-opstartcontrole

Standaard werkt Programma-opstartcontrole in de modus Black list. Dit onderdeel staat alle gebruikers toe om alle programma's te starten. Wanneer een gebruiker probeert om een programma te starten dat door regels van Programma-opstartcontrole is geblokkeerd, blokkeert Kaspersky Endpoint Security de start van het programma (als de actie **Blokkeren** is geselecteerd) of slaat het informatie over de start van het programma op in een rapport (als de actie **Melden** is geselecteerd).

Regels van Programma-opstartcontrole beheren

U kunt de volgende acties voor regels van Programma-opstartcontrole uitvoeren:

- Een nieuwe regel toevoegen
- De voorwaarden voor de activatie van een regel aanmaken of wijzigen
- De regelstatus bewerken

  Een regel van Programma-opstartcontrole kan worden ingeschakeld (het selectievakje naast de regel is ingeschakeld) of uitgeschakeld (het selectievakje naast de regel is uitgeschakeld). Een regel van Programma-opstartcontrole wordt standaard ingeschakeld nadat deze is aangemaakt.
- Regel verwijderen

Een regel van Programma-opstartcontrole toevoegen en bewerken

Zo voegt u een regel van Programma-opstartcontrole toe en bewerkt u die:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.
3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.
4. Voer een van de volgende acties uit:

   - Klik op de knop **Toevoegen** om een regel toe te voegen.
   - Als u een bestaande regel wilt bewerken, selecteert u die in de lijst met regels en klikt u op de knop **Bewerken**.

   Het venster **Regel van Programma-opstartcontrole** wordt geopend.
5. Geef de instellingen van de regel op of bewerk ze:

   a. Typ of bewerk in het veld **Naam regel** de naam van de regel.

   b. In de tabel **Uitvoeringsvoorwaarden** maakt of bewerkt u de lijst met uitvoeringsvoorwaarden die een regel activeren door op de knoppen **Toevoegen**, **Bewerken**, **Verwijderen** en **Omzetten naar uitzondering** te klikken.

   c. In de tabel **Uitzonderingsvoorwaarden** maakt of bewerkt u de lijst met uitzonderingsvoorwaarden die een regel activeren door op de knoppen **Toevoegen**, **Bewerken**, **Verwijderen** en **Omzetten naar uitvoering** te klikken.

d. Wijzig indien nodig de soort voorwaarde voor de activatie van de voorwaarde:

- Als u de soort voorwaarde wilt veranderen van een uitvoeringsvoorwaarde naar een uitzonderingsvoorwaarde, selecteert u een voorwaarde in de tabel **Uitvoeringsvoorwaarden** en klikt u op de knop **Omzetten naar uitzondering**.
- Als u de soort voorwaarde wilt veranderen van een uitzonderingsvoorwaarde naar een uitvoeringsvoorwaarde, selecteert u een voorwaarde in de tabel **Uitzonderingsvoorwaarden** en klikt u op de knop **Omzetten naar uitvoering**.

e. Maak of bewerk een lijst met gebruikers en/of groepen van gebruikers die al dan niet programma's mogen starten die aan de activeringsvoorwaarden van de regel voldoen. Klik hiervoor op de knop **Toevoegen** in de tabel **Principals en hun rechten**.

Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend. In dit venster kunt u gebruikers en/of groepen van gebruikers selecteren.

De waarde **Iedereen** is standaard toegevoegd aan de lijst met gebruikers. De regel geldt voor alle gebruikers.

> Als er geen gebruiker in de tabel is opgegeven, kan de regel niet worden opgeslagen.

f. Schakel in de tabel **Principals en hun rechten** de selectievakjes **Toestaan** of **Blokkeren** naast de gebruikers en/of groepen van gebruikers in om hun recht voor het starten van programma's te bepalen.

Het standaard ingeschakelde selectievakje hangt af van de uitvoermodus van Programma-opstartcontrole.

g. Schakel het selectievakje **Weigeren voor andere gebruikers** in als u wilt instellen dat alle gebruikers die niet in de kolom **Principal** verschijnen en die geen lid zijn van de opgegeven groep van gebruikers in de kolom **Principal** geen programma's mogen starten die aan de voorwaarden voor de activatie van de regel voldoen.

> Als het selectievakje **Weigeren voor andere gebruikers** is uitgeschakeld, controleert Kaspersky Endpoint Security niet de opstart van programma's door gebruikers die niet zijn opgegeven in de tabel **Principals en hun rechten** en die niet behoren tot opgegeven groepen van gebruikers in de tabel **Principals en hun rechten**.

h. Als u wilt dat Kaspersky Endpoint Security programma's die voldoen aan de activeringsvoorwaarden van de regel beschouwt als vertrouwde updaters die andere programma's mogen starten waarvoor geen regels van Programma-opstartcontrole zijn gedefinieerd, schakelt u het selectievakje **Vertrouwde updaters** in.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een activeringsvoorwaarde voor een regel van Programma-opstartcontrole toevoegen

Zo voegt u een nieuwe activeringsvoorwaarde voor een regel van Programma-opstartcontrole toe:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.

3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.

4. Voer een van de volgende acties uit:

   - Als u een nieuwe regel wilt aanmaken en een activeringsvoorwaarde eraan wilt toevoegen, klikt u op de knop **Toevoegen**.

   - Als u een activeringsvoorwaarde aan een bestaande regel wilt toevoegen, selecteert u de regel in de lijst met regels en klikt u op de knop **Bewerken**.

   Het venster **Regel van Programma-opstartcontrole** wordt geopend.

5. Klik in de tabel **Uitvoeringsvoorwaarden** of **Uitzonderingsvoorwaarden** op de knop **Toevoegen**.

U kunt de vervolgkeuzelijst van de knop **Toevoegen** gebruiken om verschillende activeringsvoorwaarden aan de regel toe te voegen (raadpleeg de onderstaande instructies).

Zo voegt u een activeringsvoorwaarde voor een regel toe op basis van de eigenschappen van bestanden in de opgegeven map:

1. Selecteer in de vervolgkeuzelijst van de knop **Toevoegen** de optie **Voorwaarde(n) uit eigenschappen van bestanden in de opgegeven map**.

   Het standaardvenster **Map selecteren** wordt in Microsoft Windows geopend.

2. Selecteer in het venster **Map selecteren** een map met de uitvoerbare bestanden van programma's waarvan u de eigenschappen wilt gebruiken als basis voor een of meerdere voorwaarden voor de activatie van een regel.

3. Klik op **OK**.

   Het venster **Voorwaarde toevoegen** wordt geopend.

4. Selecteer in de vervolgkeuzelijst **Weergavecriterium** het criterium dat u wilt gebruiken om een of meerdere voorwaarden voor de activatie van een regel aan te maken: **Hash-code bestand**, **Certificaat**, **KL-categorie**, **Metagegevens** of **Pad naar map**.

   Kaspersky Endpoint Security ondersteunt geen MD5 hash-code voor bestanden en controleert de start van programma's niet op basis van een MD5 hash. Een SHA256 hash wordt als activeringsvoorwaarde voor regels gebruikt.

5. Als u **Metagegevens** in de vervolgkeuzelijst **Weergavecriterium** hebt geselecteerd, schakelt u de selectievakjes naast de eigenschappen van uitvoerbare bestanden in die u in de activeringsvoorwaarde van de regel wilt gebruiken: **Bestandsnaam**, **Bestandsversie**, **Programmanaam**, **Programmaversie** en **Leverancier**.

   Als geen opgegeven eigenschappen zijn geselecteerd, kan de regel niet worden opgeslagen.

6. Als u **Certificaat** in de vervolgkeuzelijst **Weergavecriterium** hebt geselecteerd, schakelt u de selectievakjes naast de instellingen in die u in de activeringsvoorwaarde van de regel wilt gebruiken: **Verlener**, **Principal** en **Vingerafdruk**.

   Als geen opgegeven instellingen zijn geselecteerd, kan de regel niet worden opgeslagen.

   U wordt afgeraden om alleen de criteria **Verlener** en **Principal** als activeringsvoorwaarden voor regels te gebruiken. Het gebruik van deze criteria is onbetrouwbaar.

7. Schakel de selectievakjes naast de namen van de uitvoerbare bestanden van programma's in waarvan u de eigenschappen wilt opnemen in de activeringsvoorwaarden voor regels.

8. Klik op de knop **Volgende**.

   Een lijst met geformuleerde activeringsvoorwaarden voor regels wordt weergegeven.

9. In de lijst met geformuleerde activeringsvoorwaarden voor regels schakelt u de selectievakjes naast de activeringsvoorwaarden voor regels in die u aan de regel van Programma-opstartcontrole wilt toevoegen.

10. Klik op de knop **Beëindigen**.

Zo voegt u een activeringsvoorwaarde voor een regel toe op basis van de eigenschappen van programma's die op de computer zijn gestart:

1. Selecteer in de vervolgkeuzelijst van de knop **Toevoegen** de optie **Voorwaarde(n) uit eigenschappen van gestarte programma's**.

2. Selecteer in de vervolgkeuzelijst **Weergavecriterium** in het venster **Voorwaarde toevoegen** het criterium dat u wilt gebruiken om een of meerdere voorwaarden voor de activatie van een regel aan te maken: **Hash-code bestand**, **Certificaat**, **KL-categorie**, **Metagegevens** of **Pad naar map**.

3. Als u **Metagegevens** in de vervolgkeuzelijst **Weergavecriterium** hebt geselecteerd, schakelt u de selectievakjes naast de eigenschappen van uitvoerbare bestanden in die u in de activeringsvoorwaarde van de regel wilt gebruiken: **Bestandsnaam**, **Bestandsversie**, **Programmanaam**, **Programmaversie** en **Leverancier**.

   Als geen opgegeven eigenschappen zijn geselecteerd, kan de regel niet worden opgeslagen.

4. Als u **Certificaat** in de vervolgkeuzelijst **Weergavecriterium** hebt geselecteerd, schakelt u de selectievakjes naast de instellingen in die u in de activeringsvoorwaarde van de regel wilt gebruiken: **Verlener**, **Principal** en **Vingerafdruk**.

   Als geen opgegeven instellingen zijn geselecteerd, kan de regel niet worden opgeslagen.

   U wordt afgeraden om alleen de criteria **Verlener** en **Principal** als activeringsvoorwaarden voor regels te gebruiken. Het gebruik van deze criteria is onbetrouwbaar.

5. Schakel de selectievakjes naast de namen van de uitvoerbare bestanden van programma's in waarvan u de eigenschappen wilt opnemen in de activeringsvoorwaarden voor regels.

6. Klik op de knop **Volgende**.

   Een lijst met geformuleerde activeringsvoorwaarden voor regels wordt weergegeven.

7. In de lijst met geformuleerde activeringsvoorwaarden voor regels schakelt u de selectievakjes naast de activeringsvoorwaarden voor regels in die u aan de regel van Programma-opstartcontrole wilt toevoegen.

8. Klik op de knop **Beëindigen**.

Zo voegt u een activeringsvoorwaarde voor een regel toe op basis van een KL-categorie:

1. Selecteer in de vervolgkeuzelijst van de knop **Toevoegen** de optie **Voorwaarde(n) "KL-categorie"**.

   Een *KL-categorie* is een lijst met programma's die dezelfde themakenmerken hebben. De lijst wordt door experts van Kaspersky bijgewerkt. De KL-categorie "Office-programma's" bevat bijvoorbeeld programma's uit de Microsoft Office-suite, Adobe® Acrobat® en andere.

2. Schakel in het venster **Voorwaarde(n) "KL-categorie"** de selectievakjes naast de namen van de KL-categorieën in die u wilt gebruiken om activeringsvoorwaarden voor regels aan te maken.

3. Klik op **OK**.

Zo voegt u een activeringsvoorwaarde voor een regel toe:

1. Selecteer in de vervolgkeuzelijst van de knop **Toevoegen** de optie **Aangepaste voorwaarde**.
2. Klik in het venster **Aangepaste voorwaarde** de knop **Selecteren** en geef het pad naar het uitvoerbare bestand van het programma op.
3. Selecteer het criterium dat u wilt gebruiken om een activeringsvoorwaarde voor een regel aan te maken: **Hash-code bestand**, **Certificaat**, **Metagegevens** of **Pad naar bestand of map**.

   Als u symbolische koppelingen in het veld **Pad naar bestand of map** gebruikt, doet u er goed aan de symbolische koppelingen om te zetten opdat de regel van Programma-opstartcontrole correct zou werken. Klik hiertoe op de knop **Symbolische koppeling omzetten**.

4. Configureer indien nodig de instellingen van het geselecteerde criterium.
5. Klik op **OK**.

Zo voegt u een activeringsvoorwaarde voor een regel toe op basis van de informatie over de schijf waarop het uitvoerbare bestand van een programma is opgeslagen:

1. Selecteer in de vervolgkeuzelijst van de knop **Toevoegen** de optie **Voorwaarde op basis van station**.
2. Selecteer In de vervolgkeuzelijst **Schijf** in het venster **Voorwaarde op basis van station** het type van de schijf met de gestarte programma's dat als activeringsvoorwaarde voor een regel moet dienen.
3. Klik op **OK**.

De status van een regel van Programma-opstartcontrole wijzigen

Zo wijzigt u de status van een regel van Programma-opstartcontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.

3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.
4. Selecteer de regel waarvan u de status wilt bewerken.
5. Doe in de kolom **Status** het volgende:
   - Als u het gebruik van een regel wilt inschakelen, schakelt u het selectievakje naast de regel in.
   - Als u het gebruik van een regel wilt uitschakelen, schakelt u het selectievakje naast de regel uit.
6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels van Programma-opstartcontrole testen

Als u ervoor wilt zorgen dat Programma-opstartcontrole geen programma's blokkeert die u nodig hebt voor uw werk, wordt u aanbevolen om nieuwe regels in de testmodus te plaatsen en hun werking te analyseren.

Voor een analyse van de werking van de regels van Programma-opstartcontrole moeten de gebeurtenissen van Programma-opstartcontrole die worden gerapporteerd aan Kaspersky Security Center worden onderzocht. Als alle programma's voor het werk van de gebruiker op de computer kunnen worden gestart, zijn de regels naar behoren aangemaakt. Anders raden we aan dat u de instellingen van de gemaakte regels controleert.

De testmodus voor regels van Programma-opstartcontrole is standaard uitgeschakeld.

Zo test u de regels van Programma-opstartcontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.
3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.
4. Selecteer in de vervolgkeuzelijst **Modus van Programma-opstartcontrole** een van de volgende opties:

   - **Blacklist** als u de start van alle programma's behalve de opgegeven programma's in de Blokkeren-regels wilt toestaan.
   - **White list** als u de start van alle programma's behalve de opgegeven programma's in de Toestaan-regels wilt blokkeren.
5. Selecteer in de vervolgkeuzelijst **Actie** de optie **Melden**.
6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Kaspersky Endpoint Security blokkeert geen programma's waarvan de opstart is verboden door regels van Programma-opstartcontrole maar stuurt wel meldingen over de opstart ervan naar de Administration Server.

Berichtsjablonen van Programma-opstartcontrole bewerken

Wanneer een gebruiker een programma probeert te starten dat door een regel van Programma-opstartcontrole is geblokkeerd, toont Kaspersky Endpoint Security een bericht met de melding dat de start van het programma is geblokkeerd. Als de gebruiker vindt dat de start van een programma per vergissing is geblokkeerd, kan de gebruiker de koppeling in de tekst van het bericht gebruiken om een bericht naar de lokale netwerkbeheerder te sturen.

Speciale sjablonen zijn beschikbaar voor het bericht dat wordt weergegeven wanneer de start van een programma wordt geblokkeerd en voor het bericht dat naar de beheerder wordt verstuurd. U kunt de berichtsjablonen wijzigen.

Zo bewerkt u een berichtsjabloon:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.

3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.

4. Klik op de knop **Sjablonen**.

   Het venster **Berichtsjablonen** wordt geopend.

5. Voer een van de volgende acties uit:

   - Als u de sjabloon wilt bewerken voor het bericht dat wordt weergegeven wanneer de start van een programma wordt geblokkeerd, selecteert u het tabblad **Blokkering**.
   - Als u de sjabloon wilt bewerken voor het bericht dat naar de netwerkbeheerder wordt verstuurd, selecteert u het tabblad **Bericht aan beheerder**.

6. Wijzig de sjabloon van het bericht dat wordt weergegeven wanneer de start van een programma wordt geblokkeerd of van het bericht dat naar de beheerder wordt verstuurd. Gebruik hiervoor de knoppen **Standaard** en **Variabele**.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Over de uitvoermodi van Programma-opstartcontrole

Het onderdeel Programma-opstartcontrole werkt in twee modi:

- **Blacklist**. In deze modus staat Programma-opstartcontrole toe dat alle gebruikers alle programma's starten, behalve de programma's die in Blokkeren-regels van Programma-opstartcontrole zijn opgegeven.

  Deze modus van Programma-opstartcontrole is standaard ingeschakeld.

- **White list**. In deze modus staat Programma-opstartcontrole niet toe dat alle gebruikers alle programma's starten, behalve de programma's die in Toestaan-regels van Programma-opstartcontrole zijn opgegeven.

  Als de Toestaan-regels van Programma-opstartcontrole volledig zijn geconfigureerd, staat het onderdeel niet toe dat nieuwe programma's die niet zijn gecontroleerd door de netwerkbeheerder worden gestart. Het staat wel toe dat het besturingssysteem en vertrouwde programma's die gebruikers voor hun werk gebruiken worden uitgevoerd.

Elke modus heeft twee acties om op actieve programma's toe te passen: Kaspersky Endpoint Security kan verhinderen dat de programma's worden gestart of kan de gebruiker verwittigen dat er een programma is gestart dat aan de voorwaarden van de regels van Programma-opstartcontrole voldoet.

De werking van Programma-opstartcontrole in deze modi kan zowel in de lokale interface van Kaspersky Endpoint Security als in Kaspersky Security Center worden geconfigureerd.

Kaspersky Security Center beschikt wel over tools die niet beschikbaar zijn in de lokale interface van Kaspersky Endpoint Security, zoals de noodzakelijke tools voor de volgende taken:

- Categorieën van programma's aanmaken.

De regels van Programma-opstartcontrole die worden aangemaakt in de Beheerconsole van Kaspersky Security Center zijn gebaseerd op aangepaste categorieën van programma's en niet op uitvoerings- of uitzonderingsvoorwaarden zoals in de lokale interface van Kaspersky Endpoint Security.

- Informatie over geïnstalleerde programma's op netwerkcomputers verzamelen.

Dit is de reden waarom u wordt aanbevolen om Kaspersky Security Center te gebruiken voor de configuratie van de werking van het onderdeel Programma-opstartcontrole.

De modus van Programma-opstartcontrole selecteren

Zo selecteert u de modus van Programma-opstartcontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.
3. Schakel het selectievakje **Programma-opstartcontrole inschakelen** in om de instellingen van het onderdeel te kunnen bewerken.
4. Selecteer in de vervolgkeuzelijst **Modus van Programma-opstartcontrole** een van de volgende opties:

   - **Blacklist** als u de start van alle programma's behalve de opgegeven programma's in de Blokkeren-regels wilt toestaan.
   - **White list** als u de start van alle programma's behalve de opgegeven programma's in de Toestaan-regels wilt blokkeren.

     Wanneer deze modus is geselecteerd, worden standaard twee regels van Programma-opstartcontrole aangemaakt: **Golden Image** en **Vertrouwde updaters**. U kunt deze regels niet verwijderen. De instellingen van deze regels kunnen niet worden bewerkt. U kunt deze regels inschakelen of uitschakelen door het selectievakje naast de relevante regel in of uit te schakelen. Standaard is de regel **Golden Image** ingeschakeld en is de regel **Vertrouwde updaters** uitgeschakeld. Alle gebruikers mogen programma's starten die aan de activeringsvoorwaarden van deze regels voldoen.

   Alle gemaakte regels tijdens de geselecteerde modus worden opgeslagen nadat de modus wordt gewijzigd zodat de regels opnieuw kunnen worden gebruikt. Om deze regels opnieuw te gebruiken, hoeft u gewoon de noodzakelijke modus in de vervolgkeuzelijst **Modus van Programma-opstartcontrole** te selecteren.
5. Selecteer in de vervolgkeuzelijst **Actie** de actie die door het onderdeel moet worden uitgevoerd wanneer een gebruiker een programma probeert te starten dat door de regels van Programma-opstartcontrole is geblokkeerd.
6. Schakel het selectievakje **Monitor DLL and drivers** in als u wilt dat Kaspersky Endpoint Security het laden van DLL-modules monitort wanneer programma's worden gestart door gebruikers.

   Informatie over de module en het programma dat de module heeft geladen wordt in een rapport opgeslagen.

Als het selectievakje is ingeschakeld, worden DLL-modules en stuurprogramma's gemonitord voordat Kaspersky Endpoint Security wordt gestart. Om voortaan alle DLL-modules en stuurprogramma's ook te monitoren vóór de opstart van het programma start u de computer opnieuw op nadat u het selectievakje **DLL en stuurprogramma's monitoren** hebt ingeschakeld. Als u de computer niet opnieuw kunt opstarten, kunt u na de inschakeling van het selectievakje **DLL en stuurprogramma's monitoren** DLL en stuurprogramma's laden terwijl Kaspersky Endpoint Security actief is. In dit geval wordt de monitoring alleen toegepast op DLL-modules en stuurprogramma's die worden geladen wanneer Kaspersky Endpoint Security actief is.

Tijdens de monitoring van DLL-modules en stuurprogramma's gebruikt u beter geen regels van Programma-opstartcontrole die op basis van de KL-categorieën zijn aangemaakt. De KL-categorieën (inclusief de regels 'Besturingssysteem en onderdelen ervan') voor DLL-modules en stuurprogramma's worden mogelijk niet naar behoren bepaald. De regel "Besturingssysteem en onderdelen ervan" is met name standaard aangemaakt en wordt niet verdeeld bij de start van DLL-modules en stuurprogramma's. Wanneer u deze functie inschakelt, moet u aparte Toestaan-regels voor DLL-modules en stuurprogramma's aanmaken. Het gebruik van de functie **DLL en stuurprogramma's monitoren** zonder zulke Toestaan-regels kan het systeem instabiel maken.

We raden aan dat u de wachtwoordbeveiliging voor de configuratie van programma-instellingen inschakelt zodat u Toestaan-regels die de start van essentiële DLL-modules en stuurprogramma's blokkeren kunt uitschakelen terwijl u tegelijk geen instellingen van het Kaspersky Security Center-beleid wijzigt.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels van Programma-opstartcontrole beheren via Kaspersky Security Center

In deze sectie vindt u informatie over het gebruik van Kaspersky Security Center voor de configuratie van de regels van Programma-opstartcontrole en krijgt u aanbevelingen voor het optimaal gebruik van Programma-opstartcontrole.

Informatie over geïnstalleerde programma's op netwerkcomputers verzamelen

Om optimale regels voor Programma-opstartcontrole aan te maken, moet u eerst weten welke programma's op de computers in het lokale netwerk worden gebruikt. Hiertoe kunt u de volgende informatie verkrijgen:

- Leveranciers, versies en taalversies van de gebruikte programma's in het bedrijfsnetwerk.
- Frequentie van programma-updates.
- Bedrijfsbeleid voor het gebruik van programma's (dit is mogelijk het beveiligingsbeleid of het administratieve beleid).
- Opslaglocatie van de distributiepakketten van programma's.

Informatie over programma's die worden gebruikt op computers in het bedrijfsnetwerk vindt u in de mappen **Programmaregister** en **Uitvoerbare bestanden**. De mappen **Programmaregister** en **Uitvoerbare bestanden** bevinden zich in de map **Programmabeheer** in de structuur van de Beheerconsole van Kaspersky Security Center.

De map **Programmaregister** bevat de lijst met programma's die zijn gevonden door Netwerkagent dat op de clientcomputer is geïnstalleerd.

De map **Uitvoerbare bestanden** bevat een lijst met alle uitvoerbare bestanden die ooit zijn gestart op clientcomputers of die tijdens de inventarisatie van Kaspersky Endpoint Security zijn gevonden.

Om algemene informatie over het programma en de uitvoerbare bestanden ervan te bekijken en om de lijst met computers waarop een programma is geïnstalleerd te zien, opent u het venster met de eigenschappen van een geselecteerd programma in de mappen **Programmaregister** of **Uitvoerbare bestanden**.

Categorieën van programma's aanmaken

Om makkelijker regels aan te maken, kunt u categorieën van programma's aanmaken en ze gebruiken wanneer u regels voor Programma-opstartcontrole aanmaakt.

U wordt aanbevolen de categorie "Programma's voor werk" aan te maken waarin u de standaardprogramma's van uw werk onderbrengt. Als andere gebruikersgroepen andere programma's voor hun werk gebruiken, kunt u een aparte categorie van programma's aanmaken voor elke gebruikersgroep.

Zo maakt u een categorie van programma's aan:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Extra** → **Programmabeheer** → **Programmacategorieën**.
3. Klik op de knop **Categorie aanmaken** in de werkruimte.

   De wizard voor het aanmaken van een gebruikerscategorie wordt gestart.
4. Volg de instructies van de wizard voor het aanmaken van een gebruikerscategorie.

Regels van Programma-opstartcontrole aanmaken via Kaspersky Security Center

Zo maakt u een regel voor Programma-opstartcontrole aan via Kaspersky Security Center:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Endpoint-controle** het subgedeelte **Programma-opstartcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.

7. Klik op de knop **Toevoegen**.

   Het venster **Regel van Programma-opstartcontrole** wordt geopend.

8. Selecteer in de vervolgkeuzelijst **Categorie** de aangemaakte programmacategorie die u als basis wilt gebruiken om een regel aan te maken.

9. Geef de lijst met gebruikers en / of groepen van gebruikers op waarvoor u wilt instellen dat ze programma's uit de geselecteerde categorie mogen starten. Klik hiervoor in de tabel **Principals en hun rechten** op de knop **Toevoegen**.

   Het standaardvenster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend. In dit venster kunt u gebruikers en/of groepen van gebruikers selecteren.

10. In de tabel **Principals en hun rechten**:

    - Als u wilt toestaan dat gebruikers en / of groepen van gebruikers programma's uit de geselecteerde categorie mogen starten, schakelt u het selectievakje **Toestaan** naast die gebruikers in.

    - Als u niet wilt toestaan dat gebruikers en / of groepen van gebruikers programma's uit de geselecteerde categorie mogen starten, schakelt u het selectievakje **Blokkeren** naast die gebruikers in.

11. Schakel het selectievakje **Weigeren voor andere gebruikers** in als u wilt instellen dat alle gebruikers die niet in de kolom **Principal** verschijnen en die geen lid zijn van de opgegeven groep van gebruikers in de kolom **Principal** geen programma's mogen starten die tot de geselecteerde categorie behoren.

12. Als u wilt dat Kaspersky Endpoint Security programma's uit de opgegeven categorie in de regel beschouwt als vertrouwde updaters die andere programma's mogen starten waarvoor geen regels van Programma-opstartcontrole zijn gedefinieerd, schakelt u het selectievakje **Vertrouwde updaters** in.

13. Klik op **OK**.

14. Klik in het gedeelte **Programma-opstartcontrole** van het venster met de eigenschappen van het beleid op de knop **Toepassen**.

De status van een regel van Programma-opstartcontrole wijzigen via Kaspersky Security Center

Zo wijzigt u de status van een regel van Programma-opstartcontrole:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

- Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Endpoint-controle** het subgedeelte **Programma-opstartcontrole**.
   Rechts in het venster ziet u de instellingen van het onderdeel Programma-opstartcontrole.
7. Selecteer de regel van Programma-opstartcontrole waarvan u de status wilt wijzigen.
8. Doe in de kolom **Status** een van het volgende:
   - Als u het gebruik van een regel wilt inschakelen, schakelt u het selectievakje naast de regel in.
   - Als u het gebruik van een regel wilt uitschakelen, schakelt u het selectievakje naast de regel uit.
9. Klik op de knop **Toepassen**.

Controle van programmabevoegdheden

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Controle van programmabevoegdheden en leest u hoe u de instellingen van het onderdeel configureert.

Over Controle van programmabevoegdheden

Controle van programmabevoegdheden voorkomt dat programma's acties uitvoeren die mogelijk gevaarlijk zijn voor het besturingssysteem en controleert de toegang tot bronnen van het besturingssysteem en identiteitsgegevens.

Dit onderdeel controleert de activiteit van programma's, inclusief de toegang ervan tot beschermde bronnen (zoals bestanden en mappen, registersleutels), door middel van *regels voor programmacontrole*. De regels voor programmacontrole zijn een reeks beperkingen die worden toegepast op verschillende acties van programma's in het besturingssysteem en op rechten voor de toegang tot computerbronnen.

De netwerkactiviteit van programma's wordt door het onderdeel Firewall gemonitord.

Wanneer een programma voor het eerst wordt gestart, scant Controle van programmabevoegdheden het programma en plaatst het het programma in een vertrouwensgroep. Een vertrouwensgroep definieert de regels voor programmacontrole die Kaspersky Endpoint Security toepast wanneer de programma-activiteit wordt gecontroleerd.

We raden aan dat u deelneemt aan Kaspersky Security Network om Controle van programmabevoegdheden efficiënter te laten werken. Met de gegevens die worden verkregen via Kaspersky Security Network kunt u programma's beter groeperen en kunt u optimale regels voor programmacontrole toepassen.

De volgende keer dat het programma wordt gestart, controleert Controle van programmabevoegdheden de integriteit van het programma. Als het programma niet is gewijzigd, past het onderdeel de huidige regels voor programmacontrole erop toe. Als het programma is gewijzigd, scant Controle van programmabevoegdheden het opnieuw alsof het voor het eerst wordt gestart.

Beperkingen van de controle van audio- en videoapparaten

Over de bescherming van audiostreams

Bij de bescherming van audiostreams moet u rekening houden met de volgende speciale aandachtspunten:

- Het onderdeel Controle van programmabevoegdheden moet ingeschakeld zijn opdat deze functionaliteit zou werken.

- Als het programma de audiostream al ontving voordat het onderdeel Controle van programmabevoegdheden was gestart, staat Kaspersky Endpoint Security toe dat het programma de audiostream ontvangt en toont het geen meldingen.
- Als u het programma hebt verplaatst naar de groep **Niet vertrouwd** of **Zeer beperkt** nadat het programma de audiostream begon te ontvangen, staat Kaspersky Endpoint Security toe dat het programma de audiostream ontvangt en toont het geen meldingen.
- Na het wijzigen van de instellingen voor de toegang van programma's tot geluidsopnameapparaten (u hebt bijvoorbeeld in het venster met de instellingen van Programmacontrole ingesteld dat het programma geen audiostreams mag ontvangen), moet dit programma opnieuw worden gestart opdat het geen audiostreams meer zou ontvangen.
- De controle van de toegang tot de audiostream van geluidsopnameapparaten is niet afhankelijk van de instellingen voor de webcamtoegang van een programma.
- Kaspersky Endpoint Security beschermt alleen de toegang tot ingebouwde en externe microfoons. Andere apparaten voor het streamen van audio worden niet ondersteund.
- Kaspersky Endpoint Security kan de bescherming van een audiostream vanaf apparaten zoals DSLR-camera's, draagbare videocamera's en actiecamera's niet verzekeren.

Speciale aandachtspunten bij het gebruik van audio- en videoapparaten tijdens de installatie en de upgrade van Kaspersky Endpoint Security

Wanneer u voor het eerst programma's voor het opnemen of afspelen van audio en video start na de installatie van Kaspersky Endpoint Security, wordt het afspelen of opnemen van audio en video mogelijk onderbroken. Dit is nodig om de functionaliteit in te schakelen die de toegang van programma's tot geluidsopnameapparaten controleert. De systeemservice die de audiohardware controleert, wordt opnieuw gestart wanneer Kaspersky Endpoint Security voor het eerst wordt uitgevoerd.

Over de toegang van programma's tot webcams

Bij de functionaliteit voor de bescherming van de toegang tot webcams moet u rekening houden met de volgende speciale aandachtspunten en beperkingen:

- Het programma controleert video's en afbeeldingen die uit gegevens van webcams worden verwerkt.
- Het programma controleert de audiostream als die deel uitmaakt van de videostream afkomstig van de webcam.
- Het programmacontrole controleert alleen webcams die via USB of IEEE1394 zijn aangesloten en die als **Beeldapparaten** in Windows Apparaatbeheer worden weergegeven.

Ondersteunde webcams

Kaspersky Endpoint Security ondersteunt de volgende webcams:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210

- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky kan de ondersteuning voor webcams die niet voorkomen in deze lijst niet verzekeren.

Controle van programmabevoegdheden inschakelen en uitschakelen

Controle van programmabevoegdheden is standaard ingeschakeld en werkt in een modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig Controle van programmabevoegdheden uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Controle van programmabevoegdheden in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Endpoint-controle**.

   Het gedeelte **Endpoint-controle** wordt geopend.
4. Klik rechts om het contextmenu van de regel weer te geven dat informatie over het onderdeel Controle van programmabevoegdheden bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:

   - Selecteer **Starten** om Controle van programmabevoegdheden in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel Controle van programmabevoegdheden, wijzigt in het pictogram .
   - Selecteer **Stoppen** om Controle van programmabevoegdheden uit te schakelen.

     Het statuspictogram van het onderdeel , links in de regel Controle van programmabevoegdheden, wijzigt in het pictogram .

Zo schakelt u Controle van programmabevoegdheden in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Doe rechts in het venster één van het volgende:

   - Schakel het selectievakje **Controle van programmabevoegdheden inschakelen** in om Controle van programmabevoegdheden in te schakelen.
   - Schakel het selectievakje **Controle van programmabevoegdheden inschakelen** uit om Controle van programmabevoegdheden uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Vertrouwensgroepen voor programma's beheren

Wanneer een programma voor het eerst wordt gestart, controleert het onderdeel Controle van programmabevoegdheden de beveiliging van het programma en plaatst het het programma in een vertrouwensgroep.

Tijdens de eerste fase van de scan van het programma zoekt Kaspersky Endpoint Security in de interne database van bekende programma's naar een overeenkomstig programma en stuurt het tegelijkertijd een verzoek naar de database van Kaspersky Security Network (als een internetverbinding beschikbaar is). Op basis van de resultaten van de zoekopdracht in de interne database en de database van Kaspersky Security Network wordt het programma in een vertrouwensgroep geplaatst. Telkens als het programma wordt gestart, stuurt Kaspersky Endpoint Security een nieuw verzoek naar de database van KSN. Kaspersky Endpoint Security plaatst het programma in een andere vertrouwensgroep als de reputatie van het programma in de database van KSN is gewijzigd.

U kunt een vertrouwensgroep selecteren waaraan Kaspersky Endpoint Security alle onbekende programma's automatisch moet toewijzen. Programma's die zijn gestart vóór Kaspersky Endpoint Security worden automatisch verplaatst naar de vertrouwensgroep die in het venster **Vertrouwensgroep selecteren** is opgegeven.

Het onderdeel controleert alleen de netwerkactiviteit van programma's die zijn gestart vóór Kaspersky Endpoint Security op basis van de ingestelde netwerkregels in de instellingen van Firewall.

De instellingen voor de toewijzing van programma's aan vertrouwensgroepen configureren

Als de deelname aan Kaspersky Security Network is ingeschakeld, verstuurt Kaspersky Endpoint Security een verzoek over de reputatie van een programma naar KSN telkens als het programma wordt gestart. Naargelang het antwoord van KSN kan het programma worden verplaatst naar een vertrouwensgroep die verschilt van de opgegeven groep in de instellingen van Controle van programmabevoegdheden.

Zo configureert u de instellingen voor de toewijzing van programma's aan vertrouwensgroepen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Als u digitaal ondertekende programma's van vertrouwde leveranciers automatisch in de groep Vertrouwd wilt plaatsen, schakelt u het selectievakje **Vertrouw programma's met digitale handtekening** in.

   Vertrouwde leveranciers zijn de softwareleveranciers die door Kaspersky in de vertrouwde groep zijn opgenomen. U kunt ook handmatig een leverancierscertificaat toevoegen aan de vertrouwde systeemcertificatenopslag.
4. Kies de manier waarop onbekende programma's worden toegewezen aan vertrouwensgroepen:

   - Om de heuristische analyse voor de toewijzing van onbekende programma's aan vertrouwensgroepen te gebruiken, selecteert u de optie **Gebruik heuristische analyse om groep te definiëren** en geeft u de toegestane duur voor het scannen van het gestarte programma op in het veld **Maximale tijd om groep te definiëren**.
   - Als u alle onbekende programma's wilt toewijzen aan een opgegeven vertrouwensgroep, selecteert u de optie **Verplaats automatisch naar groep** en kiest u de gepaste vertrouwensgroep in de vervolgkeuzelijst.

     Om veiligheidsredenen wordt de groep **Vertrouwd** niet opgenomen in de waarden van de instelling **Verplaats automatisch naar groep**.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een vertrouwensgroep wijzigen

Wanneer een programma voor het eerst wordt gestart, plaatst Kaspersky Endpoint Security het programma automatisch in een vertrouwensgroep. U kunt indien nodig het programma handmatig verplaatsen naar een andere vertrouwensgroep.

Experts van Kaspersky raden af dat u programma's verplaatst van de automatisch toegewezen vertrouwensgroep naar een andere vertrouwensgroep. U kunt daarentegen de regels voor een individueel programma bewerken.

Zo wijzigt u de vertrouwensgroep waaraan een programma automatisch wordt toegewezen door Kaspersky Endpoint Security wanneer het voor eerst wordt gestart:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Programma's**.

   Het tabblad **Regels voor programmacontrole** in het venster **Programma's** wordt geopend.
4. Selecteer het relevante programma op het tabblad **Regels voor programmacontrole**.

5. Voer een van de volgende acties uit:

   - Klik rechts om het contextmenu van het programma weer te geven. Selecteer in het contextmenu van het programma de optie **Verplaatsen naar groep** → <γροεπσνααμ>.

   - Klik op de koppeling **Vertrouwd** / **Deels beperkt** / **Zeer beperkt** / **Niet vertrouwd** om het contextmenu te openen. Selecteer in het contextmenu de vereiste vertrouwensgroep.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security worden gestart

Het onderdeel controleert alleen de netwerkactiviteit van programma's die vóór Kaspersky Endpoint Security zijn gestart. De controle wordt uitgevoerd met de netwerkregels die in de instellingen van Firewall zijn opgegeven. U moet een vertrouwensgroep selecteren om op te geven welke netwerkregels u wilt toepassen op de monitoring van de netwerkactiviteit van deze programma's.

Zo selecteert u de vertrouwensgroep voor programma's die vóór Kaspersky Endpoint Security worden gestart:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.

3. Klik op de knop **Bewerken**.

   Hiermee opent u het venster **Vertrouwensgroep selecteren**.

4. Selecteer de noodzakelijke vertrouwensgroep.

5. Klik op **OK**.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels van Programmacontrole beheren

Standaard wordt de programma-activiteit beheerd door regels voor programmacontrole die zijn gedefinieerd voor de vertrouwensgroep waaraan Kaspersky Endpoint Security het programma heeft toegewezen wanneer dat programma voor het eerst werd gestart. U kunt indien nodig de regels voor programmacontrole bewerken voor een hele vertrouwensgroep, voor een individueel programma of voor een groep van programma's in een vertrouwensgroep.

Regels voor programmacontrole die zijn gedefinieerd voor individuele programma's of groepen van programma's in een vertrouwensgroep hebben een hogere prioriteit dan regels voor programmacontrole die voor een vertrouwensgroep zijn gedefinieerd. Als de instellingen van de regels voor programmacontrole voor een individueel programma of een groep van programma's in een vertrouwensgroep dus verschilt van de instellingen van de regels voor programmacontrole voor de vertrouwensgroep, beheert Controle van programmabevoegdheden de activiteit van het programma of de groep van programma's in de vertrouwensgroep volgens de regels voor programmacontrole die voor het programma of de groep van programma's zijn gedefinieerd.

Regels voor programmacontrole wijzigen voor vertrouwensgroepen en groepen van programma's

De optimale regels voor programmacontrole voor verschillende vertrouwensgroepen zijn standaard aangemaakt. De instellingen van de regels voor de controle van programmagroepen nemen de waarden van de instellingen van de regels voor de controle van vertrouwensgroepen over. U kunt de vooraf ingestelde regels voor de controle van vertrouwensgroepen en de regels voor de controle van programmagroepen bewerken.

Zo bewerkt u de regels voor de controle van vertrouwensgroepen of de regels voor de controle van programmagroepen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Programma's**.

   Hiermee opent u het tabblad **Regels voor programmacontrole** in het venster **Controle van programmabevoegdheden**.
4. Selecteer de noodzakelijke vertrouwensgroep of programmagroep.
5. Selecteer **Groepsregels** in het contextmenu van een vertrouwensgroep of een groep van programma's.

   Het venster **Regels voor controle van programmagroepen** wordt geopend.
6. Doe in het venster **Regels voor controle van programmagroepen** één van het volgende:

   - Selecteer het tabblad **Bestanden en systeemregister** om de regels voor de controle van vertrouwensgroepen of de regels voor de controle van programmagroepen te bewerken die de rechten van de vertrouwensgroep of de programmagroep voor de toegang tot het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
   - Selecteer het tabblad **Rechten** om de regels voor de controle van vertrouwensgroepen of de regels voor de controle van programmagroepen te bewerken die de rechten van de vertrouwensgroep of de programmagroep voor de toegang tot processen van het besturingssysteem en objecten beheren.
7. Klik rechts in de kolom met de overeenkomstige actie voor de vereiste bron om het contextmenu te openen.
8. Selecteer de vereiste optie in het contextmenu.

   - **Overnemen**
   - **Toestaan**

- **Blokkeren**
- **Gebeurtenissen registreren**

> Als u regels voor de controle van een vertrouwensgroep bewerkt, is de optie **Overnemen** niet beschikbaar.

9. Klik op **OK**.
10. Klik in het venster **Programma's** op **OK**.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een regel voor programmacontrole bewerken

De instellingen van de regels voor programmacontrole voor programma's die behoren tot een programmagroep of een vertrouwensgroep nemen standaard de waarden van de instellingen van de regels voor de controle van vertrouwensgroepen over. U kunt de instellingen van de regels voor programmacontrole bewerken.

Zo wijzigt u een regel voor programmacontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Programma's**.

   Hiermee opent u het tabblad **Regels voor programmacontrole** in het venster **Controle van programmabevoegdheden**.
4. Selecteer het noodzakelijke programma.
5. Voer een van de volgende acties uit:

   - Selecteer in het contextmenu van het programma de optie **Programmaregels**.
   - Klik op de knop **Extra** in de rechterbenedenhoek van het tabblad **Regels voor programmacontrole**.

   Het venster **Regels voor programmacontrole** wordt geopend.
6. Doe in het venster **Regels voor programmacontrole** één van het volgende:

   - Selecteer het tabblad **Bestanden en systeemregister** om de regels voor programmacontrole te bewerken die de rechten van het programma voor de toegang tot het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
   - Selecteer het tabblad **Rechten** om de regels voor programmacontrole te bewerken die de rechten van het programma voor de toegang tot processen van het besturingssysteem en objecten beheren.
7. Klik rechts in de kolom met de overeenkomstige actie voor de vereiste bron om het contextmenu te openen.

8. Selecteer de vereiste optie in het contextmenu.
    - **Overnemen**
    - **Toestaan**
    - **Blokkeren**
    - **Gebeurtenissen registreren**
9. Klik op **OK**.
10. Klik in het venster **Programma's** op **OK**.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels voor programmacontrole downloaden en bijwerken vanaf de Kaspersky Security Network-database uitschakelen

Wanneer nieuwe informatie over een programma wordt gevonden in de database van Kaspersky Security Network, zal Kaspersky Endpoint Security standaard de controleregels die vanaf de KSN-database zijn gedownload toepassen op dit programma. U kunt de controleregels voor het programma daarna handmatig bewerken.

Als een programma niet voorkwam in de database van Kaspersky Security Network wanneer het voor het eerst werd gestart en er is later informatie erover toegevoegd aan de database, werkt Kaspersky Endpoint Security standaard de controleregels voor dit programma bij.

U kunt het downloaden van regels voor programmacontrole vanaf de database van Kaspersky Security Network en het automatisch bijwerken van controleregels voor eerder onbekende programma's uitschakelen.

Zo schakelt u het downloaden en het bijwerken van regels voor programmacontrole vanaf de Kaspersky Security Network-database uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

    Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Schakel het selectievakje **Werk controleregels bij voor eerder onbekende programma's uit KSN-databases** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Overname van de beperkingen van het bovenliggende proces uitschakelen

De gebruiker of een ander actief programma kan het programma starten. Als het programma door een ander programma wordt gestart, wordt een opstartsequentie gemaakt die uit bovenliggende en onderliggende processen bestaat.

Wanneer een programma toegang tot een beschermde bron probeert te krijgen, analyseert Controle van programmabevoegdheden alle bovenliggende processen van het programma om te bepalen of deze processen over toegangsrechten voor de beschermde bron beschikken. De regel van de laagste prioriteit wordt dan gehanteerd: wanneer de toegangsrechten van het programma worden vergeleken met die van het bovenliggende proces, worden de toegangsrechten met de laagste prioriteit toegepast op de activiteit van het programma.

De prioriteit van de toegangsrechten is als volgt:

1. **Toestaan** Dit toegangsrecht heeft de hoogste prioriteit.
2. **Blokkeren** Dit toegangsrecht heeft de laagste prioriteit.

Dit mechanisme voorkomt dat een niet-vertrouwd programma of een programma met beperkte rechten een vertrouwd programma gebruikt om acties uit te voeren waarvoor bepaalde bevoegdheden vereist zijn.

Als de activiteit van een programma wordt geblokkeerd wegens onvoldoende rechten die aan een bovenliggend proces worden verleend, kunt u deze rechten bewerken of de overname van de beperkingen van het bovenliggende proces uitschakelen.

Zo schakelt u de overname van de beperkingen van het bovenliggende proces uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Programma's**.

   Hiermee opent u het tabblad **Regels voor programmacontrole** in het venster **Controle van programmabevoegdheden**.
4. Selecteer het noodzakelijke programma.
5. Selecteer in het contextmenu van het programma de optie **Programmaregels**.

   Het venster **Regels voor programmacontrole** wordt geopend.
6. Selecteer in het venster **Regels voor programmacontrole** het tabblad **Uitzonderingen**.
7. Schakel het selectievakje **Neem geen beperkingen van bovenliggend proces (programma) over** in.
8. Klik op **OK**.
9. Klik in het venster **Programma's** op **OK**.
10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Specifieke acties van programma's uitsluiten van regels voor programmacontrole

Zo sluit u specifieke acties van programma's uit van regels voor programmacontrole:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.

3. Klik op de knop **Programma's**.

   Hiermee opent u het tabblad **Regels voor programmacontrole** in het venster **Controle van programmabevoegdheden**.

4. Selecteer het noodzakelijke programma.

5. Selecteer in het contextmenu van het programma de optie **Programmaregels**.

   Het venster **Regels voor programmacontrole** wordt geopend.

6. Selecteer het tabblad **Uitzonderingen**.

7. Schakel de selectievakjes naast de programma-acties in die niet moeten worden gemonitord.

8. Klik op **OK**.

9. Klik in het venster **Programma's** op **OK**.

10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Verouderde regels voor programmacontrole verwijderen

Standaard worden controleregels voor programma's die in 60 dagen niet meer zijn gebruikt automatisch verwijderd. U kunt de opslagduur voor controleregels voor ongebruikte programma's wijzigen of de automatische verwijdering van regels uitschakelen.

Zo verwijdert u verouderde regels voor programmacontrole:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.

3. Voer een van de volgende acties uit:

   - Als u wilt dat Kaspersky Endpoint Security controleregels voor ongebruikte programma's verwijdert, schakelt u het selectievakje **Wis regels voor programma's die niet zijn gestart gedurende meer dan** in en geeft u het relevante aantal dagen op.

   - Om de automatische verwijdering van controleregels voor ongebruikte programma's uit te schakelen, schakelt u het selectievakje **Wis regels voor programma's die niet zijn gestart gedurende meer dan** uit.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bronnen van het besturingssysteem en identiteitsgegevens beschermen

Controle van programmabevoegdheden beheert de rechten van programma's voor het uitvoeren van bewerkingen op diverse categorieën van besturingssysteembronnen en identiteitsgegevens.

Experts van Kaspersky hebben vooraf ingestelde categorieën van beschermde bronnen gemaakt. U kunt de vooraf ingestelde categorieën van beschermde bronnen of de beschermde bronnen in deze categorieën niet bewerken of verwijderen.

U kunt de volgende acties uitvoeren:

- Een nieuwe categorie van beschermde bronnen toevoegen.
- Een nieuwe beschermde bron toevoegen.
- De bescherming van een bron uitschakelen.

Een categorie van beschermde bronnen toevoegen

Zo voegt u een nieuwe categorie van beschermde bronnen toe:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Bronnen**.

   Hiermee opent u het tabblad **Beschermde bronnen** van het venster **Controle van programmabevoegdheden**.
4. Selecteer links op het tabblad **Beschermde bronnen** een gedeelte of een categorie van beschermde bronnen waaraan u een nieuwe categorie van beschermde bronnen wilt toevoegen.
5. Klik op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst de optie **Categorie**.

   Het venster **Categorie van beschermde bronnen** wordt geopend.
6. Typ in het geopende venster **Categorie van beschermde bronnen** een naam voor de nieuwe categorie van beschermde bronnen.
7. Klik op **OK**.

   Een nieuwe optie wordt in de lijst met categorieën van beschermde bronnen weergegeven.
8. Klik in het venster **Controle van programmabevoegdheden** op **OK**.
9. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Nadat u een categorie van beschermde bronnen hebt toegevoegd, kunt u deze bewerken of verwijderen door te klikken op de knoppen **Bewerken** of **Verwijderen** links op het tabblad **Beschermde bronnen**.

Een beschermde bron toevoegen

Zo voegt u een beschermde bron toe:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik op de knop **Bronnen**.

   Hiermee opent u het tabblad **Beschermde bronnen** van het venster **Controle van programmabevoegdheden**.
4. Selecteer links op het tabblad **Beschermde bronnen** een categorie van beschermde bronnen waaraan u een nieuwe beschermde bron wilt toevoegen.
5. Klik op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst het type bron dat u wilt toevoegen:

   - **Bestand of map**.
   - **Registersleutel**.

   Het venster **Beschermde bron** wordt geopend.
6. Typ in het venster **Beschermde bron** de naam van de beschermde bron in het veld **Naam**.
7. Klik op de knop **Bladeren**.
8. Geef in het geopende venster de noodzakelijke instellingen op afhankelijk van het type beschermde bron dat u wilt toevoegen. Klik op **OK**.
9. Klik in het venster **Beschermde bron** op **OK**.

   Een nieuwe optie verschijnt in de lijst met beschermde bronnen van de geselecteerde categorie op het tabblad **Beschermde bronnen**.
10. Klik in het venster **Controle van programmabevoegdheden** op **OK**.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Nadat u een beschermde bron hebt toegevoegd, kunt u deze bewerken of verwijderen door te klikken op de knoppen **Bewerken** of **Verwijderen** links op het tabblad **Beschermde bronnen**.

Bescherming van bronnen uitschakelen

Zo schakelt u de bescherming van bronnen uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Controle van programmabevoegdheden**.

   Rechts in het venster ziet u de instellingen van het onderdeel Controle van programmabevoegdheden.
3. Klik rechts in het venster op de knop **Bronnen**.

Hiermee opent u het tabblad **Beschermde bronnen** van het venster **Controle van programmabevoegdheden**.

4. Voer een van de volgende acties uit:

   - Selecteer in de lijst met beschermde bronnen links op het tabblad de bron waarvoor u de bescherming wilt uitschakelen en schakel het selectievakje naast de naam ervan uit.

   - Klik op **Uitzonderingen** en doe het volgende:

     a. Klik in het venster **Uitzonderingen** op de knop **Toevoegen**. Selecteer in de vervolgkeuzelijst het type bron dat u wilt toevoegen aan de lijst met bronnen die niet moeten worden beschermd door het onderdeel Controle van programmabevoegdheden: **Bestand of map** of **Registersleutel**.

     Het venster **Beschermde bron** wordt geopend.

     b. Typ in het venster **Beschermde bron** de naam van de beschermde bron in het veld **Naam**.

     c. Klik op de knop **Bladeren**.

     d. Geef in het geopende venster de noodzakelijke instellingen op afhankelijk van het type beschermde bron dat u wilt toevoegen aan de lijst met bronnen die niet moeten worden beschermd door het onderdeel Controle van programmabevoegdheden.

     e. Klik op **OK**.

     f. Klik in het venster **Beschermde bron** op **OK**.

     Een nieuw element verschijnt in de lijst met bronnen die niet worden beschermd door het onderdeel Controle van programmabevoegdheden.

     > Na het toevoegen van een bron aan de lijst met bronnen die niet moeten worden beschermd door het onderdeel Controle van programmabevoegdheden kunt u deze bron bewerken of verwijderen door te klikken op de knoppen **Bewerken** of **Verwijderen** boven in het venster **Uitzonderingen**.

     g. Klik in het venster **Uitzonderingen** op **OK**.

5. Klik in het venster **Controle van programmabevoegdheden** op **OK**.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Kwetsbaarheidsbewaking

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Kwetsbaarheidsbewaking en instructies voor de in- en uitschakeling van het onderdeel.

Over Kwetsbaarheidsbewaking

Het onderdeel Kwetsbaarheidsbewaking voert in real time een kwetsbaarheidsscan van programma's uit die op de computer van de gebruiker actief zijn en door de gebruiker worden gestart. Wanneer het onderdeel Kwetsbaarheidsbewaking is ingeschakeld, moet u de Kwetsbaarheidsscan niet starten. Deze scan is relevant wanneer een Kwetsbaarheidsscan voor geïnstalleerde programma's op de computer van de gebruiker al lange tijd geleden is uitgevoerd of nog helemaal niet is uitgevoerd.

Kwetsbaarheidsbewaking inschakelen en uitschakelen

Het onderdeel Kwetsbaarheidsbewaking is standaard uitgeschakeld. U kunt indien nodig Kwetsbaarheidsbewaking inschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Zo schakelt u Kwetsbaarheidsbewaking in of uit op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Endpoint-controle**.

   Het gedeelte **Endpoint-controle** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Kwetsbaarheidsbewaking bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:

   - Selecteer **Starten** om Kwetsbaarheidsbewaking in te schakelen.

     Het statuspictogram van het onderdeel , links in de regel **Kwetsbaarheidsbewaking**, wijzigt in het pictogram .
   - Selecteer **Stoppen** om Kwetsbaarheidsbewaking uit te schakelen.

Het statuspictogram van het onderdeel , links in de regel **Kwetsbaarheidsbewaking**, wijzigt in het pictogram .

Zo schakelt u Kwetsbaarheidsbewaking in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster de optie **Kwetsbaarheidsbewaking**.

   Rechts in het venster ziet u de instellingen van het onderdeel Kwetsbaarheidsbewaking.
3. Doe rechts in het venster één van het volgende:

   - Als u wilt dat Kaspersky Endpoint Security een kwetsbaarheidsscan start voor de programma's die actief zijn op de computer van de gebruiker of door de gebruiker worden gestart, schakelt u het selectievakje **Kwetsbaarheidsbewaking inschakelen** in.
   - Als u niet wilt dat Kaspersky Endpoint Security een kwetsbaarheidsscan start voor de programma's die actief zijn op de computer van de gebruiker of door de gebruiker worden gestart, schakelt u het selectievakje **Kwetsbaarheidsbewaking inschakelen** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Apparaatcontrole

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Apparaatcontrole en leest u hoe u de instellingen van het onderdeel configureert.

Over Apparaatcontrole

Apparaatcontrole verzekert de beveiliging van vertrouwelijke gegevens door de toegang van gebruikers tot apparaten die op de computer zijn geïnstalleerd of erop zijn aangesloten te beperken. Deze apparaten zijn onder andere:

- Apparaten voor gegevensopslag (harde schijven, verwisselbare schijven, tapestations, cd-/dvd-stations)
- Tools voor gegevensoverdracht (modems, externe netwerkkaarten)
- Apparaten die ontworpen zijn voor het converteren van gegevens naar exemplaren (printers)
- Verbindingsbussen (ook gewoon "bussen" genoemd), verwijzend naar interfaces voor de aansluiting van apparaten op computers (zoals USB, FireWire en Infrarood)

Apparaatcontrole beheert de toegang van gebruikers tot apparaten door *regels voor de toegang tot apparaten* (ook "toegangsregels" genoemd) en *regels voor de toegang tot verbindingsbussen* (ook "toegangsregels voor bussen" genoemd) toe te passen.

Apparaatcontrole inschakelen en uitschakelen

Apparaatcontrole is standaard ingeschakeld. U kunt indien nodig Apparaatcontrole uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

*Zo schakelt u Apparaatcontrole in of uit op het tabblad **Bescherming en controle** van het hoofdvenster van het programma:*

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Endpoint-controle**.

   Het gedeelte **Endpoint-controle** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Apparaatcontrole bevat.

Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.

5. Voer een van de volgende acties uit:

   - Selecteer **Starten** in het menu om Apparaatcontrole in te schakelen.
   - Selecteer **Stoppen** in het menu om Apparaatcontrole uit te schakelen.

Zo schakelt u Apparaatcontrole in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Apparaatcontrole inschakelen** in om Apparaatcontrole in te schakelen.
   - Schakel het selectievakje **Apparaatcontrole inschakelen** uit om Apparaatcontrole uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Over de toegangsregels voor apparaten en verbindingsbussen

Een toegangsregel voor apparaten is een combinatie van parameters die de volgende functies van het onderdeel Apparaatcontrole definiëren:

- Geselecteerde gebruikers en / of gebruikersgroep toegang verlenen tot specifieke soorten apparaten tijdens specifieke perioden.

  U kunt een gebruiker en / of een gebruikersgroep selecteren en een toegangsschema voor apparaten ervoor maken.
- Het recht voor het lezen van de inhoud van geheugenapparaten instellen.
- Het recht voor het schrijven van de inhoud van geheugenapparaten instellen.

Standaard worden toegangsregels aangemaakt voor alle soorten apparaten in de classificatie van het onderdeel Apparaatcontrole. Deze regels verlenen alle gebruikers altijd volledige toegang tot de apparaten als de toegang tot de verbindingsbussen van de respectieve soorten apparaten is toegestaan.

De toegangsregel voor verbindingsbussen staat de toegang tot de verbindingsbus al dan niet toe.

Regels die de toegang tot bussen toestaan, worden standaard aangemaakt voor alle verbindingsbussen in de classificatie van het onderdeel Apparaatcontrole.

U kunt geen toegangsregels voor apparaten of toegangsregels voor verbindingsbussen aanmaken of verwijderen. U kunt ze alleen bewerken.

Over vertrouwde apparaten

Vertrouwde apparaten zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

De volgende acties zijn beschikbaar voor vertrouwde apparaten:

- Het apparaat aan de lijst met vertrouwde apparaten toevoegen.
- De gebruiker en / of de groep van gebruikers die toegang heeft tot het vertrouwde apparaat wijzigen.
- Het apparaat uit de lijst met vertrouwde apparaten verwijderen.

Als u een apparaat aan de lijst met vertrouwde apparaten hebt toegevoegd en een toegangsregel voor dit type apparaat hebt gemaakt die de toegang blokkeert of beperkt, beslist Kaspersky Endpoint Security of de toegang tot het apparaat wordt verleend op basis van de aanwezigheid ervan in de lijst met vertrouwde apparaten. De aanwezigheid ervan in de lijst met vertrouwde apparaten heeft een hogere prioriteit dan een toegangsregel.

Standaardbeslissingen voor de toegang tot apparaten

Kaspersky Endpoint Security beslist of de toegang tot een apparaat moet worden verleend nadat de gebruiker het apparaat op de computer heeft aangesloten.

Standaardbeslissingen voor de toegang tot apparaten

Nr.	Uitgangspositie	Tussenstappen tot een beslissing over de toegang tot het apparaat is genomen			Beslissing over de toegang tot het apparaat
		Controleren of het apparaat voorkomt in de lijst met vertrouwde apparaten	Toegang tot het apparaat testen op basis van de toegangsregel	Toegang tot de bus testen op basis van de toegangsregel voor de bus	
1	Het apparaat komt niet voor in de classificatie van apparaten van het onderdeel Apparaatcontrole.	Niet in de lijst met vertrouwde apparaten.	Geen toegangsregel.	Moet niet worden gescand.	Toegang toegestaan.
2	Het apparaat wordt vertrouwd.	Staat in de lijst met vertrouwde apparaten.	Moet niet worden gescand.	Moet niet worden gescand.	Toegang toegestaan.
3	De toegang tot het apparaat wordt toegestaan.	Niet in de lijst met vertrouwde apparaten.	Toegang toegestaan.	Moet niet worden gescand.	Toegang toegestaan.
4	De toegang tot het apparaat hangt af van de bus.	Niet in de lijst met vertrouwde apparaten.	Toegang hangt af van de bus.	Toegang toegestaan.	Toegang toegestaan.
5	De toegang tot het	Niet in de lijst met	Toegang hangt	Toegang	Toegang

	apparaat hangt af van de bus.	vertrouwde apparaten.	af van de bus.	geblokkeerd.	geblokkeerd.
6	De toegang tot het apparaat wordt toegestaan. Geen toegangsregel voor bussen gevonden.	Niet in de lijst met vertrouwde apparaten.	Toegang toegestaan.	Geen toegangsregel voor bussen.	Toegang toegestaan.
7	De toegang tot het apparaat wordt geblokkeerd.	Niet in de lijst met vertrouwde apparaten.	Toegang geblokkeerd.	Moet niet worden gescand.	Toegang geblokkeerd.
8	Er is geen toegangsregel voor apparaten of bussen gevonden.	Niet in de lijst met vertrouwde apparaten.	Geen toegangsregel.	Geen toegangsregel voor bussen.	Toegang toegestaan.
9	Er is geen toegangsregel voor apparaten.	Niet in de lijst met vertrouwde apparaten.	Geen toegangsregel.	Toegang toegestaan.	Toegang toegestaan.
10	Er is geen toegangsregel voor apparaten.	Niet in de lijst met vertrouwde apparaten.	Geen toegangsregel.	Toegang geblokkeerd.	Toegang geblokkeerd.

U kunt de toegangsregel voor apparaten bewerken nadat u het apparaat hebt aangesloten. Als het apparaat is aangesloten en de toegangsregel de toegang ertoe toestaat maar u later de toegangsregel bewerkt en de toegang blokkeert, zal Kaspersky Endpoint Security de toegang blokkeren de volgende keer dat een bestandsbewerking wordt aangevraagd vanaf het apparaat (mapstructuur bekijken, lezen, schrijven). Een apparaat zonder een bestandssysteem wordt pas geblokkeerd de volgende keer dat het apparaat wordt aangesloten.

Als een gebruiker van de computer waarop Kaspersky Endpoint Security is geïnstalleerd toegang tot een apparaat moet vragen omdat de gebruiker vindt dat de blokkering van de toegang een vergissing is, stuurt u de gebruiker de instructies voor het aanvragen van de toegang.

Een regel voor toegang tot apparaten bewerken

Afhankelijk van het type apparaat kunt u verschillende toegangsinstellingen wijzigen, zoals de lijst met gebruikers die toegang tot het apparaat krijgen, het toegangsschema en de toegestane / geblokkeerde toegang.

Zo bewerkt u een regel voor toegang tot apparaten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Selecteer rechts in het venster het tabblad **Apparaattypen**.

   Het tabblad **Apparaattypen** bevat toegangsregels voor alle apparaten die in de classificatie van het onderdeel Apparaatcontrole zijn opgenomen.
4. Selecteer de toegangsregel die u wilt bewerken.
5. Klik op de knop **Bewerken**. Deze knop is alleen beschikbaar voor soorten apparaten met een bestandssysteem.

   Het venster **Regel voor toegang tot apparaten configureren** wordt geopend.

Standaard geeft een regel voor toegang tot apparaten alle gebruikers op elk moment volledige toegang tot het opgegeven type van apparaten. In de lijst **Gebruikers en/of groepen van gebruikers** bevat deze toegangsregel de groep **Alle**. In de tabel **Rechten van de geselecteerde groep van gebruikers volgens toegangsschema's** bevat deze toegangsregel het **Standaardschema** voor toegang tot apparaten met de rechten om alle soorten bewerkingen met apparaten uit te voeren.

6. Zo bewerkt u de instellingen van een regel voor toegang tot apparaten:

   a. Selecteer een gebruiker en/of groep van gebruikers uit de lijst **Gebruikers en/of groepen van gebruikers**.

   Om de lijst **Gebruikers en/of groepen van gebruikers** te bewerken, gebruikt u de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.

   b. Configureer in de tabel **Rechten van de geselecteerde groep van gebruikers volgens toegangsschema's** het toegangsschema voor apparaten voor de geselecteerde gebruiker en / of groep van gebruikers. Hiervoor schakelt u de selectievakjes naast de namen van de toegangsschema's voor apparaten in die u wilt gebruiken in de regel voor toegang tot apparaten die wordt bewerkt.

   Om de lijst met toegangsschema's voor apparaten te bewerken, gebruikt u de knoppen **Maken**, **Bewerken**, **Kopiëren** en **Verwijderen** in de tabel **Rechten van de geselecteerde groep van gebruikers volgens toegangsschema's**.

   c. Voor elk toegangsschema voor apparaten dat wordt gebruikt in de regel die wordt bewerkt geeft u de bewerkingen op die tijdens het werken met apparaten zijn toegestaan. Hiertoe schakelt u in de tabel **Rechten van de geselecteerde groep van gebruikers volgens toegangsschema's** de selectievakjes in de kolommen met de namen van de relevante bewerkingen in.

   d. Klik op **OK**.

   Nadat u de standaardinstellingen van een regel voor toegang tot apparaten hebt bewerkt, wordt de instelling voor de toegang tot het soort apparaat in de kolom **Toegang** in de tabel op het tabblad **Apparaattypen** gewijzigd in de waarde *Beperk volgens regels*.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Records toevoegen aan of verwijderen uit het gebeurtenislogboek

De registratie van gebeurtenissen is alleen beschikbaar voor bewerkingen met bestanden op verwisselbare schijven.

Zo schakelt u de registratie gebeurtenissen in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.

3. Selecteer rechts in het venster het tabblad **Apparaattypen**.

   Het tabblad **Apparaattypen** bevat toegangsregels voor alle apparaten die in de classificatie van het onderdeel Apparaatcontrole zijn opgenomen.

4. Selecteer **Verwisselbare schijven** in de tabel met apparaten.

   De knop **Logboeken** wordt boven in de tabel beschikbaar.

5. Klik op de knop **Logboeken**.

   Hiermee opent u het venster **Instellingen van logboeken**.

6. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Logboeken inschakelen** in als u de registratie van het verwijderen en schrijven van bestanden op verwisselbare schijven wilt inschakelen.

     Kaspersky Endpoint Security slaat een gebeurtenis in het logboekbestand op en stuurt een bericht naar de Administration Server van Kaspersky Security Center telkens als de gebruiker bestanden op verwisselbare schijven schrijft of verwijdert.

   - In het andere geval schakelt u het selectievakje **Logboeken inschakelen** uit.

7. Geef op welke bewerkingen moeten worden geregistreerd. Doe hiervoor één van het volgende:

   - Als u Kaspersky Endpoint Security alle gebeurtenissen wilt laten registreren, schakelt u het selectievakje **Informatie over alle bestanden opslaan** in.

   - Als u Kaspersky Endpoint Security alleen informatie over bestanden met een specifieke indeling wilt laten registreren, schakelt u in het gedeelte **Filteren op bestandsindelingen** de selectievakjes naast de relevante bestandsindelingen in.

8. Geef op welke acties van Kaspersky Endpoint Security-gebruikers u wilt registreren als gebeurtenissen. Hiertoe doet u het volgende:

   a. Klik in het gedeelte **Gebruikers** op de knop **Selecteren**.

      Het standaardvenster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.

   b. Geef de lijst met gebruikers en/of groepen van gebruikers op of bewerk deze lijst.

   Als de gebruikers uit het gedeelte **Gebruikers** schrijven naar bestanden op verwisselbare schijven of bestanden van verwisselbare schijven verwijderen, slaat Kaspersky Endpoint Security informatie over zulke bewerkingen in het gebeurtenislogboek op en stuurt het een bericht naar de Administration Server van Kaspersky Security Center.

9. Klik in het venster **Instellingen van logboeken** op **OK**.

10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

U kunt gebeurtenissen met bestanden op verwisselbare schijven bekijken in de Beheerconsole van Kaspersky Security Center, met name in de werkruimte van het **Administration Server**-knooppunt op het tabblad **Gebeurtenissen**. Voor de weergave van gebeurtenissen in het lokale gebeurtenislogboek van Kaspersky Endpoint Security moet u het selectievakje **Bestandsbewerking uitgevoerd** in de instellingen voor meldingen voor het onderdeel Apparaatcontrole inschakelen.

Een wifinetwerk toevoegen aan de lijst Vertrouwd

U kunt gebruikers toestaan om verbinding te maken met wifinetwerken die u als veilig beschouwt, zoals draadloze bedrijfsnetwerken. Hiertoe moet u het netwerk aan de lijst met vertrouwde wifinetwerken toevoegen. Apparaatcontrole blokkeert de toegang tot alle wifinetwerken behalve de netwerken die in de lijst Vertrouwd zijn opgegeven.

Zo voegt u een wifinetwerk toe aan de lijst Vertrouwd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Selecteer rechts in het venster het tabblad **Apparaattypen**.

   Het tabblad **Apparaattypen** bevat toegangsregels voor alle apparaten die in de classificatie van het onderdeel Apparaatcontrole zijn opgenomen.
4. Klik met de rechtermuisknop in de kolom **Toegang** naast het **Wifi**-apparaat om het contextmenu te openen.
5. Selecteer de optie **Blokkeren met uitzonderingen**.
6. Selecteer in de lijst met apparaten de optie **Wifi** en klik op de knop **Bewerken**.

   Hiermee opent u het venster **Vertrouwde Wi-Fi-netwerken**.
7. Klik op de knop **Toevoegen**.

   Hiermee opent u het venster **Vertrouwd Wi-Fi-netwerk**.
8. In het venster **Vertrouwd Wi-Fi-netwerk**:

   - Geef in het veld **Netwerknaam** de naam van het wifinetwerk op dat u aan de lijst Vertrouwd wilt toevoegen.
   - Selecteer in de vervolgkeuzelijst **Authenticatietype** het gebruikte type authenticatie voor de verbinding met het vertrouwde wifinetwerk.
   - Selecteer in de vervolgkeuzelijst **Encryptietype** het gebruikte type encryptie voor de beveiliging van het verkeer van het vertrouwde wifinetwerk.
   - In het veld **Opmerking** kunt u informatie over het toegevoegde wifinetwerk opgeven.

   Een wifinetwerk wordt als vertrouwd beschouwd als de instellingen ervan overeenkomen met alle opgegeven instellingen in de regel.
9. Klik in het venster **Vertrouwd Wi-Fi-netwerk** op **OK**.
10. Klik in het venster **Vertrouwde Wi-Fi-netwerken** op **OK**.

Een toegangsregel voor verbindingsbussen bewerken

Zo bewerkt u een toegangsregel voor verbindingsbussen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Selecteer het tabblad **Verbindingsbussen**.

   Op het tabblad **Verbindingsbussen** ziet u de toegangsregels voor alle verbindingsbussen die in het onderdeel Apparaatcontrole zijn geclassificeerd.

4. Selecteer de toegangsregel voor verbindingsbussen die u wilt bewerken.
5. Wijzig de waarde van de toegangsparameter:
   - Als u de toegang tot een verbindingsbus wilt toestaan, klikt u op de kolom **Toegang** om het contextmenu te openen en selecteert u **Toestaan**.
   - Als u de toegang tot een verbindingsbus wilt blokkeren, klikt u op de kolom **Toegang** om het contextmenu te openen en selecteert u **Blokkeren**.
6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bewerkingen met vertrouwde apparaten

In deze sectie vindt u informatie over bewerkingen met vertrouwde apparaten.

Een apparaat vanuit de programma-interface toevoegen aan de lijst Vertrouwd

Wanneer een apparaat wordt toegevoegd aan de lijst met vertrouwde apparaten, wordt de toegang tot het apparaat standaard verleend aan alle gebruikers (de groep van gebruikers genaamd 'Iedereen').

Zo voegt u een apparaat vanuit de programma-interface toe aan de lijst Vertrouwd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.
4. Klik op de knop **Selecteren**.

   Het venster **Vertrouwde apparaten selecteren** wordt geopend.
5. Schakel het selectievakje naast de naam van een apparaat in dat u aan de lijst met vertrouwde apparaten wilt toevoegen.

   De lijst in de kolom **Apparaten** hangt af van de geselecteerde waarde in de vervolgkeuzelijst **Geef verbonden apparaten weer**.
6. Klik op de knop **Selecteren**.

   Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.
7. In het venster **Gebruikers of groepen selecteren** in Microsoft Windows geeft u gebruikers en/of groepen van gebruikers op waarvoor Kaspersky Endpoint Security de geselecteerde apparaten als vertrouwd herkent.

   De namen van opgegeven gebruikers en/of groepen van gebruikers in het venster **Selecteer gebruikers en / of groepen van gebruikers** van Microsoft Windows worden in het veld **Sta toe aan gebruikers en/of groepen van gebruikers** weergegeven.
8. Klik in het vertrouwde apparaten **Vertrouwde apparaten selecteren** op **OK**.

In de tabel op het tabblad **Vertrouwde apparaten** van het venster met de instellingen van het onderdeel **Apparaatcontrole** verschijnt een regel met de parameters van het vertrouwde apparaat dat is toegevoegd.

9. Herhaal stappen 4-7 voor elk apparaat dat u wilt toevoegen aan de lijst met vertrouwde apparaten voor de opgegeven gebruikers en/of groepen van gebruikers.

10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Apparaten op basis van het apparaatmodel of -ID toevoegen aan de lijst Vertrouwd

Wanneer een apparaat wordt toegevoegd aan de lijst met vertrouwde apparaten, wordt de toegang tot het apparaat standaard verleend aan alle gebruikers (de groep van gebruikers genaamd 'Iedereen').

Zo voegt u apparaten op basis van het apparaatmodel of -ID toe aan de lijst Vertrouwd:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een lijst met vertrouwde apparaten wilt aanmaken.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Endpoint-controle** het subgedeelte **Apparaatcontrole**.

7. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.

8. Klik op de knop **Toevoegen**.

   Het contextmenu van de knop wordt geopend.

9. Doe in het contextmenu van de knop **Toevoegen** een van het volgende:

   - Selecteer de knop **Apparaten per ID** als u apparaten met bekende unieke ID's wilt selecteren die u aan de lijst met vertrouwde apparaten wilt toevoegen.

   - Selecteer de optie **Apparaten per model** als u vertrouwde apparaten waarvan het VID (Vendor ID) en het PID (Product ID) bekend zijn aan de lijst wilt toevoegen.

10. Selecteer in de vervolgkeuzelijst **Apparaattype** in het geopende venster het type van apparaten dat in de onderstaande tabel moet worden weergegeven.

11. Klik op de knop **Vernieuwen**.

    In de tabel ziet u een lijst met apparaten waarvan de apparaat-ID's en / of -modellen bekend zijn en die tot het selecteerde type in de vervolgkeuzelijst **Apparaattype** behoren.

12. Schakel de selectievakjes naast de namen van de apparaten in die u aan de lijst met vertrouwde apparaten wilt toevoegen.

13. Klik op de knop **Selecteren**.

    Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.

14. In het venster **Gebruikers of groepen selecteren** in Microsoft Windows geeft u gebruikers en/of groepen van gebruikers op waarvoor Kaspersky Endpoint Security de geselecteerde apparaten als vertrouwd herkent.

    De namen van opgegeven gebruikers en/of groepen van gebruikers in het venster **Selecteer gebruikers en / of groepen van gebruikers** van Microsoft Windows worden in het veld **Sta toe aan gebruikers en/of groepen van gebruikers** weergegeven.

15. Klik op **OK**.

    Regels met parameters van de toegevoegde vertrouwde apparaten verschijnen in de tabel op het tabblad **Vertrouwde apparaten**.

16. Klik op **OK** of **Toepassen** om de wijzigingen toe te passen.

Apparaten op basis van het masker van het apparaat-ID toevoegen aan de lijst Vertrouwd

Wanneer een apparaat wordt toegevoegd aan de lijst met vertrouwde apparaten, wordt de toegang tot het apparaat standaard verleend aan alle gebruikers (de groep van gebruikers genaamd 'Iedereen').

In de Beheerconsole van Kaspersky Security Center kunt u ook apparaten op basis van het masker van hun ID toevoegen aan de lijst Vertrouwd.

Zo voegt u apparaten op basis van het masker van hun apparaat-ID toe aan de lijst Vertrouwd:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een lijst met vertrouwde apparaten wilt aanmaken.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Endpoint-controle** het subgedeelte **Apparaatcontrole**.

7. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.

8. Klik op de knop **Toevoegen**.

   Het contextmenu van de knop wordt geopend.

9. Selecteer in het contextmenu van de knop **Toevoegen** de optie **Apparaten per ID-masker**.

   Het venster **Vertrouwde apparaten op ID-masker toevoegen** wordt geopend.

10. Voer in het venster **Vertrouwde apparaten op ID-masker toevoegen** het masker voor apparaat-ID's in het veld **Masker** in.

11. Klik op de knop **Selecteren**.

    Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.

12. In het venster **Gebruikers of groepen selecteren** in Microsoft Windows geeft u gebruikers en/of groepen van gebruikers op waarvoor Kaspersky Endpoint Security de apparaten waarvan de modellen of ID's overeenkomen met het opgegeven masker als vertrouwd beschouwt.

    De namen van opgegeven gebruikers en/of groepen van gebruikers in het venster **Selecteer gebruikers en / of groepen van gebruikers** van Microsoft Windows worden in het veld **Sta toe aan gebruikers en/of groepen van gebruikers** weergegeven.

13. Klik op **OK**.

    In de tabel op het tabblad **Vertrouwde apparaten** van het venster met de instellingen van **Apparaatcontrole** verschijnt een regel met de instellingen van de regel voor het toevoegen van apparaten aan de lijst met vertrouwde apparaten op basis van het masker van hun ID's.

14. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Toegang van gebruikers tot een vertrouwd apparaat configureren

Wanneer een apparaat wordt toegevoegd aan de lijst met vertrouwde apparaten, wordt de toegang tot het apparaat standaard verleend aan alle gebruikers (de groep van gebruikers genaamd 'Iedereen'). U kunt de toegang van gebruikers (of groepen van gebruikers) tot een vertrouwd apparaat configureren.

Zo configureert u de toegang van gebruikers tot een vertrouwd apparaat:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.

3. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.

4. Selecteer in de lijst met vertrouwde apparaten een apparaat waarvoor u toegangsregels wilt bewerken.

5. Klik op de knop **Bewerken**.

   Het venster **Regel voor toegang tot vertrouwd apparaat configureren** wordt geopend.

6. Klik op de knop **Selecteren**.

   Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.

7. In het venster **Gebruikers of groepen selecteren** in Microsoft Windows geeft u gebruikers en/of groepen van gebruikers op waarvoor Kaspersky Endpoint Security de geselecteerde apparaten als vertrouwd herkent.

8. Klik op **OK**.

De namen van opgegeven gebruikers en/of groepen van gebruikers in het venster **Selecteer gebruikers en / of groepen van gebruikers** van Microsoft Windows worden in het veld **Sta toe aan gebruikers en / of groepen van gebruikers** van het venster **Regel voor toegang tot vertrouwd apparaat configureren** weergegeven.

9. Klik op **OK**.
10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een apparaat uit de lijst met vertrouwde apparaten verwijderen

Zo verwijdert u een apparaat uit de lijst met vertrouwde apparaten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.
   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.
4. Selecteer het apparaat dat u wilt verwijderen uit de lijst met vertrouwde apparaten.
5. Klik op de knop **Verwijderen**.
6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Kaspersky Endpoint Security gebruikt de toegangsregels voor apparaten en verbindingsbussen om beslissingen te nemen over de toegang tot apparaten die u hebt verwijderd uit de lijst met vertrouwde apparaten.

Berichtsjablonen van Apparaatcontrole bewerken

Wanneer de gebruiker probeert toegang te krijgen tot een geblokkeerd apparaat, toont Kaspersky Endpoint Security een bericht met de melding dat de toegang tot het apparaat is geblokkeerd of dat een bewerking met de inhoud van het apparaat verboden is. Als de gebruiker vindt dat de toegang tot het apparaat per vergissing is geblokkeerd of dat een bewerking met de inhoud van het apparaat per vergissing is verboden, kan de gebruiker een bericht naar de lokale netwerkbeheerder versturen door op de koppeling in het bericht over de geblokkeerde actie te klikken.

Er zijn sjablonen beschikbaar voor berichten over de geblokkeerde toegang tot apparaten of verboden bewerkingen met inhoud van het apparaat en voor het bericht dat naar de beheerder wordt verstuurd. U kunt de berichtsjablonen wijzigen.

Zo bewerkt u de sjablonen voor berichten van Apparaatcontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Apparaatcontrole**.
   Rechts in het venster ziet u de instellingen van het onderdeel Apparaatcontrole.
3. Klik rechts in het venster op de knop **Sjablonen**.
   Het venster **Berichtsjablonen** wordt geopend.

4. Voer een van de volgende acties uit:

   - Selecteer het tabblad **Blokkering** voor de bewerking van de sjabloon voor het bericht over de geblokkeerde toegang tot een apparaat of over een verboden bewerking met de inhoud van het apparaat.

   - Selecteer het tabblad **Bericht aan beheerder** voor de bewerking van de sjabloon voor het bericht dat naar de netwerkbeheerder wordt verstuurd.

5. Bewerk de sjabloon van het bericht. U kunt ook de volgende knoppen gebruiken: **Variabele**, **Standaard** en **Koppeling** (deze knop is alleen beschikbaar op het tabblad **Blokkering**).

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Toegang tot een geblokkeerd apparaat verkrijgen

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

> De functionaliteit van Kaspersky Endpoint Security die tijdelijke toegang tot een apparaat verleent is alleen beschikbaar als Kaspersky Endpoint Security onder het Kaspersky Security Center-beleid wordt uitgevoerd en als deze functionaliteit in de beleidsinstellingen is ingeschakeld (raadpleeg de *beheerdershandleiding van Kaspersky Security Center*).

Zo vraagt u toegang tot een geblokkeerd apparaat vanuit het venster met de instellingen van het onderdeel Apparaatcontrole:

1. Selecteer in het hoofdvenster van het programma het tabblad **Bescherming en controle**.

2. Klik op het gedeelte **Endpoint-controle**.

   Het gedeelte **Endpoint-controle** wordt geopend.

3. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Apparaatcontrole bevat.

   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.

4. Klik op de knop **Toegang tot apparaat**.

   Het venster **Toegang tot apparaat vragen** wordt geopend.

5. Selecteer in de lijst met aangesloten apparaten het apparaat waartoe u toegang wilt krijgen.

6. Klik op de knop **Bestand met toegangsaanvraag genereren**.

   Hiermee opent u het venster **Bestand met toegangsaanvraag aanmaken**.

7. Geef in het veld **Duur van toegang** op hoelang u toegang tot het apparaat wilt hebben.

8. Klik op de knop **Opslaan**.

   Hiermee opent u het standaardvenster **Bestand met toegangsaanvraag opslaan** in Microsoft Windows.

9. Selecteer in het venster **Bestand met toegangsaanvraag opslaan** in Microsoft Windows de map waarin u het bestand met de toegangsaanvraag voor het apparaat wilt opslaan en klik op de knop **Opslaan**.

10. Stuur het bestand met de toegangsaanvraag voor het apparaat naar de netwerkbeheerder.

11. Ontvang het bestand met de toegangscode voor het apparaat van de netwerkbeheerder.

12. Klik in het venster **Toegang tot apparaat vragen** op de knop **Toegangscode activeren**.

    Het standaardvenster **Toegangscode openen** wordt in Microsoft Windows geopend.

13. Selecteer in het venster **Toegangscode openen** in Microsoft Windows het bestand met de toegangscode voor het apparaat dat u van de netwerkbeheerder hebt gekregen en klik op **Openen**.

    Het venster **Toegangscode voor het apparaat activeren** wordt geopend. In dit venster ziet u informatie over de verleende toegang.

14. Klik in het venster **Toegangscode voor het apparaat activeren** op **OK**.

Zo vraagt u toegang tot een geblokkeerd apparaat door te klikken op de koppeling in het bericht met de melding dat het apparaat is geblokkeerd:

1. Klik op de koppeling **Toegang vragen** in het venster van het bericht met de melding dat een apparaat of een verbindingsbus is geblokkeerd.

   Hiermee opent u het venster **Bestand met toegangsaanvraag aanmaken**.

2. Geef in het veld **Duur van toegang** op hoelang u toegang tot het apparaat wilt hebben.

3. Klik op de knop **Opslaan**.

   Hiermee opent u het standaardvenster **Bestand met toegangsaanvraag opslaan** in Microsoft Windows.

4. Selecteer in het venster **Bestand met toegangsaanvraag opslaan** in Microsoft Windows de map waarin u het bestand met de toegangsaanvraag voor het apparaat wilt opslaan en klik op de knop **Opslaan**.

5. Stuur het bestand met de toegangsaanvraag voor het apparaat naar de netwerkbeheerder.

6. Ontvang het bestand met de toegangscode voor het apparaat van de netwerkbeheerder.

7. Klik in het venster **Toegang tot apparaat vragen** op de knop **Toegangscode activeren**.

   Het standaardvenster **Toegangscode openen** wordt in Microsoft Windows geopend.

8. Selecteer in het venster **Toegangscode openen** in Microsoft Windows het bestand met de toegangscode voor het apparaat dat u van de netwerkbeheerder hebt gekregen en klik op **Openen**.

   Het venster **Toegangscode voor het apparaat activeren** wordt geopend. In dit venster ziet u informatie over de verleende toegang.

9. Klik in het venster **Toegangscode voor het apparaat activeren** op **OK**.

De tijd van de verleende toegang tot het apparaat kan verschillen van de gevraagde tijd. De toegang tot het apparaat wordt verleend gedurende de tijd die de netwerkbeheerder heeft opgegeven wanneer die de toegangscode voor het apparaat heeft aangemaakt.

Een code voor de toegang tot een geblokkeerd apparaat aanmaken via Kaspersky Security Center

Om een gebruiker tijdelijk toegang tot een geblokkeerd apparaat te geven, hebt u een toegangscode voor het apparaat nodig. U kunt een toegangscode via Kaspersky Security Center aanmaken.

Zo maakt u een toegangscode voor een geblokkeerd apparaat aan:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer in de lijst met clientcomputers de computer waarvan de gebruiker tijdelijke toegang tot een vergrendeld apparaat moet krijgen.
5. Selecteer in het contextmenu van de computer de optie **Verleen toegang tot apparaten en gegevens in offline modus**.

   Het venster **Verleen toegang tot apparaten en gegevens in offline modus** wordt geopend.
6. Selecteer het tabblad **Apparaatcontrole**.
7. Klik op het tabblad **Apparaatcontrole** op de knop **Bladeren**.

   Het standaardvenster **Bestand met toegangsaanvraag selecteren** wordt in Microsoft Windows geopend.
8. Selecteer in het venster **Bestand met toegangsaanvraag selecteren** het bestand met de toegangsaanvraag dat u van de gebruiker hebt gekregen en klik op de knop **Openen**.

   Op het tabblad **Apparaatcontrole** ziet u de gegevens van het vergrendelde apparaat waartoe de gebruiker toegang heeft gevraagd.
9. Geef de waarde van de instelling **Duur van toegang** op.

   Deze instelling definieert hoelang u de gebruiker toegang tot het vergrendelde apparaat wilt geven. De standaardwaarde is de waarde die door de gebruiker is opgegeven wanneer het bestand met de toegangsaanvraag is aangemaakt.
10. Geef de waarde van de instelling **Activatieperiode** op.

    Deze instelling definieert de tijd die de gebruiker heeft om de toegang tot het geblokkeerde apparaat te activeren met de verstrekte toegangscode.
11. Klik op de knop **Opslaan**.

    Hiermee opent u het standaardvenster **Toegangscode opslaan** in Microsoft Windows.
12. Selecteer de doelmap waarin u het bestand met de toegangscode voor het geblokkeerde apparaat wilt opslaan.
13. Klik op de knop **Opslaan**.

Webcontrole

Dit onderdeel is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Dit onderdeel is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over Webcontrole en leest u hoe u de instellingen van het onderdeel configureert.

Over Webcontrole

Met Webcontrole kunt u acties van netwerkgebruikers controleren door de toegang tot webbronnen te beperken en te blokkeren.

Een webbron is een individuele webpagina of verschillende webpagina's of een website of verschillende websites die iets gemeenschappelijk hebben.

Webcontrole beschikt over de volgende opties:

- Volume van het verkeer laten dalen.

  Het verkeer wordt gecontroleerd door de downloads van multimediabestanden te beperken of te blokkeren of door de toegang tot webbronnen die niets te maken hebben met de taken van gebruikers te beperken of te blokkeren.

- Toegang beperken volgens inhoudscategorieën van webbronnen.

  Om het volume van het verkeer te laten dalen en het mogelijke verlies door de verkeerde aanwending van de tijd van werknemers te verkleinen, kunt u de toegang tot specifieke categorieën van webbronnen beperken of blokkeren (blokkeer bijvoorbeeld de toegang tot webbronnen die tot de categorie “Online communicatie” behoren).

- Gecentraliseerde controle van toegang tot webbronnen.

  Wanneer u Kaspersky Security Center gebruikt, beschikt u over persoonlijke en groepsinstellingen voor de toegang tot webbronnen.

Alle beperkingen en blokkeringen die worden toegepast op de toegang tot webbronnen worden als toegangsregels voor webbronnen geïmplementeerd.

Webcontrole inschakelen en uitschakelen

Webcontrole is standaard ingeschakeld. U kunt indien nodig Webcontrole uitschakelen.

Er zijn twee manieren om het onderdeel in of uit te schakelen:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

*Zo schakelt u Webcontrole in of uit op het tabblad **Bescherming en controle** van het hoofdvenster van het programma:*

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Endpoint-controle**.
   Het gedeelte **Endpoint-controle** wordt geopend.
4. Klik rechts om het contextmenu van de regel te openen dat informatie over het onderdeel Webcontrole bevat.
   Er wordt een menu geopend waarin u acties voor het onderdeel kunt selecteren.
5. Voer een van de volgende acties uit:
   - Selecteer **Starten** in het menu om Webcontrole in te schakelen.
   - Selecteer **Stoppen** in het menu om Webcontrole uit te schakelen.

Zo schakelt u Webcontrole in of uit vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.
   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **Webcontrole inschakelen** in om Webcontrole in te schakelen.
   - Schakel het selectievakje **Webcontrole inschakelen** uit om Webcontrole uit te schakelen.

   Als Webcontrole is uitgeschakeld, controleert Kaspersky Endpoint Security de toegang tot webbronnen niet.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Inhoudscategorieën van webbronnen

De hieronder vermelde inhoudscategorieën van webbronnen (hierna de "categorieën") zijn geselecteerd om de soorten gegevens die door webbronnen worden gehost het best te beschrijven, rekening houdende met de functionele en thematische kenmerken ervan. De volgorde waarin de categorieën in deze lijst worden weergegeven is geen weerspiegeling van het relatieve belang of de prevalentie van deze categorieën op het internet. De categorienamen zijn niet definitief en worden uitsluitend gebruikt voor doeleinden in producten en op websites van Kaspersky. De namen weerspiegelen niet noodzakelijk de wettelijk geïmpliceerde betekenis. Eén webbron kan tot verschillende categorieën tegelijk behoren.

Erotische inhoud

Deze categorie bevat de volgende soorten webbronnen:

- Webbronnen met foto's of video's waarop/waarin geslachtsorganen van mensen of mensachtige wezens, geslachtsgemeenschap of masturbatie door mensen of mensachtige wezens te zien is.

- Webbronnen met teksten, inclusief literair en artistiek materiaal, waarin geslachtsorganen van mensen of mensachtige wezens, geslachtsgemeenschap of masturbatie door mensen of mensachtige wezens beschreven worden.
- Webbronnen met discussies over het seksuele aspect van relaties tussen mensen.

  Overlapt de categorie 'Online communicatiemedia'.

- Webbronnen met erotisch materiaal, werken die een realistisch portret van seksueel gedrag van mensen vormen, of kunstwerken die zijn ontworpen om de seksuele opwinding te stimuleren.
- Webbronnen van officiële media en online gemeenschappen met een specifiek doelpubliek die over een speciaal gedeelte en/of individuele artikelen over het seksuele aspect van relaties tussen mensen beschikken.
- Webbronnen over seksuele perversies.
- Webbronnen die reclame maken voor artikelen voor gebruik tijdens seksuele handelingen en opwinding, seksuele diensten en intieme dating, inclusief online diensten via erotische videochats, "telefoonseks", "sexting" (virtuele seks) en die ook verkopen.
- Webbronnen met de volgende inhoud:
  - Artikelen en blogs over seksuele voorlichting met zowel wetenschappelijke als algemene thema's.
  - Medische encyclopedieën, in het bijzonder de hoofdstukken over geslachtelijke voortplanting.
  - Bronnen van medische instellingen, in het bijzonder de hoofdstukken over be behandeling van geslachtsorganen.

Software, audio, video

Deze categorie bevat de volgende subcategorieën die u individueel kunt selecteren:

- **Audio en video**.

  Deze subcategorie bevat webbronnen die audio- en videomateriaal verdelen: films, opnames van sportuitzendingen, opnames van concerten, muzieknummers, videoclips, video's, audio- en video-opnames voor zelfstudies, enzovoort.

- **Torrents**.

  Deze subcategorie bevat websites van torrent trackers die bedoeld zijn om bestanden met een onbeperkte grootte te delen.

- **Bestandsdeling**.

  Deze subcategorie bevat websites voor bestandsdeling ongeacht de fysieke locatie van de bestanden die worden verdeeld.

Alcohol, tabak, drugs

Deze categorie bevat webbronnen waarvan de inhoud rechtstreeks of onrechtstreeks te maken heeft met alcoholische producten, tabaksproducten en verdovende, psychotrope en/of bedwelmende middelen.

- Webbronnen die reclame maken voor zulke middelen en uitrusting voor het verbruik ervan en die ook verkopen.

Overlapt de categorie “E-commerce”.

- Webbronnen met instructies voor het verbruik of de productie van verdovende, psychotrope en/of bedwelmende middelen.

Deze categorie bevat webbronnen over wetenschappelijke en medische onderwerpen.

Geweld

Deze categorie bevat webbronnen met foto’s, video’s of teksten die handelingen van fysiek of psychologisch geweld jegens mensen of een wrede behandeling van dieren tonen of beschrijven.

- Webbronnen met scènes van executies, martelingen of misbruik, alsook gereedschap dat bedoeld is voor zulke daden.

  Overlapt de categorie ‘Wapens, explosieven, vuurwerk’.

- Webbronnen met scènes van moorden, gevechten, aanrandingen of verkrachtingen, scènes waarin mensen, dieren of denkbeeldige wezens worden misbruikt of vernederd.
- Webbronnen met informatie die aanzet tot daden die levensgevaarlijk zijn en/of een gezondheidsrisico inhouden, inclusief zelfbeschadiging of zelfmoord.
- Webbron met informatie die geweld en/of wreedheid goedkeurt of rechtvaardigt, of aanzet tot gewelddadige handelingen jegens mensen of dieren.
- Webbronnen met bijzonder realistische voorstellingen of beschrijvingen van slachtoffers en wreedheden van oorlog, gewapende conflicten, militaire gevechten, ongelukken, catastrofes, natuurrampen, industriële of sociale rampen of menselijk leed.
- Computergames met gewelddadige en wrede scènes, inclusief de zogenaamde “shooters”, “fightings”, “slashers”, enzovoort.

  Overlapt de categorie ‘Computergames’.

Wapens, explosieven, vuurwerk

Deze categorie bevat webbronnen met informatie over wapens, explosieven en vuurwerk:

- Websites van fabrikanten en winkels van wapens, explosieven en vuurwerk.

  Overlapt de categorie “E-commerce”.

- Webbronnen die zijn gespecialiseerd in de vervaardiging of het gebruik van wapens, explosieven of vuurwerk.

- Webbronnen met analytisch, historisch, productie- en encyclopedisch materiaal over wapens, explosieven en vuurwerk.

Onder de term “wapens” verstaan we instrumenten, middelen en hulpmiddelen om het leven of de gezondheid van mensen en dieren in gevaar te brengen en/of om apparatuur en gebouwen te beschadigen.

Schelden

Deze categorie bevat webbronnen met een obsceen taalgebruik.

Overlapt de categorie “Erotische inhoud”.

Deze categorie bevat ook webbronnen met taalkundig en filologisch materiaal waarin schelden het onderwerp van een studie is.

Gokken, loterijen, sweepstakes

Deze categorie bevat webbronnen die gebruikers aanbieden om met echt geld te gokken, zelfs als het gokken niet verplicht is om toegang tot de website te krijgen. Deze categorie bevat webbronnen die het volgende aanbieden:

- Gokken waarbij deelnemers een financiële bijdrage moeten doen.

  Overlapt de categorie ‘Computergames’.

- Sweepstakes waarbij met echt geld wordt gegokt.
- Loterijen die loten of nummers verkopen.
- Informatie die de drang om deel te nemen aan gokken, sweepstakes en loterijen kan opwekken.

Overlapt de categorie “E-commerce”.

Deze categorie bevat games die een gratis deelname als afzonderlijke modus aanbieden, alsook webbronnen die actief reclame maken voor andere webbronnen uit deze categorie.

Netwerkcommunicatie

Deze categorie bevat webbronnen die (al dan niet geregistreerde) gebruikers kunnen gebruiken om persoonlijke berichten naar andere gebruikers van de relevante webbronnen of andere online services te sturen en/of om inhoud (hetzij openbaar hetzij privé) naar de relevante webbronnen onder bepaalde voorwaarden toe te voegen. U kunt de volgende subcategorieën individueel selecteren:

- **Chats en forums**.

Deze subcategorie bevat webbronnen die bedoeld zijn voor openbare discussies over diverse onderwerpen met behulp van speciale webtoepassingen, alsook webbronnen die zijn ontworpen voor de distributie of de ondersteuning van chatprogramma's waarmee mensen in real time kunnen communiceren.

- **Blogs**.

  Deze subcategorie bevat blogs: websites die betaalde of gratis diensten voor het maken of onderhouden van blogs aanbieden.

- **Sociale netwerken**.

  Deze subcategorie bevat websites die zijn ontworpen voor het maken, weergeven en beheren van contacten tussen personen, organisaties en overheden en waarvoor u een geregistreerd gebruikersaccount nodig hebt om deel te nemen.

- **Datingsites**.

  Deze subcategorie bevat webbronnen die werken als een soort sociaal netwerk dat betaalde of gratis diensten aanbiedt.

  > Overlapt de categorieën 'Erotische inhoud' en 'E-commerce'.

- **Webmail**.

  Deze subcategorie bevat uitsluitend aanmeldingspagina's van e-maildiensten en mailboxen die e-mails en gerelateerde gegevens bevatten (zoals persoonlijke contacten). Deze categorie bevat geen andere webpagina's van een internetprovider die ook e-maildiensten aanbiedt.

E-tailers, banken en betaalsystemen

Deze categorie bevat webbronnen die zijn ontworpen voor online transacties die niet contant gebeuren met behulp van speciale webtoepassingen die hiervoor zijn ontworpen. U kunt de volgende subcategorieën individueel selecteren:

- **Winkels en veilingen**.

  Deze subcategorie bevat online shops en veilingen die goederen, werk of diensten verkopen aan personen en/of juridische entiteiten, inclusief websites van winkels die uitsluitend online verkopen en online profielen van fysieke winkels die online betalingen aanvaarden.

- **Banken**.

  Deze subcategorie bevat gespecialiseerde webpagina's van banken met functionaliteit voor online betalingen, inclusief (elektronische) bankoverschrijvingen tussen bankrekeningen, bankdeposito's, valutaomwisselingen, betalingen voor diensten van derden, enzovoort.

- **Betaalsystemen**.

  Deze subcategorie bevat webpagina's van elektronische betaalsystemen die toegang tot het persoonlijk account van de gebruiker bieden.

> In technische termen kan de betaling worden gedaan met zowel een willekeurige bankpas (plastic of virtueel, debet of credit, lokaal of internationaal) als elektronisch geld. Webbronnen kunnen tot deze categorie behoren ongeacht of ze al dan niet technische aspecten zoals gegevensoverdracht via het SSL-protocol, het gebruik van 3D Secure-verificatie, enzovoort hebben.

Jobsites

Deze categorie bevat webbronnen die zijn ontworpen om werkgevers en werkzoekenden samen te brengen:

- Websites van wervingsbureaus (uitzendbureaus en/of headhuntersbureaus).
- Websites van werkgevers met beschrijvingen van vacatures en hun voordelen.
- Onafhankelijke portals met vacatures van werkgevers en wervingsbureaus.
- Professionele netwerken die het vooral mogelijk maken om informatie over specialisten die niet actief op zoek zijn naar werk te publiceren of te vinden.

> Overlapt de categorie 'Online communicatiemedia'.

Systemen voor anonieme toegang

Deze categorie bevat webbronnen die als een verbindingsschakel werken voor de download van inhoud vanaf andere webbronnen via special webtoepassingen voor de volgende doeleinden:

- Omzeilen van beperkingen die een netwerkbeheerder heeft ingesteld voor de toegang tot webadressen of IP-adressen;
- Anonieme toegang tot webbronnen, inclusief webbronnen die HTTP-verzoeken van bepaalde IP-adressen of hun groepen (bijvoorbeeld IP-adressen gegroepeerd op land van oorsprong) weigeren.

> Deze categorie bevat zowel webbronnen die uitsluitend bedoeld zijn voor de eerder vermelde doeleinden ("anonymizers") als webbronnen met een vergelijkbare technische functionaliteit.

Computergames

Deze categorie bevat webbronnen die zijn gespecialiseerd in computergames van verschillende genres:

- Websites van ontwikkelaars van computergames.
- Webbronnen met discussies over computergames.

> Overlapt de categorie 'Online communicatiemedia'.

- Webbronnen met de technische capaciteit voor online deelname aan games, samen met andere deelnemers of individueel, met de lokale installatie van programma's of zonder zo'n installatie ("browsergames").
- Webbronnen waar games worden geadverteerd, verdeeld en ondersteund.

> Overlapt de categorie "E-commerce".

Godsdienst, religieuze groeperingen

Deze categorie bevat webbronnen met inhoud over sociale bewegingen, verenigingen en organisaties met een religieuze ideologie en/of cult in manifestaties.

- Websites van officiële religieuze organisaties op verschillende niveaus, gaande van internationale godsdiensten tot lokale religieuze gemeenschappen.
- Websites van niet-geregistreerde religieuze verenigingen en gemeenschappen die historisch zijn ontstaan door zich af te scheiden van een dominante religieuze vereniging of gemeenschap.
- Websites van religieuze verenigingen en gemeenschappen die onafhankelijk van traditionele religieuze bewegingen zijn ontstaan, inclusief op het initiatief van een specifieke stichter.
- Websites van interconfessionele organisaties die streven naar samenwerking tussen vertegenwoordigers van verschillende traditionele godsdiensten.
- Webbronnen met educatief, historisch en encyclopedisch materiaal over godsdiensten.
- Webbronnen met gedetailleerde voorstellingen of beschrijvingen van de verering als onderdeel van religieuze sekten, inclusief riten en rituelen die het aanbidden van God, wezens en/of items waarvan gedacht wordt dat ze bovennatuurlijke krachten hebben inhouden.

Nieuwsbronnen

Deze categorie bevat webbronnen met openbaar nieuws dat is gemaakt door de media of online publicaties waarmee gebruikers hun eigen nieuwsberichten kunnen toevoegen:

- Websites van officiële media.
- Websites die informatievoorzieningen met het kenmerk van officiële informatiebronnen aanbieden.
- Websites die diensten aanbieden die nieuws van verschillende officiële en officieuze bronnen verzamelen.
- Websites waar het nieuws door de gebruikers zelf wordt gemaakt (“sociale nieuwssites").

> Overlapt de categorie ‘Online communicatiemedia’.

Banners

Deze categorie bevat webbronnen met banners. Het adverteren van informatie op banners kan gebruikers afleiden van hun activiteiten, terwijl het verkeer toeneemt door de downloads van banners.

Over toegangsregels voor webbronnen

Een toegangsregel voor webbronnen is een reeks filters en acties die Kaspersky Endpoint Security toepast wanneer de gebruiker tijdens de opgegeven periode in de regelplanning webbronnen bezoekt die in de regel zijn beschreven. Met filters kunt u een aantal webbronnen preciseren waarvoor de toegang ertoe wordt gecontroleerd door het onderdeel Webcontrole.

De volgende filters zijn beschikbaar:

- **Filteren op inhoud**. Webcontrole categoriseert webbronnen op inhouds- en gegevenstype. U kunt de toegang van gebruikers tot webbronnen met inhouds- en gegevenstypen van bepaalde categorieën beheren. Wanneer de gebruikers webbronnen bezoeken die tot de geselecteerde categorie van inhouds- en gegevenstypen behoren, voert Kaspersky Endpoint Security de actie uit die in de regel is opgegeven.

- **Filteren op adressen van webbronnen**. U kunt de toegang van gebruikers tot alle adressen van webbronnen of tot individuele adressen van webbronnen en / of groepen van adressen van webbronnen beheren.

  Als het filteren op inhoud en het filteren op adressen van webbronnen zijn opgegeven en de opgegeven adressen van webbronnen en / groepen van adressen van webbronnen behoren tot de geselecteerde inhoudscategorieën of categorieën van gegevenstypen, controleert Kaspersky Endpoint Security niet de toegang tot alle webbronnen in de geselecteerde inhoudscategorieën en / of categorieën van gegevenstypen. In plaats daarvan controleert het programma alleen de toegang tot de opgegeven adressen van webbronnen en / of groepen van adressen van webbronnen.

- **Filteren op namen van gebruikers en groepen van gebruikers**. U kunt de namen van gebruikers en/of groepen van gebruikers opgeven waarvoor de toegang tot webbronnen wordt gecontroleerd overeenkomstig de regel.

- **Regelplanning**. U kunt de regelplanning opgeven. De regelplanning bepaalt de periode wanneer Kaspersky Endpoint Security de toegang tot de opgegeven webbronnen in de regel monitort.

Na de installatie van Kaspersky Endpoint Security is de lijst met regels van het onderdeel Webcontrole niet leeg. Twee regels zijn vooraf ingesteld:

- De regel 'Scenario's en stijltabellen' die alle gebruikers altijd toegang verleent tot webbronnen waarvan de adressen namen van bestanden met de extensies css, js of vbs bevatten. Bijvoorbeeld: http://www.voorbeeld.com/style.css, http://www.voorbeeld.com/style.css?mode=normal.

- De 'Standaardregel' die alle gebruikers altijd toegang tot webbronnen verleent.

Bewerkingen voor toegangsregels voor webbronnen

U kunt de volgende acties op toegangsregels voor webbronnen uitvoeren:

- Een nieuwe regel toevoegen

- Een regel bewerken

- Prioriteit aan een regel toewijzen

  De prioriteit van een regel wordt bepaald door de positie van de regel met een beknopte beschrijving van deze regel in de tabel met toegangsregels in het venster met de instellingen van het onderdeel Webcontrole. Dit betekent dat een regel die in de tabel met toegangsregels hoger is geplaatst dan andere regels ook een hogere prioriteit heeft dan die regels.

  Als de webbron die de gebruiker probeert te openen overeenkomt met de parameters van verschillende regels, voert Kaspersky Endpoint Security een actie uit volgens de regel met de hoogste prioriteit.

- Een regel testen.

  U kunt de consistentie van regel controleren met de functie Diagnose van regels.

- Schakel een regel in en uit.

  Een toegangsregel voor webbronnen kan worden ingeschakeld (status van werking: *Aan*) of uitgeschakeld (status van werking: *Uit*). Na het aanmaken van een regel wordt deze standaard ingeschakeld (status van werking: *Aan)*. U kunt de regel uitschakelen.

- Regel verwijderen

Een toegangsregel voor webbronnen toevoegen en bewerken

Zo voegt u een toegangsregel voor webbronnen toe en bewerkt u er een:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.
   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Voer een van de volgende acties uit:
   - Klik op de knop **Toevoegen** om een regel toe te voegen.
   - Als u een regel wilt bewerken, selecteert u de regel in de tabel en klikt u op de knop **Bewerken**.

   Het venster **Regel voor toegang tot webbronnen** wordt geopend.
4. Geef de instellingen van de regel op of bewerk ze. Hiertoe doet u het volgende:
   a. Typ of bewerk in het veld **Naam** de naam van de regel.
   b. Selecteer in de vervolgkeuzelijst **Filter inhoud** de vereiste optie:
      - **Alle inhoud**.
      - **Op inhoudscategorieën**.
      - **Op gegevenstypen**.
      - **Op inhoudscategorieën en gegevenstypen**.
   c. Als een andere optie dan **Alle inhoud** is geselecteerd, worden gedeelten geopend waarin u de inhoudscategorieën en/of de gegevenstypen kunt selecteren. Schakel de selectievakjes naast de namen van de vereiste inhoudscategorieën en/of gegevenstypen in.
      Met de inschakeling van het selectievakje naast de naam van een inhoudscategorie en/of een gegevenstype past Kaspersky Endpoint Security de regel voor de controle van de toegang tot webbronnen die tot de geselecteerde inhoudscategorieën en/of gegevenstypen behoren toe.
   d. Selecteer in de vervolgkeuzelijst **Pas toe op adressen** de vereiste optie:
      - **Op alle adressen**.
      - **Op individuele adressen**.
   e. Als de optie **Op individuele adressen** is geselecteerd, wordt een gedeelte geopend waarin u een lijst met webbronnen kunt aanmaken. U kunt de adressen van webbronnen toevoegen of bewerken met de knoppen **Toevoegen**, **Bewerken** en **Verwijderen**.
   f. Schakel het selectievakje **Geef gebruikers en/of groepen op**.
   g. Klik op de knop **Selecteren**.

Het venster **Gebruikers of groepen selecteren** wordt in Microsoft Windows geopend.

h. Geef de lijst met gebruikers en/of groepen van gebruikers op waarvoor de toegang tot webbronnen die in de regel zijn beschreven wordt toegestaan of geblokkeerd of bewerk de lijst.

i. Selecteer in de vervolgkeuzelijst **Actie** de vereiste optie:

- **Toestaan** Als deze waarde is geselecteerd, wordt de toegang tot webbronnen die aan de parameters van de regel voldoen toegestaan door Kaspersky Endpoint Security.
- **Blokkeren** Als deze waarde is geselecteerd, wordt de toegang tot webbronnen die aan de parameters van de regel voldoen geblokkeerd door Kaspersky Endpoint Security.
- **Waarschuwen**. Als deze waarde is geselecteerd, toont Kaspersky Endpoint Security een waarschuwing met de melding dat een webbron ongewenst is wanneer de gebruiker webbronnen probeert te openen die aan de regel voldoen. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

j. Selecteer in de vervolgkeuzelijst **Regelplanning** de naam van de noodzakelijke planning of maak een nieuwe planning op basis van de geselecteerde regelplanning. Hiertoe doet u het volgende:

1. Klik naast de vervolgkeuzelijst **Regelplanning** op de knop **Instellingen**.

   Het venster **Regelplanning** wordt geopend.

2. Als u een periode wanneer de regel niet van toepassing is wilt toevoegen aan de regelplanning, klikt u in de tabel met de regelplanning op de cellen die overeenkomen met de tijd en de dag van de week die u wilt selecteren.

   De kleur van de cellen wordt grijs.

3. Als u een periode wanneer de regel van toepassing is wilt vervangen door een periode wanneer de regel niet van toepassing is, klikt u op de grijze cellen in de tabel die overeenkomen met de tijd en de dag van de week die u wilt selecteren.

   De kleur van de cellen wordt groen.

4. Klik op de knop **Opslaan als**.

   Het venster **Naam regelplanning** wordt geopend.

5. Typ een naam voor de regelplanning of laat de voorgestelde standaardnaam ongewijzigd.

6. Klik op **OK**.

5. Klik in het venster **Regel voor toegang tot webbronnen** op **OK**.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Prioriteiten aan toegangsregels voor webbronnen toewijzen

U kunt prioriteiten aan elke regel uit de lijst met regels toewijzen door de regels in een bepaalde volgorde te zetten.

Zo wijst u een prioriteit toe aan een toegangsregel voor webbronnen:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.

3. Selecteer rechts in het venster de regel waarvan u de prioriteit wilt wijzigen.

4. Gebruik de knoppen **Omhoog** en **Omlaag** om de regel naar de gewenste plaats in de lijst met regels te bewegen.

5. Herhaal stappen 3–4 voor de regels waarvan u de prioriteit wilt wijzigen.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Toegangsregels voor webbronnen testen

Om de doeltreffendheid van de regels van Webcontrole te controleren, kunt u ze testen. Daarom beschikt het onderdeel Webcontrole over de functie Diagnose van regels.

Zo test u de toegangsregels voor webbronnen:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.

3. Klik rechts in het venster op de knop **Diagnose**.

   Het venster **Diagnose van regels** wordt geopend.

4. Vul de velden in het gedeelte **Voorwaarden** in:

   a. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot een specifieke webbron te controleren, schakelt u het selectievakje **Geef adres op** in. Voer het adres van de webbron in het veld eronder in.

   b. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot webbronnen te controleren voor opgegeven gebruikers en/of groepen van gebruikers, geeft u een lijst met gebruikers en/of groepen van gebruikers op.

   c. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot webbronnen van opgegeven inhoudscategorieën en / of categorieën van gegevenstypen te controleren, selecteert u in de vervolgkeuzelijst **Filter inhoud** de vereiste optie (**Op inhoudscategorieën**, **Op gegevenstypen** of **Op inhoudscategorieën en gegevenstypen**).

   d. Als u de regels wilt testen terwijl rekening wordt gehouden met de tijd en de dag van de week wanneer er wordt geprobeerd om toegang te krijgen tot webbronnen die in de diagnostische voorwaarden van de regel zijn opgegeven, schakelt u het selectievakje **Voeg tijdstip van toegangspoging toe** in. Geef dan de dag van de week en de tijd op.

5. Klik op de knop **Testen**.

Na de voltooiing van de test ziet u een bericht met informatie over de actie die door Kaspersky Endpoint Security is uitgevoerd, overeenkomstig de eerste regel die wordt geactiveerd bij de poging tot het krijgen van toegang tot de opgegeven webbron (toestaan, blokkeren of waarschuwen). De eerste regel die wordt geactiveerd is de regel die in de lijst met regels van Webcontrole hoger staat dan andere regels die aan de diagnostische voorwaarden voldoen. Het bericht wordt rechts van de knop **Testen** weergegeven. De volgende tabel bevat de resterende geactiveerde regels en geeft de actie van Kaspersky Endpoint Security aan. De regels worden in volgorde van afnemende prioriteit weergegeven.

Een toegangsregel voor webbronnen inschakelen en uitschakelen

Zo schakelt u een toegangsregel voor webbronnen in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Selecteer rechts in het venster de regel die u wilt inschakelen of uitschakelen.
4. Doe in de kolom **Status** het volgende:
   - Selecteer de waarde *Aan* als u het gebruik van de regel wilt inschakelen.
   - Selecteer de waarde *Uit* als u het gebruik van de regel wilt uitschakelen.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Toegangsregels voor webbronnen migreren vanaf oudere versies van het programma

Wanneer Service Pack 1 Maintenance Release 1 of een oudere versie van het programma wordt geüpgraded naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, worden de toegangsregels voor webbronnen op basis van de inhoudscategorieën van webbronnen als volgt gemigreerd:

- De toegangsregels voor webbronnen op basis van een of meer inhoudscategorieën van webbronnen uit de lijsten “Forums en chats”, “Webmail” en “Sociale netwerken” worden naar de inhoudscategorie “Online communicatiemedia” voor webbronnen gemigreerd.
- De toegangsregels voor webbronnen op basis van een of meer inhoudscategorieën van webbronnen uit de lijsten “Online winkels” en “Betaalsystemen” worden naar de inhoudscategorie “E-commerce” voor webbronnen gemigreerd.
- De toegangsregels voor webbronnen op basis van de inhoudscategorie “Gokken” worden naar de inhoudscategorie “Gokken, loterijen, sweepstakes” voor webbronnen gemigreerd.
- De toegangsregels voor webbronnen op basis van de inhoudscategorie “Browsergames” worden naar de inhoudscategorie “Computergames” voor webbronnen gemigreerd.
- De toegangsregels voor webbronnen op basis van de inhoudscategorieën van webbronnen die niet voorkomen in de bovenstaande lijst worden zonder wijzigingen gemigreerd.

De lijst met adressen van webbronnen exporteren en importeren

Als u een lijst met adressen van webbronnen in een toegangsregel voor webbronnen hebt gemaakt, kunt u die lijst naar een TXT-bestand exporteren. U kunt de lijst dan importeren vanuit dit bestand zodat u geen nieuwe lijst met adressen van webbronnen handmatig hoeft te maken wanneer u een toegangsregel configureert. De optie voor het exporteren en importeren van de lijst met adressen van webbronnen is wellicht nuttig wanneer u bijvoorbeeld toegangsregels met vergelijkbare parameters maakt.

Zo exporteert u een lijst met adressen van webbronnen naar een bestand:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Selecteer de regel waarvan u de lijst met adressen van webbronnen u wilt exporteren naar een bestand.
4. Klik op de knop **Bewerken**.

   Het venster **Regel voor toegang tot webbronnen** wordt geopend.
5. Als u niet de volledige lijst met adressen van webbronnen wilt exporteren maar gewoon een deel ervan, selecteert u de gewenste adressen van webbronnen.
6. Klik op de knop  rechts van het veld met de lijst met adressen van webbronnen.

   Het venster voor de bevestiging van de actie wordt geopend.
7. Voer een van de volgende acties uit:

   - Als u alleen de geselecteerde items in de lijst met adressen van webbronnen wilt exporteren, klikt u in het venster voor de bevestiging van de actie op de knop **Ja**.
   - Als u alle items uit de lijst met adressen van webbronnen wilt exporteren, klikt u in het venster voor de bevestiging van de actie op de knop **Nee**.

     Het standaardvenster **Opslaan als** wordt in Microsoft Windows geopend.
8. Selecteer in het venster **Opslaan als** in Microsoft Windows het bestand waarnaar u de lijst met adressen van webbronnen wilt exporteren. Klik op de knop **Opslaan**.

Zo importeert u de lijst met adressen van webbronnen vanuit een bestand in een regel:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Voer een van de volgende acties uit:

   - Klik op de knop **Toevoegen** als u een nieuwe toegangsregel voor webbronnen wilt aanmaken.
   - Selecteer de toegangsregel voor webbronnen die u wilt bewerken. Klik vervolgens op de knop **Bewerken**.

   Het venster **Regel voor toegang tot webbronnen** wordt geopend.

4. Voer een van de volgende acties uit:

   - Als u een nieuwe toegangsregel voor webbronnen aanmaakt, selecteert u **Op individuele adressen** in de vervolgkeuzelijst **Pas toe op adressen**.
   - Als u een toegangsregel voor webbronnen bewerkt, gaat u naar stap 5 van deze instructies.

5. Klik op de knop rechts van het veld met de lijst met adressen van webbronnen.

   Als u een nieuwe regel aanmaakt, wordt het standaardvenster **Bestand openen** in Microsoft Windows geopend.

   Als u een regel bewerkt, wordt een bevestigingsvenster geopend.

6. Voer een van de volgende acties uit:

   - Als u een nieuwe toegangsregel voor webbronnen bewerkt, gaat u naar stap 7 van deze instructies.
   - Als u een toegangsregel voor webbronnen bewerkt, doet u een van het volgende in het venster voor de bevestiging van de actie:
     - Klik op de knop **Ja** als u geïmporteerde items van de lijst met adressen van webbronnen wilt toevoegen aan de bestaande items.
     - Klik op de knop **Nee** als u de bestaande items van de lijst met adressen van webbronnen wilt verwijderen en de geïmporteerde items wilt toevoegen.

   Het venster **Bestand openen** wordt in Microsoft Windows geopend.

7. Selecteer in het venster **Bestand openen** in Microsoft Windows een bestand met een lijst met adressen van webbronnen die u wilt importeren.

8. Klik op de knop **Openen**.

9. Klik in het venster **Regel voor toegang tot webbronnen** op **OK**.

Maskers voor adressen van webbronnen bewerken

Een *adresmasker voor webbronnen* (ook "adresmasker" genoemd) is wellicht nuttig als u talrijke vergelijkbare adressen van webbronnen moet invoeren wanneer u een toegangsregel voor webbronnen aanmaakt. Eén adresmasker kan een groot aantal adressen van webbronnen vervangen als het goed bedacht is.

Volg deze regels wanneer u een adresmasker maakt:

1. Het teken `*` vervangt een willekeurige reeks met nul of meer tekens.

   Als u bijvoorbeeld het adresmasker *abc* invoert, wordt de toegangsregel toegepast op alle webbronnen met de reeks abc. Voorbeeld: http://www.voorbeeld.com/pagina_0-9abcdef.html.

   Om het teken `*` aan het adresmasker toe te voegen, voert u het teken `*` tweemaal in.

2. De tekenreeks `www.` bij het begin van het adresmasker wordt beschouwd als een `*.`-reeks.

   Voorbeeld: het adresmasker www.voorbeeld.com wordt als *.voorbeeld.com behandeld.

3. Als een adresmasker niet begint met het teken `*`, is de inhoud van het adresmasker gelijk aan dezelfde inhoud met het voorvoegsel `*.`.

4. Een reeks van `*.`-tekens bij het begin van een adresmasker wordt beschouwd als `*.` of een lege tekenreeks.

   Voorbeeld: het adresmasker http://www.*.voorbeeld.com omvat ook het adres http://www2.voorbeeld.com.

5. Als een adresmasker eindigt met een ander teken dan `/` of `*`, is de inhoud van het adresmasker gelijk aan dezelfde inhoud met het achtervoegsel `/*`.

   Voorbeeld: het adresmasker http://www.voorbeeld.com omvat adressen zoals http://www.voorbeeld.com/abc, waarbij a, b en c willekeurige tekens zijn.

6. Als een adresmasker eindigt met het teken `/`, is de inhoud van het adresmasker gelijk aan dezelfde inhoud met het achtervoegsel `/*.`.

7. De tekens `/*` op het einde van een adresmasker wordt beschouwd als `/*` of een lege tekenreeks.

8. De adressen van webbronnen worden vergeleken met een adresmasker, waarbij rekening wordt gehouden met het protocol (http of https):

   - Als het adresmasker geen netwerkprotocol bevat, omvat dit adresmasker alle adressen met een willekeurig netwerkprotocol.

     Voorbeeld: het adresmasker voorbeeld.com omvat de adressen http://voorbeeld.com en https://voorbeeld.com.

   - Als het adresmasker een netwerkprotocol bevat, omvat dit adresmasker alleen adressen met hetzelfde netwerkprotocol als dat van het adresmasker.

     Voorbeeld: het adresmasker http://*.voorbeeld.com omvat het adres http://www.voorbeeld.com maar niet https://www.voorbeeld.com.

9. Een adresmasker tussen dubbele aanhalingstekens wordt verwerkt zonder rekening te houden met andere vervangingen, met uitzondering van het teken `*` als het initieel was toegevoegd aan het adresmasker. Regels 5 en 7 zijn niet van toepassing op adresmaskers tussen dubbele aanhalingstekens (zie voorbeelden 14 – 18 in de onderstaande tabel).

10. De gebruikersnaam en het wachtwoord, de verbindingspoort en de letterkast worden tijdens de vergelijking met het adresmasker van een webbron genegeerd.

Voorbeelden van hoe u regels gebruikt om adresmaskers te maken

Nr.	Adresmasker	Te vergelijken adres van webbron	Omvat het adresmasker het adres	Opmerking
1	*.voorbeeld.com	http://www.123voorbeeld.com	Nee	Zie regel 1.
2	*.voorbeeld.com	http://www.123.voorbeeld.com	Ja	Zie regel 1.
3	*voorbeeld.com	http://www.123voorbeeld.com	Ja	Zie regel 1.
4	*voorbeeld.com	http://www.123.voorbeeld.com	Ja	Zie regel 1.
5	http://www.*.voorbeeld.com	http://www.123voorbeeld.com	Nee	Zie regel 1.
6	www.voorbeeld.com	http://www.voorbeeld.com	Ja	Zie regels 2, 1.
7	www.voorbeeld.com	https://www.voorbeeld.com	Ja	Zie regels 2, 1.
8	http://www.*.voorbeeld.com	http://123.voorbeeld.com	Ja	Zie regels 2, 4, 1.
9	www.voorbeeld.com	http://www.voorbeeld.com/abc	Ja	Zie regels 2, 5, 1.
10	voorbeeld.com	http://www.voorbeeld.com	Ja	Zie regels 3, 1.

11	http://voorbeeld.com/	http://voorbeeld.com/abc	Ja	Zie regel 6.
12	http://voorbeeld.com/*	http://voorbeeld.com	Ja	Zie regel 7.
13	http://voorbeeld.com	https://voorbeeld.com	Nee	Zie regel 8.
14	"voorbeeld.com"	http://www.voorbeeld.com	Nee	Zie regel 9.
15	"http://www.voorbeeld.com"	http://www.voorbeeld.com/abc	Nee	Zie regel 9.
16	"*.voorbeeld.com"	http://www.voorbeeld.com	Ja	Zie regels 1, 9.
17	"http://www.voorbeeld.com/*"	http://www.voorbeeld.com/abc	Ja	Zie regels 1, 9.
18	"www.voorbeeld.com"	http://www.voorbeeld.com; https://www.voorbeeld.com	Ja	Zie regels 9, 8.
19	www.voorbeeld.com/abc/123	http://www.voorbeeld.com/abc	Nee	Een adresmasker bevat meer informatie dan het adres van een webbron.

Berichtsjablonen van Webcontrole bewerken

Afhankelijk van het type actie dat in de eigenschappen van de regels van Webcontrole is opgegeven, toont Kaspersky Endpoint Security een van de volgende soorten berichten wanneer gebruikers toegang tot internetbronnen proberen te krijgen (het programma vervangt een HTML-pagina door een bericht voor het antwoord van de HTTP-server):

- Waarschuwingsbericht. Dit bericht waarschuwt de gebruiker dat een bezoek aan de webbron wordt afgeraden en/of het beveiligingsbeleid van het bedrijf schendt. Kaspersky Endpoint Security toont een waarschuwingsbericht als de optie **Waarschuwen** is geselecteerd in de vervolgkeuzelijst **Actie** in de instellingen van de regel die deze webbron beschrijft.

  Als de gebruiker vindt dat de waarschuwing een vergissing is, kan die klikken op de koppeling in de waarschuwing om een vooraf gegenereerd bericht naar de lokale netwerkbeheerder te sturen.

- Bericht met informatie over blokkering van een webbron. Kaspersky Endpoint Security toont een bericht met de melding dat een webbron is geblokkeerd als de optie **Blokkeren** is geselecteerd in de vervolgkeuzelijst **Actie** in de instellingen van de regel die deze webbron beschrijft.

  Als de gebruiker vindt dat de blokkering van de webbron een vergissing is, kan die klikken op de koppeling in het bericht over de blokkering van de webbron om een vooraf gegenereerd bericht naar de lokale netwerkbeheerder te sturen.

Voor het waarschuwingsbericht, het bericht met de melding dat een webbron is geblokkeerd en het bericht dat naar de netwerkbeheerder wordt verstuurd zijn speciale sjablonen voorzien. U kunt de inhoud ervan wijzigen.

Zo wijzigt u de sjabloon voor berichten van Webcontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Endpoint-controle** links in het venster het subgedeelte **Webcontrole**.

   Rechts in het venster ziet u de instellingen van het onderdeel Webcontrole.
3. Klik rechts in het venster op de knop **Sjablonen**.

Het venster **Berichtsjablonen** wordt geopend.

4. Voer een van de volgende acties uit:

   - Selecteer het tabblad **Waarschuwing** voor de bewerking voor de sjabloon van het waarschuwingsbericht waarin de gebruiker wordt afgeraden de webbron te bezoeken.

   - Selecteer het tabblad **Blokkering** voor de bewerking van de sjabloon voor het bericht waarin de gebruiker wordt gemeld dat de toegang tot de webbron is geblokkeerd.

   - Selecteer het tabblad **Bericht aan beheerder** voor de bewerking van de sjabloon voor het bericht dat naar de beheerder wordt verstuurd.

5. Bewerk de sjabloon van het bericht. U kunt ook de vervolgkeuzelijst **Variabele** gebruiken, alsook de knoppen **Standaard** en **Koppeling** (deze knop is niet beschikbaar op het tabblad **Bericht aan beheerder**).

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

KATA Endpoint Sensor

De instellingen van het onderdeel KATA Endpoint Sensor zijn alleen beschikbaar in de Beheerconsole van Kaspersky Security Center. Om dit onderdeel te gebruiken, moet u de beheerplug-in installeren.

In deze sectie vindt u informatie over KATA Endpoint Sensor en instructies voor de in- en uitschakeling van dit onderdeel.

Over KATA Endpoint Sensor

KATA Endpoint Sensor is een onderdeel van het Kaspersky Anti Targeted Attack Platform. Deze oplossing is bedoeld voor de snelle detectie van bedreigingen zoals doelgerichte aanvallen.

Dit onderdeel is op clientcomputers geïnstalleerd. Op deze computers monitort het onderdeel voortdurend processen, actieve netwerkverbindingen en bestanden die worden gewijzigd en stuurt het deze informatie door naar het Kaspersky Anti Targeted Attack Platform.

De functionaliteit van het onderdeel is beschikbaar op de volgende besturingssystemen:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition,
  Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Voor aanvullende informatie over het Kaspersky Anti Targeted Attack Platform, die u niet in dit document vindt, raadpleegt u de Help van het Kaspersky Anti Targeted Attack Platform.

Inkomende verbindingen naar computers met het onderdeel KATA Endpoint Sensor moeten rechtstreeks vanaf het Kaspersky Anti Targeted Attack Platform worden toegestaan, zonder een proxyserver.

Het onderdeel KATA Endpoint Sensor inschakelen en uitschakelen

Zo schakelt u het onderdeel KATA Endpoint Sensor in en uit:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de relevante beheergroep waarvoor u beleidsinstellingen wilt bewerken.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Geavanceerde instellingen** het subgedeelte **KATA Endpoint Sensor**.

7. Voer een van de volgende acties uit:

   - Schakel het selectievakje **KATA Endpoint Sensor** in als u KATA Endpoint Sensor wilt inschakelen.
   - Schakel het selectievakje **KATA Endpoint Sensor** uit als u KATA Endpoint Sensor wilt uitschakelen.

8. Als u tijdens de vorige stap het selectievakje **KATA Endpoint Sensor** hebt ingeschakeld, geeft u in het veld **Serveradres** het adres van Kaspersky Anti Targeted Attack Platform-server op dat uit de volgende delen bestaat:

   a. Protocolnaam

   b. IP-adres of volledig gekwalificeerde domeinnaam (FQDN) van de server

   c. Pad naar de Windows Event Collector op de server

9. Klik op **OK**.

10. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Gegevensencryptie

Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations, is de functionaliteit voor gegevensencryptie volledig beschikbaar. Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers, is alleen de encryptie van harde schijven met de technologie BitLocker-stationsversleuteling beschikbaar.

In deze sectie vindt u informatie over de encryptie en de decryptie van harde schijven, verwisselbare schijven en bestanden en mappen op lokale schijven van de computer. U leest ook hoe u de encryptie en de decryptie van gegevens kunt configureren en uitvoeren met behulp van Kaspersky Endpoint Security en de beheerplug-in van Kaspersky Endpoint Security.

Als u geen toegang tot geëncrypte gegevens hebt, raadpleegt u de speciale instructies voor het werken met geëncrypte gegevens (Werken met geëncrypte bestanden in het geval van beperkte functionaliteit voor bestandsencryptie, Werken met geëncrypte apparaten als er geen toegang toe is).

De weergave van encryptie-instellingen in het Kaspersky Security Center-beleid inschakelen

Zo schakelt u de weergave van encryptie-instellingen in het Kaspersky Security Center-beleid in:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in het contextmenu van het knooppunt **Administration Server – <Naam van computer>** in de structuur van de Beheerconsole achtereenvolgens **Weergave** → **Interface-instellingen**.

   Het venster **Interface-instellingen** wordt geopend.
3. Schakel in het venster **Interface-instellingen** het selectievakje **Encryptie en gegevensbescherming tonen** in.
4. Klik op **OK**.

Over gegevensencryptie

Met Kaspersky Endpoint Security kunt u bestanden en mappen op lokale en verwisselbare schijven of volledige verwisselbare schijven en harde schijven encrypten. Een gegevensencryptie minimaliseert het risico op het uitlekken van informatie wanneer een draagbare computer, een verwisselbare schijf of een harde schijf verloren raakt of gestolen wordt of wanneer de gegevens door onbevoegde gebruikers of programma's worden geopend.

Als de licentie is verlopen, encrypt het programma geen nieuwe gegevens en de oude geëncrypte gegevens blijven geëncrypt en beschikbaar. In dit geval moet voor de encryptie van nieuwe gegevens het programma worden geactiveerd met een nieuwe licentie die het gebruik van encryptie toestaat.

Als uw licentie is verlopen, de Gebruiksrechtovereenkomst wordt geschonden of de code, Kaspersky Endpoint Security of encryptieonderdelen zijn verwijderd, kan de geëncrypte toestand van eerder geëncrypte bestanden niet worden verzekerd. De reden hiervoor is omdat bepaalde programma's (zoals Microsoft Office Word) tijdens bewerkingen een tijdelijke kopie van bestanden maken. Wanneer het originele bestand wordt opgeslagen, wordt het originele exemplaar vervangen door het tijdelijke exemplaar. Op een computer zonder encryptiefunctionaliteit of zonder toegang tot de encryptiefunctionaliteit behoudt het bestand hierdoor een niet-geëncrypte toestand.

Kaspersky Endpoint Security beschikt over de volgende aspecten voor gegevensbescherming:

- **Bestanden op schijven van een lokale computer encrypten**. U kunt lijsten met bestanden maken volgens extensie of groep van extensies en lijsten met mappen op lokale schijven van de computer en regels maken voor de encryptie van bestanden die door specifieke programma's zijn aangemaakt. Nadat een Kaspersky Security Center-beleid is toegepast, encrypt en decrypt Kaspersky Endpoint Security de volgende bestanden:

  - Individuele bestanden die aan encryptie- en decryptielijsten zijn toegevoegd.
  - Bestanden in mappen die aan encryptie- en decryptielijsten zijn toegevoegd.
  - Bestanden die door afzonderlijke programma's zijn aangemaakt.

  Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

- **Encryptie van verwisselbare schijven**. U kunt een standaard encryptieregel opgeven waarmee het programma dezelfde actie toepast op alle verwisselbare schijven of u kunt encryptieregels voor individuele verwisselbare schijven opgeven.

  De standaard encryptieregel heeft een lagere prioriteit dan de encryptieregels die voor individuele verwisselbare schijven zijn gemaakt. Encryptieregels die voor een specifiek model van verwisselbare schijven zijn gemaakt, hebben een lagere prioriteit dan encryptieregels die voor verwisselbare schijven met een opgegeven apparaat-ID zijn gemaakt.

  Om een encryptieregel voor regels op een verwisselbare schijf te selecteren, controleert Kaspersky Endpoint Security of het model en het ID van het apparaat gekend zijn. Het programma voert dan een van de volgende bewerkingen uit:

  - Als alleen het model van het apparaat is gekend, gebruikt het programma de gemaakte encryptieregel (als er een is) voor het specifieke model van de verwisselbare schijven.
  - Als alleen het ID van het apparaat is gekend, gebruikt het programma de gemaakte encryptieregel (als er een is) voor verwisselbare schijven met het specifieke apparaat-ID.
  - Als het model en het ID van het apparaat zijn gekend, past het programma de gemaakte encryptieregel (als er een is) voor verwisselbare schijven met het specifieke apparaat-ID toe. In het geval dat er zo geen regel bestaat maar wel een voor het specifieke model van verwisselbare schijven, past het programma deze regel toe. Als geen encryptieregel is opgegeven voor het specifieke apparaat-ID of voor het specifieke model van het apparaat, past het programma de standaard encryptieregel toe.
  - Als noch het model van het apparaat noch het apparaat-ID zijn gekend, gebruikt het programma de standaard encryptieregel.

  Met het programma kunt u een verwisselbare schijf voorbereiden op het gebruik van de geëncrypte gegevens erop in de portable modus. Na de inschakeling van de portable modus hebt u toegang tot geëncrypte bestanden op verwisselbare schijven die zijn aangesloten op een computer zonder encryptiefunctionaliteit.

  Het programma voert de opgegeven actie in de encryptieregel uit wanneer het Kaspersky Security Center-beleid wordt toegepast.

- **Regels voor toegang van programma's tot geëncrypte bestanden beheren**. U kunt voor alle programma's een toegangsregel voor geëncrypte bestanden maken waarmee de toegang tot geëncrypte bestanden wordt geblokkeerd of waarmee de toegang tot geëncrypte bestanden alleen als gecodeerde tekst wordt toegestaan. Deze gecodeerde tekst is een reeks tekens die tijdens de toepassing van de encryptie wordt verkregen.

- **Geëncrypte archieven aanmaken**. U kunt geëncrypte archieven aanmaken en de toegang tot zulke archieven beveiligen met een wachtwoord. De toegang tot de inhoud van geëncrypte archieven is alleen mogelijk door de wachtwoorden in te voeren waarmee u de toegang tot die archieven hebt beveiligd. Zulke archieven kunnen veilig worden verzonden via netwerken of naar verwisselbare schijven.

- **Encryptie van harde schijven**. U kunt een encryptietechnologie selecteren: Kaspersky Disk Encryption of BitLocker-stationsversleuteling (hierna ook gewoon "BitLocker" genoemd).

  BitLocker is een technologie die een onderdeel van het Windows-besturingssysteem is. Als een computer over een Trusted Platform Module (TPM) beschikt, gebruikt BitLocker die module om herstelsleutels op te slaan die toegang tot een geëncrypte harde schijf kunnen geven. Wanneer de computer wordt opgestart, vraagt BitLocker de herstelsleutels voor de harde schijf op bij de Trusted Platform Module en ontgrendelt het de schijf. U kunt het gebruik van een wachtwoord en/of pincode voor de toegang tot herstelsleutels configureren.

  U kunt de standaard encryptieregel voor harde schijven opgeven en een lijst met harde schijven maken die niet moeten worden geëncrypt. Kaspersky Endpoint Security voert de encryptie van harde schijven sector per sector uit nadat het Kaspersky Security Center-beleid is toegepast. Het programma encrypt alle logische partities van harde schijven tegelijkertijd. Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

  Na de encryptie van de harde schijven van het systeem moet de gebruiker bij de volgende opstart van de computer diens identiteit verifiëren met behulp van de Verificatie-agent. Pas daarna wordt toegang tot de harde schijven verleend en wordt het besturingssysteem geladen. Hiertoe moet het wachtwoord van de token of de smartcard die is aangesloten op de computer worden ingevoerd of moeten de gebruikersnaam en het wachtwoord van het account in Verificatie-agent worden ingevoerd. Dit account is door de netwerkbeheerder aangemaakt met een taak voor het accountbeheer in Verificatie-agent. Dit account is gebaseerd op een Microsoft Windows-account waarmee een gebruiker zich bij het besturingssysteem aanmeldt. U kunt accounts in Verificatie-agent beheren en de Eenmalige aanmelding (SSO) gebruiken waarmee u zich automatisch bij het besturingssysteem kunt aanmelden met de gebruikersnaam en het wachtwoord van het account in Verificatie-agent.

  > Als u een back-up van de computer maakt en dan de gegevens op de computer encrypt om vervolgens de back-up van de computer terug te zetten en de gegevens van de computer opnieuw te encrypten, maakt Kaspersky Endpoint Security duplicaten van de accounts in Verificatie-agent. Om de dubbele accounts te verwijderen, moet u het hulpprogramma 'klmover' met de sleutel `dupfix` gebruiken. Het hulpprogramma 'klmover' is een onderdeel van de Kaspersky Security Center-build. U kunt meer over de werking ervan lezen in de *beheerdershandleiding van Kaspersky Security Center*.

  > Wanneer de versie van het programma wordt geüpgraded naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, wordt de lijst met accounts van Verificatie-agent niet opgeslagen.

  De toegang tot geëncrypte harde schijven is alleen mogelijk vanaf computers waarop Kaspersky Endpoint Security met encryptiefunctionaliteit voor harde schijven is geïnstalleerd. Deze voorzorgsmaatregel minimaliseert het risico op het uitlekken van gegevens die op een geëncrypte harde schijf staan wanneer iemand van buiten het lokale bedrijfsnetwerk toegang ertoe probeert te krijgen.

Om harde schijven en verwisselbare schijven te encrypten, kunt u de functie **Alleen gebruikte schijfruimte encrypten** gebruiken. U wordt aanbevolen deze functie alleen te gebruiken voor nieuwe apparaten die niet eerder zijn gebruikt. Als u een encryptie toepast op een apparaat dat al wordt gebruikt, wordt u aanbevolen het gehele apparaat te encrypten. Dit verzekert dat alle gegevens zijn beschermd, zelfs verwijderde gegevens die mogelijk nog ophaalbare informatie bevatten.

Kaspersky Endpoint Security verkrijgt de kaart met bestandssysteemsectoren alvorens de encryptie te starten. De eerste encryptiefase is gericht op sectoren die worden ingenomen door bestanden op het moment dat de encryptie wordt gestart. De tweede encryptiefase is gericht op sectoren waarnaar er is geschreven nadat de encryptie werd gestart. Wanneer de encryptie is voltooid, zijn alle sectoren met gegevens geëncrypt.

Wanneer de encryptie is voltooid en een gebruiker een bestand verwijdert, worden de sectoren waar het verwijderde bestand was opgeslagen opnieuw beschikbaar. In die sectoren kan dan nieuwe informatie op bestandssysteemniveau worden opgeslagen die ook geëncrypt zal zijn. Dit betekent ook dat bij het schrijven van nieuwe bestanden naar een nieuw apparaat tijdens de start van een normale encryptie waarbij de functie **Alleen gebruikte schijfruimte encrypten** is ingeschakeld op de computer, alle sectoren na een bepaalde tijd geëncrypt zullen zijn.

De benodigde gegevens voor de decryptie van de bestanden worden door de Administration Server van Kaspersky Security Center geleverd die de computer op het moment van de encryptie beheerde. Als de computer met geëncrypte bestanden om een willekeurige reden onder de controle van een andere Administration Server staat en de geëncrypte bestanden zijn niet eenmaal geopend geweest, kan op de volgende manieren toegang worden verkregen:

- toegang tot geëncrypte objecten vragen aan de netwerkbeheerder;
- toegang tot geëncrypte bestanden herstellen met de Herstelvoorziening;
- Gebruik een back-up voor het herstellen van de configuratie van de Administration Server van Kaspersky Security Center die de computer op het moment van de encryptie controleerde en gebruik deze configuratie op de Administration Server die de computer met de geëncrypte objecten nu beheert.

Het programma maakt tijdens de encryptie servicebestanden aan. Ongeveer twee tot drie procent van niet-gefragmenteerde vrije ruimte op de harde schijf is vereist voor de opslag ervan. Als er onvoldoende niet-gefragmenteerde vrije ruimte op de harde schijf is, wordt de encryptie pas gestart wanneer er voldoende ruimte is vrijgemaakt.

De compatibiliteit tussen de encryptiefunctionaliteit van Kaspersky Endpoint Security en Kaspersky Anti-Virus voor UEFI wordt niet ondersteund. De encryptie van de harde schijven van computers waarop Kaspersky Anti-Virus voor UEFI is geïnstalleerd zorgt ervoor dat Kaspersky Anti-Virus voor UEFI onklaar wordt gemaakt.

Beperkingen van de encryptiefunctionaliteit

Het maken van nieuwe partities op geëncrypte harde schijven en het formatteren van bestaande partities op geëncrypte harde schijven kan leiden tot gegevensverlies op deze harde schijven.

De encryptie van harde schijven met Kaspersky Disk Encryption is niet beschikbaar voor harde schijven die niet aan de hardware- en softwarevereisten voldoen.

Kaspersky Endpoint Security ondersteunt de volgende configuraties niet:

- Het opstartlaadprogramma staat op een schijf terwijl het besturingssysteem op een andere schijf staat.
- Het systeem bevat ingebedde software met de UEFI 32-standaard.

- Intel® Rapid Start Technology en schijven met een sluimerstandpartitie zelfs als Intel® Rapid Start Technology is uitgeschakeld.
- Schijven in MBR-indeling met meer dan vier uitgebreide partities.
- Het wisselbestand staat op een schijf waarop het systeem niet staat.
- Systeem met meerdere opstartmogelijkheden dankzij verschillende geïnstalleerde besturingssystemen.
- Dynamische partities (alleen primaire partities worden ondersteund).
- Schijven met minder dan 2% vrije, niet-gefragmenteerde schijfruimte.
- Schijven met een sectorgrootte verschillend van 512 bytes of 4096 bytes die 512 bytes emuleren.
- Hybride stations.

Het encryptiealgoritme wijzigen

Het encryptiealgoritme dat wordt gebruikt door Kaspersky Endpoint Security voor de gegevensencryptie hangt af van de encryptiebibliotheken die in het distributiepakket zijn opgenomen.

Zo wijzigt u het encryptiealgoritme:

1. Decrypt objecten die Kaspersky Endpoint Security heeft geëncrypt voordat u het encryptiealgoritme begint te wijzigen.

   Na de wijziging van het encryptiealgoritme zijn eerder geëncrypte objecten niet meer beschikbaar.

2. Verwijder Kaspersky Endpoint Security.
3. Installeer Kaspersky Endpoint Security met het distributiepakket dat encryptiebibliotheken voor verschillende bitversies bevat.

Eenmalige aanmelding (SSO) inschakelen

De technologie Eenmalige aanmelding (SSO) is niet compatibel met andere providers van accountgegevens.

Zo schakelt u de technologie Eenmalige aanmelding (SSO) in:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de technologie Eenmalige aanmelding (SSO) wilt inschakelen.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Algemene encryptie-instellingen**.
7. Klik in het subgedeelte **Algemene encryptie-instellingen** op de knop **Configureren** in het gedeelte **Wachtwoordinstellingen**.

   Hiermee opent u het tabblad **Verificatie-agent** van het venster **Instellingen van encryptiewachtwoord**.

8. Schakel het selectievakje **Eenmalige aanmelding (SSO) gebruiken** in.
9. Klik op **OK**.
10. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.
11. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Speciale aandachtspunten bij bestandsencryptie

Wanneer u de functionaliteit voor bestandsencryptie gebruikt, moet u rekening houden met het volgende:

- Het Kaspersky Security Center-beleid met vooraf geconfigureerde instellingen voor de encryptie van verwisselbare schijven is opgesteld voor een specifieke groep van beheerde computers. Daarom hangt het resultaat van de toepassing van het beleid voor encryptie/decryptie van bestanden op verwisselbare schijven af van de computer waarop de verwisselbare schijven zijn aangesloten.
- Kaspersky Endpoint Security encrypt of decrypt geen bestanden met een alleen-lezenstatus die op verwisselbare schijven zijn opgeslagen.
- Kaspersky Endpoint Security encrypt of decrypt bestanden in vooraf gedefinieerde mappen alleen voor lokale gebruikersprofielen van het besturingssysteem. Kaspersky Endpoint Security encrypt of decrypt geen bestanden in vooraf gedefinieerde mappen van zwervende gebruikersprofielen, verplichte gebruikersprofielen, tijdelijke gebruikersprofielen en omgeleide mappen. De lijst met standaardmappen die Kaspersky aanbeveelt te encrypten zijn onder andere de volgende mappen:

  - Documenten
  - Favorieten
  - Cookies
  - Bureaublad
  - Tijdelijke Internet Explorer-bestanden
  - Tijdelijke bestanden
  - Outlook-bestanden

- Kaspersky Endpoint Security encrypt geen bestanden of mappen wanneer het besturingssysteem of de geïnstalleerde programma's hierdoor beschadigd kunnen raken. De volgende bestanden en mappen met alle geneste mappen staan bijvoorbeeld op de lijst met encryptie-uitzonderingen:

  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - Windows-registerbestanden.

  De lijst met encryptie-uitzonderingen kan niet worden bekeken of bewerkt. Hoewel bestanden en mappen uit de lijst met encryptie-uitzonderingen kunnen worden toegevoegd aan de encryptielijst, worden ze toch niet geëncrypt tijdens een encryptietaak voor bestanden of mappen.

- De volgende soorten apparaten worden als verwisselbare schijven ondersteund:

  - Gegevensmedia aangesloten via de USB-bus
  - Harde schijven aangesloten via USB- en FireWire-bussen
  - SSD-schijven aangesloten via USB- en FireWire-bussen

Bestanden op schijven van een lokale computer encrypten

De encryptie van bestanden op de lokale schijven van de computer is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. De encryptie van bestanden op de lokale schijven van de computer is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie wordt de encryptie van bestanden op de lokale schijven van de computer besproken en leest u hoe u de encryptie van bestanden op de lokale schijven van de computer kunt configureren en uitvoeren met Kaspersky Endpoint Security en de plug-in van de Kaspersky Endpoint Security-console.

Bestanden op schijven van een lokale computer encrypten

Zo encrypt u bestanden op lokale schijven:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de encryptie van bestanden op lokale schijven wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

- Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van bestanden en mappen**.

7. Selecteer rechts in het venster het tabblad **Encryptie**.

8. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Standaardregels**.

9. Klik op het tabblad **Encryptie** op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst een van de volgende opties:

   a. Selecteer de optie **Vooraf gedefinieerde mappen** om bestanden uit mappen van lokale gebruikersprofielen voorgesteld door experts van Kaspersky toe te voegen aan een encryptieregel.

   Het venster **Vooraf gedefinieerde mappen selecteren** wordt geopend.

   b. Selecteer de optie **Aangepaste map** om een handmatig ingevoerd pad naar een map toe te voegen aan een encryptieregel.

   Het venster **Aangepaste map toevoegen** wordt geopend.

   c. Selecteer de optie **Bestanden op extensie** om bestandsextensies aan een encryptieregel toe te voegen. Kaspersky Endpoint Security encrypt bestanden met de opgegeven extensies op alle lokale schijven van de computer.

   Het venster **Lijst met bestandsextensies toevoegen/bewerken** wordt geopend.

   d. Selecteer de optie **Bestanden op groep(en) van extensies** om groepen van bestandsextensies aan een encryptieregel toe te voegen. Kaspersky Endpoint Security encrypt bestanden met extensies uit de groepen van extensies op alle lokale schijven van de computer.

   Het venster **Groepen van bestandsextensies selecteren** wordt geopend.

10. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

11. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Zodra het beleid is toegepast, encrypt Kaspersky Endpoint Security de bestanden die in de encryptieregel zijn opgenomen en niet in de decryptieregel zijn opgenomen.

> Als hetzelfde bestand is toegevoegd aan de encryptieregel en de decryptieregel, encrypt Kaspersky Endpoint Security dit bestand niet als het niet is geëncrypt en decrypt Kaspersky Endpoint Security het bestand als het is geëncrypt.

Kaspersky Endpoint Security encrypt niet-geëncrypte bestanden als hun eigenschappen (bestandspad / bestandsnaam / bestandsextensie) nog steeds voldoen aan de criteria van de encryptieregel na de wijziging.

Kaspersky Endpoint Security encrypt geopende bestanden pas nadat ze zijn gesloten.

Wanneer de gebruiker een nieuw bestand aanmaakt waarvan de eigenschappen voldoen aan de criteria van de encryptieregel, encrypt Kaspersky Endpoint Security het bestand zodra het wordt geopend.

Als u een geëncrypt bestand naar een andere map op de lokale schijf verplaatst, blijft het bestand geëncrypt ongeacht of deze map al dan niet is opgenomen in de encryptieregel.

Toegangsregels voor geëncrypte bestanden maken voor programma's

Zo maakt u toegangsregels voor geëncrypte bestanden voor programma's:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u toegangsregels voor geëncrypte bestanden wilt configureren voor programma's.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van bestanden en mappen**.
7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Standaardregels**.

   Toegangsregels worden alleen in de modus **Standaardregels** toegepast. Als u na het toepassen van de toegangsregels in de modus **Standaardregels** overschakelt naar de modus **Ongewijzigd laten**, negeert Kaspersky Endpoint Security alle toegangsregels. Alle programma's hebben dan toegang tot alle geëncrypte bestanden.

8. Selecteer rechts in het venster het tabblad **Regels voor programma's**.
9. Als u programma's uitsluitend uit de Kaspersky Security Center-lijst wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Programma's uit Kaspersky Security Center-lijst**.

   Het venster **Programma's van Kaspersky Security Center-lijst toevoegen** wordt geopend.

   Doe het volgende:

   a. Geef filters op om de lijst met programma's in de tabel te beperken. Kies hiervoor de waarden van de parameters **Programma**, **Leverancier** en **Periode toegevoegd** alsook alle selectievakjes uit het gedeelte **Groep**.

   b. Klik op de knop **Vernieuwen**.

      In de tabel ziet u programma's die aan de toegepaste filters voldoen.

   c. Schakel in de kolom **Programma's** de selectievakjes naast de programma's in waarvoor u toegangsregels voor geëncrypte bestanden wilt maken.

   d. Selecteer in de vervolgkeuzelijst **Regel voor programma('s)** de regel die de toegang van programma's tot geëncrypte bestanden zal bepalen.

   e. Selecteer in de vervolgkeuzelijst **Acties voor programma's die eerder zijn geselecteerd** de actie die Kaspersky Endpoint Security moet uitvoeren op de toegangsregels voor geëncrypte bestanden die eerder voor die programma's zijn gemaakt.

f. Klik op **OK**.

De details van een toegangsregel voor geëncrypte bestanden voor programma's verschijnen in de tabel op het tabblad **Regels voor programma's**.

10. Als u programma's handmatig wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Aangepaste programma's**.

    Het venster **Namen van uitvoerbare bestanden van programma's toevoegen / bewerken** wordt geopend.

    Doe het volgende:

    a. Typ in het invoerveld de naam of lijst met namen van uitvoerbare bestanden van programma's, inclusief hun extensies.

    U kunt ook de namen van uitvoerbare bestanden van programma's vanuit de Kaspersky Security Center-lijst toevoegen door op de knop **Toevoegen vanaf Kaspersky Security Center-lijst** te klikken.

    b. Voer indien nodig in het veld **Beschrijving** een beschrijving voor de lijst met programma's in.

    c. Selecteer in de vervolgkeuzelijst **Regel voor programma('s)** de regel die de toegang van programma's tot geëncrypte bestanden zal bepalen.

    d. Klik op **OK**.

    De details van een toegangsregel voor geëncrypte bestanden voor programma's verschijnen in de tabel op het tabblad **Regels voor programma's**.

11. Klik op **OK** om de wijzigingen op te slaan.

Bestanden die zijn gemaakt of gewijzigd door specifieke programma's encrypten

U kunt een regel maken waarmee Kaspersky Endpoint Security alle bestanden encrypt die door de opgegeven programma's in de regel worden gemaakt of gewijzigd.

Bestanden die door de specifieke programma's werden gemaakt of gewijzigd voordat de encryptieregel is toegepast, worden niet geëncrypt.

Zo configureert u de encryptie van bestanden die zijn gemaakt of gewijzigd door specifieke programma's:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de relevante beheergroep waarvoor u de encryptie van bestanden die zijn gemaakt door specifieke programma's wilt configureren.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

    - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

- Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van bestanden en mappen**.

7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Standaardregels**.

   Encryptieregels worden alleen in de modus **Standaardregels** toegepast. Als u na het toepassen van de encryptieregels in de modus **Standaardregels** overschakelt naar de modus **Ongewijzigd laten**, negeert Kaspersky Endpoint Security alle encryptieregels. Bestanden die eerder werden geëncrypt blijven geëncrypt.

8. Selecteer rechts in het venster het tabblad **Regels voor programma's**.

9. Als u programma's uitsluitend uit de Kaspersky Security Center-lijst wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Programma's uit Kaspersky Security Center-lijst**.

   Het venster **Programma's van Kaspersky Security Center-lijst toevoegen** wordt geopend.

   Doe het volgende:

   a. Geef filters op om de lijst met programma's in de tabel te beperken. Kies hiervoor de waarden van de parameters **Programma**, **Leverancier** en **Periode toegevoegd** alsook alle selectievakjes uit het gedeelte **Groep**.

   b. Klik op de knop **Vernieuwen**.

      In de tabel ziet u programma's die aan de toegepaste filters voldoen.

   c. Schakel in de kolom **Programma** de selectievakjes in naast de programma's die bestanden aanmaken die u wilt encrypten.

   d. Selecteer in de vervolgkeuzelijst **Regel voor programma('s)** de optie **Alle gemaakte bestanden encrypten**.

   e. Selecteer in de vervolgkeuzelijst **Acties voor programma's die eerder zijn geselecteerd** de actie die Kaspersky Endpoint Security moet uitvoeren op de encryptieregels voor bestanden die eerder voor die programma's zijn gemaakt.

   f. Klik op **OK**.

   Informatie over de encryptieregel voor bestanden die door de geselecteerde programma's zijn aangemaakt of gewijzigd verschijnt in de tabel op het tabblad **Regels voor programma's**.

10. Als u programma's handmatig wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Aangepaste programma's**.

    Het venster **Namen van uitvoerbare bestanden van programma's toevoegen / bewerken** wordt geopend.

    Doe het volgende:

    a. Typ in het invoerveld de naam of lijst met namen van uitvoerbare bestanden van programma's, inclusief hun extensies.

       U kunt ook de namen van uitvoerbare bestanden van programma's vanuit de Kaspersky Security Center-lijst toevoegen door op de knop **Toevoegen vanaf Kaspersky Security Center-lijst** te klikken.

    b. Voer indien nodig in het veld **Beschrijving** een beschrijving voor de lijst met programma's in.

    c. Selecteer in de vervolgkeuzelijst **Regel voor programma('s)** de optie **Alle gemaakte bestanden encrypten**.

d. Klik op **OK**.

Informatie over de encryptieregel voor bestanden die door de geselecteerde programma's zijn aangemaakt of gewijzigd verschijnt in de tabel op het tabblad **Regels voor programma's**.

11. Klik op **OK** om de wijzigingen op te slaan.

Een decryptieregel genereren

Zo genereert u een decryptieregel:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een lijst met te decrypten bestanden wilt aanmaken.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van bestanden en mappen**.
7. Selecteer rechts in het venster het tabblad **Decryptie**.
8. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Standaardregels**.
9. Klik op het tabblad **Decryptie** op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst een van de volgende opties:

   a. Selecteer de optie **Vooraf gedefinieerde mappen** om bestanden uit mappen van lokale gebruikersprofielen, voorgesteld door experts van Kaspersky, toe te voegen aan een decryptieregel.

   Het venster **Vooraf gedefinieerde mappen selecteren** wordt geopend.

   b. Selecteer de optie **Aangepaste map** om een handmatig ingevoerd pad naar een map toe te voegen aan een decryptieregel.

   Het venster **Aangepaste map toevoegen** wordt geopend.

   c. Selecteer de optie **Bestanden op extensie** om bestandsextensies aan een decryptieregel toe te voegen. Kaspersky Endpoint Security encrypt geen bestanden met de opgegeven extensies op alle lokale schijven van de computer.

   Het venster **Lijst met bestandsextensies toevoegen/bewerken** wordt geopend.

   d. Selecteer de optie **Bestanden op groep(en) van extensies** om groepen van bestandsextensies aan een decryptieregel toe te voegen. Kaspersky Endpoint Security encrypt geen bestanden met extensies uit de groepen van extensies op alle lokale schijven van computers.

   Het venster **Groepen van bestandsextensies selecteren** wordt geopend.

10. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

11. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Als hetzelfde bestand is toegevoegd aan de encryptieregel en de decryptieregel, encrypt Kaspersky Endpoint Security dit bestand niet als het niet is geëncrypt en decrypt Kaspersky Endpoint Security het bestand als het is geëncrypt.

Bestanden op schijven van een lokale computer decrypten

Zo decrypt u bestanden op lokale schijven:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de decryptie van bestanden op lokale schijven wilt configureren.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van bestanden en mappen**.

7. Selecteer rechts in het venster het tabblad **Encryptie**.

8. Verwijder de mappen en de bestanden die u wilt decrypten uit de encryptielijst. Selecteer hiervoor de bestanden en kies de optie **Regel verwijderen en bestanden decrypten** in het contextmenu van de knop **Verwijderen**.

   U kunt verschillende items tegelijk verwijderen uit de encryptielijst. Hiertoe houdt u de **CTRL**-toets ingedrukt en selecteert u de nodige bestanden door er met de linkermuisknop op te klikken. Vervolgens kiest u de optie **Regel verwijderen en bestanden decrypten** in het contextmenu van de knop **Verwijderen**.

   Bestanden en mappen die worden verwijderd uit de encryptielijst worden automatisch toegevoegd aan de decryptielijst.

9. Maak een decryptielijst voor bestanden.

10. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

11. Pas het beleid toe.

Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Zodra het beleid is toegepast, decrypt Kaspersky Endpoint Security geëncrypte bestanden die aan de decryptielijst zijn toegevoegd.

Kaspersky Endpoint Security decrypt geëncrypte bestanden als hun parameters (bestandspad /bestandsnaam /bestandsextensie) zodanig wijzigen dat ze voldoen aan de parameters van objecten die aan de decryptielijst zijn toegevoegd.

Kaspersky Endpoint Security decrypt geopende bestanden pas nadat ze zijn gesloten.

Geëncrypte pakketten aanmaken

Kaspersky Endpoint Security comprimeert geen bestanden wanneer het een geëncrypt pakket aanmaakt.

Zo maakt u een geëncrypt pakket aan:

1. Gebruik op een computer met Kaspersky Endpoint Security en ingeschakelde encryptiefunctionaliteit een bestandsverkenner om bestanden en/of mappen te selecteren die u aan een geëncrypt pakket wilt toevoegen. Klik rechts om het contextmenu ervan te openen.

2. Selecteer in het contextmenu de optie **Toevoegen aan geëncrypt pakket**.

   Het standaarddialoogvenster **Kies het pad waar u het geëncrypte pakket wilt opslaan** in Microsoft Windows wordt geopend.

3. Selecteer in het standaarddialoogvenster **Kies het pad waar u het geëncrypte pakket wilt opslaan** in Microsoft Windows een doelmap waarin u het geëncrypte pakket op de verwisselbare schijf wilt opslaan. Klik op de knop **Opslaan**.

   Het venster **Toevoegen aan geëncrypt pakket** wordt geopend.

4. Typ in het venster **Toevoegen aan geëncrypt pakket** een wachtwoord en bevestig het.

5. Klik op de knop **Maken**.

   Het aanmaken van het geëncrypte pakket wordt gestart. Wanneer het proces is voltooid, is een zelfuitpakkend geëncrypt pakket met wachtwoordbeveiliging aangemaakt in de geselecteerde doelmap op de verwisselbare schijf.

Als u het aanmaken van een geëncrypt pakket annuleert, voert Kaspersky Endpoint Security de volgende bewerkingen uit:

1. Het kopiëren van bestanden naar het pakket wordt stopgezet en de eventuele actieve encryptie van het pakket wordt beëindigd.

2. Alle tijdelijke bestanden die tijdens het aanmaken en encrypten van het pakket zijn aangemaakt en het bestand van het geëncrypte pakket zelf worden verwijderd.

3. De gebruiker ziet een bericht met de melding dat het aanmaken van het geëncrypte pakket geforceerd beëindigd is.

Geëncrypte pakketten uitpakken

Zo pakt u een geëncrypt pakket uit:

1. Selecteer in een bestandsverkenner een geëncrypt pakket. Klik erop om de wizard Uitpakken te starten.

   Het venster **Wachtwoord invoeren** wordt geopend.

2. Voer het wachtwoord in waarmee het geëncrypte pakket is beveiligd.

3. Klik in het venster **Wachtwoord invoeren** op **OK**.

   Als het juiste wachtwoord is ingevoerd, wordt het standaarddialoogvenster **Bladeren** in Microsoft Windows geopend.

4. Selecteer in het standaarddialoogvenster **Bladeren** in Microsoft Windows de doelmap waarin u het geëncrypte pakket wilt uitpakken en klik op **OK**.

   Het uitpakken van het geëncrypte pakket in de doelmap wordt gestart.

Als het geëncrypte pakket eerder is uitgepakt in de opgegeven doelmap, worden de bestaande bestanden in de map overschreven door de bestanden van het geëncrypte pakket.

Als u het uitpakken van een geëncrypt pakket annuleert, voert Kaspersky Endpoint Security de volgende bewerkingen uit:

1. De decryptie van het pakket wordt gestopt en het kopiëren van bestanden vanuit het geëncrypte pakket wordt beëindigd als dat aan de gang is.

2. Alle tijdelijke bestanden die tijdens het decrypten en uitpakken van het geëncrypte pakket zijn aangemaakt worden verwijderd, alsook alle bestanden die al vanuit het geëncrypte pakket naar de doelmap zijn gekopieerd.

3. De gebruiker ziet een bericht met de melding dat het uitpakken van het geëncrypte pakket geforceerd beëindigd is.

Encryptie van verwisselbare schijven

De encryptie van verwisselbare schijven is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. De encryptie van verwisselbare schijven is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

In deze sectie vindt u informatie over de encryptie van verwisselbare schijven en leest u hoe u de encryptie van verwisselbare schijven kunt configureren en uitvoeren met behulp van Kaspersky Endpoint Security en de beheerplug-in van Kaspersky Endpoint Security.

Encryptie van verwisselbare schijven starten

Zo encrypt u verwisselbare schijven:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de encryptie van verwisselbare schijven wilt configureren.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van verwisselbare schijven**.

7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de standaardactie die Kaspersky Endpoint Security moet uitvoeren op alle verwisselbare schijven die zijn aangesloten op computers in de geselecteerde beheergroep:

   - **Gehele verwisselbare schijf encrypten**. Als deze optie is geselecteerd wanneer het Kaspersky Security Center-beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, wordt de inhoud van verwisselbare schijven sector per sector geëncrypt door Kaspersky Endpoint Security. Hierdoor encrypt het programma niet alleen bestanden op verwisselbare schijven maar ook bestandssystemen van verwisselbare schijven, inclusief de bestandsnamen en de mapstructuren. Kaspersky Endpoint Security encrypt al geëncrypte verwisselbare schijven niet opnieuw.

     Dit encryptiescenario is mogelijk gemaakt door de encryptiefunctionaliteit van Kaspersky Endpoint Security voor harde schijven.

   - **Alle bestanden encrypten**. Als deze optie is geselecteerd wanneer het Kaspersky Security Center-beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, worden alle bestanden op verwisselbare schijven geëncrypt door Kaspersky Endpoint Security. Kaspersky Endpoint Security encrypt al geëncrypte bestanden niet opnieuw. Het programma encrypt geen bestandssystemen van verwisselbare schijven, inclusief de namen van de geëncrypte bestanden en mapstructuren.

   - **Alleen nieuwe bestanden encrypten**. Als deze optie is geselecteerd wanneer het Kaspersky Security Center-beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, worden na de laatste toepassing van het Kaspersky Security Center-beleid alleen de bestanden die zijn toegevoegd aan verwisselbare schijven of die waren opgeslagen op de verwisselbare schijven en zijn gewijzigd geëncrypt door Kaspersky Endpoint Security.

   - **Gehele verwisselbare schijf decrypten**. Als deze optie is geselecteerd wanneer het Kaspersky Security Center-beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, worden alle geëncrypte bestanden op verwisselbare schijven gedecrypt door Kaspersky Endpoint Security evenals de bestandssystemen van de verwisselbare schijven als die eerder waren geëncrypt.

     Dit encryptiescenario is mogelijk gemaakt door de encryptiefunctionaliteit van Kaspersky Endpoint Security voor bestanden en harde schijven.

   - **Ongewijzigd laten**. Als deze optie is geselecteerd wanneer het Kaspersky Security Center-beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, worden bestanden op verwisselbare schijven niet geëncrypt of gedecrypt door Kaspersky Endpoint Security.

8. Maak encryptieregels voor bestanden op verwisselbare schijven waarvan u de inhoud wilt encrypten.

9. Pas het beleid toe.

Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Zodra het beleid is toegepast en de gebruiker een verwisselbare schijf aansluit of als er al een verwisselbare schijf is aangesloten, meldt Kaspersky Endpoint Security de gebruiker dat de verwisselbare schijf onderhevig is aan een encryptieregel waarbij gegevens op de verwisselbare schijf worden geëncrypt.

Als de regel *Ongewijzigd laten* is opgegeven voor de encryptie van gegevens op een verwisselbare schijf, ziet de gebruiker geen meldingen van het programma.

Het programma waarschuwt de gebruiker dat de encryptie enige tijd kan duren.

De gebruiker wordt door het programma gevraagd om de encryptie te bevestigen en het programma voert de volgende acties uit:

- Encrypt de gegevens volgens de beleidsinstellingen als de gebruiker de encryptie bevestigt.
- Encrypt de gegevens niet als de gebruiker de encryptie weigert en beperkt de toegang tot de bestanden op de verwisselbare schijf tot alleen lezen.
- Encrypt de gegevens niet als de gebruiker de vraag over de encryptie negeert, beperkt de toegang tot de bestanden op de verwisselbare schijf tot alleen lezen en vraagt de gebruiker opnieuw om de gegevensencryptie te bevestigen de volgende keer dat het Kaspersky Security Center-beleid wordt toegepast of de volgende keer dat een verwisselbare schijf wordt aangesloten.

Het Kaspersky Security Center-beleid met vooraf geconfigureerde instellingen voor de decryptie van gegevens op verwisselbare schijven is opgesteld voor een specifieke groep van beheerde computers. Daarom hangt het resultaat van de encryptie van gegevens op verwisselbare schijven af van de computer waarop de verwisselbare schijven zijn aangesloten.

Als de gebruiker de veilige verwijdering van een verwisselbare schijf start tijdens de encryptie van de gegevens, onderbreekt Kaspersky Endpoint Security de encryptie van de gegevens en staat het de verwijdering van de verwisselbare schijf toe voordat de encryptie wordt voltooid.

Als de decryptie van een verwisselbare schijf is mislukt, raadpleegt u het rapport **Gegevensencryptie** in de Kaspersky Endpoint Security-interface. De toegang tot bestanden wordt mogelijk geblokkeerd door een ander programma. In dit geval koppelt u de verwisselbare schijf los van de computer en sluit u deze opnieuw aan.

Een encryptieregel voor verwisselbare schijven toevoegen

Zo voegt u een encryptieregel voor verwisselbare schijven toe:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u encryptieregels voor verwisselbare schijven wilt toevoegen.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van verwisselbare schijven**.

7. Klik met de linkermuisknop op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst een van de volgende opties:

   - Als u encryptieregels wilt toevoegen voor verwisselbare schijven die voorkomen in de lijst met vertrouwde apparaten van het onderdeel Apparaatcontrole, selecteert u **Uit lijst met vertrouwde apparaten van dit beleid**.

     Het venster **Apparaten uit lijst met vertrouwde apparaten toevoegen** wordt geopend.

   - Als u encryptieregels wilt toevoegen voor verwisselbare schijven die voorkomen in de lijst van Kaspersky Security Center, selecteert u **Uit Kaspersky Security Center-lijst met apparaten**.

     Het venster **Apparaten uit Kaspersky Security Center-lijst toevoegen** wordt geopend.

8. Als u tijdens de vorige stap **Uit Kaspersky Security Center-lijst met apparaten** hebt geselecteerd, geeft u de filters voor weergave van apparaten in de tabel op. Hiertoe doet u het volgende:

   a. Geef de waar van de volgende parameters op: **Geef apparaten in de tabel weer waarvoor het volgende is gedefinieerd**, **Apparaattype**, **Naam**, **Computer** en **Kaspersky Disk Encryption**.

   b. Klik op de knop **Vernieuwen**.

9. Schakel in de kolom **Apparaattype** de selectievakjes naast de namen van verwisselbare schijven in waarvoor u encryptieregels wilt aanmaken.

10. Selecteer in de vervolgkeuzelijst **Encryptiemodus voor geselecteerde apparaten** de actie die Kaspersky Endpoint Security moet uitvoeren op de bestanden die op de geselecteerde verwisselbare schijven zijn opgeslagen.

11. Schakel het selectievakje **Portable modus** in als u wilt dat Kaspersky Endpoint Security verwisselbare schijven voorbereidt vóór de encryptie, waardoor het mogelijk is om opgeslagen bestanden op die schijven te gebruiken in de portable modus.

    Met de portable modus kunt u geëncrypte bestanden gebruiken die zijn opgeslagen op verwisselbare schijven die zijn aangesloten op computers zonder encryptiefunctionaliteit.

12. Schakel het selectievakje **Alleen gebruikte schijfruimte encrypten** in als u wilt dat Kaspersky Endpoint Security alleen schijfsectoren met bestanden encrypt.

    Als u een encryptie toepast op een schijf die al wordt gebruikt, wordt u aanbevolen de gehele schijf te encrypten. Dit verzekert dat alle gegevens zijn beschermd, zelfs verwijderde gegevens die mogelijk nog ophaalbare informatie bevatten. De functie **Alleen gebruikte schijfruimte encrypten** wordt aanbevolen voor nieuwe schijven die nog niet eerder zijn gebruikt.

    Als een apparaat eerder is geëncrypt met de functie **Alleen gebruikte schijfruimte encrypten**, worden sectoren met bestanden na de toepassing van een beleid in de modus **Gehele verwisselbare schijf encrypten** nog steeds niet geëncrypt.

13. Selecteer in de vervolgkeuzelijst **Acties voor apparaten die eerder zijn geselecteerd** de actie die Kaspersky Endpoint Security moet uitvoeren volgens de encryptieregels die eerder waren ingesteld voor verwisselbare

schijven:

- Als u wilt dat de eerder aangemaakte encryptieregel voor de verwisselbare schijf ongewijzigd blijft, selecteert u **Overslaan**.
- Als u wilt dat een eerder aangemaakte encryptieregel voor een verwisselbare schijf wordt vervangen door de nieuwe regel, selecteert u **Update**.

14. Klik op **OK**.

    In de tabel **Aangepaste regels** verschijnen regels met de parameters van de aangemaakte encryptieregels.

15. Klik op **OK** om de wijzigingen op te slaan.

De toegevoegde encryptieregels voor verwisselbare schijven worden toegepast op verwisselbare schijven die zijn aangesloten op computers die door het aangepaste beleid van Kaspersky Security Center worden beheerd.

Een encryptieregel voor verwisselbare schijven bewerken

Zo bewerkt u een encryptieregel voor een verwisselbare schijf:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een encryptieregel voor een verwisselbare schijf wilt bewerken.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van verwisselbare schijven**.
7. Selecteer in de lijst met verwisselbare schijven waarvoor encryptieregels zijn geconfigureerd een item dat overeenkomt met de gewenste verwisselbare schijf.
8. Klik op de knop **Een regel instellen** om de encryptieregel voor de geselecteerde verwisselbare schijf te bewerken.

   Het contextmenu van de knop **Een regel instellen** wordt geopend.
9. Selecteer in het contextmenu van de knop **Een regel instellen** de actie die Kaspersky Endpoint Security moet uitvoeren op bestanden die op de geselecteerde verwisselbare schijf zijn opgeslagen.
10. Klik op **OK** om de wijzigingen op te slaan.

De gewijzigde encryptieregels voor verwisselbare schijven worden toegepast op verwisselbare schijven die zijn aangesloten op computers die door het aangepaste beleid van Kaspersky Security Center worden beheerd.

Portable modus voor toegang tot geëncrypte bestanden op verwisselbare schijven inschakelen

Zo schakelt u de portable modus voor toegang tot geëncrypte bestanden op verwisselbare schijven in:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de portable modus voor de toegang tot geëncrypte bestanden op verwisselbare schijven wilt inschakelen.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van verwisselbare schijven**.
7. Schakel het selectievakje **Portable modus** in.

   De portable modus is alleen beschikbaar voor de encryptie van alle bestanden of nieuwe bestanden.

8. Klik op **OK**.
9. Pas het beleid toe.

   Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.
10. Sluit de verwisselbare schijf aan op een apparaat waarop het Kaspersky Security Center-beleid is toegepast.
11. Bevestig de encryptie van de verwisselbare schijf.

    U ziet nu een venster waarin u een wachtwoord voor Portable bestandsbeheer kunt aanmaken.
12. Geef een wachtwoord op dat sterk genoeg is en bevestig het.
13. Klik op **OK**.

    Kaspersky Endpoint Security encrypt de bestanden op een verwisselbare schijf volgens de gedefinieerde encryptieregels in het Kaspersky Security Center-beleid. Het programma Portable bestandsbeheer (voor het werken met geëncrypte bestanden) wordt ook naar de verwisselbare schijf geschreven.

Na de inschakeling van de portable modus hebt u toegang tot geëncrypte bestanden op verwisselbare schijven die zijn aangesloten op een computer zonder encryptiefunctionaliteit.

Decryptie van verwisselbare schijven

Zo decrypt u verwisselbare schijven:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de decryptie van verwisselbare schijven wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van verwisselbare schijven**.
7. Als u alle geëncrypte bestanden op verwisselbare schijven wilt decrypten, selecteert u in de vervolgkeuzelijst **Encryptiemodus** de optie **Gehele verwisselbare schijf decrypten**.
8. Om gegevens op individuele verwisselbare schijven te decrypten, bewerkt u de encryptieregels voor de verwisselbare schijven waarvan u de gegevens wilt decrypten. Hiertoe doet u het volgende:
   a. Selecteer in de lijst met verwisselbare schijven waarvoor encryptieregels zijn geconfigureerd een item dat overeenkomt met de gewenste verwisselbare schijf.
   b. Klik op de knop **Een regel instellen** om de encryptieregel voor de geselecteerde verwisselbare schijf te bewerken.

      Het contextmenu van de knop **Een regel instellen** wordt geopend.
   c. Selecteer de optie **Alle bestanden decrypten** in het contextmenu van de knop **Een regel instellen**.
9. Klik op **OK** om de wijzigingen op te slaan.
10. Pas het beleid toe.

Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Nadat het beleid is toegepast en de gebruiker een verwisselbare schijf aansluit of er is al een verwisselbare schijf aangesloten, meldt Kaspersky Endpoint Security de gebruiker dat de verwisselbare schijf onderhevig is aan een encryptieregel waarbij geëncrypte bestanden op de verwisselbare schijf alsook het bestandssysteem van de verwisselbare schijf (als die is geëncrypt) worden gedecrypt. Het programma waarschuwt de gebruiker dat de decryptie enige tijd kan duren.

Het Kaspersky Security Center-beleid met vooraf geconfigureerde instellingen voor de decryptie van gegevens op verwisselbare schijven is opgesteld voor een specifieke groep van beheerde computers. Daarom hangt het resultaat van de decryptie van gegevens op verwisselbare schijven af van de computer waarop de verwisselbare schijven zijn aangesloten.

Als de gebruiker de veilige verwijdering van een verwisselbare schijf start tijdens de decryptie van de gegevens, onderbreekt Kaspersky Endpoint Security de decryptie van de gegevens en staat het de verwijdering van de verwisselbare schijf toe voordat de decryptie wordt voltooid.

Als de decryptie van een verwisselbare schijf is mislukt, raadpleegt u het rapport **Gegevensencryptie** in de Kaspersky Endpoint Security-interface. De toegang tot bestanden wordt mogelijk geblokkeerd door een ander programma. In dit geval koppelt u de verwisselbare schijf los van de computer en sluit u deze opnieuw aan.

Encryptie van harde schijven

Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations, kunnen BitLocker-stationsversleuteling en Kaspersky Disk Encryption worden gebruikt voor encrypties. Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers, is alleen BitLocker-stationsversleuteling beschikbaar.

In deze sectie vindt u informatie over de encryptie van harde schijven en leest u hoe u de encryptie van harde schijven kunt configureren en uitvoeren met behulp van Kaspersky Endpoint Security en de plug-in van Kaspersky Endpoint Security-console.

Over de encryptie van harde schijven

Voordat het programma de encryptie van een harde schijf begint, voert het een aantal controles uit om te bepalen of het apparaat kan worden geëncrypt. Het programma controleert bijvoorbeeld of de harde schijf van het systeem compatibel is met Verificatie-agent en de BitLocker-encryptieonderdelen. Om de compatibiliteit te controleren, moet de computer opnieuw worden opgestart. Wanneer de computer opnieuw is opgestart, voert het programma alle noodzakelijke controles automatisch uit. Als de compatibiliteitscontrole met succes is voltooid, begint de encryptie van de harde schijf nadat het besturingssysteem is opgestart en het programma is gestart. Als de harde schijf van het systeem niet compatibel is met Verificatie-agent of de BitLocker-encryptieonderdelen, moet de computer opnieuw worden opgestart door op de hardwareknop Reset te drukken. Kaspersky Endpoint Security registreert informatie over de incompatibiliteit. Op basis van deze informatie start het programma de encryptie van harde schijven niet bij de opstart van het besturingssysteem. Informatie over deze gebeurtenis wordt in rapporten van Kaspersky Security Center geregistreerd.

Als de hardwareconfiguratie van de computer is gewijzigd, moet de informatie over de incompatibiliteit die tijdens de vorige controle is geregistreerd worden verwijderd om te controleren of de harde schijf van het systeem compatibel is met Verificatie-agent en de BitLocker-encryptieonderdelen. Hiertoe typt u vóór de encryptie van de harde schijven `avp pbatestreset` op de opdrachtregel. Als het besturingssysteem niet wordt geladen nadat de harde schijf van het systeem is gecontroleerd op compatibiliteit met Verificatie-agent, moet u de resterende objecten en gegevens na de test van Verificatie-agent verwijderen met behulp van de Herstelvoorziening. Daarna start u Kaspersky Endpoint Security en voert u de opdracht `avp pbatestreset` opnieuw uit.

Wanneer de encryptie van harde schijven is gestart, encrypt Kaspersky Endpoint Security alle gegevens die naar harde schijven worden geschreven.

Als de gebruiker de computer uitschakelt of opnieuw opstart tijdens de decryptie van de harde schijven, wordt Verificatie-agent vóór de volgende opstart van het besturingssysteem geladen. Kaspersky Endpoint Security hervat de encryptie van de harde schijven na de geslaagde verificatie in Verificatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de sluimerstand gaat tijdens de encryptie van de harde schijven, wordt Verificatie-agent geladen wanneer het besturingssysteem uit de sluimerstand wordt gehaald. Kaspersky Endpoint Security hervat de encryptie van de harde schijven na de geslaagde verificatie in Verificatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de slaapstand gaat tijdens de encryptie van de harde schijven, hervat Kaspersky Endpoint Security de encryptie van de harde schijven wanneer het besturingssysteem uit de slaapstand wordt gehaald zonder de Verificatie-agent te laden.

De gebruikersverificatie in Verificatie-agent kan op twee manieren worden uitgevoerd:

- Typ de naam en het wachtwoord van het account in Verificatie-agent dat door de netwerkbeheerder is aangemaakt met Kaspersky Security Center-tools.
- Typ het wachtwoord van een token of een smartcard die op de computer is aangesloten.

Verificatie-agent ondersteunt toetsenbordindelingen voor de volgende talen:

- Engels (VK)
- Engels (VS)
- Arabisch (Algerije, Marokko, Tunesië; AZERTY-indeling)
- Spaans (Latijns-Amerika)
- Italiaans
- Duits (Duitsland en Oostenrijk)
- Duits (Zwitserland)
- Portugees (Brazilië, ABNT2-indeling)
- Russisch (voor IBM- / Windows-toetsenborden met 105 toetsen en QWERTY-indeling)
- Turks (QWERTY-indeling)
- Frans (Frankrijk)
- Frans (Zwitserland)
- Frans (België, AZERTY-indeling)
- Japans (voor toetsenborden met 106 toetsen en de QWERTY-indeling)

Een toetsenbordindeling wordt beschikbaar in Verificatie-agent als deze indeling is toegevoegd in de taal- en regio-instellingen van het besturingssysteem en beschikbaar is in het welkomstscherm van Microsoft Windows.

Als de naam van het account in Verificatie-agent tekens bevat die niet met de beschikbare toetsenbordindelingen van Verificatie-agent kunnen worden ingevoerd, hebt u pas toegang tot geëncrypte harde schijven nadat ze zijn hersteld met de Herstelvoorziening of nadat de accountnaam en het wachtwoord voor Verificatie-agent zijn hersteld.

Kaspersky Endpoint Security ondersteunt de volgende tokens, smartcardlezers en smartcards:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smartcard)
- SafeNet eToken 4100 72K Java (Smartcard)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smartcard)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Encryptie van harde schijven met Kaspersky Disk Encryption-technologie

Alvorens harde schijven op een computer te encrypten raden we aan dat u controleert of de computer niet geïnfecteerd is. U kunt dit doen door een Volledige Scan of Kritieke Gebiedenscan te starten. De encryptie van een harde schijf van de computer die met een rootkit is geïnfecteerd kan ertoe leiden dat u die niet meer kunt gebruiken.

Zo encrypt u harde schijven met Kaspersky Disk Encryption-technologie:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de encryptie van harde schijven wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

- Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
- Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van harde schijven**.
7. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **Kaspersky Disk Encryption**.

   Kaspersky Disk Encryption-technologie kan niet worden gebruikt als de computer harde schijven heeft die met BitLocker zijn geëncrypt.

8. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven encrypten**.

   Als u wilt instellen dat enkele harde schijven niet moeten worden geëncrypt, maakt u een lijst met die harde schijven aan.

9. Selecteer één van de volgende encryptiemethoden:
   - Als u alleen schijfsectoren met bestanden wilt encrypten, schakelt u het selectievakje **Alleen gebruikte schijfruimte encrypten** in.

     Als u een encryptie toepast op een schijf die al wordt gebruikt, wordt u aanbevolen de gehele schijf te encrypten. Dit verzekert dat alle gegevens zijn beschermd, zelfs verwijderde gegevens die mogelijk nog ophaalbare informatie bevatten. De functie **Alleen gebruikte schijfruimte encrypten** wordt aanbevolen voor nieuwe schijven die nog niet eerder zijn gebruikt.
   - Als u de gehele harde schijf wilt encrypten, schakelt u het selectievakje **Alleen gebruikte schijfruimte encrypten** uit.

     Deze functie is alleen van toepassing op apparaten die niet zijn geëncrypt. Als een apparaat eerder is geëncrypt met de functie **Alleen gebruikte schijfruimte encrypten**, worden sectoren met bestanden na de toepassing van een beleid in de modus **Alle harde schijven encrypten** nog steeds niet geëncrypt.

10. Klik op **OK** om de wijzigingen op te slaan.
11. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Harde schijven encrypten met de technologie van BitLocker-stationsversleuteling

Alvorens harde schijven op een computer te encrypten raden we aan dat u controleert of de computer niet geïnfecteerd is. U kunt dit doen door een Volledige Scan of Kritieke Gebiedenscan te starten. De encryptie van een harde schijf van de computer die met een rootkit is geïnfecteerd kan ertoe leiden dat u die niet meer kunt gebruiken.

Het gebruik van de technologie BitLocker-stationsversleuteling op computers met een serverbesturingssysteem vereist mogelijk de installatie van het onderdeel **BitLocker-stationsversleuteling** via de wizard 'Functies en onderdelen toevoegen'.

Zo encrypt u harde schijven met BitLocker-stationsversleuteling:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de encryptie van harde schijven wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van harde schijven**.
7. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **BitLocker-stationsversleuteling**.
8. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven encrypten**.
9. Als u een schermtoetsenbord wilt gebruiken om informatie in een preboot-omgeving in te voeren, schakelt u het selectievakje **Verificatie met toetsenbordinvoer vóór opstart toestaan op tablets** in.

   U wordt aanbevolen deze instelling alleen te gebruiken voor apparaten die beschikken over alternatieve middelen voor gegevensinvoer, zoals een USB-toetsenbord in een preboot-omgeving.

10. Selecteer één van de volgende soorten encryptie:
    - Schakel het selectievakje **Hardware-encryptie gebruiken** in als u hardware-encryptie wilt gebruiken.
    - Schakel het selectievakje **Hardware-encryptie gebruiken** uit als u software-encryptie wilt gebruiken.
11. Selecteer één van de volgende encryptiemethoden:
    - Als u alleen schijfsectoren met bestanden wilt encrypten, schakelt u het selectievakje **Alleen gebruikte schijfruimte encrypten** in.
    - Als u de gehele harde schijf wilt encrypten, schakelt u het selectievakje **Alleen gebruikte schijfruimte encrypten** uit.

      Deze functie is alleen van toepassing op apparaten die niet zijn geëncrypt. Als een apparaat eerder is geëncrypt met de functie **Alleen gebruikte schijfruimte encrypten**, worden sectoren met bestanden na de toepassing van een beleid in de modus **Alle harde schijven encrypten** nog steeds niet geëncrypt.

12. Selecteer een methode voor de toegang tot harde schijven die met BitLocker zijn geëncrypt.

- Als u een Trusted Platform Module (TPM) wilt gebruiken om encryptiesleutels te bewaren, selecteert u de optie **Trusted Platform Module (TPM) gebruiken**.

- Als u geen Trusted Platform Module (TPM) voor de encryptie van harde schijven gebruikt, selecteert u de optie **Wachtwoord gebruiken** en geeft u in het veld **Minimale lengte van wachtwoord** op hoeveel tekens een wachtwoord minimaal moet hebben.

De beschikbaarheid van een Trusted Platform Module (TPM) is verplicht bij Windows 7 en Windows 2008 R2, alsook voor oudere systemen.

13. Als u tijdens de vorige stap de optie **Trusted Platform Module (TPM) gebruiken** hebt geselecteerd:

    - Als u een pincode wilt instellen die wordt gevraagd wanneer de gebruiker probeert om toegang tot een encryptiesleutel te krijgen, schakelt u het selectievakje **Pincode gebruiken** in en geeft u in het veld **Minimale lengte van pincode** op hoeveel cijfers een pincode minimaal moet hebben.

    - Als u met een wachtwoord toegang wilt krijgen tot geëncrypte harde schijven zonder een Trusted Platform Module op de computer, schakelt u het selectievakje **Wachtwoord gebruiken als Trusted Platform Module (TPM) niet beschikbaar is** in en geeft u in het veld **Minimale lengte van wachtwoord** op hoeveel tekens het wachtwoord minimaal moet bevatten.

      In dit geval hebt u met het opgegeven wachtwoord toegang tot de encryptiesleutels net alsof het selectievakje **Wachtwoord gebruiken** is ingeschakeld.

      Als het selectievakje **Wachtwoord gebruiken als Trusted Platform Module (TPM) niet beschikbaar is** is uitgeschakeld en geen Trusted Platform Module beschikbaar is, wordt de encryptie van de harde schijf niet gestart.

14. Klik op **OK** om de wijzigingen op te slaan.

15. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Na de toepassing van het beleid op de clientcomputer waarop Kaspersky Endpoint Security is geïnstalleerd, gebeurt het volgende:

- Als het encryptiebeleid is toegepast op de systeemschijf, wordt het venster voor de pincode weergegeven wanneer de Trusted Platform Module wordt gebruikt. In het andere geval verschijnt het venster waarin het wachtwoord wordt gevraagd voor de autorisatie vóór het laden.

- Als de modus voor compatibiliteit met FIPS (Federal Information Processing Standard) is ingeschakeld in het besturingssysteem van de computer, ziet de gebruiker in Windows 8 en hoger een venster voor het aansluiten van een USB-apparaat om het bestand met de herstelsleutel op te slaan.

Als er geen toegang tot encryptiesleutels is, kan de gebruiker een herstelsleutel vragen aan de netwerkbeheerder (in het geval dat de herstelsleutel niet eerder is opgeslagen op het USB-apparaat of verloren is gegaan).

Een lijst met harde schijven maken die niet moeten worden geëncrypt

U kunt een exclusieve lijst met encryptie-uitzonderingen maken voor de Kaspersky Disk Encryption-technologie.

Zo maakt u een lijst met harde schijven die niet moeten worden geëncrypt:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een lijst met harde schijven die niet moeten worden geëncrypt wilt aanmaken.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van harde schijven**.
7. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **Kaspersky Disk Encryption**.

   De items die overeenkomen met harde schijven die niet moeten worden geëncrypt worden in de tabel **Encrypt de volgende harde schijven niet** weergegeven. Deze tabel is leeg als u eerder geen lijst met harde schijven die niet moeten worden geëncrypt hebt gemaakt.
8. Zo voegt u harde schijven toe aan de lijst met harde schijven die niet moeten worden geëncrypt:
   a. Klik op de knop **Toevoegen**.

      Het venster **Apparaten uit Kaspersky Security Center-lijst toevoegen** wordt geopend.
   b. Geef in het venster **Apparaten uit Kaspersky Security Center-lijst toevoegen** de waarden voor de volgende parameters op: **Naam**, **Computer**, **Schijftype** en **Kaspersky Disk Encryption**.
   c. Klik op de knop **Vernieuwen**.
   d. Schakel in de kolom **Naam** de selectievakjes in de rijen met de namen van de harde schijven in die u wilt toevoegen aan de lijst met harde schijven die niet moeten worden geëncrypt.
   e. Klik op **OK**.

   De geselecteerde harde schijven worden in de tabel **Encrypt de volgende harde schijven niet** weergegeven.
9. Als u de harde schijven wilt verwijderen uit de tabel met uitzonderingen, selecteert u een of verschillende items in de tabel **Encrypt de volgende harde schijven niet** en klikt u op de knop **Verwijderen**.

   Om meerdere items in de tabel te selecteren, selecteert u ze terwijl u de **CTRL**-toets ingedrukt houdt.
10. Klik op **OK** om de wijzigingen op te slaan.

Decryptie van harde schijven

U kunt harde schijven decrypten zelfs als er geen actieve licentie is die gegevensencryptie toestaat.

Zo decrypt u harde schijven:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de decryptie van harde schijven wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Encryptie van harde schijven**.
7. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de technologie waarmee de harde schijven zijn geëncrypt.
8. Voer een van de volgende acties uit:
   - Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven decrypten** als u alle geëncrypte harde schijven wilt decrypten.
   - Voeg de geëncrypte harde schijven die u wilt decrypten toe aan de tabel **Encrypt de volgende harde schijven niet**.

     Deze optie is alleen beschikbaar voor Kaspersky Disk Encryption-technologie.
9. Klik op **OK** om de wijzigingen op te slaan.
10. Pas het beleid toe.

    Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Als de gebruiker de computer uitschakelt of opnieuw opstart tijdens de decryptie van harde schijven die zijn geëncrypt met de technologie Kaspersky Disk Encryption, wordt Verificatie-agent vóór de volgende opstart van het besturingssysteem geladen. Kaspersky Endpoint Security hervat de decryptie van de harde schijf na de geslaagde verificatie in Verificatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de sluimerstand gaat wanneer harde schijven worden gedecrypt die werden geëncrypt met de technologie Kaspersky Disk Encryption, wordt Verificatie-agent geladen wanneer het besturingssysteem uit de sluimerstand wordt gehaald. Kaspersky Endpoint Security hervat de decryptie van de harde schijf na de geslaagde verificatie in Verificatie-agent en de opstart van het besturingssysteem. Na de decryptie van de harde schijven is de sluimerstand pas beschikbaar wanneer het besturingssysteem opnieuw wordt opgestart.

Als het besturingssysteem in de slaapstand gaat tijdens de decryptie van de harde schijf, hervat Kaspersky Endpoint Security de decryptie van de harde schijf wanneer het besturingssysteem uit de slaapstand wordt gehaald zonder de Verificatie-agent te laden.

Verificatie-agent beheren

Als de harde schijven van het systeem zijn geëncrypt, wordt Verificatie-agent geladen vóór de opstart van het besturingssysteem. Gebruik Verificatie-agent voor de verificatie van uw identiteit om toegang tot geëncrypte harde schijven van het systeem te krijgen en het besturingssysteem te laden.

Na de geslaagde voltooiing van de verificatie wordt het besturingssysteem geladen. Het verificatieproces wordt herhaald telkens als het besturingssysteem opnieuw wordt gestart.

In bepaalde gevallen kan de verificatie van de identiteit van de gebruiker mislukken. Een verificatie is bijvoorbeeld niet mogelijk als de gebruiker de accountgegevens voor Verificatie-agent vergeten is, als de gebruiker het wachtwoord voor een token of een smartcard vergeten is of als de gebruiker de token of de smartcard kwijt is.

Als de gebruiker de accountgegevens voor Verificatie-agent of het wachtwoord van een token of smartcard is vergeten, moet u contact opnemen met de netwerkbeheerder van het bedrijf om ze recupereren.

Als een gebruiker een token of smartcard heeft verloren, moet de beheerder het bestand van een elektronisch token- of smartcardcertificaat toevoegen aan de opdracht voor het aanmaken van een account voor Verificatie-agent. Vervolgens moet de gebruiker de procedure voor het herstellen van gegevens op geëncrypte apparaten voltooien.

Een token en een smartcard met Verificatie-agent gebruiken

Een token of een smartcard kan voor de verificatie tijdens de toegang tot geëncrypte harde schijven worden gebruikt. Hiertoe moet u het bestand van een elektronisch token- of smartcardcertificaat toevoegen aan de opdracht voor het maken van een account in Verificatie-agent.

Het gebruik van een token of een smartcard is alleen beschikbaar als de harde schijven van de computer zijn geëncrypt met het AES256-encryptiealgoritme. Als de harde schijven van de computer zijn geëncrypt met het AES56-encryptiealgoritme, wordt het toevoegen van het elektronisch-certificaatbestand aan de opdracht geweigerd.

Om een elektronisch token- of smartcardcertificaat toe te voegen aan de opdracht voor het maken van een account in Verificatie-agent, moet u het bestand eerst opslaan met software van andere leveranciers voor het beheer van certificaten.

Het token- of smartcardcertificaat moet de volgende eigenschappen hebben:

- Het certificaat moet voldoen aan de X.509-standaard en het certificaatbestand moet een DER-codering hebben.

Als het elektronische certificaat van de token of de smartcard niet aan deze vereiste voldoet, laadt de beheerplug-in het bestand van dit certificaat niet in de opdracht voor het maken van een account in Verificatie-agent en wordt een foutbericht weergegeven.

- De parameter `KeyUsage` die het doel van het certificaat definieert moet de waarde `keyEncipherment` of `dataEncipherment` hebben.

  Als het elektronische certificaat van de token of de smartcard niet aan deze vereiste voldoet, laadt de beheerplug-in het bestand van dit certificaat in de opdracht voor het maken van een account in Verificatie-agent en wordt een waarschuwingsbericht weergegeven.

- Het certificaat bevat een RSA-sleutel met een minimale lengte van 1024 bits.

  Als het elektronische certificaat van de token of de smartcard niet aan deze vereiste voldoet, laadt de beheerplug-in het bestand van dit certificaat niet in de opdracht voor het maken van een account in Verificatie-agent en wordt een foutbericht weergegeven.

Help-berichten van Verificatie-agent bewerken

Alvorens Help-berichten van Verificatie-agent te bewerken, moet u de lijst met ondersteunde tekens in een preboot-omgeving bekijken.

Zo bewerkt u Help-berichten van Verificatie-agent:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u Help-berichten van Verificatie-agent wilt bewerken.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Algemene encryptie-instellingen**.
7. Klik in het gedeelte **Sjablonen** op de knop **Help**.

   Zo opent u het venster **Help-berichten van Verificatie-agent**.
8. Doe het volgende:
   - Selecteer het tabblad **Verificatie** voor de bewerking van de weergegeven Help-tekst in het venster van Verificatie-agent tijdens de invoer van de accountgegevens.
   - Selecteer het tabblad **Wachtwoord wijzigen** voor de bewerking van de weergegeven Help-tekst in het venster van Verificatie-agent wanneer het wachtwoord van het account in Verificatie-agent wordt gewijzigd.

- Selecteer het tabblad **Wachtwoord herstellen** voor de bewerking van de weergegeven Help-tekst in het venster van Verificatie-agent wanneer het wachtwoord van het account in Verificatie-agent wordt hersteld.

9. Bewerk de Help-berichten.

   Als u de originele tekst wilt herstellen, klikt u op de knop **Standaard**.

10. Klik op **OK**.

11. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

Beperkte ondersteuning voor tekens in Help-berichten van Verificatie-agent

In een preboot-omgeving worden de volgende unicode-tekens ondersteund:

- Latijn (Basis) (0000 - 007F)
- Latijn-1 - Toevoeging (0080 - 00FF)
- Latijn - Uitgebreid-A (0100 - 017F)
- Latijn - Uitgebreid-B (0180 - 024F)
- Niet-gecombineerde uitgebreide ID-tekens (02B0 - 02FF)
- Gecombineerde diakritische tekens (0300 - 036F)
- Grieks en Koptisch (0370 - 03FF)
- Cyrillisch (0400 - 04FF)
- Hebreeuws (0590 - 05FF)
- Arabisch (0600 - 06FF)
- Latijn Uitgebreid - Toevoeging (1E00 - 1EFF)
- Leestekens (2000 - 206F)
- Munteenheidsymbolen (20A0 - 20CF)
- Letterachtige symbolen (2100 - 214F)
- Geometrische figuren (25A0 - 25FF)
- Presentatievormen van Arabisch schrift-B (FE70 - FEFF)

Tekens die niet in deze lijst voorkomen worden niet in een preboot-omgeving ondersteund. U wordt afgeraden zulke tekens in Help-berichten van Verificatie-agent te gebruiken.

Het traceniveau voor Verificatie-agent selecteren

Het programma registreert in het tracebestand service-informatie over de werking van Verificatie-agent en informatie over de bewerkingen van de gebruiker met Verificatie-agent. Het tracebestand van Verificatie-agent kan zeer nuttig zijn wanneer u gegevens op geëncrypte harde schijven moet herstellen.

Zo selecteert u het traceniveau voor Verificatie-agent:

1. Zodra een computer met geëncrypte harde schijven wordt opgestart, drukt u op de **F3**-knop om een venster voor de configuratie van de instellingen van Verificatie-agent aan te roepen.

2. Selecteer het traceniveau in het venster met de instellingen van Verificatie-agent:

   - **Registratie voor foutopsporing uitschakelen (standaard)**. Als deze optie is geselecteerd, registreert het programma in het tracebestand geen informatie over gebeurtenissen van Verificatie-agent.

   - **Registratie voor foutopsporing inschakelen**. Als deze optie is geselecteerd, registreert het programma in het tracebestand informatie over de werking van Verificatie-agent en de bewerkingen die de gebruiker met Verificatie-agent heeft uitgevoerd.

   - **Uitgebreide registratie inschakelen**. Als deze optie is geselecteerd, registreert het programma in het tracebestand gedetailleerde informatie over de werking van Verificatie-agent en de bewerkingen die de gebruiker met Verificatie-agent heeft uitgevoerd.

     Met deze optie worden meer details geregistreerd in vergelijking met de optie **Registratie voor foutopsporing inschakelen**. De registratie van meer details kan de opstart van Verificatie-agent en het besturingssysteem vertragen.

   - **Registratie voor foutopsporing inschakelen en seriële poort selecteren**. Als deze optie is geselecteerd, registreert het programma in het tracebestand informatie over de werking van Verificatie-agent en de bewerkingen die de gebruiker met Verificatie-agent heeft uitgevoerd en stuurt het die informatie via de COM-poort door.

     Als een computer met geëncrypte harde schijven via de COM-poort is verbonden met een andere computer, kunnen gebeurtenissen van Verificatie-agent vanaf de andere computer worden onderzocht.

   - **Uitgebreide registratie voor foutopsporing inschakelen en seriële poort selecteren**. Als deze optie is geselecteerd, registreert het programma in het tracebestand gedetailleerde informatie over de werking van Verificatie-agent en de bewerkingen die de gebruiker met Verificatie-agent heeft uitgevoerd en stuurt het die informatie via de COM-poort door.

     Met deze optie worden meer details geregistreerd in vergelijking met de optie **Registratie voor foutopsporing inschakelen en seriële poort selecteren**. De registratie van meer details kan de opstart van Verificatie-agent en het besturingssysteem vertragen.

De gegevens worden in het tracebestand van Verificatie-agent geregistreerd als de computer geëncrypte harde schijven heeft of tijdens de encryptie van harde schijven.

Het tracebestand van Verificatie-agent wordt niet naar Kaspersky verstuurd, in tegenstelling tot andere tracebestanden van het programma. De systeembeheerder kan indien nodig het tracebestand van Verificatie-agent handmatig versturen naar Kaspersky voor analyse.

Accounts in Verificatie-agent beheren

De volgende tools van Kaspersky Security Center kunt u gebruiken voor het beheer van accounts in Verificatie-agent:

- Groepstaak voor het beheer van accounts in Verificatie-agent. Met deze taak kunt u accounts in Verificatie-agent beheren voor een groep clientcomputers.
- De lokale taak **Encryptie (accountbeheer)**. Met deze taak kunt u accounts in Verificatie-agent beheren voor individuele clientcomputers.

Zo configureert u de instellingen van de taak voor het beheer van accounts in Verificatie-agent:

1. Maak (Een lokale taak aanmaken, Een groepstaak aanmaken) een taak voor het beheer van accounts voor Verificatie-agent aan.
2. Open het gedeelte **Instellingen** in het venster **Eigenschappen: <naam van taak voor beheer van account in Verificatie-agent>**.
3. Voeg opdrachten voor het aanmaken van accounts in Verificatie-agent toe.
4. Voeg opdrachten voor het bewerken van accounts in Verificatie-agent toe.
5. Voeg opdrachten voor het verwijderen van gebruikersaccounts in Verificatie-agent toe.
6. Bewerk indien nodig de toegevoegde opdrachten voor het beheer van accounts in Verificatie-agent. Selecteer hiervoor een opdracht in de tabel **Opdrachten voor beheer van accounts in Verificatie-agent** en klik op de knop **Bewerken**.
7. Verwijder indien nodig de toegevoegde opdrachten voor het beheer van accounts in Verificatie-agent. Selecteer hiervoor een of meer opdrachten in de tabel **Opdrachten voor beheer van accounts in Verificatie-agent:** en klik op de knop **Verwijderen**.

   Om meerdere items in de tabel te selecteren, selecteert u ze terwijl u de **CTRL**-toets ingedrukt houdt.

8. Klik op **OK** in het venster met de taakeigenschappen om de wijzigingen op te slaan.
9. Start de taak.

De aan de taak toegevoegde opdrachten voor het beheer van accounts in Verificatie-agent worden uitgevoerd.

Een opdracht voor het aanmaken van een account in Verificatie-agent toevoegen

Zo voegt u een opdracht voor het aanmaken van een account in Verificatie-agent toe:

1. Open het gedeelte **Instellingen** in het venster **Eigenschappen: <naam van taak voor beheer van account in Verificatie-agent>**.

2. Klik op de knop **Toevoegen** en selecteer in de vervolgkeuzelijst de optie **Opdracht voor toevoegen van account**.

   Het venster **Gebruikersaccount toevoegen** wordt geopend.

3. Geef in het veld **Gebruikersaccount toevoegen** in het venster **Windows-account** de Microsoft Windows-accountnaam op die als basis zal worden gebruikt voor het aanmaken van het account voor Verificatie-agent.

   Voer hiervoor de accountnaam handmatig in of klik op de knop **Selecteren**.

4. Als u de naam van een Microsoft Windows-account handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om het beveiligings-ID (SID) van het account te bepalen.

   Als u ervoor kiest om het beveiligings-ID (SID) niet te laten bepalen door op de knop **Toestaan** te klikken, wordt het ID bepaald wanneer de taak op de computer wordt uitgevoerd.

   > De bepaling van het SID van het Microsoft Windows-account tijdens het toevoegen van een opdracht voor het aanmaken van een account in Verificatie-agent is een handige manier om ervoor te zorgen dat de handmatig ingevoerde Microsoft Windows-accountnaam correct is. Als het ingevoerde Microsoft Windows-gebruikersaccount niet bestaat, aan een niet-vertrouwd domein toebehoort of niet op de computer staat waarvoor de lokale taak **Encryptie (accountbeheer)** wordt gewijzigd, eindigt de taak voor het beheer van accounts in Verificatie-agent met een fout.

5. Schakel het selectievakje **Huidig gebruikersaccount wijzigen** in om een eerder gemaakt account met dezelfde naam in Verificatie-agent te vervangen door het nieuwe account.

   > Deze stap is beschikbaar als u een opdracht voor het aanmaken van een account in Verificatie-agent toevoegt aan de eigenschappen van een groepstaak voor het beheer van accounts in Verificatie-agent. Deze stap is niet beschikbaar als u een opdracht voor het aanmaken van een account in Verificatie-agent toevoegt aan de eigenschappen van de lokale taak **Encryptie (accountbeheer)**.

6. Typ in het veld **Gebruikersnaam** de naam van het account voor Verificatie-agent dat tijdens de verificatie voor de toegang tot geëncrypte harde schijven moet worden ingevoerd.

7. Schakel het selectievakje **Verificatie met wachtwoord toestaan** in als u wilt dat het programma de gebruiker vraagt om het wachtwoord voor het account van Verificatie-agent in te voeren tijdens de verificatie voor de toegang tot geëncrypte harde schijven.

8. Als u tijdens de vorige stap het selectievakje **Verificatie met wachtwoord toestaan** hebt ingeschakeld:

   a. Typ in het veld **Wachtwoord** het wachtwoord van het account voor Verificatie-agent dat tijdens de verificatie voor de toegang tot geëncrypte harde schijven moet worden ingevoerd.

   b. Bevestig in het veld **Bevestig wachtwoord** het wachtwoord van het account voor Verificatie-agent dat tijdens de vorige stap is ingevoerd.

   c. Voer een van de volgende acties uit:

   - Selecteer de optie **Wachtwoord bij eerste verificatie wijzigen** als u wilt dat het programma de gebruiker vraagt om het wachtwoord te wijzigen wanneer die voor het eerst diens identiteit moet verifiëren voor het opgegeven account in de opdracht.

   - In het andere geval selecteert u de optie **Wijziging van wachtwoord niet verplichten**.

9. Schakel het selectievakje **Verificatie met certificaat toestaan** in als u wilt dat het programma de gebruiker vraagt om een token of een smartcard op de computer aan te sluiten tijdens de verificatie voor de toegang tot

geëncrypte harde schijven.

10. Als u tijdens de vorige stap het selectievakje **Verificatie met certificaat toestaan** hebt ingeschakeld, klikt u op de knop **Bladeren** en selecteert u het bestand van het elektronische token- of smartcardcertificaat in het venster **Certificaatbestand selecteren**.

11. Typ indien nodig in het veld **Beschrijving van opdracht** de gegevens van het account in Verificatie-agent dat u nodig hebt voor het beheer van de opdracht.

12. Voer een van de volgende acties uit:

    - Schakel het selectievakje **Verificatie toestaan** in als u wilt dat het programma toestaat dat de gebruiker het opgegeven account in de opdracht gebruikt om het verificatievenster in Verificatie-agent te openen.

    - Schakel het selectievakje **Verificatie blokkeren** in als u wilt dat het programma niet toestaat dat de gebruiker het opgegeven account in de opdracht gebruikt om het verificatievenster in Verificatie-agent te openen.

13. Klik in het venster **Gebruikersaccount toevoegen** op **OK**.

Een opdracht voor het bewerken van account in Verificatie-agent toevoegen

Zo voegt u een opdracht voor het bewerken van een account in Verificatie-agent toe:

1. Open in het gedeelte **Instellingen** van het venster **Eigenschappen: <naam van taak voor beheer van account in Verificatie-agent>** het contextmenu van de knop **Toevoegen** en selecteer de optie **Opdracht voor bewerken van account**.

   Het venster **Gebruikersaccount bewerken** wordt geopend.

2. Geef in het veld **Windows-account** in het venster **Gebruikersaccount bewerken** de naam van het Microsoft Windows-gebruikersaccount op dat is gebruikt om het account in Verificatie-agent aan te maken dat u nu wilt bewerken. Voer hiervoor de accountnaam handmatig in of klik op de knop **Selecteren**.

3. Als u de naam van een Microsoft Windows-gebruikersaccount handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om het beveiligings-ID (SID) van het gebruikersaccount te bepalen.

   Als u ervoor kiest om het beveiligings-ID (SID) niet te laten bepalen door op de knop **Toestaan** te klikken, wordt het ID bepaald wanneer de taak op de computer wordt uitgevoerd.

   > De bepaling van het SID van het Microsoft Windows-account tijdens het toevoegen van een opdracht voor het bewerken van een account in Verificatie-agent is een handige manier om ervoor te zorgen dat de handmatig ingevoerde naam van het Microsoft Windows-gebruikersaccount correct is. Als het ingevoerde Microsoft Windows-gebruikersaccount niet bestaat of aan een niet-vertrouwd domein toebehoort, eindigt de groepstaak voor het beheren van accounts in Verificatie-agent met een fout.

4. Schakel het selectievakje **Gebruikersnaam wijzigen** in en voer een nieuwe naam voor het account in Verificatie-agent in als u wilt dat Kaspersky Endpoint Security de gebruikersnaam wijzigt in de naam die in het veld eronder is getypt voor alle accounts in Verificatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.

5. Schakel het selectievakje **Instellingen voor verificatie met wachtwoord wijzigen** in om de instellingen voor de verificatie met een wachtwoord te kunnen bewerken.

6. Schakel het selectievakje **Verificatie met wachtwoord toestaan** in als u wilt dat het programma de gebruiker vraagt om het wachtwoord voor het account van Verificatie-agent in te voeren tijdens de verificatie voor de toegang tot geëncrypte harde schijven.

7. Als u tijdens de vorige stap het selectievakje **Verificatie met wachtwoord toestaan** hebt ingeschakeld:

   a. Voer in het veld **Wachtwoord** het nieuwe wachtwoord van het account voor Verificatie-agent in.

   b. Bevestig in het veld **Bevestig wachtwoord** het wachtwoord dat tijdens de vorige stap is ingevoerd.

8. Schakel het selectievakje **Regel voor wijziging van wachtwoord bij verificatie in Verificatie-agent bewerken** in als u wilt dat Kaspersky Endpoint Security de waarde van de instelling voor het wijzigen van de wachtwoorden wijzigt in de eronder opgegeven waarde voor alle accounts in Verificatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.

9. Geef de waarde voor de wijziging van wachtwoorden bij de verificatie in Verificatie-agent op.

10. Schakel het selectievakje **Instellingen voor verificatie met certificaat wijzigen** in om de instellingen voor de verificatie met het elektronische token- of smartcardcertificaat te kunnen bewerken.

11. Schakel het selectievakje **Verificatie met certificaat toestaan** in als u wilt dat het programma de gebruiker vraagt om het wachtwoord in te voeren voor een aangesloten token of smartcard tijdens de verificatie voor de toegang tot geëncrypte harde schijven.

12. Als u tijdens de vorige stap het selectievakje **Verificatie met certificaat toestaan** hebt ingeschakeld, klikt u op de knop **Bladeren** en selecteert u het bestand van het elektronische token- of smartcardcertificaat in het venster **Certificaatbestand selecteren**.

13. Schakel het selectievakje **Beschrijving van opdracht bewerken** in en bewerk de beschrijving van de opdracht als u wilt dat Kaspersky Endpoint Security de opdrachtbeschrijving wijzigt voor alle accounts in Verificatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.

14. Schakel het selectievakje **Regel voor toegang tot verificatie in Verificatie-agent bewerken** in als u wilt dat Kaspersky Endpoint Security de regel voor de toegang van gebruikers tot het verificatievenster in Verificatie-agent wijzigt in de eronder opgegeven waarde voor alle accounts in Verificatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.

15. Geef de regel voor de toegang tot het verificatievenster in Verificatie-agent op.

16. Klik in het venster **Gebruikersaccount bewerken** op **OK**.

Een opdracht voor het verwijderen van een account in Verificatie-agent toevoegen

Zo voegt u een opdracht voor het verwijderen van een account in Verificatie-agent toe:

1. Open in het gedeelte **Instellingen** van het venster **Eigenschappen: <naam van taak voor beheer van accounts in Verificatie-agent>** het contextmenu van de knop **Toevoegen** en selecteer **Opdracht voor verwijderen van account**.

   Het venster **Gebruikersaccount verwijderen** wordt geopend.

2. Geef in het veld **Windows-account** in het venster **Gebruikersaccount verwijderen** de naam van het Microsoft Windows-gebruikersaccount op dat is gebruikt om het account in Verificatie-agent aan te maken dat u nu wilt

verwijderen. Voer hiervoor de accountnaam handmatig in of klik op de knop **Selecteren**.

3. Als u de naam van een Microsoft Windows-gebruikersaccount handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om het beveiligings-ID (SID) van het gebruikersaccount te bepalen.

   Als u ervoor kiest om het beveiligings-ID (SID) niet te laten bepalen door op de knop **Toestaan** te klikken, wordt het ID bepaald wanneer de taak op de computer wordt uitgevoerd.

   De bepaling van het SID van het Microsoft Windows-account tijdens het toevoegen van een opdracht voor het verwijderen van een account in Verificatie-agent is een handige manier om ervoor te zorgen dat de handmatig ingevoerde naam van het Microsoft Windows-gebruikersaccount correct is. Als het ingevoerde Microsoft Windows-gebruikersaccount niet bestaat of aan een niet-vertrouwd domein toebehoort, eindigt de groepstaak voor het beheren van accounts in Verificatie-agent met een fout.

4. Klik in het venster **Gebruikersaccount verwijderen** op **OK**.

Accountgegevens voor Verificatie-agent herstellen

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo herstelt u de gebruikersnaam en het wachtwoord van een account in Verificatie-agent:

1. Op een computer met geëncrypte harde schijven wordt Verificatie-agent geladen voordat het besturingssysteem wordt opgestart. Klik in de interface van Verificatie-agent op de knop **Wachtwoord vergeten** om het herstel van de gebruikersnaam en het wachtwoord van een account in Verificatie-agent te starten.

2. Volg de instructies van Verificatie-agent om de gevraagde informatie voor het herstel van de gebruikersnaam en het wachtwoord van het account in Verificatie-agent te verkrijgen.

3. Geef de inhoud van de aanvraag samen met de naam van de computer door aan de netwerkbeheerder van uw bedrijf.

4. Voer het antwoord op de aanvraag voor het herstel van de gebruikersnaam en het wachtwoord van het account in Verificatie-agent in dat door de netwerkbeheerder is gegenereerd en geleverd.

5. Voer een nieuw wachtwoord voor het account in Verificatie-agent in en bevestig het.

   De gebruikersnaam van het account in Verificatie-agent wordt gedefinieerd op basis van het antwoord op de aanvragen voor het herstel van de gebruikersnaam en het wachtwoord van het account in Verificatie-agent.

Nadat u het nieuwe wachtwoord van het account in Verificatie-agent hebt ingevoerd en bevestigd, wordt het wachtwoord opgeslagen en krijgt u toegang tot geëncrypte harde schijven.

Antwoorden op een aanvraag van een gebruiker om de gegevens van een account in Verificatie-agent te herstellen

Zo maakt en verstuurt u de gebruikersgegevens voor het antwoord op de aanvraag voor het herstel van de gebruikersnaam en het wachtwoord van een account in Verificatie-agent:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de computer van de gebruiker behoort die het herstel van de gebruikersnaam en het wachtwoord van een account in Verificatie-agent heeft gevraagd.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer op het tabblad **Apparaten** de computer van de gebruiker die het herstel van de gebruikersnaam en het wachtwoord van een account in Verificatie-agent heeft gevraagd en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang tot apparaten en gegevens in offline modus**.

   Het venster **Verleen toegang tot apparaten en gegevens in offline modus** wordt geopend.
6. Selecteer in het venster **Verleen toegang tot apparaten en gegevens in offline modus** het tabblad **Verificatie-agent**.
7. Selecteer in het gedeelte **Huidig encryptiealgoritme** het type van het encryptiealgoritme.
8. Selecteer in de vervolgkeuzelijst **Account** de naam van het gemaakte account in Verificatie-agent voor de gebruiker die het herstel van de naam en het wachtwoord van het account in Verificatie-agent heeft gevraagd.
9. Selecteer in de vervolgkeuzelijst **Harde schijf** de geëncrypte harde schijf waarvoor u de toegang wilt herstellen.
10. Voer in het gedeelte **Gebruikersaanvraag** de blokken van de aanvraag in die de gebruiker geeft.

    De inhoud van het antwoord op de aanvraag van de gebruiker voor het herstel van de gebruikersnaam en het wachtwoord van een account in Verificatie-agent wordt in het veld **Toegangscode** weergegeven.
11. Zeg de inhoud van de blokken uit het antwoord aan de gebruiker.

Details van gegevensencryptie bekijken

In deze sectie wordt beschreven hoe u de details van de gegevensencryptie kunt bekijken.

Over de encryptiestatus

Wanneer de encryptie of de decryptie aan de gang is, stuurt Kaspersky Endpoint Security informatie over de status van encryptieparameters die op clientcomputers zijn toegepast naar Kaspersky Security Center.

De encryptiestatus kan de volgende waarden hebben:

- *Beleid niet gedefinieerd*. Er is geen Kaspersky Security Center-beleid gedefinieerd voor de computer.
- *Encryptie / decryptie wordt uitgevoerd*. De encryptie en / of decryptie van gegevens wordt op de computer uitgevoerd.
- *Fout*. Er is een fout opgetreden tijdens de encryptie en / of decryptie van de gegevens op de computer.

- *Opnieuw opstarten is vereist*. Het besturingssysteem moet opnieuw worden opgestart om de encryptie of decryptie van gegevens op de computer te starten of te voltooien.
- *Conform beleid*. De encryptie en / of decryptie van gegevensversleuteling op de computer is voltooid met de encryptie-instellingen die zijn opgegeven in het Kaspersky Security Center-beleid dat op de computer is toegepast.
- *Geannuleerd door gebruiker*. De gebruiker heeft de bestandsencryptie voor de verwisselbare schijf niet bevestigd.
- *Niet ondersteund*. De encryptie van gegevens is niet beschikbaar op de computer.

De encryptiestatus bekijken

Zo bekijkt u de encryptiestatus van gegevens op de computer:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante computer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.

   Op het tabblad **Apparaten** in de werkruimte ziet u de eigenschappen van de computers uit de geselecteerde beheergroep.
4. Schuif op het tabblad **Apparaten** in de werkruimte de schuifbalk helemaal naar rechts.

   In de kolom **Encryptiestatus** ziet u de encryptiestatus van de gegevens op de computers uit de geselecteerde beheergroep. Deze status is gebaseerd op de informatie over de bestandsencryptie op lokale schijven van de computer, de encryptie van harde schijven van de computer en de encryptie van verwisselbare schijven die op de computer zijn aangesloten.

Statistieken over encryptie in informatievensters van Kaspersky Security Center bekijken

Zo bekijkt u de statistieken over encryptie in informatievensters van Kaspersky Security Center:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de consolestructuur het knooppunt **Administration Server – <Naam van computer>**.
3. Selecteer het tabblad **Statistieken** in de werkruimte rechts van de structuur van de Beheerconsole.
4. Maak een nieuwe pagina met informatievensters met statistieken over de gegevensencryptie. Hiertoe doet u het volgende:

   a. Klik op het tabblad **Statistieken** op de knop **Weergave aanpassen**.

      Het venster **Eigenschappen: Statistieken** wordt geopend.

   b. Klik in het venster **Eigenschappen: Statistieken** op **Toevoegen**.

Het venster **Eigenschappen: Nieuwe pagina** wordt geopend.

c. Typ in het gedeelte **Algemeen** van het venster **Eigenschappen: Nieuwe pagina** de naam van de pagina.

d. Klik in het gedeelte **Informatievensters** op de knop **Toevoegen**.

Het venster **Nieuw informatievenster** wordt geopend.

e. Selecteer In de groep **Beschermingsstatus** in het venster **Nieuw informatievenster** de optie **Encryptie van apparaat**.

f. Klik op **OK**.

Het venster **Eigenschappen: encryptiecontrole** wordt geopend.

g. Bewerk indien nodig de instellingen van het informatievenster. Gebruik hiervoor de gedeelten **Weergave** en **Apparaten** van het venster **Eigenschappen: Encryptie van apparaat**.

h. Klik op **OK**.

i. Herhaal stappen d tot en met h van de instructies en selecteer de optie **Encryptie van verwisselbare schijven** in het gedeelte **Beschermingsstatus** van het venster **Nieuw informatievenster**.

De toegevoegde informatievensters verschijnen in de lijst **Informatievensters** in het venster **Eigenschappen: Nieuwe pagina**.

j. Klik in het venster **Eigenschappen: Nieuwe pagina** op **OK**.

De naam van de pagina met de informatievensters die tijdens de vorige stappen zijn gemaakt verschijnt in de lijst **Pagina's** van het venster **Eigenschappen: Statistieken**.

k. Klik in het venster **Eigenschappen: Statistieken** op **Sluiten**.

5. Open op het tabblad **Statistieken** de pagina die tijdens de vorige stappen van de instructies is gemaakt.

De informatievensters verschijnen en tonen de encryptiestatus van computers en verwisselbare schijven.

Fouten tijdens bestandsencryptie op lokale schijven van de computer bekijken

Zo bekijkt u fouten tijdens de bestandsencryptie op lokale schijven van de computer:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de clientcomputer behoort waarvoor u de lijst met fouten tijdens de bestandsencryptie wilt bekijken.

3. Selecteer in de werkruimte het tabblad **Apparaten**.

4. Selecteer op het tabblad **Apparaten** de naam van de computer in de lijst en klik rechts om het contextmenu te openen.

5. Voer een van de volgende acties uit:

- Selecteer in het contextmenu van de computer de optie **Bescherming**.

- Selecteer in het contextmenu van de computer de optie **Eigenschappen**. Selecteer in het venster **Eigenschappen: <naam van computer>** het gedeelte **Bescherming**.

6. Klik in het gedeelte **Bescherming** van het venster **Eigenschappen: <naam van computer>** op de koppeling **Lijst met fouten tijdens gegevensencryptie bekijken** om het venster **Fouten tijdens gegevensencryptie** te openen.

   In het venster ziet u de details van de fouten die tijdens de bestandsencryptie op lokale schijven van de computer zijn opgetreden. Wanneer een fout wordt gecorrigeerd, verwijdert Kaspersky Security Center de gegevens van de fout uit het venster **Fouten tijdens gegevensencryptie**.

Rapport over gegevensencryptie bekijken

Zo bekijkt u het rapport over de gegevensencryptie:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Rapporten**.

3. Klik op de knop **Sjabloon voor rapport aanmaken**.

   De wizard Sjabloon voor rapport wordt gestart.

4. Volg de instructies van de wizard Sjabloon voor rapport. In het venster **Type van sjabloon voor rapport selecteren** selecteert u in het gedeelte **Overige** een van de volgende opties:

   - **Rapport over encryptiestatus van beheerd apparaat**.
   - **Rapport over encryptie van apparaten voor gegevensopslag**.
   - **Rapport over encryptiefouten**.
   - **Rapport over geblokkeerde toegang tot geëncrypte bestanden**.

   Wanneer u de wizard Nieuw sjabloon voor rapport hebt voltooid, verschijnt de nieuwe rapportsjabloon in de tabel op het tabblad **Rapporten**.

5. Selecteer de rapportsjabloon die tijdens de vorige stappen van de instructies zijn aangemaakt.

Het rapport wordt gemaakt. Het rapport wordt in een nieuw venster weergegeven.

Geëncrypte bestanden beheren met beperkte encryptiefunctionaliteit voor bestanden

Wanneer het Kaspersky Security Center-beleid wordt toegepast en de bestanden vervolgens worden geëncrypt, ontvangt Kaspersky Endpoint Security een encryptiesleutel om rechtstreekse toegang tot de geëncrypte bestanden te krijgen. Met deze encryptiesleutel kan een gebruiker met een Windows-gebruikersaccount dat tijdens de bestandsencryptie actief was rechtstreeks toegang tot de geëncrypte bestanden krijgen. Gebruikers die werken met Windows-accounts die tijdens de bestandsencryptie niet actief waren moeten verbinding maken met Kaspersky Security Center om toegang tot de geëncrypte bestanden te krijgen.

In de volgende gevallen kunnen geëncrypte bestanden niet toegankelijk zijn:

- Op de computer van de gebruiker staan encryptiesleutels maar er is geen verbinding met Kaspersky Security Center voor het beheer ervan. In dit geval moet de gebruiker toegang tot geëncrypte bestanden vragen aan de netwerkbeheerder.

  Als u geen toegang tot Kaspersky Security Center hebt, moet u:

  - een toegangscode aanvragen om toegang te krijgen tot de geëncrypte bestanden op de harde schijven van de computer;
  - om toegang te krijgen tot geëncrypte bestanden op verwisselbare schijven, afzonderlijke toegangscodes voor de geëncrypte bestanden op elke verwisselbare schijf aanvragen.

- De encryptieonderdelen op de computer van de gebruiker zijn verwijderd. In dit geval kan de gebruiker geëncrypte bestanden op lokale en verwisselbare schijven openen maar de inhoud van die bestanden zal geëncrypt verschijnen.

  De gebruiker kan werken met geëncrypte bestanden onder de volgende omstandigheden:

  - De bestanden zitten in geëncrypte pakketten die zijn aangemaakt op een computer waarop Kaspersky Endpoint Security is geïnstalleerd.
  - De bestanden zijn opgeslagen op verwisselbare schijven waarop de portable modus is toegestaan.

Toegang tot geëncrypte bestanden krijgen zonder verbinding met Kaspersky Security Center

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo krijgt u toegang tot geëncrypte bestanden zonder een verbinding met Kaspersky Security Center:

1. Probeer toegang te krijgen tot het geëncrypte bestand dat u nodig hebt.

   Als u niet bent verbonden met Kaspersky Security Center wanneer u toegang probeert te krijgen tot een bestand dat op een lokale schijf van de computer staat, genereert Kaspersky Endpoint Security een bestand met een toegangsaanvraag voor alle geëncrypte bestanden op de lokale schijven van de computer. Als u toegang probeert te krijgen tot een bestand dat op een verwisselbare schijf staat, genereert Kaspersky Endpoint Security een bestand met een toegangsaanvraag voor alle geëncrypte bestanden op de verwisselbare schijf. Het venster **Bestandstoegang geblokkeerd** wordt geopend.

2. Stuur het bestand met de toegangsaanvraag voor geëncrypte bestanden naar de netwerkbeheerder. Doe hiervoor één van het volgende:

   - Klik op de knop **Versturen per e-mail** om het bestand met de toegangsaanvraag voor geëncrypte bestanden te e-mailen naar de netwerkbeheerder.
   - Klik op de knop **Opslaan** om het bestand met de toegangsaanvraag voor geëncrypte bestanden op te slaan en op een andere manier aan de netwerkbeheerder te bezorgen.

3. Verkrijg het bestand met de toegangscode voor geëncrypte bestanden die de netwerkbeheerder heeft aangemaakt en u heeft bezorgd.

4. Activeer de code voor de toegang tot de geëncrypte bestanden op een van de volgende manieren:

- Selecteer in een bestandsverkenner het bestand met de toegangscode voor de geëncrypte bestanden. Dubbelklik erop om het te openen.

- Doe het volgende:

  a. Open het hoofdvenster van Kaspersky Endpoint Security.

  b. Klik op de knop .

  Zo opent u het venster **Gebeurtenissen**.

  c. Selecteer het tabblad **Status van toegang tot bestanden en apparaten**.

  Op het tabblad ziet u een lijst met alle toegangsaanvragen voor geëncrypte bestanden.

  d. Selecteer de aanvraag waarvoor u de toegangscode voor de geëncrypte bestanden hebt gekregen.

  e. Klik op **Bladeren** om het bestand met de toegangscode voor de geëncrypte bestanden te laden.

  Het standaarddialoogvenster **Bestand met toegangscode selecteren** wordt in Microsoft Windows geopend.

  f. Selecteer in het standaardvenster **Bestand met toegangscode selecteren** in Microsoft Windows het bestand met de extensie .kesdr dat u van de beheerder hebt gekregen. De naam van het bestand komt overeen met de naam van het bestand met de toegangsaanvraag.

  g. Klik op de knop **Openen**.

  h. Klik in het venster **Gebeurtenissen** op **OK**.

Als een bestand met een toegangsaanvraag voor geëncrypte bestanden wordt gegenereerd wanneer u toegang probeert te krijgen tot een bestand dat op een lokale schijf van de computer staat, geeft Kaspersky Endpoint Security toegang tot alle geëncrypte bestanden op de lokale schijven van de computer. Als een bestand met een toegangsaanvraag voor geëncrypte bestanden wordt gegenereerd wanneer u toegang probeert te krijgen tot een bestand op een verwisselbare schijf, geeft Kaspersky Endpoint Security toegang tot alle geëncrypte bestanden op de verwisselbare schijf. Om toegang tot geëncrypte bestanden op meerdere verwisselbare schijven te krijgen, moet u een afzonderlijke toegangscode voor elke verwisselbare schijf krijgen.

Gebruikers toegang tot geëncrypte bestanden geven zonder verbinding met Kaspersky Security Center

Zo geeft u gebruikers toegang tot geëncrypte bestanden zonder een verbinding met Kaspersky Security Center:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de computer van de gebruiker behoort die toegang tot de geëncrypte bestanden vraagt.

3. Selecteer in de werkruimte het tabblad **Apparaten**.

4. Selecteer op het tabblad **Apparaten** de computer van de gebruiker die toegang tot de geëncrypte bestanden vraagt en klik rechts om het contextmenu te openen.

5. Selecteer in het contextmenu de optie **Verleen toegang tot apparaten en gegevens in offline modus**.

   Het venster **Verleen toegang tot apparaten en gegevens in offline modus** wordt geopend.

6. Selecteer in het venster **Verleen toegang tot apparaten en gegevens in offline modus** het tabblad **Encryptie**.

7. Klik op het tabblad **Encryptie** op de knop **Bladeren**.

   Het standaarddialoogvenster **Bestand met toegangsaanvraag selecteren** wordt in Microsoft Windows geopend.

8. Kies in het venster **Bestand met toegangsaanvraag selecteren** het pad naar het bestand met de aanvraag dat u van de gebruiker hebt ontvangen en klik op **Openen**.

   Kaspersky Security Center genereert een bestand met een toegangscode voor de geëncrypte bestanden. De details van de aanvraag van de gebruiker worden op het tabblad **Encryptie** weergegeven.

9. Voer een van de volgende acties uit:

   - Om het gegenereerde bestand met de toegangscode naar de gebruiker te e-mailen, klikt u op de knop **Versturen per e-mail**.

   - Om het bestand met de toegangscode voor de geëncrypte bestanden op te slaan en op een andere manier aan de gebruiker te bezorgen, klikt u op de knop **Opslaan**.

Sjablonen van berichten voor toegang tot geëncrypte bestanden bewerken

Zo bewerkt u de sjablonen van berichten voor toegang tot geëncrypte bestanden:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de sjablonen van de berichten voor de toegang tot geëncrypte bestanden wilt bewerken.

3. Selecteer in de werkruimte het tabblad **Beleid**.

4. Selecteer het noodzakelijke beleid.

5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:

   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.

   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

6. Selecteer in het gedeelte **Gegevensencryptie** het subgedeelte **Algemene encryptie-instellingen**.

7. Klik in het gedeelte **Sjablonen** op de knop **Sjablonen**.

   Het venster **Sjablonen** wordt geopend.

8. Doe het volgende:

   - Als u de sjabloon van het bericht van de gebruiker wilt bewerken, selecteert u het tabblad **Bericht van gebruiker**. Het venster **Bestandstoegang geweigerd** wordt geopend wanneer de gebruiker toegang tot een geëncrypt bestand probeert te krijgen wanneer er geen beschikbare code op de computer is voor toegang tot geëncrypte bestanden. Met een klik op de knop **Versturen per e-mail** in het venster **Bestandstoegang geweigerd** wordt automatisch een gebruikersbericht aangemaakt. Dit bericht wordt naar de netwerkbeheerder van het bedrijf verstuurd samen met het bestand met de aanvraag voor toegang tot geëncrypte bestanden.

- Als u de sjabloon van het bericht van de beheerder wilt bewerken, selecteert u het tabblad **Bericht van beheerder**. Dit bericht wordt automatisch aangemaakt wanneer er op de knop **Versturen per e-mail** in het venster **Toegang tot geëncrypte bestanden verlenen** wordt geklikt en wordt naar de gebruiker verstuurd nadat de toegang tot geëncrypte bestanden heeft gekregen.

9. Bewerk de sjablonen van de berichten.

   U kunt de knop **Standaard** en de vervolgkeuzelijst **Variabele** gebruiken.

10. Klik op **OK**.

11. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

Werken met geëncrypte apparaten als er geen toegang toe is

Toegang tot geëncrypte apparaten verkrijgen

In de volgende gevallen moet een gebruiker mogelijk toegang tot geëncrypte apparaten aanvragen:

- De harde schijf is met een andere computer geëncrypt.
- De encryptiesleutel voor een apparaat is niet op de computer opgeslagen (bijvoorbeeld: bij de eerste poging om toegang te krijgen tot de geëncrypte verwisselbare schijf op de computer) en de computer is niet verbonden met Kaspersky Security Center.

  Nadat de gebruiker de toegangscode heeft toegepast op het geëncrypte apparaat, slaat Kaspersky Endpoint Security de encryptiesleutel op de computer van de gebruiker op en geeft het de volgende keren wel toegang tot dit apparaat zelfs als er geen verbinding met Kaspersky Security Center is.

Zo kunt u toegang tot geëncrypte apparaten verkrijgen:

1. De gebruiker gebruikt de programma-interface van Kaspersky Endpoint Security om een bestand met een toegangsaanvraag aan te maken (dit bestand heeft een KESDC-extensie) en stuurt het naar de netwerkbeheerder van het bedrijf.
2. De beheerder gebruikt de beheerconsole van Kaspersky Security Center om een bestand met een toegangscode aan te maken (dit bestand heeft een KESDR-extensie) en stuurt het naar de gebruiker.
3. De gebruiker past de toegangscode toe.

Gegevens op geëncrypte apparaten herstellen

Een gebruiker kan de herstelvoorziening voor geëncrypte apparaten gebruiken (hierna de Herstelvoorziening genoemd) om met geëncrypte apparaten te werken. Dit is mogelijk vereist in de volgende gevallen:

- De procedure voor het gebruiken van een toegangscode om toegang te verkrijgen is mislukt.
- De encryptieonderdelen zijn niet geïnstalleerd op de computer met het geëncrypte apparaat.

De benodigde gegevens voor het herstellen van de toegang tot geëncrypte apparaten met behulp van de Herstelvoorziening zitten al enige tijd in een niet-geëncrypte vorm in het geheugen van de computer van de gebruiker. Om het risico op onbevoegde toegang tot zulke gegevens te verkleinen, doet u er goed aan de toegang tot geëncrypte apparaten op vertrouwde computers te herstellen.

Zo kunt u gegevens op geëncrypte apparaten herstellen:

1. De gebruiker gebruikt de Herstelvoorziening om een bestand met een toegangsaanvraag aan te maken (dit bestand heeft een FDERTC-extensie) en stuurt het naar de netwerkbeheerder van het bedrijf.
2. De beheerder gebruikt de beheerconsole van Kaspersky Security Center om een bestand met een toegangscode aan te maken (dit bestand heeft een FDERTR-extensie) en stuurt het naar de gebruiker.
3. De gebruiker past de toegangscode toe.

Om gegevens op geëncrypte harde schijven van het systeem te herstellen, kan de gebruiker ook de accountgegevens voor Verificatie-agent opgeven in de Herstelvoorziening. Als de metagegevens van het account voor Verificatie-agent beschadigd zijn, moet de gebruiker de herstelprocedure voltooien met het bestand met de toegangsaanvraag.

Alvorens gegevens op geëncrypte apparaten te herstellen, wordt u aanbevolen het Kaspersky Security Center-encryptiebeleid te annuleren op de computer waarop deze bewerking zal worden uitgevoerd. Hiermee voorkomt u dat de schijf opnieuw wordt geëncrypt.

Toegang tot geëncrypte apparaten verkrijgen via de programma-interface

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo verkrijgt u toegang tot geëncrypte apparaten via de programma-interface:

1. Probeer toegang te krijgen tot het geëncrypte apparaat dat u nodig hebt.

   Het venster **Toegang tot gegevens is geblokkeerd** wordt geopend.

2. Stuur het bestand met de toegangsaanvraag (dit bestand heeft een KESDC-extensie) voor het geëncrypte apparaat naar de netwerkbeheerder van het bedrijf. Doe hiervoor één van het volgende:

   - Klik op de knop **Versturen per e-mail** om het aangemaakte bestand met de toegangsaanvraag voor het geëncrypte apparaat te e-mailen naar de netwerkbeheerder van het bedrijf.
   - Klik op de knop **Opslaan** om het bestand met de toegangsaanvraag voor het geëncrypte apparaat op te slaan en het op een andere manier aan de netwerkbeheerder van het bedrijf te bezorgen.

   Als u het venster **Toegang tot gegevens is geblokkeerd** hebt gesloten zonder het bestand met de toegangsaanvraag op te slaan of zonder het naar de netwerkbeheerder van het bedrijf te versturen, kunt u dit doen wanneer u dit goed uitkomt door in het venster **Gebeurtenissen** naar het tabblad **Status van toegang tot bestanden en apparaten** te gaan. Klik in het hoofdvenster van het programma op de knop  om dit venster te openen.

3. Vraag en bewaar het bestand met de toegangscode voor het geëncrypte apparaat dat de netwerkbeheerder van het bedrijf heeft aangemaakt en u heeft gegeven.

4. Gebruik een van de volgende methoden om de toegangscode voor de toegang tot het geëncrypte apparaat toe te passen.

   - Ga in een bestandsbeheerder naar het bestand met de toegangscode voor het geëncrypte apparaat en dubbelklik op het bestand om het te openen.

   - Doe het volgende:

     a. Open het hoofdvenster van Kaspersky Endpoint Security.

     b. Klik op de knop om het venster **Gebeurtenissen** te openen.

     c. Selecteer het tabblad **Status van toegang tot bestanden en apparaten**.

     Op het tabblad ziet u een lijst met alle toegangsaanvragen voor geëncrypte bestanden en apparaten.

     d. Selecteer de aanvraag waarvoor u het bestand met de toegangscode voor het geëncrypte apparaat hebt gekregen.

     e. Klik op **Bladeren** om het ontvangen bestand met de toegangscode voor het geëncrypte apparaat te laden.

     Het standaarddialoogvenster **Bestand met toegangscode selecteren** wordt in Microsoft Windows geopend.

     f. Selecteer in het standaardvenster **Bestand met toegangscode selecteren** in Microsoft Windows het bestand met de KESDR-extensie dat u van de beheerder hebt gekregen. De naam van het bestand komt overeen met de naam van het bestand met de toegangsaanvraag voor het geëncrypte apparaat.

     g. Klik op de knop **Openen**.

     h. Klik in het venster **Status van toegang tot bestanden en apparaten** op **OK**.

Kaspersky Endpoint Security geeft nu toegang tot het geëncrypte apparaat.

Gebruikers toegang tot geëncrypte apparaten verlenen

Zo verleent u gebruikers toegang tot een geëncrypt apparaat:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de computer van de gebruiker behoort die toegang tot het geëncrypte apparaat vraagt.

3. Selecteer in de werkruimte het tabblad **Apparaten**.

4. Selecteer op het tabblad **Apparaten** de computer van de gebruiker die toegang tot het geëncrypte apparaat vraagt en klik rechts om het contextmenu te openen.

5. Selecteer in het contextmenu de optie **Verleen toegang tot apparaten en gegevens in offline modus**.

   Het venster **Verleen toegang tot apparaten en gegevens in offline modus** wordt geopend.

6. Selecteer in het venster **Verleen toegang tot apparaten en gegevens in offline modus** het tabblad **Encryptie**.

7. Klik op het tabblad **Encryptie** op de knop **Bladeren**.

   Het standaarddialoogvenster **Bestand met toegangsaanvraag selecteren** wordt in Microsoft Windows geopend.

8. Geef in het venster **Bestand met toegangsaanvraag selecteren** het pad naar het bestand met de toegangsaanvraag op dat een KESDC-extensie heeft en dat u van de gebruiker hebt gekregen.

9. Klik op de knop **Openen**.

   Kaspersky Security Center genereert een bestand met een toegangscode voor het geëncrypte apparaat. Dit bestand heeft een KESDR-extensie. De details van de aanvraag van de gebruiker worden op het tabblad **Encryptie** weergegeven.

10. Voer een van de volgende acties uit:

    - Om het gegenereerde bestand met de toegangscode naar de gebruiker te e-mailen, klikt u op de knop **Versturen per e-mail**.
    - Om het bestand met de toegangscode voor het geëncrypte apparaat op te slaan en op een andere manier aan de gebruiker te bezorgen, klikt u op de knop **Opslaan**.

Een herstelsleutel voor harde schijven die zijn geëncrypt met BitLocker geven aan een gebruiker

Zo stuurt u een gebruiker een herstelsleutel voor een harde schijf van het systeem die met BitLocker is geëncrypt:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de computer van de gebruiker behoort die toegang tot de geëncrypte schijf vraagt.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer op het tabblad **Apparaten** de computer van de gebruiker die toegang tot de geëncrypte schijf vraagt.
5. Klik rechts om het contextmenu te openen en selecteer **Verleen toegang tot apparaten en gegevens in offline modus**.

   Het venster **Verleen toegang tot apparaten en gegevens in offline modus** wordt geopend.

6. Selecteer in het venster **Verleen toegang tot apparaten en gegevens in offline modus** het tabblad **Toegang tot een door BitLocker beveiligd systeemstation**.
7. Vraag de gebruiker het herstelsleutel-ID dat in het venster voor de invoer van het BitLocker-wachtwoord is vermeld en vergelijk het met het ID in het veld **ID herstelsleutel**.

   > Als de ID's niet overeenkomen, kan deze sleutel niet worden gebruikt om de toegang tot de opgegeven systeemschijf te herstellen. Controleer of de naam van de geselecteerde computer overeenkomt met de naam van de computer van de gebruiker.

8. Stuur de gebruiker de sleutel die in het veld **Herstelsleutel** is vermeld.

Zo stuurt u een gebruiker een herstelsleutel voor een harde schijf waarop het systeem niet staat en die met BitLocker is geëncrypt:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Extra** → **Encryptie en gegevensbescherming** → **Geëncrypte apparaten**.

   In de werkruimte ziet u een lijst met geëncrypte apparaten.
3. Selecteer in de werkruimte het geëncrypte apparaat waarvoor u de toegang wilt herstellen.
4. Klik rechts om het contextmenu te openen en selecteer **Krijg toegangscode voor opgegeven geëncrypt apparaat**.

   Hiermee opent u het venster **Toegang tot een met BitLocker geëncrypte schijf herstellen**.
5. Vraag de gebruiker het herstelsleutel-ID dat in het venster voor de invoer van het BitLocker-wachtwoord is vermeld en vergelijk het met het ID in het veld **ID herstelsleutel**.

   > Als de ID's niet overeenkomen, kan deze sleutel niet worden gebruikt om de toegang tot de opgegeven schijf te herstellen. Controleer of de naam van de geselecteerde computer overeenkomt met de naam van de computer van de gebruiker.
6. Stuur de gebruiker de sleutel die in het veld **Herstelsleutel** is vermeld.

Het uitvoerbare bestand van Herstelvoorziening aanmaken

> Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo maakt u het uitvoerbare bestand van Herstelvoorziening aan:

1. Open het hoofdvenster van het programma.
2. Klik op de knop links onder in het hoofdvenster van het programma om het venster **Support** te openen.
3. Klik in het venster **Support** op de knop **Geëncrypt apparaat herstellen**.

   De herstelvoorziening voor geëncrypte apparaten wordt gestart.
4. Klik op de knop **Zelfstandige herstelvoorziening maken** in het venster van Herstelvoorziening.

   Het venster **Zelfstandige herstelvoorziening maken** wordt geopend.
5. Typ in het venster **Opslaan naar** handmatig het pad naar de map voor de opslag van het uitvoerbare bestand van Herstelvoorziening of klik op de knop **Bladeren**.
6. Klik op **OK** in het venster **Zelfstandige herstelvoorziening maken**.

   Het uitvoerbare bestand van Herstelvoorziening (fdert.exe) wordt in de geselecteerde map opgeslagen.

Gegevens op geëncrypte bestanden herstellen met de Herstelvoorziening

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo herstelt u de toegang tot geëncrypte bestanden met de Herstelvoorziening:

1. Start Herstelvoorziening op een van de volgende manieren:

   - Klik op de knop in het hoofdvenster van Kaspersky Endpoint Security om het venster **Support** te openen en klik op de knop **Geëncrypt apparaat herstellen**.

   - Start het uitvoerbare bestand 'fdert.exe' van Herstelvoorziening. Dit bestand wordt door Kaspersky Endpoint Security aangemaakt.

2. Selecteer in de vervolgkeuzelijst **Selecteer een apparaat** in het venster van Herstelvoorziening een geëncrypt apparaat waarvoor u de toegang wilt herstellen.

3. Klik op de knop **Scannen** om de voorziening te laten bepalen welke actie moet worden uitgevoerd op het apparaat: ontgrendelen of decrypten.

   Als de computer toegang heeft tot de encryptiefunctionaliteit van Kaspersky Endpoint Security, wordt u door de Herstelvoorziening gevraagd om het apparaat te ontgrendelen. Hoewel het ontgrendelen van het apparaat het niet decrypt, wordt het apparaat onmiddellijk toegankelijk omdat het wordt ontgrendeld. Als de computer geen toegang heeft tot de encryptiefunctionaliteit van Kaspersky Endpoint Security, wordt u door de Herstelvoorziening gevraagd om het apparaat te decrypten.

4. Klik op de knop **MBR herstellen** als de diagnose van de geëncrypte systeemschijf als resultaat een bericht gaf over problemen met de Master Boot Record (MBR) van het apparaat.

   Door de Master Boot Record van het apparaat te herstellen kan de benodigde informatie voor de ontgrendeling of de decryptie van het apparaat sneller worden verzameld.

5. Klik op de knop **Ontgrendelen** of **Decrypten** naargelang de resultaten van de diagnose.

   Het venster **Instellingen voor ontgrendeling van apparaat** of **Decryptie-instellingen voor apparaat** wordt geopend.

6. Als u gegevens wilt herstellen via een account van Verificatie-agent:

   a. Selecteer de optie **Instellingen van account in Verificatie-agent gebruiken**.

   b. Typ in de velden **Naam** en **Wachtwoord** de gegevens van het account dat u met Verificatie-agent gebruikt.

   Deze methode is alleen mogelijk bij het herstellen van gegevens op een systeemschijf. Als de harde schijf van het systeem beschadigd is geraakt en de accountgegevens van Verificatie-agent verloren zijn geraakt, moet u een toegangscode vragen aan de netwerkbeheerder van het bedrijf om de gegevens op een geëncrypt apparaat te herstellen.

7. Als u een toegangscode wilt gebruiken om gegevens te herstellen:

   a. Selecteer de optie **Toegangscode voor apparaat handmatig opgeven**.

   b. Klik op de knop **Toegangscode ontvangen**.

c. Het venster **Toegangscode voor apparaat ontvangen** wordt geopend.

d. Klik op de knop **Opslaan** en selecteer de map waarin u het FDERTC-bestand met de toegangsaanvraag wilt opslaan.

e. Stuur het bestand met de toegangsaanvraag naar de netwerkbeheerder van het bedrijf.

> Sluit het venster **Toegangscode voor apparaat ontvangen** pas als u de toegangscode hebt ontvangen. Wanneer dit venster opnieuw wordt geopend, kunt u de toegangscode die eerder is aangemaakt door de beheerder niet toepassen.

f. Vraag en bewaar het bestand met de toegangscode dat de netwerkbeheerder van het bedrijf heeft aangemaakt en u heeft gegeven.

g. Klik op de knop **Laden** en selecteer het FDERTR-bestand met de toegangscode in het geopende venster.

8. Als u een apparaat decrypt, moet u ook de andere decryptie-instellingen in het venster **Decryptie-instellingen voor apparaat** opgeven. Hiertoe doet u het volgende:

   - Geef op welk deel u wilt decrypten:
     - Als u het volledige apparaat wilt decrypten, selecteert u de optie **Gehele apparaat decrypten**.
     - Als u een deel van de gegevens op een apparaat wilt decrypten, selecteert u de optie **Specifieke gebieden op apparaat decrypten** en gebruikt u de velden **Begin** en **Einde** om de grenzen van het te decrypten gebied op te geven.
   - Selecteer de locatie waar u de gedecrypte gegevens wilt schrijven:
     - Als u de gegevens op het originele apparaat wilt overschrijven met de gedecrypte gegevens, schakelt u het selectievakje **Gegevens in bestand opslaan na decryptie** uit.
     - Als u de gedecrypte gegevens gescheiden wilt houden van de originele geëncrypte gegevens, schakelt u het selectievakje **Gegevens in bestand opslaan na decryptie** in en gebruikt u de knop **Bladeren** om het pad op te geven waar u de gegevens wilt opslaan.

9. Klik op **OK**.

Het apparaat start de ontgrendeling of de decryptie.

Een gebruikersaanvraag voor gegevensherstel op geëncrypte apparaten beantwoorden

Zo maakt u een bestand met een toegangscode voor een geëncrypt apparaat aan en geeft u het aan een gebruiker:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Extra** → **Encryptie en gegevensbescherming** → **Geëncrypte apparaten**.
3. Selecteer in de werkruimte het geëncrypte apparaat waarvoor u een bestand met een toegangscode wilt aanmaken en kies in het contextmenu van het apparaat de optie **Krijg toegangscode voor opgegeven**

geëncrypt apparaat.

> Als u niet zeker weet voor welke computer het bestand met de toegangsaanvraag is gegenereerd, selecteert u in de structuur van de Beheerconsole de map **Extra** → **Encryptie en gegevensbescherming** en klikt u in de werkruimte op de koppeling **Krijg encryptiesleutel voor apparaat**.

Het venster **Toegang tot het apparaat toestaan** wordt geopend.

4. Selecteer het encryptiealgoritme dat momenteel wordt gebruikt. Selecteer hiervoor één van de volgende opties:

   - **AES256**, als Kaspersky Endpoint Security is geïnstalleerd met een distributiepakket uit de aes256-map op de computer die het apparaat heeft geëncrypt.
   - **AES56**, als Kaspersky Endpoint Security is geïnstalleerd met een distributiepakket uit de aes56-map op de computer die het apparaat heeft geëncrypt.

5. Klik op de knop **Bladeren**.

   Het standaarddialoogvenster **Bestand met toegangsaanvraag selecteren** wordt in Microsoft Windows geopend.

6. Geef in het venster **Bestand met toegangsaanvraag selecteren** het pad naar het bestand met de toegangsaanvraag op dat de extensie FDERTC heeft en dat u van de gebruiker hebt gekregen.

7. Klik op de knop **Openen**.

   Kaspersky Security Center genereert een bestand met een toegangscode dat de extensie FDERTR heeft en dat toegang tot het geëncrypte apparaat verleent.

8. Voer een van de volgende acties uit:

   - Om het gegenereerde bestand met de toegangscode naar de gebruiker te e-mailen, klikt u op de knop **Versturen per e-mail**.
   - Om het bestand met de toegangscode voor het geëncrypte apparaat op te slaan en op een andere manier aan de gebruiker te bezorgen, klikt u op de knop **Opslaan**.

Toegang tot geëncrypte gegevens herstellen na fout in besturingssysteem

Na een fout in het besturingssysteem kunt u de toegang tot gegevens alleen voor File Level Encryption (FLE) herstellen. U kunt de toegang tot gegevens niet herstellen als Full Disk Encryption (FDE) wordt gebruikt.

Zo herstelt u de toegang tot geëncrypte gegevens na een fout in het besturingssysteem:

1. Installeer het besturingssysteem opnieuw zonder de harde schijf te formatteren.
2. Installeer Kaspersky Endpoint Security.
3. Maak een verbinding tussen de computer en de Administration Server van Kaspersky Security Center die de computer beheerde tijdens de encryptie van de gegevens.

De toegang tot de geëncrypte gegevens wordt verleend onder dezelfde voorwaarden die vóór de fout in het besturingssysteem van toepassing waren.

Een herstelschijf voor het besturingssysteem aanmaken

De herstelschijf van het besturingssysteem kan handig zijn wanneer er om een bepaalde reden geen toegang tot een geëncrypte harde schijf kan worden verkregen en het besturingssysteem niet kan worden opgestart.

U kunt de herstelschijf gebruiken om een schijfkopie van het Windows-besturingssysteem te laden en kunt de Herstelvoorziening in de schijfkopie van het besturingssysteem gebruiken om de toegang tot de geëncrypte harde schijf te herstellen.

Zo maakt u een herstelschijf voor het besturingssysteem aan:

1. Maak een uitvoerbaar bestand voor de herstelvoorziening voor geëncrypte apparaten aan.

2. Maak een aangepaste schijfkopie van de preboot-omgeving van Windows aan. Voeg het uitvoerbare bestand van de Herstelvoorziening toe aan de aangepaste schijfkopie van preboot-omgeving van Windows.

3. Sla de aangepaste schijfkopie van de preboot-omgeving van Windows op opstartbare media op, zoals een cd of een verwisselbare schijf.

   Raadpleeg de Microsoft Help-bestanden voor instructies voor het maken van een aangepaste schijfkopie van de preboot-omgeving van Windows (bijvoorbeeld in de Microsoft TechNet-bron).

Netwerkbescherming

In deze sectie vindt u informatie over de monitoring van netwerkverkeer en instructies voor de configuratie van de instellingen van gemonitorde netwerkpoorten.

Over netwerkbeveiliging

Tijdens de werking van Kaspersky Endpoint Security monitoren onderdelen zoals Mail Anti-Virus, Web Anti-Virus en IM Anti-Virus gegevensstromen waarvan de overdracht via specifieke protocollen en via specifieke geopende TCP- en UDP-poorten op de computer gebeurt. Mail Anti-Virus scant bijvoorbeeld de overdracht van gegevens via SMTP terwijl Web Anti-Virus de overdracht van gegevens via HTTP en FTP scant.

Kaspersky Endpoint Security verdeelt TCP- en UDP-poorten van het besturingssysteem in verschillende groepen, afhankelijk van het mogelijke gevaar via deze poorten. Bepaalde netwerkpoorten zijn voorbehouden voor services die mogelijk kwetsbaar zijn. U wordt aanbevolen deze poorten goed te monitoren omdat de kans op aanvallen via deze poorten groter is. Als u niet-standaardservices gebruikt die niet-standaardnetwerkpoorten nodig hebben, kunnen deze netwerkpoorten ook het doelwit zijn van een aanvallende computer. U kunt lijsten maken met netwerkpoorten en programma's die netwerktoegang vragen. Deze poorten en programma's krijgen dan extra aandacht van de onderdelen Mail Anti-Virus, Web Anti-Virus en IM Anti-Virus wanneer ze het netwerkverkeer monitoren.

Instellingen voor monitoring van netwerkverkeer configureren

U kunt het volgende doen om de instellingen voor de monitoring van netwerkverkeer te configureren:

- Schakel de bewaking van alle netwerkpoorten in.
- Maak een lijst met bewaakte netwerkpoorten aan.
- Maak een lijst met programma's aan waarvoor alle netwerkpoorten worden gemonitord.

Bewaking van alle netwerkpoorten inschakelen

Zo schakelt u de bewaking van alle netwerkpoorten in:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Antivirusbescherming**.
   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Selecteer in het gedeelte **Bewaakte poorten** de optie **Alle netwerkpoorten bewaken**.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een lijst met bewaakte netwerkpoorten aanmaken

Zo maakt u een lijst met bewaakte netwerkpoorten aan:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Antivirusbescherming**.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Selecteer in het gedeelte **Gemonitorde poorten** de optie **Alleen geselecteerde poorten bewaken**.
4. Klik op de knop **Instellingen**.

   Het venster **Netwerkpoorten** wordt geopend. In het venster **Netwerkpoorten** ziet u een lijst met netwerkpoorten die normaal worden gebruikt voor de verzending van e-mail en netwerkverkeer. Deze lijst met netwerkpoorten wordt bij het pakket van Kaspersky Endpoint Security meegeleverd.
5. Doe in de lijst met netwerkpoorten het volgende:

   - Schakel de selectievakjes in naast de netwerkpoorten die u in de lijst met bewaakte netwerkpoorten wilt opnemen.

     Standaard zijn de selectievakjes naast alle netwerkpoorten in het venster **Netwerkpoorten** ingeschakeld.
   - Schakel de selectievakjes uit naast de netwerkpoorten die u uit de lijst met bewaakte netwerkpoorten wilt uitsluiten.
6. Als een netwerkpoort niet in de lijst met netwerkpoorten wordt weergegeven, voegt u die toe door het volgende te doen:

   a. Klik onder de lijst met netwerkpoorten op de koppeling **Toevoegen** om het venster **Netwerkpoort** te openen.

   b. Voer het nummer van de netwerkpoort in het veld **Poort** in.

   c. Voer de naam van de netwerkpoort in het veld **Beschrijving** in.

   d. Klik op **OK**.

      Het venster **Netwerkpoort** wordt gesloten. De recent toegevoegde netwerkpoort wordt op het einde in de lijst met netwerkpoorten weergegeven.
7. Klik in het venster **Netwerkpoorten** op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Wanneer het FTP-protocol in de passieve modus werkt, kan de verbinding tot stand worden gebracht via een willekeurige netwerkpoort die niet aan de lijst met bewaakte netwerkpoorten is toegevoegd. Om zulke verbindingen te beschermen, schakelt u het selectievakje **Alle netwerkpoorten bewaken** in het gedeelte **Gemonitorde poorten** in of configureert u de bewaking van alle poorten voor programma's die de FTP-verbinding tot stand brengen.

Een lijst met programma's aanmaken waarvoor alle netwerkpoorten worden gemonitord

U kunt een lijst met programma's aanmaken waarvoor Kaspersky Endpoint Security alle netwerkpoorten monitort.

We raden aan dat u alle programma's die gegevens verzenden of ontvangen via het FTP-protocol toevoegt aan de lijst met programma's waarvoor Kaspersky Endpoint Security alle netwerkpoorten monitort.

Zo maakt u een lijst met programma's aan waarvoor alle netwerkpoorten worden gemonitord:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Antivirusbescherming**.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Selecteer in het gedeelte **Gemonitorde poorten** de optie **Alleen geselecteerde poorten bewaken**.
4. Klik op de knop **Instellingen**.

   Het venster **Netwerkpoorten** wordt geopend.
5. Schakel het selectievakje **Bewaak alle poorten voor de opgegeven programma's** in.
6. Doe in de lijst met programma's onder het selectievakje **Bewaak alle poorten voor de opgegeven programma's** het volgende:

   - Schakel de selectievakjes in naast de namen van programma's waarvoor u alle netwerkpoorten wilt monitoren.

     Standaard zijn de selectievakjes naast alle programma's in het venster **Netwerkpoorten** ingeschakeld.
   - Schakel de selectievakjes uit naast de namen van programma's waarvoor u niet alle netwerkpoorten wilt monitoren.
7. Als een programma niet is opgenomen in de lijst met programma's, voegt u het als volgt toe:

   a. Klik op de koppeling **Toevoegen** onder de lijst met programma's en open het contextmenu.

   b. Selecteer in het contextmenu de manier waarop u het programma wilt toevoegen aan de lijst met programma's:

      - Om een programma te selecteren uit de lijst met programma's die op de computer zijn geïnstalleerd, selecteert u de opdracht **Programma's**. Het venster **Programma selecteren** wordt geopend. Hierin kunt u de naam van het programma opgeven.
      - Om de locatie van het uitvoerbare bestand van het programma op te geven, selecteert u de opdracht **Bladeren**. Het standaardvenster **Openen** wordt in Microsoft Windows geopend. Hierin kunt u de naam van het uitvoerbare bestand van het programma opgeven.

      Het venster **Programma** wordt geopend nadat u het programma hebt geselecteerd.

   c. Typ in het veld **Naam** een naam voor het geselecteerde programma.

   d. Klik op **OK**.

      Het venster **Programma** wordt gesloten. Het programma dat u hebt toegevoegd wordt op het einde van de lijst met programma's weergegeven.
8. Klik in het venster **Netwerkpoorten** op **OK**.
9. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Databases en softwaremodules van het programma bijwerken

In deze sectie vindt u informatie over updates voor de databases en de programmamodules (ook gewoon "updates" genoemd) en instructies voor de configuratie van de update-instellingen.

Over het bijwerken van de databases en programmamodules

Het bijwerken van de databases en programmamodules van Kaspersky Endpoint Security zorgt voor een up-to-date bescherming op de computer. Nieuwe virussen en andere soorten malware duiken elke dag wereldwijd op. De databases van Kaspersky Endpoint Security bevatten informatie over bedreigingen en methoden om ze onschadelijk te maken. Voor een snelle bedreigingsdetectie wordt u aanbevolen de databases en programmamodules regelmatig bij te werken.

Voor periodieke updates hebt u een actieve licentie nodig. Zonder actieve licentie kunt u maar één keer een update uitvoeren.

De voornaamste updatebron voor Kaspersky Endpoint Security zijn de updateservers van Kaspersky.

De computer moet verbonden zijn met het internet om het updatepakket te downloaden vanaf de updateservers van Kaspersky. Standaard worden de instellingen voor de internetverbinding automatisch bepaald. Als u een proxyserver gebruikt, moet u de instellingen van de verbinding aanpassen.

Tijdens het bijwerken worden de volgende objecten gedownload en geïnstalleerd op de computer:

- De databases van Kaspersky Endpoint Security. De computerbescherming wordt geleverd aan de hand van databases die definities van virussen en andere bedreigingen bevatten, alsook methoden om ze onschadelijk te maken. De beschermingsonderdelen gebruiken deze informatie wanneer ze geïnfecteerde bestanden op de computer zoeken en onschadelijk maken. De databases worden voortdurend bijgewerkt met records van nieuwe bedreigingen en methoden om ze onschadelijk te maken. Daarom raden we aan dat u de databases regelmatig bijwerkt.

  Naast de databases van Kaspersky Endpoint Security worden ook de netwerkstuurprogramma's bijgewerkt waarmee de programmaonderdelen het netwerkverkeer onderscheppen.

- Programmamodules. Naast de databases van Kaspersky Endpoint Security kunt u ook de programmamodules bijwerken. Het bijwerken van de programmamodules verhelpt kwetsbaarheden in Kaspersky Endpoint Security, voegt nieuwe functies toe of verbetert bestaande functies.

Tijdens het bijwerken worden de programmamodules en de databases op de computer vergeleken met de up-tot-date versie op de updatebron. Als uw huidige databases en programmamodules verschillen van de overeenkomstige up-tot-date versies, wordt het ontbrekende deel van de updates op de computer geïnstalleerd.

Contextuele Help-bestanden kunnen samen met de updates voor de programmamodules worden bijgewerkt.

Als de databases verouderd zijn, is het updatepakket mogelijk groot waardoor het netwerkverkeer hoger zal zijn (tot wel tientallen megabytes meer).

De informatie over de huidige status van de Kaspersky Endpoint Security-databases ziet u in **Update**, in het gedeelte **Taken** op het tabblad **Bescherming en controle** van het hoofdvenster van het programma.

Informatie over de resultaten van de updates en over alle gebeurtenissen tijdens de uitvoering van de updatetaak wordt in het rapport van Kaspersky Endpoint Security geregistreerd.

Over updatebronnen

Een *updatebron* is een bron die updates voor de databases en de programmamodules van Kaspersky Endpoint Security bevat.

Updatebronnen zijn onder andere de server van Kaspersky Security Center, Kaspersky-updateservers en netwerk- of lokale mappen.

Als u geen toegang tot de Kaspersky-updateservers hebt (de toegang tot internet is bijvoorbeeld beperkt), kunt u contact opnemen met het hoofdkantoor van Kaspersky om contactgegevens van Kaspersky-partners te vragen. De Kaspersky-partners geven u dan de updates op een verwisselbare schijf.

Wanneer u updates op een verwisselbare schijf bestelt, vermeldt u best ook of u updates voor de programmamodules wenst.

Update-instellingen configureren

U kunt de volgende acties uitvoeren om de update-instellingen te configureren:

- Voeg nieuwe updatebronnen toe.

  Op de standaardlijst met updatebronnen staan Kaspersky Security Center en Kaspersky-updateservers. U kunt andere updatebronnen aan de lijst toevoegen. U kunt HTTP-/FTP-servers en gedeelde mappen als updatebronnen opgeven.

  Als verschillende bronnen als updatebronnen zijn geselecteerd, probeert Kaspersky Endpoint Security met de ene na de andere verbinding te maken, te beginnen boven aan de lijst, en voert het dan de updatetaak uit door het updatepakket vanaf de eerste beschikbare bron op te halen.

  Als u een bron buiten het netwerk kiest als updatebron, moet u verbonden zijn met het internet om een update uit te voeren.

- Selecteer de regio van de Kaspersky-updateserver.

  Als u Kaspersky-updateservers als updatebron gebruikt, kunt u de Kaspersky-updateserver voor de download van het updatepakket selecteren. De Kaspersky-updateservers bevinden zich in verschillende landen. Door de dichtstbijzijnde Kaspersky-updateservers te gebruiken worden de updatepakketten sneller opgehaald.

  Standaard gebruikt het programma informatie over de huidige regio vanuit het register van het besturingssysteem.

- Configureer het bijwerken van Kaspersky Endpoint Security vanuit een gedeelde map.

  Om internetverkeer te besparen, kunt u de updates voor Kaspersky Endpoint Security zodanig configureren dat computers in het netwerk de updates in een gedeelde map ophalen. Hiervoor ontvangt een van de computers in het netwerk een up-to-date updatepakket vanaf de Kaspersky Security Center-server of vanaf de Kaspersky-updateservers en kopieert die computer het ontvangen updatepakket naar een gedeelde map. Daarna kunnen andere computers in het netwerk het updatepakket in deze gedeelde map ophalen.

- Selecteer de uitvoermodus voor de updatetaak.

Als de updatetaak om een willekeurige reden niet kan worden uitgevoerd (de computer is bijvoorbeeld uitgeschakeld op dat moment), kunt u instellen dat de overgeslagen taak automatisch moet worden gestart zodra dit mogelijk is.

U kunt de start van de updatetaak na de start van het programma uitstellen als u de uitvoermodus **Volgens schema** voor de updatetaak selecteert en als de starttijd van Kaspersky Endpoint Security overeenkomt met het startschema van de updatetaak. De updatetaak kan pas worden gestart wanneer het opgegeven tijdsinterval na de opstart van Kaspersky Endpoint Security is verstreken.

- Stel in dat de updatetaak met de rechten van een ander gebruikersaccount moet worden uitgevoerd.

Een updatebron toevoegen

Zo voegt u een updatebron toe:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.
3. Klik in het gedeelte **Uitvoermodus en updatebron** op de knop **Updatebron**.

   Hiermee opent u het tabblad **Bron** in het venster **Update**.
4. Klik op het tabblad **Bron** op de knop **Toevoegen**.

   Het venster **Updatebron selecteren** wordt geopend.
5. Selecteer in het venster **Updatebron selecteren** een map met het updatepakket of voer het volledige pad naar de map in het veld **Bron** in.
6. Klik op **OK**.
7. Klik in het venster **Update** op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regio van updateserver selecteren

Zo selecteert u de regio van de updateserver:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.
3. Klik in het gedeelte **Uitvoermodus en updatebron** op de knop **Updatebron**.

   Hiermee opent u het tabblad **Bron** in het venster **Update**.
4. Op het tabblad **Bron** kiest u in het gedeelte **Regionale instellingen** de optie **Selecteer uit de lijst**.

5. Selecteer in de vervolgkeuzelijst het dichtstbijzijnde land.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bijwerken vanuit een gedeelde map configureren

Volg deze stappen om het bijwerken van Kaspersky Endpoint Security vanuit een gedeelde map te configureren:

1. Schakel het kopiëren van een updatepakket naar een gedeelde map in op een van de computers in het lokale netwerk.
2. Configureer het bijwerken van Kaspersky Endpoint Security vanuit de opgegeven gedeelde map voor de resterende computers in het lokale netwerk.

Zo schakelt u het kopiëren van het updatepakket naar de gedeelde map in:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.
3. Schakel in het gedeelte **Extra** het selectievakje **Updates naar map kopiëren** in.
4. Geef het pad naar de gedeelde map op waar het updatepakket moet worden geplaatst. U kunt dit doen op één van de volgende manieren:
   - Voer het pad naar de gedeelde map in het veld onder het selectievakje **Updates naar map kopiëren** in.
   - Klik op de knop **Bladeren**. Selecteer vervolgens in het geopende venster **Map selecteren** de noodzakelijke map en klik op **OK**.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Zo configureert u het bijwerken van Kaspersky Endpoint Security vanuit een gedeelde map:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.
3. Klik in het gedeelte **Uitvoermodus en updatebron** op de knop **Updatebron**.

   Hiermee opent u het tabblad **Bron** in het venster **Update**.
4. Klik op het tabblad **Bron** op de knop **Toevoegen**.

   Het venster **Updatebron selecteren** wordt geopend.
5. Selecteer in het venster **Updatebron selecteren** de gedeelde map dat het updatepakket bevat of voer het volledige pad naar de gedeelde map in het veld **Bron** in.

6. Klik op **OK**.

7. Schakel op het tabblad **Bron** de selectievakjes uit naast de namen van de updatebronnen die u niet als de gedeelde map hebt opgegeven.

8. Klik op **OK**.

9. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De uitvoermodus van de updatetaak selecteren

Zo selecteert u de uitvoermodus van de updatetaak:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.

3. Klik op de knop **Uitvoermodus**.

   Het tabblad **Uitvoermodus** in het venster **Update** wordt geopend.

4. Selecteer in het gedeelte **Uitvoermodus** een van de volgende opties voor het starten van een updatetaak:

   - Als u Kaspersky Endpoint Security de updatetaak wilt laten uitvoeren ongeacht of er een updatepakket beschikbaar is op de updatebron, selecteert u **Automatisch**. De frequentie van de controles op updatepakketten door Kaspersky Endpoint Security neemt tijdens virusuitbraken toe en neemt anders af.

   - Selecteer **Handmatig** als u een updatetaak handmatig wilt starten.

   - Selecteer **Volgens schema** als u een opstartschema voor de updatetaak wilt configureren.

5. Voer een van de volgende acties uit:

   - Als u de optie **Automatisch** of **Handmatig** hebt geselecteerd, gaat u naar stap 6 in de instructies.

   - Als u de optie **Volgens schema** hebt geselecteerd, geeft u de instellingen van het schema voor de uitvoering van de updatetaak op. Hiertoe doet u het volgende:

     a. Geef in de vervolgkeuzelijst **Frequentie** op wanneer u de updatetaak wilt starten. Selecteer een van de volgende opties: **Minuten**, **Uren**, **Dagen**, **Elke week**, **Op een opgegeven tijdstip**, **Elke maand** of **Na programmastart**.

     b. Afhankelijk van de geselecteerde optie in de vervolgkeuzelijst **Frequentie** geeft u waarden voor de instellingen op die bepalen wanneer de updatetaak moet worden gestart.

     c. Geef in het veld **Stel start na programmastart uit met** op hoelang de start van de updatetaak wordt uitgesteld na de start van Kaspersky Endpoint Security.

     > Als de optie **Na programmastart** in de vervolgkeuzelijst **Frequentie** wordt geselecteerd, is het veld **Stel start na programmastart uit met** niet beschikbaar.

d. Als u Kaspersky Endpoint Security overgeslagen updatetaken zo snel mogelijk wilt laten uitvoeren, schakelt u het selectievakje **Overgeslagen taken starten** in.

> Als **Uren**, **Minuten** of **Na programmastart** is geselecteerd in de vervolgkeuzelijst **Frequentie**, is het selectievakje **Overgeslagen taken starten** niet beschikbaar.

6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een updatetaak met de rechten van een ander gebruikersaccount starten

Standaard wordt de updatetaak van Kaspersky Endpoint Security gestart namens de gebruiker wiens account u hebt gebruikt om u bij het besturingssysteem aan te melden. Kaspersky Endpoint Security kan echter worden bijgewerkt vanaf een updatebron waartoe u geen toegang hebt omdat de gebruiker niet over de vereiste rechten beschikt (bijvoorbeeld vanuit een gedeelde map dat een updatepakket bevat) of omdat de gebruiker niet over de rechten van een bevoegde gebruiker van de proxyserver beschikt. In de instellingen van Kaspersky Endpoint Security kunt u een gebruiker opgeven die over zulke rechten beschikt en de updatetaak van Kaspersky Endpoint Security starten met dat gebruikersaccount.

Zo start u een updatetaak met een ander gebruikersaccount:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.
3. Klik in het gedeelte **Uitvoermodus en updatebron** op de knop **Uitvoermodus**.

   Het tabblad **Uitvoermodus** in het venster **Update** wordt geopend.
4. Schakel op het tabblad **Uitvoermodus** in het gedeelte **Gebruiker** het selectievakje **Voer taak uit als** in.
5. Voer in het veld **Naam** de naam van het gebruikersaccount in waarvan u de rechten nodig hebt om toegang tot de updatebron te krijgen.
6. Voer in het veld **Wachtwoord** het wachtwoord van de gebruiker in wiens rechten u nodig hebt om toegang tot de updatebron te krijgen.
7. Klik op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Updates voor programmamodules configureren

Zo configureert u updates voor programmamodules:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.

   Rechts in het venster ziet u de update-instellingen van het programma.

3. Doe in het gedeelte **Extra** een van het volgende:

   - Schakel het selectievakje **Updates voor programmamodules downloaden** in als u het programma ook updates voor programmamodules wilt laten opnemen in de updatepakketten.
   - Anders schakelt u het selectievakje **Updates voor programmamodules downloaden** uit.

4. Als tijdens de vorige stap het selectievakje **Updates voor programmamodules downloaden** werd ingeschakeld, geeft u de voorwaarden op waaronder het programma de updates voor de programmamodules moet installeren.

   - Selecteer de optie **Essentiële en goedgekeurde updates installeren** als u wilt dat het programma essentiële updates voor programmamodules automatisch installeert, en andere updates wanneer hun installatie is goedgekeurd, via de lokale programma-interface of Kaspersky Security Center.
   - Selecteer de optie **Alleen goedgekeurde updates installeren** als u wilt dat het programma via de lokale programma-interface of Kaspersky Security Center updates voor programmamodules installeert nadat de installatie ervan is goedgekeurd.

5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een updatetaak starten en stoppen

U kunt een updatetaak van Kaspersky Endpoint Security altijd starten of stoppen, ongeacht de geselecteerde uitvoermodus voor de updatetaak.

Voor het downloaden van een updatepakket vanaf Kaspersky-servers hebt u een internetverbinding nodig.

Zo start of stopt u een updatetaak:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Taken**.

   Het gedeelte **Taken** wordt geopend.

4. Klik rechts om het contextmenu van de regel met de naam van de updatetaak weer te geven.

   Door te klikken op deze regel opent u een menu met acties die u op de updatetaak kunt uitvoeren.

5. Voer een van de volgende acties uit:

   - Selecteer **Update starten** in het menu als u de updatetaak wilt starten.

     De voortgang van de updatetaak die u rechts van de knop **Update** ziet, wijzigt in *Actief*.

   - Selecteer **Update stoppen** in het menu als u de updatetaak wilt stoppen.

     De voortgang van de updatetaak die u rechts van de knop **Update** ziet, wijzigt in *Gestopt*.

Meest recente update terugdraaien

Nadat de databases en de programmamodules voor het eerst zijn bijgewerkt, wordt de functie voor het terugdraaien van de databases en de programmamodules naar hun vorige versies beschikbaar.

Telkens als een gebruiker het updateproces start, maakt Kaspersky Endpoint Security een back-up van de huidige databases en de programmamodules. Zo kunt u indien nodig de databases en de programmamodules terugdraaien naar hun vorige versies. Het terugdraaien van de meest recente update is bijvoorbeeld handig wanneer de nieuwe versie van de databases een ongeldige definitie bevat die ervoor zorgt dat Kaspersky Endpoint Security een veilig programma blokkeert.

Zo draait u de meest recente update terug:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Taken**.
   Het gedeelte **Taken** wordt geopend.
4. Klik rechts om het contextmenu van de taak **Update** te openen.
5. Selecteer **Update ongedaan maken**.

Proxyserverinstellingen configureren

Zo configureert u de proxyserverinstellingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Update**.
   Rechts in het venster ziet u de update-instellingen van het programma.
3. Klik in het gedeelte **Proxyserver** op de knop **Instellingen**.
   Het venster **Proxyserverinstellingen** wordt geopend.
4. Schakel in het venster **Proxyserverinstellingen** het selectievakje **Proxyserver gebruiken** in.
5. Geef de proxyserverinstellingen op.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

U kunt ook de proxyserverinstellingen in het hoofdvenster van het programma configureren. Ga hiervoor naar het tabblad **Instellingen** in het gedeelte **Geavanceerde instellingen**.

Computer scannen

Een virusscan is noodzakelijk om de computer veilig te houden. Start daarom regelmatig een virusscan en voorkom de mogelijke verspreiding van malware die niet door de beschermingsonderdelen wordt gedetecteerd wegens een te laag beschermingsniveau of andere redenen.

In deze sectie leest u meer over de specifieke eigenschappen en instellingen van scantaken, beveiligingsniveaus, scanmethoden en -technologieën en instructies voor het omgaan met bestanden die Kaspersky Endpoint Security niet tijdens een virusscan heeft verwerkt.

Over scantaken

Voor het zoeken naar virussen en de controle van de integriteit van de programmamodules beschikt Kaspersky Endpoint Security over de volgende taken:

- **Volledige Scan**. Een grondige scan van de hele computer. Standaard scant Kaspersky Endpoint Security de volgende objecten:
  - Kernelgeheugen
  - Objecten die bij de opstart van het besturingssysteem worden geladen
  - Opstartsectoren
  - Back-up van het besturingssysteem
  - Alle harde en verwisselbare schijven
- **Kritieke Gebiedenscan**. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.
- **Aangepaste Scan**. Kaspersky Endpoint Security scant de objecten die door de gebruiker worden geselecteerd. U kunt een willekeurig object uit de volgende lijst scannen:
  - Kernelgeheugen
  - Objecten die bij de opstart van het besturingssysteem worden geladen
  - Back-up van het besturingssysteem
  - Outlook-mailbox
  - Alle harde, verwisselbare en netwerkschijven
  - Een geselecteerd bestand
- **Integriteitscontrole**. Kaspersky Endpoint Security controleert de programmamodules op beschadiging of wijzigingen.

De taken Volledige Scan en Kritieke Gebiedenscan zijn enigszins verschillend van de andere taken. Bij deze taken wordt u aanbevolen het scanbereik niet te bewerken:

Na de start van de scantaken wordt de voortgang van hun voltooiing weergegeven in het veld naast de naam van de actieve scantaak, in het gedeelte **Taken** op het tabblad **Bescherming en controle** in het hoofdvenster van Kaspersky Endpoint Security.

Informatie over de scanresultaten en gebeurtenissen die zich tijdens de uitvoering van de scantaken voordeden wordt in een rapport van Kaspersky Endpoint Security geregistreerd.

Een scantaak starten of stoppen

U kunt altijd een scantaak starten of stoppen, ongeacht de geselecteerde uitvoermodus voor de scantaak.

Zo start of stopt u een scantaak:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Taken**.

   Het gedeelte **Taken** wordt geopend.
4. Klik rechts om het contextmenu van de regel met de naam van de scantaak weer te geven.

   Een menu met acties voor de scantaak wordt geopend.
5. Voer een van de volgende acties uit:

   - Selecteer **Scan starten** in het menu als u de scantaak wilt starten.

     De voortgang van de taak rechts van de knop met de naam van deze scantaak wijzigt in *Actief*.
   - Selecteer **Scan stoppen** in het menu als u de scantaak wilt stoppen.

     De voortgang van de taak rechts van de knop met de naam van deze scantaak wijzigt in *Gestopt*.

Instellingen van scantaken configureren

U kunt het volgende doen om de instellingen van scantaken te configureren:

- Wijzig het beschermingsniveau.

  U kunt een van de vooraf ingestelde beschermingsniveaus selecteren of instellingen voor een beschermingsniveau handmatig configureren. Als u de instellingen van een beschermingsniveau wijzigt, kunt u altijd de aanbevolen instellingen van het beschermingsniveau herstellen.
- Wijzig de actie die Kaspersky Endpoint Security uitvoert als het een geïnfecteerd bestand vindt.
- Bewerk het scanbereik.

  U kunt het scanbereik vergroten of verkleinen door scanobjecten toe te voegen of te verwijderen of door te wijzigen welke soort bestanden u wilt scannen.
- Optimaliseer de scans.

U kunt het scannen van bestanden optimaliseren: kort de duur van scans in en laat Kaspersky Endpoint Security sneller werken. Hiertoe scant u gewoon de nieuwe bestanden en de bestanden die sinds de vorige scan zijn gewijzigd. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing. U kunt ook een limiet voor het scannen van een enkel bestand instellen. Wanneer het opgegeven tijdsinterval is verstreken, sluit Kaspersky Endpoint Security het bestand uit van de huidige scan (behalve archieven en objecten met meerdere bestanden).

U kunt ook het gebruik van de iChecker- en iSwift-technologieën inschakelen. Deze technologieën optimaliseren de snelheid waarmee bestanden worden gescand door de bestanden die sinds de laatste scan niet zijn gewijzigd uit te sluiten.

- Configureer het scannen van samengestelde bestanden.
- Configureer het gebruik van scanmethoden.

  Kaspersky Endpoint Security gebruikt een analyse op basis van definities als deze functie is ingeschakeld. Tijdens de analyse op basis van definities controleert Kaspersky Endpoint Security of het gevonden object in de database voorkomt. Op aanbeveling van de Kaspersky-experts is de analyse op basis van definities altijd ingeschakeld.

  Om de doeltreffendheid van de bescherming te verhogen, kunt u de heuristische analyse gebruiken. Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van objecten in het besturingssysteem. De heuristische analyse kan kwaadaardige objecten vinden die momenteel niet voorkomen in de database van Kaspersky Endpoint Security.

- Selecteer de uitvoermodus voor de scantaak.

  Als de scantaak om een willekeurige reden niet kan worden uitgevoerd (de computer is bijvoorbeeld uitgeschakeld op dat moment), kunt u instellen dat de overgeslagen taak automatisch moet worden gestart zodra dit mogelijk is.

  U kunt de scantaak na de opstart van het programma uitstellen als u de uitvoermodus **Volgens schema** voor de updatetaak hebt geselecteerd en als de starttijd van Kaspersky Endpoint Security overeenkomt met het uitvoerschema van de scantaak. De scantaak kan pas worden gestart wanneer het opgegeven tijdsinterval na de opstart van Kaspersky Endpoint Security is verstreken.

- Stel in dat de scantaak met een ander gebruikersaccount moet worden uitgevoerd.
- Geef instellingen op voor het scannen van verwisselbare schijven wanneer ze zijn aangesloten.

Het beschermingsniveau wijzigen

Kaspersky Endpoint Security gebruikt verschillende combinaties van instellingen om scantaken uit te voeren. Deze combinaties van instellingen die in het programma zijn opgeslagen, noemen we *beschermingsniveaus*. Er bestaan drie vooraf ingestelde beschermingsniveaus: **Hoog**, **Aanbevolen** en **Laag**. De instellingen van het beschermingsniveau **Aanbevolen** worden als optimaal beschouwd. Deze zijn aanbevolen door experts van Kaspersky.

Zo wijzigt u een beschermingsniveau:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Doe in het gedeelte **Beschermingsniveau** een van het volgende:

- Als u een van de vooraf ingestelde beschermingsniveaus wilt toepassen (**Hoog**, **Aanbevolen** of **Laag**), selecteert u het niveau met de schuifregelaar.
- Als u een aangepast beschermingsniveau wilt configureren, klikt u op de knop **Instellingen** en geeft u in het geopende venster met de naam van de scantaak de instellingen op.

  Nadat u een aangepast beschermingsniveau hebt geconfigureerd, wordt de naam van het beschermingsniveau in het gedeelte **Beschermingsniveau** gewijzigd in **Aangepast**.
- Als u het beschermingsniveau wilt wijzigen in **Aanbevolen**, klikt u op de knop **Standaard**.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De uit te voeren actie op geïnfecteerde bestanden wijzigen

Zo wijzigt u de actie die op geïnfecteerde bestanden moet worden uitgevoerd:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Selecteer in het gedeelte **Actie bij detectie van een bedreiging** de vereiste optie:
   - **Actie automatisch selecteren**.
   - **Actie uitvoeren**.
4. Als u tijdens de vorige stap de optie **Actie uitvoeren** hebt geselecteerd, schakelt u de volgende selectievakjes in:
   - Schakel het selectievakje **Desinfecteren** in als u Kaspersky Endpoint Security objecten wilt laten desinfecteren waarin bedreigingen zijn gevonden.

     Zelfs als deze optie wordt geselecteerd, past Kaspersky Endpoint Security de actie **Verwijderen** toe op bestanden die tot het Windows Store-programma behoren.
   - Schakel het selectievakje **Verwijderen** in als u Kaspersky Endpoint Security objecten wilt laten verwijderen waarin bedreigingen zijn gevonden.
   - Schakel de selectievakjes **Desinfecteren** en **Verwijderen** in als u wilt dat Kaspersky Endpoint Security probeert om objecten waarin bedreigingen zijn gevonden te desinfecteren en de objecten verwijdert die niet kunnen worden gedesinfecteerd.
   - Schakel de selectievakjes **Desinfecteren** en **Verwijderen** uit als u wilt dat Kaspersky Endpoint Security geen actie uitvoert op objecten waarin bedreigingen zijn gevonden maar gewoon een melding over de resultaten van de scan van deze objecten toont aan de gebruiker.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een lijst met te scannen objecten genereren

Om een lijst met te scannen objecten te genereren, kunt u een van de volgende twee methoden gebruiken:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

> Deze methode is alleen beschikbaar voor de taken **Volledige Scan** en **Kritieke Gebiedenscan**. De lijst met te scannen objecten voor de taak **Aangepaste Scan** kan alleen op het tabblad **Bescherming en controle** worden aangemaakt.

Zo maakt u een lijst met te scannen objecten aan op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Taken**.
   Het gedeelte **Taken** wordt geopend.
4. Klik rechts om het contextmenu van de regel met de taaknaam te openen en selecteer **Scanbereik**.
   Het venster **Scanbereik** wordt geopend.
5. Als u een nieuw object aan het scanbereik wilt toevoegen:
   a. Klik op de knop **Toevoegen**.
      Het venster **Scanbereik selecteren** wordt geopend.
   b. Selecteer het object en klik op **Toevoegen**.
      Alle geselecteerde objecten in het venster **Scanbereik selecteren** worden in de lijst **Scanbereik** weergegeven.
   c. Klik op **OK**.
6. Als u het pad naar een object in het scanbereik wilt wijzigen:
   a. Selecteer het object in het scanbereik.
   b. Klik op de knop **Bewerken**.
      Het venster **Scanbereik selecteren** wordt geopend.
   c. Voer het nieuwe pad naar het object in het scanbereik in.
   d. Klik op **OK**.
7. Als u een object uit het scanbereik wilt verwijderen:
   a. Selecteer het object dat u uit het scanbereik wilt verwijderen.

Om meerdere objecten te selecteren, selecteert u ze terwijl u de **CTRL**-toets ingedrukt houdt.

b. Klik op de knop **Verwijderen**.

Een venster wordt geopend waarin u de verwijdering kunt bevestigen.

c. Klik op **Ja** in het venster voor de verwijdering van de bevestiging.

U kunt geen objecten verwijderen of bewerken die in het standaard scanbereik zijn opgenomen.

8. Om een object uit te sluiten van het scanbereik, schakelt u het selectievakje naast het object in het venster **Scanbereik** uit.

Het object blijft in de lijst met objecten van het scanbereik staan maar wordt pas gescand wanneer de scantaak wordt uitgevoerd.

9. Klik op **OK**.

10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Zo maakt u een lijst met te scannen objecten aan vanuit het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak: **Volledige Scan** of **Kritieke Gebiedenscan**.

Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.

3. Klik op de knop **Scanbereik**.

Het venster **Scanbereik** wordt geopend.

4. Maak een lijst met te scannen objecten volgens stappen 5-10 van de bovenstaande instructies.

Het type van te scannen bestanden selecteren

U kunt de volgende twee methoden gebruiken om het type van de te scannen bestanden te selecteren:

- Op het tabblad **Bescherming en controle** van het hoofdvenster van het programma
- Vanuit het venster met de programma-instellingen

Deze methode is alleen beschikbaar voor de taken **Volledige Scan** en **Kritieke Gebiedenscan**. Het type van de te scannen bestanden voor de taak **Aangepaste Scan** kan alleen op het tabblad **Bescherming en controle** worden geselecteerd.

Zo selecteert u het type van de te scannen bestanden op het tabblad Bescherming en controle van het hoofdvenster van het programma:

1. Open het hoofdvenster van het programma.

2. Selecteer het tabblad **Bescherming en controle**.

3. Klik op het gedeelte **Taken**.

   Het gedeelte **Taken** wordt geopend.

4. Klik rechts om het contextmenu van de regel met de taaknaam te openen en selecteer **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.

5. Selecteer het tabblad **Bereik** in het venster met de naam van de geselecteerde scantaak.

6. Geef in het gedeelte **Bestandstypen** op welke bestanden u wilt scannen wanneer de geselecteerde scantaak wordt uitgevoerd:

   - Als u alle bestanden wilt scannen, selecteert u **Alle bestanden**.
   - Als u bestanden met indelingen die het meest kwetsbaar zijn voor infecties wilt scannen, selecteert u **Bestanden gescand op indeling**.
   - Als u bestanden met extensies die doorgaans het meest kwetsbaar zijn voor infecties wilt scannen, selecteert u **Bestanden gescand op extensie**.

   Wanneer u selecteert welke bestanden moeten worden gescand, moet u rekening houden met het volgende:

   - Er zijn bepaalde bestandsindelingen (zoals TXT) waarbij het risico op binnendringing van kwaadaardige code en de daaropvolgende activatie klein is. Tegelijkertijd bestaan er ook bestandsindelingen die (mogelijk) uitvoerbare code bevatten (zoals .exe, .dll en .doc). Het risico op binnendringing en de activatie van kwaadaardige code in zulke bestanden is groot.
   - Een indringer kan een virus of een ander kwaadaardig programma naar uw computer sturen in een uitvoerbaar bestand waarvan de extensie in .txt is gewijzigd. Als u het scannen van bestanden op extensie selecteert, slaat het programma dit bestand tijdens de scan over. Als het scannen van bestanden volgens indeling is geselecteerd, analyseert Anti-Virus voor bestanden de bestandsheader, ongeacht de extensie. Als deze analyse aangeeft dat het bestand normaal een EXE-indeling heeft, scant het programma het bestand.

7. Klik op **OK** in het venster met de naam van de scantaak.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Zo selecteert u het type van de te scannen bestanden in het venster met de programma-instellingen:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak: **Volledige Scan** of **Kritieke Gebiedenscan**.

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.

3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.

4. Selecteer het tabblad **Bereik** in het venster met de naam van de geselecteerde scantaak.

5. Volg stappen 5-7 van de bovenstaande instructies.

Het scannen van bestanden optimaliseren

Zo optimaliseert u het scannen van bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.
4. Selecteer in het geopende venster het tabblad **Bereik**.
5. Voer in het gedeelte **Scanoptimalisatie** de volgende acties uit:
   - Schakel het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** in.
   - Schakel het selectievakje **Sla bestanden over waarvan de scan langer duurt dan** in en geef de scanduur voor één bestand op (in seconden).
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Samengestelde bestanden scannen

Een vaak gebruikte techniek voor het verbergen van virussen en andere malware is de insluiting ervan in samengestelde bestanden zoals archieven of databases. Om virussen en andere malware te vinden die op deze manier zijn verborgen, moet het samengestelde bestand worden uitgepakt waardoor het scannen wordt vertraagd. U kunt de soorten samengestelde bestanden die moeten worden gescand beperken om zo de scan sneller te voltooien.

Zo configureert u het scannen van samengestelde bestanden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.
4. Selecteer in het geopende venster het tabblad **Bereik**.
5. Geef in het gedeelte **Scan van samengestelde bestanden** op welke samengestelde bestanden u wilt scannen: archieven, installatiepakketten, bestanden met een Office-indeling, bestanden met een e-mailindeling en archieven die met een wachtwoord beveiligd zijn.
6. Als het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** in het gedeelte **Scanoptimalisatie** is uitgeschakeld, klikt u op de koppeling **alles / nieuw** naast de naam van het type samengesteld bestand als u

voor elk type samengesteld bestand wilt opgeven of u alle bestanden van dit type of alleen nieuwe bestanden van dit type wilt scannen.

Deze koppeling verandert wanneer u er op klikt.

Als het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** is ingeschakeld, worden alleen nieuwe bestanden gescand.

7. Klik op de knop **Extra**.

   Het venster **Samengestelde bestanden** wordt geopend.

8. Doe in het gedeelte **Beperking van grootte** een van het volgende:

   - Als u geen grote samengestelde bestanden wilt uitpakken, schakelt u het selectievakje **Grote samengestelde bestanden niet uitpakken** in en geeft u de vereiste waarde in het veld **Maximale bestandsgrootte** op.
   - Als u grote samengestelde bestanden wilt uitpakken ongeacht de grootte ervan, schakelt u het selectievakje **Grote samengestelde bestanden niet uitpakken** uit.

   Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Grote samengestelde bestanden niet uitpakken** is ingeschakeld.

9. Klik op **OK**.
10. Klik op **OK** in het venster met de naam van de scantaak.
11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Scanmethoden gebruiken

Zo gebruikt u scanmethoden:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.

3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.

4. Selecteer in het geopende venster het tabblad **Extra**.
5. Als u wilt dat het programma een heuristische analyse tijdens de scantaak gebruikt, schakelt u in het gedeelte **Scanmethoden** het selectievakje Heuristische analyse in. Gebruik dan de schuifregelaar om het niveau van de heuristische analyse in te stellen: **Oppervlakkige scan**, **Gemiddelde scan** of **Gedetailleerde scan**.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Scantechnologieën gebruiken

Zo gebruikt u scantechnologieën:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste scantaak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Klik in het gedeelte **Beschermingsniveau** op de knop **Instellingen**.

   Een venster met de naam van de geselecteerde scantaak wordt geopend.
4. Selecteer in het geopende venster het tabblad **Extra**.
5. Schakel in het gedeelte **Scantechnologieën** de selectievakjes in naast de namen van de technologieën die u tijdens de scan wilt gebruiken.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Uitvoermodus voor de scantaak selecteren

Zo selecteert u de uitvoermodus voor de scantaak:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste taak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.
3. Klik op de knop **Uitvoermodus**.

   Een venster met de eigenschappen van de geselecteerde taak op het tabblad **Uitvoermodus** wordt geopend.
4. Selecteer in het gedeelte **Uitvoermodus** de uitvoermodus voor de taak: **Handmatig** of **Volgens schema**.
5. Als u de optie **Volgens schema** hebt geselecteerd, geeft u de instellingen van het schema op. Hiertoe doet u het volgende:

   a. Selecteer in de vervolgkeuzelijst **Frequentie** hoe vaak de taak moet worden uitgevoerd (**Minuten**, **Uren**, **Dagen**, **Elke week**, **Op een opgegeven tijdstip**, **Elke maand** of **Na programmastart**, **Na elke update**).

   b. Afhankelijk van de geselecteerde frequentie configureert u geavanceerde instellingen die het schema voor de uitvoering van de taak definiëren.

   c. Als u Kaspersky Endpoint Security overgeslagen scantaken zo snel mogelijk wilt laten starten, schakelt u het selectievakje **Overgeslagen taken starten** in.

Als de optie **Minuten**, **Uren**, **Na programmastart** of **Na elke update** is geselecteerd in de vervolgkeuzelijst **Frequentie**, is het selectievakje **Overgeslagen taken starten** niet beschikbaar.

a. Als u Kaspersky Endpoint Security een taak wilt laten onderbreken wanneer er weinig computerbronnen beschikbaar zijn, schakelt u het selectievakje **Alleen starten als de computer inactief is** in.

   Deze optie van het schema helpt de beschikbaarheid van de computerbronnen in stand te houden.

6. Klik op **OK**.

7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een scantaak via het account van een andere gebruiker starten

Standaard wordt een scantaak uitgevoerd met de bevoegdheden van het account waarbij de gebruiker zich heeft aangemeld in het besturingssysteem. Het kan echter gebeuren dat u een scantaak via een ander gebruikersaccount moet uitvoeren. U kunt een gebruiker met de juiste rechten opgeven in de instellingen van de scantaak en de scantaak via het account van deze gebruiker uitvoeren.

Zo configureert u de start van een scantaak via een ander gebruikersaccount:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster het subgedeelte met de naam van de vereiste taak (**Volledige Scan**, **Kritieke Gebiedenscan** of **Aangepaste Scan**).

   Rechts in het venster ziet u de instellingen van de geselecteerde scantaak.

3. Klik op de knop **Uitvoermodus**.

   Hiermee opent u een venster met de eigenschappen van de geselecteerde taak op het tabblad **Uitvoermodus**.

4. Schakel op het tabblad **Uitvoermodus** in het gedeelte **Gebruiker** het selectievakje **Voer taak uit als** in.

5. Voer in het veld **Naam** de naam van het gebruikersaccount in waarvan u de rechten nodig hebt om de scantaak te starten.

6. Voer in het veld **Wachtwoord** het wachtwoord van de gebruiker in wiens rechten u nodig hebt om de scantaak te starten.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Verwisselbare schijven scannen wanneer ze op de computer zijn aangesloten

Bepaalde kwaadaardige programma's buiten kwetsbaarheden in het besturingssysteem uit om zich te vermenigvuldigen via lokale netwerken en verwisselbare schijven. Met Kaspersky Endpoint Security kunt u verwisselbare schijven die zijn aangesloten op de computer scannen op virussen en andere malware.

Zo configureert u het scannen van verwisselbare schijven wanneer ze zijn aangesloten:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geplande taken**.

   De taakinstellingen worden rechts in het venster weergegeven.
3. In het gedeelte **Scan verwisselbare schijven bij aansluiting** selecteert u in de vervolgkeuzelijst **Actie bij aansluiting van verwisselbare schijf** de vereiste actie:

   - **Niet scannen**
   - **Gedetailleerde Scan**

     In deze modus scant Kaspersky Endpoint Security alle bestanden op de verwisselbare schijf, inclusief bestanden in samengestelde objecten.
   - **Snelle Scan**

     In deze modus scant Kaspersky Endpoint Security alleen bestanden die mogelijk geïnfecteerd kunnen raken en pakt het geen samengestelde objecten uit.
4. Als u wilt dat Kaspersky Endpoint Security alleen verwisselbare schijven scant die kleiner zijn dan de opgegeven waarde, schakelt u het selectievakje **Maximale grootte van verwisselbare schijven** in en geeft u een waarde in megabytes in het veld ernaast op.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Onverwerkte bestanden behandelen

In deze sectie vindt u instructies voor de behandeling van geïnfecteerde en waarschijnlijk geïnfecteerde bestanden die Kaspersky Endpoint Security niet heeft verwerkt tijdens het scannen van de computer op virussen en andere bedreigingen.

Over onverwerkte bestanden

Kaspersky Endpoint Security registreert informatie over bestanden die om een bepaalde reden niet zijn verwerkt. Deze informatie wordt in de vorm van gebeurtenissen in de lijst met onverwerkte bestanden vastgelegd.

Een geïnfecteerd bestand wordt als *verwerkt* beschouwd als Kaspersky Endpoint Security tijdens het scannen van de computer op virussen en andere bedreigingen een van de volgende acties op dit bestand uitvoert volgens de opgegeven programma-instellingen:

- Desinfecteren.
- Verwijderen.
- Verwijderen als desinfectie mislukt.

Een geïnfecteerd bestand wordt als *onverwerkt* beschouwd als Kaspersky Endpoint Security tijdens het scannen van de computer op virussen en andere bedreigingen om een bepaalde reden geen actie op dit bestand heeft uitgevoerd volgens de opgegeven programma-instellingen:

Deze situatie kan zich in de volgende gevallen voordoen:

- Het gescande bestand is niet beschikbaar (het staat bijvoorbeeld op een netwerkschijf of een verwisselbare schijf zonder schrijfbevoegdheden).
- De geselecteerde actie in het gedeelte **Actie bij detectie van een bedreiging** voor scantaken is **Melden** en de gebruiker selecteert de actie **Overslaan** wanneer een melding over het geïnfecteerde bestand wordt weergegeven.

U kunt de taak Aangepaste Scan handmatig starten voor bestanden in de lijst met onverwerkte bestanden nadat de databases en programmamodules zijn bijgewerkt. De bestandsstatus kan na de scan wijzigen. U moet mogelijk de nodige acties op de bestanden uitvoeren, afhankelijk van hun status.

U kunt bijvoorbeeld de volgende acties uitvoeren:

- Verwijder bestanden met de status *Geïnfecteerd*.
- Herstel geïnfecteerde bestanden met belangrijke informatie en herstel bestanden die als *Gedesinfecteerd* of *Niet geïnfecteerd* zijn gemarkeerd.
- Plaats bestanden met de status *Waarschijnlijk geïnfecteerd* in Quarantaine.

De lijst met onverwerkte bestanden beheren

De lijst met onverwerkte bestanden wordt als een tabel weergegeven.

U kunt de volgende bewerkingen uitvoeren voor onverwerkte bestanden:

- Bekijk de lijst met onverwerkte bestanden.
- Scan onverwerkte bestanden met de huidige versie van de Kaspersky Endpoint Security-databases en -modules.
- Herstel bestanden uit de lijst met onverwerkte bestanden naar hun originele mappen of naar een andere gewenste map (wanneer er niet naar de originele map kan worden geschreven).
- Verwijder bestanden uit de lijst met onverwerkte bestanden.
- Open de originele map van het onverwerkte bestand.

U kunt ook de volgende acties uitvoeren wanneer u gegevens in de tabel beheert:

- Filter gebeurtenissen met onverwerkte bestanden op een kolomwaarde of met aangepaste filtervoorwaarden.
- Gebruik de zoekfunctie voor gebeurtenissen met onverwerkte bestanden.
- Sorteer gebeurtenissen met onverwerkte bestanden.
- Wijzig de volgorde en de reeks kolommen die in de lijst met onverwerkte bestanden worden weergegeven.
- Groepeer gebeurtenissen met onverwerkte bestanden.

U kunt indien nodig de geselecteerde gebeurtenissen met onverwerkte bestanden kopiëren naar het klembord.

Een Aangepaste Scan voor onverwerkte bestanden starten

U kunt een Aangepaste Scan voor onverwerkte bestanden handmatig starten. U kunt de scan starten als de laatste scan bijvoorbeeld werd onderbroken of als u onverwerkte bestanden opnieuw wilt scannen na de meest recente update van de databases en de programmamodules.

Zo start u een Aangepaste Scan voor onverwerkte bestanden:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Onverwerkte bestanden**.
4. Selecteer in de tabel op het tabblad **Onverwerkte bestanden** een of verschillende gebeurtenissen die te maken hebben met bestanden die u wilt scannen.

   Om meerdere gebeurtenissen te selecteren, selecteert u ze terwijl u de **CTRL**-toets ingedrukt houdt.
5. Start de Aangepaste Scan op een van de volgende manieren:
   - Klik op de knop **Opnieuw scannen**.
   - Klik rechts om het contextmenu te openen en selecteer **Opnieuw scannen**.

Bestanden uit de lijst met onverwerkte bestanden verwijderen

Zo verwijdert u bestanden uit de lijst met onverwerkte bestanden:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Onverwerkte bestanden**.
4. Selecteer in de tabel op het tabblad **Onverwerkte bestanden** een of verschillende gebeurtenissen die te maken hebben met bestanden die u wilt verwijderen.

   Om meerdere gebeurtenissen te selecteren, selecteert u ze terwijl u de **CTRL**-toets ingedrukt houdt.
5. Verwijder bestanden op een van de volgende manieren:
   - Klik op de knop **Verwijderen**.
   - Klik rechts om het contextmenu te openen en selecteer **Verwijderen**.

Kwetsbaarheidsscan

In deze sectie vindt u informatie over de specifieke eigenschappen en instellingen van de taak Kwetsbaarheidsscan en instructies voor het beheer van de lijst met kwetsbaarheden die tijdens de kwetsbaarheidsscan zijn gevonden door Kaspersky Endpoint Security.

Informatie over kwetsbaarheden van actieve programma's bekijken

Informatie over kwetsbaarheden van actieve programma's is beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor werkstations. Deze informatie is niet beschikbaar als Kaspersky Endpoint Security is geïnstalleerd op een computer met Microsoft Windows voor bestandsservers.

Zo bekijkt u informatie over kwetsbaarheden van actieve programma's:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Open het gedeelte **Endpoint-controle**.
4. Klik op de knop **Programma-activiteitenbewaking**.

   Het venster **Controle van programmabevoegdheden** wordt geopend en het tabblad **Programma-activiteitenbewaking** word weergegeven. In de tabel **Programma-activiteitenbewaking** ziet u samenvattende informatie over de activiteit van actieve programma's in het besturingssysteem. De ernst van de kwetsbaarheid van actieve programma's zoals bepaald door het onderdeel Kwetsbaarheidsbewaking wordt in de kolom **Ernst van kwetsbaarheid** weergegeven.

Over de Kwetsbaarheidsscan

Kwetsbaarheden in het besturingssysteem worden mogelijk veroorzaakt door fouten in de programmering of het ontwerp, onveilige wachtwoorden of activiteit van malware. Tijdens het scannen op kwetsbaarheden analyseert het programma het besturingssysteem en zoekt het onjuiste en beschadigde instellingen van Microsoft en andere leveranciers.

Een kwetsbaarheidsscan voert een diagnostische scan van de beveiliging van het besturingssysteem uit en vindt softwarefuncties die indringers kunnen gebruiken om kwaadaardige objecten te verspreiden en toegang tot persoonlijke gegevens te krijgen.

Nadat de kwetsbaarheidsscan is gestart, wordt de voortgang ervan weergegeven in het veld naast de naam van de **kwetsbaarheidsscan** in het gedeelte **Taken** op het tabblad **Bescherming en controle** van het hoofdvenster van Kaspersky Endpoint Security.

De resultaten van de kwetsbaarheidsscan worden in rapporten geregistreerd.

De taak Kwetsbaarheidsscan starten of stoppen

U kunt de Kwetsbaarheidsscan altijd starten of stoppen, ongeacht de geselecteerde uitvoermodus voor de taak.

Zo start of stopt u de taak Kwetsbaarheidsscan:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Klik op het gedeelte **Taken**.

   Het gedeelte **Taken** wordt geopend.
4. Klik rechts om het contextmenu van de regel met de naam van de Kwetsbaarheidsscan weer te geven.

   Een menu met bewerkingen voor de taak Kwetsbaarheidsscan wordt geopend.
5. Voer een van de volgende acties uit:

   - Selecteer **Scan starten** in het menu om de Kwetsbaarheidsscan te starten.

     De voortgang van de taak rechts van de knop met de naam van de Kwetsbaarheidsscan wijzigt in *Actief*.
   - Selecteer **Scan stoppen** in het menu om de Kwetsbaarheidsscan te stoppen.

     De voortgang van de taak rechts van de knop met de naam van de Kwetsbaarheidsscan wijzigt in *Gestopt*.

Instellingen van Kwetsbaarheidsscan configureren

Om de instellingen van Kwetsbaarheidsscan te configureren, kunt u de volgende acties uitvoeren:

- Maak een bereik voor de Kwetsbaarheidsscan.

  U kunt het scanbereik vergroten of verkleinen door programma's die u wilt scannen op kwetsbaarheden toe te voegen of te verwijderen.
- Selecteer de uitvoermodus voor de Kwetsbaarheidsscan.

  Als de taak om een willekeurige reden niet kan worden uitgevoerd (de computer is bijvoorbeeld uitgeschakeld), kunt u instellen dat de overgeslagen taak automatisch moet worden gestart zodra dit mogelijk is.
- Stel in dat de taak met de rechten van een ander gebruikersaccount moet worden uitgevoerd.

  Standaard wordt een scantaak uitgevoerd met de bevoegdheden van het account waarbij de gebruiker zich heeft aangemeld in het besturingssysteem. Het kan echter gebeuren dat u een scantaak via een ander gebruikersaccount moet uitvoeren. U kunt een gebruiker met de juiste rechten opgeven in de instellingen van de taak en de taak via het account van deze gebruiker uitvoeren.

Het bereik van de Kwetsbaarheidsscan instellen

Het bereik van de Kwetsbaarheidsscan is een softwareleverancier of een pad naar de map waar de software is geïnstalleerd (bijvoorbeeld alle Microsoft-programma's die in de map 'Program Files' zijn geïnstalleerd).

Zo stelt u het bereik van de Kwetsbaarheidsscan in:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Kwetsbaarheidsscan**.

   Rechts in het venster ziet u de instellingen van de taak Kwetsbaarheidsscan.

3. In het gedeelte **Scanbereik**:

   a. Schakel het selectievakje **Microsoft** in als u Kaspersky Endpoint Security wilt laten zoeken naar kwetsbaarheden in Microsoft-programma's die op de computer zijn geïnstalleerd.

   b. Schakel het selectievakje **Andere ontwikkelaars** in als u Kaspersky Endpoint Security wilt laten zoeken naar kwetsbaarheden in alle geïnstalleerde programma's op de computer behalve Microsoft-programma's.

   c. Klik in het venster **Extra gebied voor Kwetsbaarheidsscan** op de knop **Instellingen**.

      Het venster **Bereik van Kwetsbaarheidsscan** wordt geopend.

   d. Het bereik van de kwetsbaarheidsscan instellen Gebruik hiervoor de knoppen **Toevoegen** en **Verwijderen**.

   e. Klik in het venster **Bereik van Kwetsbaarheidsscan** op **OK**.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De uitvoermodus voor de Kwetsbaarheidsscan selecteren

Zo selecteert u de uitvoermodus voor de Kwetsbaarheidsscan:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Kwetsbaarheidsscan**.

   Rechts in het venster ziet u de instellingen van de taak Kwetsbaarheidsscan.

3. Klik op de knop **Uitvoermodus**.

   Hiermee opent u het tabblad **Uitvoermodus** in het venster **Kwetsbaarheidsscan**.

4. Selecteer in het gedeelte **Uitvoermodus** een van de volgende opties voor het starten van de Kwetsbaarheidsscan:

   - Selecteer **Handmatig** als u de Kwetsbaarheidsscan handmatig wilt starten.
   - Selecteer **Volgens schema** als u een opstartschema voor de Kwetsbaarheidsscan wilt configureren.

5. Voer een van de volgende acties uit:

   - Als u de optie **Handmatig** hebt geselecteerd, gaat u naar stap 6 van deze instructies.
   - Als u de optie **Volgens schema** hebt geselecteerd, geeft u de opstartinstellingen voor de Kwetsbaarheidsscan op. Hiertoe doet u het volgende:

     a. Geef in de vervolgkeuzelijst **Frequentie** op wanneer u de Kwetsbaarheidsscan wilt starten. Selecteer een van de volgende opties: **Dagen**, **Elke week**, **Op een opgegeven tijdstip**, **Elke maand**, **Na programmastart** of **Na elke update**.

     b. Afhankelijk van de geselecteerde optie in de vervolgkeuzelijst **Frequentie** geeft u waarden voor de instellingen op die bepalen wanneer de Kwetsbaarheidsscan moet worden gestart.

c. Als u Kaspersky Endpoint Security overgeslagen kwetsbaarheidsscans zo snel mogelijk wilt laten starten, schakelt u het selectievakje **Overgeslagen taken starten** in.

> Als u **Na programmastart** of **Na elke update** hebt geselecteerd in de vervolgkeuzelijst **Frequentie**, is het selectievakje **Overgeslagen taken starten** niet beschikbaar.

6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De Kwetsbaarheidsscan met de rechten van een ander gebruikersaccount starten

Standaard wordt de Kwetsbaarheidsscan gestart met het account waarmee de gebruiker bij het besturingssysteem is aangemeld. Het kan echter gebeuren dat u de Kwetsbaarheidsscan met een ander gebruikersaccount moet starten. U kunt een gebruiker met deze rechten opgeven in de instellingen van de Kwetsbaarheidsscan en de Kwetsbaarheidsscan met het account van deze gebruiker starten.

Zo configureert u de start van de Kwetsbaarheidsscan met een ander gebruikersaccount:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Kwetsbaarheidsscan**.

   Rechts in het venster ziet u de instellingen van de taak Kwetsbaarheidsscan.
3. Klik op de knop **Uitvoermodus**.

   Hiermee opent u het tabblad **Uitvoermodus** in het venster **Kwetsbaarheidsscan**.
4. Schakel op het tabblad **Uitvoermodus** in het gedeelte **Gebruiker** het selectievakje **Voer taak uit als** in.
5. Voer in het veld **Naam** de accountnaam van de gebruiker in wiens rechten u nodig hebt om de Kwetsbaarheidsscan te starten.
6. Voer in het veld **Wachtwoord** het wachtwoord van de gebruiker in wiens rechten u nodig hebt om de Kwetsbaarheidsscan te starten.
7. Klik op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Lijst met kwetsbaarheden beheren

Tijdens het beheer van de lijst met kwetsbaarheden kunt u de volgende acties uitvoeren:

- Bekijk de lijst met kwetsbaarheden.
- Start de Kwetsbaarheidsscan opnieuw nadat u de databases en de programmamodules hebt bijgewerkt.

- Bekijk gedetailleerde informatie over de kwetsbaarheid en aanbevelingen voor het herstel ervan in een apart gedeelte.
- Verberg geselecteerde vermeldingen in de lijst met kwetsbaarheden.
- Filter de lijst met kwetsbaarheden op belang.
- Filter de lijst met kwetsbaarheden op de statuswaarden *Hersteld* en *Verborgen*.

U kunt ook de volgende acties uitvoeren wanneer u gegevens in de tabel beheert:

- Filter de lijst met kwetsbaarheden op kolomwaarden of op aangepaste filtervoorwaarden.
- Gebruik de zoekfunctie voor kwetsbaarheden.
- Sorteer vermeldingen in de lijst met kwetsbaarheden.
- Wijzig de volgorde en de indeling van kolommen die in de lijst met kwetsbaarheden worden weergegeven.
- Groepeer vermeldingen in de lijst met kwetsbaarheden.

Over de lijst met kwetsbaarheden

Kaspersky Endpoint Security registreert de resultaten van de taak Kwetsbaarheidsscan in de lijst met kwetsbaarheden.

Nadat u specifieke kwetsbaarheden hebt bekeken en de aanbevolen acties hebt uitgevoerd om ze te verhelpen, wijzigt Kaspersky Endpoint Security de status van de kwetsbaarheden in *Opgelost*.

Als u specifieke kwetsbaarheden niet in de lijst met kwetsbaarheden wilt weergegeven, kunt u ervoor kiezen om ze te verbergen. Kaspersky Endpoint Security wijst deze kwetsbaarheden de status *Verborgen* toe.

De lijst met kwetsbaarheden wordt als een tabel weergegeven. Elke rij van de tabel bevat de volgende informatie:

- Een pictogram dat de ernst van de kwetsbaarheid aangeeft. Kwetsbaarheden kunnen de volgende ernst hebben:
  - Pictogram . **Kritiek**. Deze ernst is van toepassing op zeer gevaarlijke kwetsbaarheden die onmiddellijk moeten worden opgelost. Indringers buiten kwetsbaarheden met deze ernst zeer vaak uit om het besturingssysteem van de computer te infecteren of om toegang tot de persoonlijke gegevens van de gebruiker te krijgen. Kaspersky raadt aan dat u onmiddellijk alle noodzakelijke stappen onderneemt om kwetsbaarheden met de ernst “Kritiek” op te lossen.
  - Pictogram . **Belangrijk**. Deze ernst is van toepassing op belangrijke kwetsbaarheden die snel moeten worden opgelost. Indringers kunnen kwetsbaarheden met deze ernst vaak uit. Indringers buiten kwetsbaarheden met de ernst “Belangrijk” momenteel niet uit. Kaspersky raadt aan dat u onmiddellijk alle noodzakelijke stappen onderneemt om kwetsbaarheden met de ernst “Belangrijk” op te lossen.
  - Pictogram . **Waarschuwing**. Deze ernst is van toepassing op kwetsbaarheden die op een later ogenblik kunnen worden opgelost. Zulke kwetsbaarheden kunnen later wel een veiligheidsrisico voor de beveiliging van de computer vormen.
- Kwetsbaarheid-ID.

- Naam het programma waarin de kwetsbaarheid is gevonden.
- Beknopte beschrijving van de kwetsbaarheid.
- Informatie over de leverancier van de software, zoals aangegeven in de digitale handtekening.
- Resultaat van de ondernomen acties om de kwetsbaarheid te verhelpen.

De Kwetsbaarheidsscan opnieuw starten

Als u informatie over eerder gevonden kwetsbaarheden wilt bijwerken, kunt u de Kwetsbaarheidsscan opnieuw starten. Wellicht moet u de scantaak opnieuw starten als de Kwetsbaarheidsscan om een bepaalde reden is onderbroken of als u de computer wilt scannen op kwetsbaarheden na de laatste update van de databases en programmamodules.

Zo start u de Kwetsbaarheidsscan opnieuw:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Kwetsbaarheden**.

   Op het tabblad **Kwetsbaarheden** ziet u een lijst met kwetsbaarheden die Kaspersky Endpoint Security tijdens de Kwetsbaarheidsscan heeft gevonden.
4. Klik in de rechterbenedenhoek van het venster **Opslag** op de knop **Opnieuw scannen**.

   Kaspersky Endpoint Security werkt gedetailleerde informatie over kwetsbaarheden in de lijst met kwetsbaarheden bij.

De status van een kwetsbaarheid die door de installatie van een voorgestelde patch is hersteld, wijzigt niet na een nieuwe kwetsbaarheidsscan.

Een kwetsbaarheid verhelpen

U kunt een kwetsbaarheid verhelpen door een update voor het besturingssysteem te installeren, de configuratie van het programma te wijzigen of door een patch voor het programma te installeren.

Gevonden kwetsbaarheden zijn mogelijk niet van toepassing op de geïnstalleerde programma's maar op hun kopieën. Een patch kan een kwetsbaarheid alleen verhelpen als het programma is geïnstalleerd.

Zo verhelpt u een kwetsbaarheid:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.

3. Selecteer in het venster **Opslag** het tabblad **Kwetsbaarheden**.

   Op het tabblad **Kwetsbaarheden** ziet u een lijst met kwetsbaarheden die Kaspersky Endpoint Security tijdens de Kwetsbaarheidsscan heeft gevonden.

4. Selecteer in de lijst met kwetsbaarheden de vermelding van de relevante kwetsbaarheid.

   Een gedeelte met informatie over deze kwetsbaarheid en aanbevelingen om die te verhelpen wordt onder aan de lijst met kwetsbaarheden geopend.

   De volgende informatie is beschikbaar voor elke geselecteerde kwetsbaarheid:

   - Naam het programma waarin de kwetsbaarheid is gevonden.
   - Versie van het programma waarin de kwetsbaarheid is gevonden.
   - Ernst van een kwetsbaarheid.
   - Kwetsbaarheid-ID.
   - Datum en tijd wanneer de kwetsbaarheid het laatst is gevonden.
   - Aanbevelingen om de kwetsbaarheid te verhelpen (bijvoorbeeld een koppeling naar een website met een update voor het besturingssysteem of een patch voor het programma).
   - Koppeling naar een website met een beschrijving van de kwetsbaarheid.

5. Om een gedetailleerde beschrijving van de kwetsbaarheid te bekijken, klikt u op de koppeling **Extra informatie** om een webpagina te openen waar u een beschrijving van het veiligheidsrisico van de geselecteerde kwetsbaarheid kunt lezen. Via de website www.secunia.com kunt u de noodzakelijke update voor de huidige versie van het programma downloaden en installeren.

6. Selecteer een van de volgende manieren om een kwetsbaarheid te verhelpen:

   - Als een of meer patches voor het programma beschikbaar zijn, installeert u de noodzakelijke patch door de instructies te volgen die naast de naam van de patch worden gegeven.
   - Als een update voor het besturingssysteem beschikbaar is, installeert u de noodzakelijke update door de instructies te volgen die naast de naam van de update worden gegeven.

   De kwetsbaarheid is na de installatie van de patch of de update verholpen. Kaspersky Endpoint Security wijst deze kwetsbaarheid een status toe die aangeeft dat de kwetsbaarheid is verholpen. De vermelding over de verholpen kwetsbaarheid wordt in de lijst met kwetsbaarheden in het grijs weergegeven.

7. Als u onder in het venster geen informatie ziet om een kwetsbaarheid te verhelpen, kunt u de Kwetsbaarheidsscan opnieuw starten nadat u de databases en de modules van Kaspersky Endpoint Security hebt bijgewerkt. Aangezien Kaspersky Endpoint Security het systeem op kwetsbaarheden scant met behulp van een database met kwetsbaarheden, verschijnt een vermelding over een opgeloste kwetsbaarheid mogelijk pas wanneer het programma is bijgewerkt.

Vermeldingen in de lijst met kwetsbaarheden verbergen

U kunt een geselecteerde kwetsbaarheid verbergen. Kaspersky Endpoint Security wijst de status *Verborgen* toe aan de geselecteerde vermeldingen in de lijst met kwetsbaarheden en die als verborgen zijn gemarkeerd. U kunt dan de lijst met kwetsbaarheden filteren op de statuswaarde *Verborgen*.

Zo verbergt u een vermelding in de lijst met kwetsbaarheden:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Kwetsbaarheden**.

   Op het tabblad **Kwetsbaarheden** ziet u een lijst met kwetsbaarheden die Kaspersky Endpoint Security tijdens de Kwetsbaarheidsscan heeft gevonden.
4. Selecteer in de lijst met kwetsbaarheden de vermelding over de kwetsbaarheid die u wilt verbergen.

   Een gedeelte met informatie over deze kwetsbaarheid en aanbevelingen om die te verhelpen wordt onder aan de lijst met kwetsbaarheden geopend.
5. Klik op de knop **Verbergen**.

   Kaspersky Endpoint Security wijst de status *Verborgen* aan de geselecteerde kwetsbaarheid toe. Vermeldingen over kwetsbaarheden met de status *Verborgen* worden naar het einde van de lijst met kwetsbaarheden verplaatst en in het grijs weergegeven.
6. Om een vermelding over een kwetsbaarheid in de lijst met kwetsbaarheden te verbergen, schakelt u het selectievakje **Verborgen** boven aan de lijst in.

De lijst met kwetsbaarheden filteren op ernst

Zo filtert u de lijst met kwetsbaarheden op ernst:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Kwetsbaarheden**.

   Op het tabblad **Kwetsbaarheden** ziet u een lijst met kwetsbaarheden die Kaspersky Endpoint Security tijdens de Kwetsbaarheidsscan heeft gevonden. Drie pictogrammen voor de ernst van de kwetsbaarheid (Waarschuwing, Belangrijk, Kritiek) worden boven in de lijst met kwetsbaarheden in de rij **Toon ernst** weergegeven. Door op deze pictogrammen te klikken kunt u de lijst met kwetsbaarheden filteren op ernst.
4. Klik op een, twee of drie pictogrammen van de ernst van de kwetsbaarheid. De kwetsbaarheden die overeenkomen met de geselecteerde ernst worden in de lijst weergegeven. Om kwetsbaarheden met een specifieke ernst niet meer weer te geven in de lijst, klikt u nogmaals op het pictogram van de relevante ernst. Als geen enkele ernst is geselecteerd, is de lijst met kwetsbaarheden leeg.

De opgegeven filtervoorwaarden voor kwetsbaarheden worden na het sluiten van het venster **Opslag** opgeslagen.

De lijst met kwetsbaarheden filteren op de statuswaarden Hersteld en Verborgen

Zo filtert u de lijst met kwetsbaarheden op de statuswaarden Hersteld en Verborgen:

1. Open het hoofdvenster van het programma.

2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.

3. Selecteer in het venster **Opslag** het tabblad **Kwetsbaarheden**.

   Op het tabblad **Kwetsbaarheden** ziet u een lijst met kwetsbaarheden die Kaspersky Endpoint Security tijdens de Kwetsbaarheidsscan heeft gevonden.

4. Selectievakjes die de status van de kwetsbaarheden aangeven worden naast de instelling **Toon kwetsbaarheden** weergegeven. Doe een van het volgende om de lijst met kwetsbaarheden te filteren op de status *Hersteld*:

   - Schakel het selectievakje **Hersteld** in om vermeldingen over verholpen kwetsbaarheden in de lijst met kwetsbaarheden weer te geven. Vermeldingen over verholpen kwetsbaarheden worden grijs weergegeven in de lijst met kwetsbaarheden.

   - Schakel het selectievakje **Hersteld** uit om vermeldingen over verholpen kwetsbaarheden in de lijst met kwetsbaarheden te verbergen.

5. Doe een van het volgende om de lijst met kwetsbaarheden te filteren op de status *Verborgen*:

   - Schakel het selectievakje **Verborgen** in om vermeldingen over verborgen kwetsbaarheden in de lijst met kwetsbaarheden weer te geven. Vermeldingen over verborgen kwetsbaarheden worden grijs weergegeven in de lijst met kwetsbaarheden.

   - Schakel het selectievakje **Verborgen** uit om vermeldingen over verborgen kwetsbaarheden in de lijst met kwetsbaarheden te verbergen.

De opgegeven filtervoorwaarden voor kwetsbaarheden worden na het sluiten van het venster **Opslag** niet opgeslagen.

Integriteit van programmamodules controleren

In deze sectie vindt u informatie over de specifieke eigenschappen en instellingen van de integriteitscontrole.

Over de integriteitscontrole

Kaspersky Endpoint Security controleert de programmamodules in de installatiemap van het programma op beschadiging of wijzigingen. Als een programmamodule een onjuiste digitale handtekening heeft, wordt de module als beschadigd beschouwd.

Nadat de integriteitscontrole is gestart, wordt de voortgang ervan weergegeven in het veld naast de naam van de taak in het gedeelte **Taken** op het tabblad **Bescherming en controle** van het hoofdvenster van Kaspersky Endpoint Security.

De resultaten van de integriteitscontrole worden in rapporten vastgelegd.

Een integriteitscontrole starten of stoppen

U kunt een integriteitscontrole altijd starten of stoppen, ongeacht de geselecteerde uitvoermodus voor de taak.

Zo start of stopt u een integriteitscontrole:

1. Open het hoofdvenster van het programma.
2. Selecteer het tabblad **Bescherming en controle**.
3. Open het gedeelte **Taken**.
4. Klik rechts om het contextmenu van de regel met de naam van de integriteitscontrole weer te geven.
5. Voer een van de volgende acties uit:
   - Selecteer **Scan starten** in het contextmenu om de integriteitscontrole te starten.
     De voortgang van de taak rechts van de knop met de naam van deze taak wijzigt in *Actief*.
   - Selecteer **Scan stoppen** in het contextmenu als u de integriteitscontrole wilt stoppen.
     De voortgang van de taak rechts van de knop met de naam van deze taak wijzigt in *Gestopt*.

Uitvoermodus voor de integriteitscontrole selecteren

Zo selecteert u de uitvoermodus voor de integriteitscontrole:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geplande taken** links in het venster de optie **Integriteitscontrole**.
   Rechts in het venster ziet u de instellingen van de taak Integriteitscontrole.

3. Kies in het gedeelte **Uitvoermodus** een van de volgende opties:

   - Selecteer **Handmatig** als u de taak Integriteitscontrole handmatig wilt starten.
   - Selecteer **Volgens schema** als u het opstartschema voor de taak Integriteitscontrole wilt configureren.

4. Als u tijdens de vorige stap de optie **Volgens schema** hebt geselecteerd, geeft u de instellingen van het schema voor de uitvoering van de taak op. Hiertoe doet u het volgende:

   a. Geef in de vervolgkeuzelijst **Frequentie** op wanneer de integriteitscontrole moet worden gestart. Selecteer een van de volgende opties: **Minuten**, **Uren**, **Dagen**, **Elke week**, **Op een opgegeven tijdstip**, **Elke maand** of **Na programmastart**.

   b. Afhankelijk van de geselecteerde optie in de vervolgkeuzelijst **Frequentie** geeft u de waarden voor de instellingen op die bepalen wanneer de taak moet worden gestart.

   c. Als u Kaspersky Endpoint Security overgeslagen integriteitscontroles zo snel mogelijk wilt laten starten, schakelt u het selectievakje **Overgeslagen taken starten** in.

      Als de optie **Na programmastart**, **Minuten** of **Uren** is geselecteerd in de vervolgkeuzelijst **Frequentie**, is het selectievakje **Overgeslagen taken starten** niet beschikbaar.

   d. Als u Kaspersky Endpoint Security een taak wilt laten onderbreken wanneer er weinig computerbronnen beschikbaar zijn, schakelt u het selectievakje **Alleen starten als de computer inactief is** in.

      Deze optie van het schema helpt de beschikbaarheid van de computerbronnen in stand te houden.

5. Klik op **OK**.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Rapporten beheren

In deze sectie wordt beschreven hoe u de instellingen voor rapporten kunt configureren en rapporten kunt beheren.

Beginselen van het beheer van rapporten

Informatie over de werking van elk Kaspersky Endpoint Security-onderdeel, de prestaties van elke scantaak, de updatetaak, de integriteitscontrole, de Kwetsbaarheidsscan en de algemene werking van het programma wordt in rapporten vastgelegd.

De rapportgegevens worden als een tabel voorgesteld die een lijst met gebeurtenissen bevat. Elke regel van de tabel bevat informatie over een specifieke gebeurtenis. De kenmerken van de gebeurtenis ziet u in de kolommen van de tabel. Bepaalde kolommen zijn samengestelde kolommen die geneste kolommen met extra kenmerken bevatten. Om de extra kenmerken te bekijken, moet u op de knop ⊞ naast de naam van de grafiek drukken. Gebeurtenissen die tijdens de werking van verschillende onderdelen of de uitvoering van diverse taken zijn geregistreerd, hebben verschillende kenmerken.

De volgende rapporten zijn beschikbaar:

- Het rapport **Systeemaudit**. Dit bevat informatie over gebeurtenissen tijdens de interactie tussen de gebruiker en het programma en tijdens de algemene werking van het programma die niets te maken hebben een specifieke onderdelen of taken van Kaspersky Endpoint Security.
- Het rapport **Alle beschermingsonderdelen**. Dit bevat informatie over gebeurtenissen die tijdens de werking van de volgende Kaspersky Endpoint Security-onderdelen zijn geregistreerd:
  - Anti-Virus voor bestanden
  - Mail Anti-Virus.
  - Web Anti-Virus.
  - IM Anti-Virus.
  - Systeembewaking.
  - Firewall.
  - Network Attack Blocker.
  - BadUSB Attack Prevention.
- Rapport over de werking van een Kaspersky Endpoint Security-onderdeel of de uitvoering van een taak.
- Het rapport **Encryptie**. Bevat informatie over gebeurtenissen die zich tijdens de encryptie en decryptie van gegevens voordoen.

In rapporten kunnen gebeurtenissen het volgende belang hebben:

- **Informatieve gebeurtenissen**. Pictogram ℹ. Formele gebeurtenissen die normaal geen belangrijke informatie bevatten.

- **Belangrijke gebeurtenissen**. Pictogram ⚠. Gebeurtenissen die uw aandacht vereisen omdat ze belangrijke situaties in de werking van Kaspersky Endpoint Security weerspiegelen.
- **Kritieke gebeurtenissen**. Pictogram ⚠. Gebeurtenissen van kritiek belang die problemen in de werking van Kaspersky Endpoint Security of kwetsbaarheden in de bescherming van de computer van de gebruiker aangeven.

Voor de handige verwerking van rapporten kunt u de voorstelling van gegevens op het scherm wijzigen op de volgende manieren:

- Filter de lijst met gebeurtenissen op verschillende criteria.
- Gebruik de zoekfunctie om een specifieke gebeurtenis te vinden.
- Bekijk de geselecteerde gebeurtenis in een apart gedeelte.
- Sorteer de lijst met gebeurtenissen op elke kolom in het rapport.
- Toon en verberg gebeurtenissen die met filters voor gebeurtenissen zijn gegroepeerd.
- Wijzig de volgorde en de indeling van kolommen die in het rapport worden weergegeven.

U kunt indien nodig een gegenereerd rapport opslaan als een tekstbestand.

U kunt ook gegroepeerde rapportgegevens over onderdelen en taken van Kaspersky Endpoint Security verwijderen. Kaspersky Endpoint Security verwijdert alle vermeldingen van de geselecteerde rapporten vanaf de eerste vermelding tot het huidige tijdstip.

Instellingen voor rapporten configureren

U kunt de instellingen voor rapporten configureren op de volgende manieren:

- Configureer de maximale opslagduur voor rapporten.

  De standaard maximale opslagduur voor rapporten met gebeurtenissen die door Kaspersky Endpoint Security worden geregistreerd, is 30 dagen. Na die tijd worden de oudste gegevens uit het rapportbestand automatisch verwijderd door Kaspersky Endpoint Security. U kunt de tijdsbeperking annuleren of de maximale opslagduur voor rapporten wijzigen.

- Configureer de maximale grootte van het rapportbestand.

  U kunt de maximale grootte van het rapportbestand opgeven. De maximale bestandsgrootte voor rapporten is standaard 1024 MB. Om te vermijden dat de maximale bestandsgrootte van rapporten wordt overschreden, worden de oudste gegevens in het rapportbestand automatisch verwijderd door Kaspersky Endpoint Security wanneer de maximale bestandsgrootte voor het rapport wordt bereikt. U kunt de beperking van de grootte van het rapportbestand annuleren of een andere waarde instellen.

Maximale opslagduur voor rapporten configureren

Zo wijzigt u de maximale opslagduur voor rapporten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.

3. Doe in het gedeelte **Rapportparameters** rechts in het venster een van het volgende:

   - Schakel het selectievakje **Bewaar rapporten maximaal** in om de opslagduur voor rapporten te beperken. Geef in het veld naast het selectievakje **Bewaar rapporten maximaal** op hoelang u rapporten maximaal wilt bewaren.

     De standaard maximale opslagduur voor rapporten is 30 dagen.

   - Schakel het selectievakje **Bewaar rapporten maximaal** om de beperking van de opslagduur voor rapporten te annuleren.

   De beperking van de opslagduur voor rapporten is standaard ingeschakeld.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Maximale grootte van het rapportbestand configureren

Zo configureert u de maximale grootte van het rapportbestand:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.
3. Doe in het gedeelte **Rapportparameters** rechts in het venster een van het volgende:

   - Schakel het selectievakje **Maximale bestandsgrootte** in om de grootte van het rapportbestand te beperken. Geef in het veld rechts van het selectievakje **Maximale bestandsgrootte** de maximale grootte voor het rapportbestand op.

     De grootte van het rapportbestand is standaard beperkt tot 1024 MB.

   - Schakel het selectievakje **Maximale bestandsgrootte** uit om de beperking van de grootte van het rapportbestand op te heffen.

   De beperking van de grootte van het rapportbestand is standaard ingeschakeld.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Rapporten bekijken

Zo bekijkt u rapporten:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Rapporten** boven in het hoofdvenster van het programma om het venster **Rapporten** te openen.
3. Om het rapport Alle beschermingsonderdelen te genereren, selecteert u links in het venster **Rapporten** de optie **Alle beschermingsonderdelen** in de lijst met onderdelen en taken.

   Het rapport Alle beschermingsonderdelen wordt rechts in het venster weergegeven en bevat een lijst met gebeurtenissen die zich tijdens de werking van alle beschermingsonderdelen van Kaspersky Endpoint Security hebben voorgedaan.

4. Om een rapport over de werking van een onderdeel of een taak te genereren, selecteert u links in het venster **Rapporten** een onderdeel of een taak in de lijst met onderdelen en taken.

   Rechts in het venster wordt een rapport weergegeven dat een lijst met gebeurtenissen bevat die zich tijdens de werking van het geselecteerde onderdeel of de geselecteerde taak van Kaspersky Endpoint Security hebben voorgedaan.

Standaard worden de gebeurtenissen in het rapport oplopend gesorteerd op de waarden van de kolom **Datum gebeurtenis**.

Informatie van gebeurtenissen in een rapport bekijken

U kunt een gedetailleerde samenvatting van elke gebeurtenis in het rapport bekijken.

Zo bekijkt u een gedetailleerde samenvatting van een gebeurtenis in het rapport:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Rapporten** boven in het hoofdvenster van het programma om het venster **Rapporten** te openen.
3. Selecteer links in het venster het relevante rapport over het onderdeel of de taak.

   Gebeurtenissen uit het bereik van het rapport worden in de tabel rechts in het venster weergegeven. Om specifieke gebeurtenissen in het rapport te vinden, gebruikt u de filter-, zoek- of sorteerfuncties.
4. Selecteer de relevante gebeurtenis in het rapport.

Een gedeelte met de samenvatting van de gebeurtenis wordt onder in het venster weergegeven.

Een rapport als een bestand opslaan

U kunt het gegenereerde rapport als een bestand met tekstindeling (TXT) of als een CSV-bestand opslaan.

Kaspersky Endpoint Security registreert gebeurtenissen in het rapport zoals ze op het scherm worden weergegeven: d.w.z. met dezelfde kenmerken in dezelfde volgorde.

Zo slaat u een rapport als een bestand op:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Rapporten** boven in het hoofdvenster van het programma om het venster **Rapporten** te openen.
3. Voer een van de volgende acties uit:

   - Selecteer **Alle beschermingsonderdelen** in de lijst met onderdelen en taken om het rapport 'Alle beschermingsonderdelen' te genereren.

     Het rapport 'Alle beschermingsonderdelen' wordt rechts in het venster weergegeven en bevat een lijst met gebeurtenissen die zich tijdens de werking van alle beschermingsonderdelen hebben voorgedaan.

   - Als u een rapport over de werking van een specifiek onderdeel of een specifieke taak wilt genereren, selecteert u dit onderdeel of deze taak in de lijst met onderdelen en taken.

Rechts in het venster wordt een rapport weergegeven dat een lijst met gebeurtenissen bevat die zich tijdens de werking van het geselecteerde onderdeel of de geselecteerde taak hebben voorgedaan.

4. U kunt indien nodig de voorstelling van de gegevens in het rapport wijzigen door het volgende te doen:
   - Gebeurtenissen filteren
   - Zoekopdrachten voor gebeurtenissen uitvoeren
   - Kolommen rangschikken
   - Gebeurtenissen sorteren
5. Klik in de rechterbovenhoek van het venster op de knop **Rapport opslaan**.

   Een contextmenu wordt geopend.
6. Selecteer in het contextmenu de codering voor de opslag van het rapportbestand: **Opslaan als ANSI** of **Opslaan als Unicode**.

   Het standaardvenster **Opslaan als** wordt in Microsoft Windows geopend.
7. Geef in het venster **Opslaan als** de doelmap voor het rapportbestand op.
8. Typ in het veld **Bestandsnaam** de bestandsnaam voor het rapport.
9. Selecteer in het veld **Bestandstype** de noodzakelijke bestandsindeling voor het rapport: TXT of CSV.
10. Klik op de knop **Opslaan**.

Rapporten wissen

Zo verwijdert u informatie uit rapporten:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.
3. Klik in het gedeelte **Rapportparameters** rechts in het venster op de knop **Rapporten verwijderen**.

   Het venster **Rapporten wissen** wordt geopend.
4. Schakel de selectievakjes naast de rapporten in waarin u informatie wilt verwijderen:
   - **Alle rapporten**.
   - **Rapport over algemene bescherming**. Bevat informatie over de werking van de volgende onderdelen van Kaspersky Endpoint Security:
     - Anti-Virus voor bestanden
     - Mail Anti-Virus.
     - Web Anti-Virus.

- IM Anti-Virus.
- Systeembewaking.
- Firewall.
- Network Attack Blocker.
- BadUSB Attack Prevention.

- **Rapport over scantaken**. Bevat informatie over voltooide scantaken:
  - Volledige Scan
  - Kritieke Gebiedenscan
  - Aangepaste Scan
  - Integriteitscontrole.
- **Rapport over updatetaken**. Bevat informatie over voltooide updatetaken:
- **Firewall-rapport**. Bevat informatie over de werking van Firewall.
- **Rapport over controle-onderdelen**. Bevat informatie over de werking van de volgende onderdelen van Kaspersky Endpoint Security:
  - Programma-opstartcontrole.
  - Controle van programmabevoegdheden.
  - Kwetsbaarheidsbewaking.
  - Apparaatcontrole.
  - Webcontrole.
- **Rapport over gegevensencryptie**.

5. Klik op **OK**.

Service voor meldingen

In deze sectie vindt u informatie over de service voor meldingen die de gebruiker op de hoogte brengt over gebeurtenissen tijdens de werking van Kaspersky Endpoint Security, alsook instructies voor de configuratie van parameters voor meldingen.

Over de meldingen van Kaspersky Endpoint Security

Tijdens de werking van Kaspersky Endpoint Security doen zich allerhande gebeurtenissen voor. Meldingen over deze gebeurtenissen kunnen algemene of belangrijke informatie bevatten. Een melding kan bijvoorbeeld een bericht over een geslaagde update van de databases en de programmamodules bevatten, of een bericht over fouten in onderdelen die moeten worden gerepareerd.

Kaspersky Endpoint Security ondersteunt de registratie van informatie over gebeurtenissen in het Microsoft Windows-logboek en/of het Kaspersky Endpoint Security-gebeurtenislogboek.

Kaspersky Endpoint Security levert meldingen op de volgende manieren:

- via pop-upmeldingen in het systeemvak van de taakbalk van Microsoft Windows;
- per e-mail.

U kunt de levering van meldingen over gebeurtenissen configureren. De methode voor de levering van meldingen wordt voor elk type gebeurtenis geconfigureerd.

De service voor meldingen configureren

U kunt het volgende doen om de service voor meldingen te configureren:

- Configureer de instellingen van gebeurtenislogboeken waarin Kaspersky Endpoint Security gebeurtenissen registreert.
- Configureer hoe meldingen op het scherm worden weergegeven.
- Configureer de levering van e-mailmeldingen.

Wanneer u de tabel met gebeurtenissen gebruikt om de service voor meldingen te configureren, kunt u de volgende acties uitvoeren:

- Filter gebeurtenissen van de service voor meldingen op kolomwaarden of op aangepaste filtervoorwaarden.
- Gebruik de zoekfunctie voor gebeurtenissen van de service voor meldingen.
- Sorteer gebeurtenissen van de service voor meldingen.
- Wijzig de volgorde en de reeks kolommen die in de lijst met gebeurtenissen van de service voor meldingen worden weergegeven.

Instellingen voor gebeurtenislogboeken configureren

Zo configureert u instellingen voor gebeurtenislogboeken:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.

   Rechts in het venster ziet u de instellingen van de rapporten en de opslag.
3. Klik in het gedeelte **Meldingen** op de knop **Instellingen**.

   Zo opent u het venster **Meldingen**.

   De onderdelen en taken van Kaspersky Endpoint Security worden links in het venster weergegeven. Rechts in het venster ziet u een lijst met gegenereerde gebeurtenissen voor het geselecteerde onderdeel of taak.
4. Selecteer links in het venster het onderdeel of de taak waarvoor u de instellingen voor het gebeurtenislogboek wilt configureren.
5. Schakel de selectievakjes naast de relevante gebeurtenissen in de kolommen **Opslaan in lokaal logboek** en **Opslaan in Windows-logboek** in.

   Gebeurtenissen met ingeschakelde selectievakjes in de kolom **Opslaan in lokaal logboek** worden in **Logboeken van programma's en services** in het gedeelte **Kaspersky-gebeurtenislogboek** weergegeven. Gebeurtenissen met ingeschakelde selectievakjes in de kolom **Opslaan in Windows-logboek** worden in **Windows-logboeken** in het gedeelte **Programma** opgeslagen. Om de gebeurtenislogboeken te openen, klikt u achtereenvolgens op **Start** → **Configuratiescherm** → **Beheer** → **Logboeken**.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Weergave en levering van meldingen configureren

Zo configureert u de weergave en de levering van meldingen:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.

   Rechts in het venster ziet u de instellingen van de rapporten en de opslag.
3. Klik in het gedeelte **Meldingen** op de knop **Instellingen**.

   Zo opent u het venster **Meldingen**.

   De onderdelen en taken van Kaspersky Endpoint Security worden links in het venster weergegeven. Rechts in het venster ziet u een lijst met gegenereerde gebeurtenissen voor het geselecteerde onderdeel of de geselecteerde taak.
4. Selecteer links in het venster het onderdeel of de taak waarvoor u de levering van meldingen wilt configureren.
5. Schakel in de kolom **Melden op scherm** de selectievakjes naast de vereiste gebeurtenissen in.

   Informatie over de geselecteerde gebeurtenissen wordt op het scherm weergegeven als pop-upberichten in het systeemvak van de taakbalk in Microsoft Windows.
6. Schakel in de kolom **Melden per e-mail** de selectievakjes naast de vereiste gebeurtenissen in.

   Informatie over de geselecteerde gebeurtenissen wordt per e-mail geleverd als de instellingen voor de levering van meldingen per e-mail zijn geconfigureerd.

7. Klik op de knop **Instellingen voor e-mailmeldingen**.

   Hiermee opent u het venster **Instellingen voor e-mailmeldingen**.

8. Schakel het selectievakje **Meldingen over gebeurtenissen versturen** in om informatie over de gebeurtenissen van Kaspersky Endpoint Security die in de kolom **Melden per e-mail** zijn geselecteerd te laten leveren.

9. Geef de instellingen voor de levering van meldingen per e-mail op.

10. Klik op **OK**.

11. Klik in het venster **Instellingen voor e-mailmeldingen** op **OK**.

12. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Weergave van waarschuwingen over de status van het programma in het systeemvak configureren

Zo configureert u de weergave van waarschuwingen over de status van het programma in het systeemvak:

1. Open het venster met de programma-instellingen.

2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Interface**.

   De instellingen van de Kaspersky Endpoint Security-interface worden rechts in het venster weergegeven.

3. Schakel in het gedeelte **Waarschuwingen** de selectievakjes naast de categorieën van gebeurtenissen in waarvoor u meldingen in het systeemvak van Microsoft Windows wilt zien.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bij gebeurtenissen die te maken hebben met de geselecteerde categorieën wijzigt het pictogram van het programma in het systeemvak in  of afhankelijk van de ernst van de waarschuwing.

Quarantaine en Back-up beheren

In deze sectie wordt beschreven hoe u Quarantaine en Back-up configureert en beheert.

Over Quarantaine en Back-up

Quarantaine is een lijst met waarschijnlijk geïnfecteerde bestanden. *Waarschijnlijk geïnfecteerde bestanden* zijn bestanden die mogelijk virussen en andere bedreigingen, of varianten van die bedreigingen, bevatten.

Wanneer Kaspersky Endpoint Security een waarschijnlijk geïnfecteerd bestand in Quarantaine plaatst, kopieert het niet het bestand maar verplaatst het het bestand: het programma verwijdert het bestand van de harde schijf of uit het e-mailbericht en slaat het bestand in een speciale gegevensopslag op. Bestanden in Quarantaine worden in een speciale indeling opgeslagen en zijn niet gevaarlijk.

Tijdens een virusscan of de werking van de onderdelen Anti-Virus voor bestanden, Mail Anti-Virus en Systeembewaking kan Kaspersky Endpoint Security een waarschijnlijk geïnfecteerd bestand vinden en in Quarantaine plaatsen.

Kaspersky Endpoint Security plaatst bestanden in Quarantaine in de volgende gevallen:

- De bestandscode gelijkt op een bekend maar deels gewijzigd kwaadaardig programma of heeft een malware-achtige structuur en komt niet voor in de database van Kaspersky Endpoint Security. In dit geval wordt het bestand na de heuristische analyse door Anti-Virus voor bestanden of Mail Anti-Virus, of tijdens een virusscan, in Quarantaine geplaatst. De heuristische analyse geeft zelden false positives als resultaat.

- De reeks uitgevoerde bewerkingen door een bestand is gevaarlijk. In dit geval wordt het bestand in Quarantaine geplaatst nadat het onderdeel Systeembewaking het gedrag ervan heeft geanalyseerd.

Back-up is een lijst met back-ups van bestanden die tijdens de desinfectie zijn verwijderd of gewijzigd. Een *back-up van een bestand* een kopie van een bestand die bij de eerste poging tot desinfectie of verwijdering van het bestand is gemaakt. Back-ups van bestanden worden in een speciale indeling opgeslagen en zijn niet gevaarlijk.

Soms is het niet mogelijk om de integriteit van bestanden tijdens de desinfectie te behouden. Als u de toegang tot belangrijke informatie in een gedesinfecteerd bestand na de desinfectie deels of volledig verliest, kunt u de gedesinfecteerde kopie van het bestand terugzetten in de originele map.

Na een nieuwe update van de databases of de softwaremodules van het programma is het mogelijk dat Kaspersky Endpoint Security wel de bedreigingen kan identificeren en onschadelijk maken. Daarom wordt u aanbevolen om bestanden in Quarantaine te scannen telkens als u de databases en softwaremodules van het programma hebt bijgewerkt.

Instellingen van Quarantaine en Back-up configureren

Quarantaine en Back-up zorgen voor de gegevensopslag. U kunt de instellingen van Quarantaine en Back-up als volgt configureren:

- Configureer de maximale opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up.

  De standaard maximale opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up is 30 dagen. Na de maximale opslagduur verwijdert Kaspersky Endpoint Security de oudste bestanden uit de gegevensopslag. U kunt de tijdsbeperking annuleren of de maximale opslagduur voor bestanden wijzigen.

- U kunt de maximale grootte van Quarantaine en Back-up configureren.

De maximale grootte van Quarantaine en Back-up is standaard 100 MB. Wanneer de gegevensopslag bijna vol is, verwijdert Kaspersky Endpoint Security automatisch de oudste bestanden uit Quarantaine en Back-up zodat de maximale grootte van de gegevensopslag niet wordt overschreden. U kunt de maximale grootte van Quarantaine en Back-up annuleren of wijzigen.

De maximale opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up configureren

Zo configureert u de maximale opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.
3. Voer een van de volgende acties uit:
   - Om de opslagduur van bestanden in Quarantaine en Back-up te beperken, schakelt u in het gedeelte **Instellingen van Quarantaine en Back-up** rechts in het venster het selectievakje **Bewaar objecten maximaal** in. Typ in het veld rechts van het selectievakje **Bewaar objecten maximaal** de maximale opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up. De opslagduur voor bestanden in Quarantaine en kopieën van bestanden in Back-up is standaard beperkt tot 30 dagen.
   - Om de beperking voor de opslagduur van bestanden in Quarantaine en Back-up te annuleren, schakelt u in het gedeelte **Instellingen van Quarantaine en Back-up** rechts in het venster het selectievakje **Bewaar objecten maximaal** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De maximale grootte van Quarantaine en Back-up configureren

Zo configureert u de maximale grootte van Quarantaine en Back-up:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.
3. Voer een van de volgende acties uit:
   - Als u de totale grootte van Quarantaine en Back-up wilt beperken, schakelt u het selectievakje **Maximale opslaggrootte** in rechts in het venster in het gedeelte **Instellingen van Quarantaine en Back-up** en typt u de maximale grootte van Quarantaine en Back-up in het veld rechts van het selectievakje **Maximale opslaggrootte**.

     De maximale opslaggrootte voor gegevens in Quarantaine en back-ups van bestanden is 100 MB.
   - Als u de beperking voor de grootte van Quarantaine en Back-up wilt opheffen, schakelt u het selectievakje **Maximale opslaggrootte** uit rechts in het venster in het gedeelte **Instellingen van Quarantaine en Back-up**.

De grootte van Quarantaine en Back-up is standaard onbeperkt.

4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Quarantaine beheren

Kaspersky Endpoint Security verwijdert automatisch bestanden met een willekeurige status uit Quarantaine nadat de gedefinieerde opslagduur in de programma-instellingen is verstreken.

De volgende bestandsbewerkingen zijn beschikbaar voor het beheer van Quarantaine:

- Bekijk de bestanden die door Kaspersky Endpoint Security in Quarantaine zijn geplaatst.
- Scan waarschijnlijk geïnfecteerde bestanden met de huidige versie van de Kaspersky Endpoint Security-databases en -modules.
- Zet bestanden vanuit Quarantaine terug naar hun oorspronkelijke mappen.
- Verwijder bestanden uit Quarantaine.
- Open de mappen waarin de bestanden oorspronkelijk stonden.

De bestanden die in Quarantaine zijn geplaatst worden als een tabel voorgesteld.

U kunt ook de volgende acties uitvoeren wanneer u gegevens in de tabel beheert:

- Filter bestanden die in Quarantaine zijn geplaatst op kolommen en met aangepaste filtervoorwaarden.
- Gebruik de zoekfunctie voor bestanden in Quarantaine.
- Sorteer bestanden in Quarantaine.
- Wijzig de volgorde en de reeks kolommen van de tabel met bestanden die in Quarantaine zijn geplaatst.

U kunt geselecteerde Quarantaine-gebeurtenissen kopiëren naar het klembord. Om meerdere bestanden in Quarantaine te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

Bestanden in Quarantaine scannen na een update inschakelen en uitschakelen

Als Kaspersky Endpoint Security tijdens de scan van een bestand tekenen van infectie detecteert maar niet kan bepalen welke specifieke kwaadaardige programma's het hebben geïnfecteerd, plaatst Kaspersky Endpoint Security dit bestand in Quarantaine. Kaspersky Endpoint Security kan de bedreigingen mogelijk wel identificeren en onschadelijk maken wanneer de databases en programmamodules zijn bijgewerkt. U kunt het automatisch scannen van bestanden in Quarantaine na elke update van de databases en programmamodules inschakelen.

We raden aan dat u de bestanden in Quarantaine regelmatig scant. De status van de bestanden kan door de scan worden gewijzigd. Bepaalde bestanden kunnen dan worden gedesinfecteerd en op hun oorspronkelijke locaties worden teruggezet zodat u ze verder kunt gebruiken.

Zo schakelt u het scannen van bestanden in Quarantaine na updates in:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster de optie **Rapporten en opslag**.

   Rechts in het venster worden de beheerinstellingen voor de rapporten en de opslag weergegeven.
3. Doe in het gedeelte **Instellingen van Quarantaine en Back-up** een van het volgende:

   - Als u het scannen van bestanden in Quarantaine na elke update van Kaspersky Endpoint Security wilt inschakelen, schakelt u het selectievakje **Quarantaine opnieuw scannen na update** in.
   - Als u het scannen van bestanden in Quarantaine na elke update van Kaspersky Endpoint Security wilt uitschakelen, schakelt u het selectievakje **Quarantaine opnieuw scannen na update** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een Aangepaste Scan voor bestanden in Quarantaine starten

Wanneer de databases en softwaremodules van het programma zijn bijgewerkt, kan Kaspersky Endpoint Security de bedreigingen in bestanden in Quarantaine mogelijk wel identificeren en onschadelijk maken. Als het programma niet is geconfigureerd om bestanden in Quarantaine automatisch te scannen telkens als de databases en de programmamodules worden bijgewerkt, kunt u een Aangepaste Scan voor bestanden in Quarantaine handmatig starten.

Zo start u een Aangepaste Scan voor bestanden in Quarantaine:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.

   Het tabblad **Quarantaine** in het venster **Opslag** wordt geopend.
3. Selecteer op het tabblad **Quarantaine** een of meer waarschijnlijk geïnfecteerde bestanden die u wilt scannen.

   Om meerdere bestanden in Quarantaine te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.
4. Start de Aangepaste Scan op een van de volgende manieren:

   - Klik op de knop **Opnieuw scannen**.
   - Klik rechts om het contextmenu te openen en selecteer **Opnieuw scannen**.

Wanneer de scan is voltooid, ziet u een melding met het aantal gescande bestanden en het aantal gevonden bedreigingen.

Bestanden vanuit Quarantaine terugzetten

Zo zet u bestanden vanuit Quarantaine terug:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.

Het tabblad **Quarantaine** in het venster **Opslag** wordt geopend.

3. Als u alle bestanden in Quarantaine wilt terugzetten, selecteert u **Alles herstellen** in het contextmenu van een bestand.

   Kaspersky Endpoint Security zet alle bestanden vanuit Quarantaine terug in hun oorspronkelijke mappen.

4. Zo zet u een of meer bestanden in Quarantaine terug:

   a. Selecteer op het tabblad **Quarantaine** een of meer bestanden die u vanuit Quarantaine wilt terugzetten.

      Om meerdere bestanden in Quarantaine te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

   b. Zet bestanden terug op een van de volgende manieren:

      - Klik op de knop **Herstellen**.
      - Klik rechts om het contextmenu te openen en selecteer **Herstellen**.

   Kaspersky Endpoint Security zet de geselecteerde bestanden terug in hun oorspronkelijke mappen.

Bestanden uit Quarantaine verwijderen

Zo verwijdert u bestanden uit Quarantaine:

1. Open het hoofdvenster van het programma.

2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.

   Het tabblad **Quarantaine** in het venster **Opslag** wordt geopend.

3. Als u alle bestanden uit Quarantaine wilt verwijderen, selecteert u **Alles verwijderen** in het contextmenu van een bestand.

   Kaspersky Endpoint Security verwijdert alle bestanden uit Quarantaine.

4. Zo verwijdert u een of meer bestanden die in Quarantaine zijn geplaatst:

   a. Selecteer in de tabel op het tabblad **Quarantaine** een of meer waarschijnlijk geïnfecteerde bestanden die u uit Quarantaine wilt verwijderen.

      Om meerdere bestanden in Quarantaine te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

   b. Verwijder bestanden op een van de volgende manieren:

      - Klik op de knop **Verwijderen**.
      - Klik rechts om het contextmenu te openen en selecteer **Verwijderen**.

Kaspersky Endpoint Security verwijdert alle geselecteerde bestanden uit Quarantaine.

Back-up beheren

Als kwaadaardige code in het bestand wordt gevonden, blokkeert Kaspersky Endpoint Security het bestand, plaatst het een kopie ervan in Back-up en probeert het het bestand te desinfecteren. Als de desinfectie van het bestand met succes wordt voltooid, wijzigt de status van de back-up van het bestand in *Gedesinfecteerd*. Het bestand is dan opnieuw te vinden in de oorspronkelijke map. Als een bestand niet kan worden gedesinfecteerd, verwijdert Kaspersky Endpoint Security het uit de oorspronkelijke map. U kunt het bestand uit de back-up terugzetten naar de oorspronkelijke map.

Bij de detectie van kwaadaardige code in een bestand van een programma uit de Windows Store verwijdert Kaspersky Endpoint Security het bestand onmiddellijk zonder een kopie van het bestand in Back-up te plaatsen. U kunt de integriteit van het programma uit de Windows Store herstellen met de gepaste tools van Microsoft Windows 8 (raadpleeg de *Help-bestanden van Microsoft Windows 8* voor informatie over het herstel van een programma uit de Windows Store).

Kaspersky Endpoint Security verwijdert automatisch back-ups van bestanden met een willekeurige status uit Back-up nadat de gedefinieerde opslagduur in de programma-instellingen is verstreken.

U kunt een kopie van een bestand ook handmatig verwijderen uit Back-up.

De back-ups van bestanden worden als een tabel voorgesteld.

Tijdens het beheer van Back-up kunt u de volgende acties op back-ups van bestanden uitvoeren:

- Bekijk de reeks back-ups van bestanden.
- Zet bestanden vanuit back-ups terug naar hun oorspronkelijke mappen.
- Verwijder back-ups van bestanden uit Back-up.

U kunt ook de volgende acties uitvoeren wanneer u gegevens in de tabel beheert:

- Filter back-ups op kolommen, of zelfs met aangepaste filtervoorwaarden.
- Gebruik de zoekfunctie voor back-ups.
- Sorteer back-ups.
- Wijzig de volgorde en de reeks kolommen die in de tabel met back-ups worden weergegeven.

U kunt geselecteerde Back-up-gebeurtenissen kopiëren naar het klembord. Om meerdere bestanden in Back-up te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

Bestanden vanuit Back-up terugzetten

Zo zet u bestanden vanuit Back-up terug:

1. Open het hoofdvenster van het programma.

2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Back-up**.
4. Als u alle bestanden uit Back-up wilt terugzetten, selecteert u **Alles herstellen** in het contextmenu van een bestand.

   Kaspersky Endpoint Security zet alle bestanden vanuit back-ups terug in hun oorspronkelijke mappen.
5. Zo zet u een of meer bestanden vanuit Back-up terug:

   a. Selecteer in de tabel op het tabblad **Back-up** een of meer bestanden uit Back-up.

   Om meerdere bestanden in Quarantaine te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

   b. Zet bestanden terug op een van de volgende manieren:

   - Klik op de knop **Herstellen**.
   - Klik rechts om het contextmenu te openen en selecteer **Herstellen**.

   Kaspersky Endpoint Security zet alle bestanden vanuit geselecteerde back-ups terug in hun oorspronkelijke mappen.

Back-ups van bestanden uit Back-up verwijderen

Zo verwijdert u back-ups van bestanden uit Back-up:

1. Open het hoofdvenster van het programma.
2. Klik op de koppeling **Quarantaine** boven in het hoofdvenster om het venster **Opslag** te openen.
3. Selecteer in het venster **Opslag** het tabblad **Back-up**.
4. Als u alle bestanden uit Back-up wilt verwijderen, voert u een van de volgende acties uit:

   - Selecteer in het contextmenu van een bestand de optie **Alles verwijderen**.
   - Klik op de knop **Opslag wissen**.

   Kaspersky Endpoint Security verwijdert alle back-ups van bestanden uit Back-up.
5. Als u een of meer bestanden uit Back-up wilt verwijderen:

   a. Selecteer in de tabel op het tabblad **Back-up** een of meer bestanden uit Back-up.

   Om meerdere bestanden in Back-up te selecteren, klikt u rechts om het contextmenu van een bestand te openen en kiest u **Alles selecteren**. Om de selectie van bestanden die u niet wilt scannen op te heffen, klikt u erop terwijl u de **CTRL**-toets ingedrukt houdt.

   b. Verwijder bestanden op een van de volgende manieren:

   - Klik op de knop **Verwijderen**.

- Klik rechts om het contextmenu te openen en selecteer **Verwijderen**.

Kaspersky Endpoint Security verwijdert de geselecteerde back-ups van bestanden uit Back-up.

Geavanceerde programma-instellingen

In deze sectie worden de geavanceerde instellingen van Kaspersky Endpoint Security beschreven en leest u hoe u ze kunt configureren.

Een configuratiebestand aanmaken en gebruiken

Met een configuratiebestand met instellingen van Kaspersky Endpoint Security kunt u de volgende taken uitvoeren:

- Gebruik de opdrachtregel om Kaspersky Endpoint Security lokaal te installeren met vooraf gedefinieerde instellingen.

  Hiertoe moet u het configuratiebestand in dezelfde map als het distributiepakket opslaan.

- Gebruik Kaspersky Security Center om Kaspersky Endpoint Security op afstand te installeren met vooraf gedefinieerde instellingen.

- Migreer de instellingen van Kaspersky Endpoint Security van de ene computer naar de andere.

Zo maakt u een configuratiebestand aan:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Instellingen beheren** op de knop **Opslaan**.

   Hiermee opent u het standaardvenster **Selecteer een configuratiebestand** in Microsoft Windows.
4. Geef het pad op waar u het configuratiebestand wilt opslaan en voer de naam ervan in.

   > Als u het configuratiebestand wilt gebruiken om Kaspersky Endpoint Security lokaal of op afstand te installeren, moet u het bestand 'install.cfg' noemen.

5. Klik op de knop **Opslaan**.

Zo importeert u de instellingen van Kaspersky Endpoint Security vanuit een configuratiebestand:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Instellingen beheren** op de knop **Laden**.

   Hiermee opent u het standaardvenster **Selecteer een configuratiebestand** in Microsoft Windows.
4. Geef het pad naar het configuratiebestand op.
5. Klik op de knop **Openen**.

Alle waarden van de instellingen van Kaspersky Endpoint Security worden overeenkomstig het geselecteerde configuratiebestand ingesteld.

Vertrouwde zone

In deze sectie vindt u informatie over de vertrouwde zone en instructies voor de configuratie van scanuitzonderingen en het maken van een lijst met vertrouwde programma's.

Over de vertrouwde zone

Een *vertrouwde zone* is een lijst met objecten en programma's die door een systeembeheerder is geconfigureerd. De objecten en programma's op deze lijst worden niet door Kaspersky Endpoint Security gemonitord wanneer ze actief zijn. Het zijn dus scanuitzonderingen.

De beheerder stelt de vertrouwde zone afzonderlijk in en houdt rekening met de functies van de objecten die worden verwerkt en de programma's die op de computer zijn geïnstalleerd. Mogelijk is het noodzakelijk om objecten en programma's toe te voegen aan de vertrouwde zone wanneer Kaspersky Endpoint Security de toegang tot een bepaald object of programma blokkeert hoewel u zeker weet dat het object of het programma ongevaarlijk is.

U kunt ervoor kiezen om de volgende objecten niet te scannen:

- Bestanden met bepaalde indelingen
- Bestanden die met een masker zijn geselecteerd
- Geselecteerde bestanden
- Mappen
- Processen van programma's

Scanuitzonderingen

Een *scanuitzondering* is een reeks voorwaarden waaraan een object niet door Kaspersky Endpoint Security wordt gescand op virussen en andere bedreigingen.

Dankzij scanuitzonderingen kan legitieme software die criminelen kunnen misbruiken om de computer of de gegevens van de gebruiker te beschadigen veilig worden gebruikt. Hoewel ze geen kwaadaardige functies hebben, kunnen zulke programma's worden gebruikt als een hulpmiddel voor malware. Voorbeelden van zulke programma's zijn onder andere tools voor extern beheer, IRC-programma's, FTP-servers, diverse hulpprogramma's voor het beëindigen of verbergen van processen, keyloggers, programma's voor het kraken van wachtwoorden en automatische inbelprogramma's. Zulke programma's zijn niet als virussen gecategoriseerd. Informatie over legitieme software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen vindt u in de Virusencyclopedie van Kaspersky op https://securelist.com/threats/detected-objects.

Zulke programma's kunnen door Kaspersky Endpoint Security worden geblokkeerd. Om te voorkomen dat ze worden geblokkeerd, kunt u scanuitzonderingen voor de actieve programma's configureren. Hiertoe voegt u de naam of het naammasker uit de Virusencyclopedie van Kaspersky toe aan de vertrouwde zone. U kunt bijvoorbeeld het programma Extern beheer vaak gebruiken. Dit is een programma voor externe toegang waarmee u de controle over een externe computer kunt krijgen. Kaspersky Endpoint Security beschouwt deze activiteit als verdacht en kan deze blokkeren. Om te voorkomen dat het programma wordt geblokkeerd, maakt u een scanuitzondering met de naam of het naammasker dat in de Virusencyclopedie van Kaspersky voorkomt.

Als een programma dat informatie verzamelt en die ter verwerking verstuurt op uw computer is geïnstalleerd, kan Kaspersky Endpoint Security dit programma als malware classificeren. Om dit te vermijden, kunt u voorkomen dat het programma wordt gescand door Kaspersky Endpoint Security te configureren zoals in dit document wordt beschreven.

Scanuitzonderingen kunnen worden gebruikt door de volgende onderdelen en taken van het programma die door de systeembeheerder zijn geconfigureerd:

- Anti-Virus voor bestanden
- Mail Anti-Virus.
- Web Anti-Virus.
- Controle van programmabevoegdheden.
- Scantaken
- Systeembewaking.

Lijst met vertrouwde programma's

De *lijst met vertrouwde programma's* is een lijst met programma's waarvan de bestands- en netwerkactiviteit (inclusief kwaadaardige activiteit) en de toegang tot het systeemregister niet worden gemonitord door Kaspersky Endpoint Security. Standaard scant Kaspersky Endpoint Security objecten die worden geopend, uitgevoerd of opgeslagen door processen van programma's en controleert het de activiteit van alle programma's en het netwerkverkeer dat deze genereren. Kaspersky Endpoint Security scant geen programma's die in de lijst met vertrouwde programma's voorkomen.

Als u bijvoorbeeld vindt dat de objecten die door het standaard Microsoft Windows-programma Kladblok worden gebruikt niet moeten worden gescand omdat u dit programma vertrouwt, kunt u het Microsoft Windows-programma Kladblok toevoegen aan de lijst met vertrouwde programma's. Tijdens de scans worden de objecten overgeslagen die door dit programma worden gebruikt.

Bepaalde acties die door Kaspersky Endpoint Security als verdacht worden beschouwd zijn mogelijk veilig als ze deel uitmaken van de functionaliteit van sommige programma's. Voorbeeld: de onderschepping van tekst die met het toetsenbord wordt getypt, is een normaal proces van programma's die de toetsenbordindeling automatisch wijzigen (zoals Punto Switcher). Om rekening te houden met de specifieke eigenschappen van zulke programma's en hun activiteit niet te monitoren, raden we aan dat u zulke programma's toevoegt aan de lijst met vertrouwde programma's.

Door het niet scannen van vertrouwde programma's worden conflicten met de compatibiliteit tussen Kaspersky Endpoint Security en andere programma's vermeden (bijvoorbeeld het netwerkverkeer van een externe computer dat twee keer wordt gescand, één keer door Kaspersky Endpoint Security en één keer door een ander antivirusprogramma) en gaat de computer beter werken, hetgeen belangrijk is wanneer servertoepassingen worden gebruikt.

Tegelijkertijd worden het uitvoerbare bestand en het proces van het vertrouwde programma nog steeds gescand op virussen en andere malware. Een programma kan tijdens scans volledig worden genegeerd door Kaspersky Endpoint Security als u een scanuitzondering voor dat programma aanmaakt.

Een scanuitzondering aanmaken

Kaspersky Endpoint Security scant een object niet als de schijf of de map met dit object is toegevoegd aan het scanbereik bij de start van een van de scantaken. De scanuitzondering wordt wel niet toegepast wanneer een Aangepaste Scan voor dit specifieke object wordt gestart.

Zo maakt u een scanuitzondering aan:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend en het tabblad **Scanuitzonderingen** wordt weergegeven.
4. Klik op de knop **Toevoegen**.

   Het venster **Scanuitzondering** wordt geopend. In dit venster kunt u een scanuitzondering aanmaken met een of beide criteria uit het gedeelte **Eigenschappen**.
5. Zo stelt u in dat een bestand of een map niet moet worden gescand:

   a. Schakel in het gedeelte **Eigenschappen** het selectievakje **Bestand of map** in.

   b. Klik op de koppeling **Bestand of map selecteren** in het gedeelte **Beschrijving van scanuitzondering** om het venster **Naam van bestand of map** te openen.

   c. Voer de naam van het bestand of de map of de naam voor het masker van het bestand of de map in of selecteer het bestand of de map in de mapstructuur door op **Bladeren** te klikken.

   In een masker van een bestands- of mapnaam kunt u een sterretje (*) gebruiken dat een willekeurige reeks tekens in de bestandsnaam voorstelt.

   U kunt bijvoorbeeld maskers gebruiken om de volgende paden toe te voegen:

   - Paden naar bestanden in een willekeurige map:
     - Het masker "*.exe" omvat alle paden naar bestanden die de EXE-extensie hebben.
     - Het masker "test" omvat alle paden naar bestanden met de naam "test".
   - Paden naar bestanden in een opgegeven map:
     - Het masker "C:\dir*.*" omvat alle paden naar bestanden in de map C:\dir\ maar niet in de submappen van C:\dir\.
     - Het masker "C:\dir*" omvat alle paden naar bestanden in de map C:\dir\ maar niet in de submappen van C:\dir\.
     - Het masker "C:\dir\" omvat alle paden naar bestanden in de map C:\dir\ maar niet in de submappen van C:\dir\.
     - Het masker "C:\dir*.exe" omvat alle paden naar bestanden met de EXE-extensie in de map C:\dir\ maar niet in de submappen van C:\dir\.
     - Het masker "C:\dir\test" omvat alle paden naar bestanden met de naam "test" in de map C:\dir\ maar niet in de submappen van C:\dir\.

- Het masker "C:\dir*\test" omvat alle paden naar bestanden met de naam "test" in de map C:\dir\ en in de submappen van C:\dir\.

- Paden naar bestanden in alle mappen met een opgegeven naam:

  - Het masker "dir*.*" omvat alle paden naar bestanden in mappen met de naam "dir" maar niet in de submappen van die mappen.

  - Het masker "dir*" omvat alle paden naar bestanden in mappen met de naam "dir" maar niet in de submappen van die mappen.

  - Het masker "dir\" omvat alle paden naar bestanden in mappen met de naam "dir" maar niet in de submappen van die mappen.

  - Het masker "dir*.exe" omvat alle paden naar bestanden met de EXE-extensie in mappen met de naam "dir" maar niet in de submappen van die mappen.

  - Het masker "dir\test" omvat alle paden naar bestanden met de naam "test" in mappen met de naam "dir" maar niet in de submappen van die mappen.

d. Klik in het venster **Naam van bestand of map** op **OK**.

Een koppeling naar het toegevoegde bestand of de toegevoegde map wordt in het gedeelte **Beschrijving van scanuitzondering** van het venster **Scanuitzondering** weergegeven.

6. Zo stelt u in dat objecten met een specifieke naam niet moeten worden gescand:

a. Schakel in het gedeelte **Eigenschappen** het selectievakje **Objectnaam** in.

b. Klik op de koppeling **Voer objectnaam in** in het gedeelte **Beschrijving van scanuitzondering** om het venster **Objectnaam** te openen.

c. Voer de objectnaam of het naammasker in volgens de classificatie van de Virusencyclopedie van Kaspersky:

d. Klik op **OK** in het venster **Objectnaam**.

Een koppeling naar de toegevoegde objectnaam wordt in het gedeelte **Beschrijving van scanuitzondering** van het venster **Scanuitzondering** weergegeven.

7. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

8. Geef de onderdelen van Kaspersky Endpoint Security op die de scanuitzondering moeten gebruiken:

a. Klik op de koppeling **Alle** in het gedeelte **Beschrijving van scanuitzondering** om de koppeling **Selecteer onderdelen** te activeren.

b. Klik op de koppeling **Selecteer onderdelen** om het venster **Beschermingsonderdelen** te openen.

c. Schakel de selectievakjes naast de onderdelen in die de scanuitzondering moeten gebruiken.

d. Klik in het venster **Beschermingsonderdelen** op **OK**.

Als de onderdelen in de instellingen van de scanuitzondering zijn opgegeven, wordt deze uitzondering alleen toegepast wanneer deze onderdelen van Kaspersky Endpoint Security scans uitvoeren.

Als de onderdelen niet in de instellingen van de scanuitzondering zijn opgegeven, wordt deze uitzondering toegepast wanneer alle onderdelen van Kaspersky Endpoint Security scans uitvoeren.

9. Klik in het venster **Scanuitzondering** op **OK**.

De scanuitzondering die u hebt toegevoegd, wordt in de tabel op het tabblad **Scanuitzonderingen** van het venster **Vertrouwde zone** weergegeven. De geconfigureerde instellingen van deze scanuitzondering worden in het gedeelte **Beschrijving van scanuitzondering** weergegeven.

10. Klik in het venster **Vertrouwde zone** op **OK**.

11. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een scanuitzondering wijzigen

Zo wijzigt u een scanuitzondering:

1. Open het venster met de programma-instellingen.

2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.

3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend en het tabblad **Scanuitzonderingen** wordt weergegeven.

4. Selecteer in de lijst de scanuitzondering die u wilt wijzigen.

5. Wijzig de instellingen van de scanuitzondering op een van de volgende manieren:

   - Klik op de knop **Bewerken**.

     Het venster **Scanuitzonderingen** wordt geopend.

   - Open het venster voor de bewerking van de noodzakelijke instelling door op de koppeling in het veld **Beschrijving van scanuitzondering** te klikken.

6. Als u tijdens de vorige stap op de knop **Bewerken** hebt geklikt, klikt u op **OK** in het venster **Scanuitzondering**.

   De gewijzigde instellingen van deze scanuitzondering worden in het gedeelte **Beschrijving van scanuitzondering** weergegeven.

7. Klik in het venster **Vertrouwde zone** op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een scanuitzondering verwijderen

Zo verwijdert u een scanuitzondering:

1. Open het venster met de programma-instellingen.

2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.

3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend en het tabblad **Scanuitzonderingen** wordt weergegeven.

4. Selecteer de gewenste scanuitzondering in de lijst met scanuitzonderingen.
5. Klik op de knop **Verwijderen**.

   De verwijderde scanuitzondering wordt niet langer in de lijst weergegeven.
6. Klik in het venster **Vertrouwde zone** op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Een scanuitzondering inschakelen en uitschakelen

Zo schakelt u een scanuitzondering in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend en het tabblad **Scanuitzonderingen** wordt weergegeven.
4. Selecteer de gewenste uitzondering in de lijst met scanuitzonderingen.
5. Voer een van de volgende acties uit:

   - Als u een scanuitzondering wilt inschakelen, schakelt u het selectievakje naast de naam van deze scanuitzondering in.
   - Als u een scanuitzondering wilt uitschakelen, schakelt u het selectievakje naast de naam van deze scanuitzondering uit.
6. Klik op **OK**.
7. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

De lijst met vertrouwde programma's bewerken

Zo bewerkt u de lijst met vertrouwde programma's:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend.
4. Selecteer in het venster **Vertrouwde zone** het tabblad **Vertrouwde programma's**.

5. Zo voegt u een programma aan de lijst met vertrouwde programma's toe:

   a. Klik op de knop **Toevoegen**.

   b. Doe in het geopende contextmenu een van het volgende:

   - Als u het programma wilt zoeken in de lijst met programma's die op de computer zijn geïnstalleerd, selecteert u de optie **Programma's** in het menu.

     Het venster **Programma selecteren** wordt geopend.

   - Selecteer **Bladeren** als u het pad naar het uitvoerbare bestand van het relevante programma wilt opgeven.

     Het standaardvenster **Bestand openen** wordt in Microsoft Windows geopend.

   c. Selecteer het programma op een van de volgende manieren:

   - Als u tijdens de vorige stap **Programma's** hebt geselecteerd, selecteert u het programma in de lijst met programma's die op de computer zijn geïnstalleerd en klikt u op **OK** in het venster **Programma selecteren**.

   - Als u tijdens de vorige stap **Bladeren** hebt geselecteerd, geeft u het pad naar het uitvoerbare bestand van het relevante programma op en klikt u op de knop **Openen** in het standaardvenster **Openen** van Microsoft Windows.

   Deze acties zorgen ervoor dat het venster **Scanuitzonderingen voor programma** wordt geopend.

   a. Schakel de selectievakjes naast de relevante regels van de vertrouwde zone voor het geselecteerde programma in:

   - **Scan geen geopende bestanden**.
   - **Bewaak geen programma-activiteit**.
   - **Neem geen beperkingen van bovenliggend proces (programma) over**.
   - **Bewaak geen activiteiten van onderliggende processen**.
   - **Blokkeer de interactie met de programma-interface niet**.
   - **Scan geen netwerkverkeer**.

   b. Klik in het venster **Scanuitzonderingen voor programma** op **OK**.

   Het vertrouwde programma dat u hebt toegevoegd, wordt in de lijst met vertrouwde programma's weergegeven.

6. Zo bewerkt u de instellingen van een vertrouwd programma:

   a. Selecteer een vertrouwd programma in de lijst met vertrouwde programma's.

   b. Klik op de knop **Bewerken**.

   c. Het venster **Scanuitzonderingen voor programma** wordt geopend.

   d. Schakel de selectievakjes naast de relevante regels van de vertrouwde zone voor het geselecteerde programma in of uit:

Als geen regels voor de vertrouwde zone zijn geselecteerd in het venster **Scanuitzonderingen voor programma**, wordt het vertrouwde programma ook gescand. In dit geval wordt het vertrouwde programma niet verwijderd uit de lijst met vertrouwde programma's maar is het selectievakje ervan wel uitgeschakeld.

e. Klik in het venster **Scanuitzonderingen voor programma** op **OK**.

7. Zo verwijdert u een vertrouwd programma uit de lijst met vertrouwde programma's:

   a. Selecteer een vertrouwd programma in de lijst met vertrouwde programma's.

   b. Klik op de knop **Verwijderen**.

8. Klik in het venster **Vertrouwde zone** op **OK**.

9. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Regels voor vertrouwde zone inschakelen en uitschakelen voor een programma in de lijst met vertrouwde programma's

Zo schakelt u de actie van regels voor de vertrouwde zone voor een programma uit de lijst met vertrouwde programma's in of uit:

1. Open het venster met de programma-instellingen.

2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.

3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend.

4. Selecteer in het venster **Vertrouwde zone** het tabblad **Vertrouwde programma's**.

5. Selecteer in de lijst met vertrouwde programma's het noodzakelijke vertrouwde programma.

6. Voer een van de volgende acties uit:

   - Schakel het selectievakje naast de naam van een vertrouwd programma in als u wilt instellen dat Kaspersky Endpoint Security het niet hoeft te scannen.

   - Schakel het selectievakje naast de naam van een vertrouwd programma uit als u wilt instellen dat Kaspersky Endpoint Security het moet scannen.

7. Klik op **OK**.

8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Vertrouwde systeemcertificatenopslag gebruiken

Dankzij de systeemcertificatenopslag kunt u instellen dat programma's die zijn ondertekend door een vertrouwde digitale handtekening niet moeten worden gescand op virussen. Kaspersky Endpoint Security wijst dergelijke programma's automatisch toe aan de groep *Vertrouwd*.

Zo gaat u aan de slag met de vertrouwde systeemcertificatenopslag:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend.
4. Selecteer in het venster **Vertrouwde zone** het tabblad **Vertrouwde systeemcertificatenopslag**.
5. Schakel het selectievakje **Vertrouwde systeemcertificatenopslag gebruiken** in.
6. Selecteer in de vervolgkeuzelijst **Vertrouwde systeemcertificatenopslag** welke systeemopslag van Kaspersky Endpoint Security moet worden beschouwd als vertrouwd.
7. Klik in het venster **Vertrouwde zone** op **OK**.
8. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Zelfbescherming van Kaspersky Endpoint Security

In deze sectie worden de mechanismen voor zelfbescherming en de bescherming tegen extern beheer van Kaspersky Endpoint Security beschreven en krijgt u instructies voor de configuratie van de instellingen van deze mechanismen.

Over de Zelfbescherming van Kaspersky Endpoint Security

Kaspersky Endpoint Security beschermt de computer tegen kwaadaardige programma's, inclusief malware die probeert om de werking van Kaspersky Endpoint Security te blokkeren of om Kaspersky Endpoint Security zelfs van de computer te verwijderen.

De stabiliteit van het beveiligingssysteem op de computer wordt verzekerd door de mechanismen voor zelfbescherming en bescherming tegen extern beheer in Kaspersky Endpoint Security.

Het mechanisme *Zelfbescherming* voorkomt de wijziging of de verwijdering van programmabestanden op de harde schijf, processen in het geheugen en vermeldingen in het systeemregister.

De *bescherming tegen extern beheer* blokkeert alle pogingen van een externe computer om services van programma's te beheren.

Op computers met 64-bits besturingssystemen is de Zelfbescherming van Kaspersky Endpoint Security alleen beschikbaar voor de wijziging en de verwijdering van programmabestanden op de harde schijf en van vermeldingen in het systeemregister.

Zelfbescherming inschakelen of uitschakelen

Het mechanisme Zelfbescherming van Kaspersky Endpoint Security is standaard ingeschakeld. U kunt indien nodig Zelfbescherming uitschakelen.

Zo schakelt u Zelfbescherming in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **Zelfbescherming inschakelen** in om Zelfbescherming in te schakelen.
   - Schakel het selectievakje **Zelfbescherming inschakelen** uit om Zelfbescherming uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Bescherming tegen extern beheer inschakelen of uitschakelen

Het mechanisme voor de bescherming tegen extern beheer is standaard ingeschakeld. U kunt indien nodig het mechanisme voor de bescherming tegen extern beheer uitschakelen.

Zo schakelt u het mechanisme voor de bescherming tegen extern beheer in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Voer een van de volgende acties uit:
   - Schakel het selectievakje **Extern beheer van systeemservice uitschakelen** in om het mechanisme voor de bescherming tegen extern beheer in te schakelen.
   - Schakel het selectievakje **Extern beheer van systeemservice uitschakelen** uit om het mechanisme voor de bescherming tegen extern beheer uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Ondersteuning voor programma's voor extern beheer

Mogelijk moet u soms een programma voor extern beheer gebruiken wanneer de bescherming tegen extern beheer is ingeschakeld.

Zo schakelt u de werking van programma's voor extern beheer in:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Antivirusbescherming** aan de linkerkant.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Scanuitzonderingen en vertrouwde programma's** op de knop **Instellingen**.

   Het venster **Vertrouwde zone** wordt geopend.
4. Selecteer in het venster **Vertrouwde zone** het tabblad **Vertrouwde programma's**.
5. Klik op de knop **Toevoegen**.
6. Doe in het geopende contextmenu een van het volgende:

   - Om het programma voor extern beheer te vinden in de lijst met programma's die op de computer zijn geïnstalleerd, selecteert u de optie **Programma's**.

     Het venster **Programma selecteren** wordt geopend.
   - Selecteer **Bladeren** om het pad naar het uitvoerbare bestand van het programma voor extern beheer op te geven.

     Het standaardvenster **Bestand openen** wordt in Microsoft Windows geopend.
7. Selecteer het programma op een van de volgende manieren:

   - Als u tijdens de vorige stap **Programma's** hebt geselecteerd, selecteert u het programma in de lijst met programma's die op de computer zijn geïnstalleerd en klikt u op **OK** in het venster **Programma selecteren**.
   - Als u tijdens de vorige stap **Bladeren** hebt geselecteerd, geeft u het pad naar het uitvoerbare bestand van het relevante programma op en klikt u op de knop **Openen** in het standaardvenster **Openen** van Microsoft Windows.

   Deze acties zorgen ervoor dat het venster **Scanuitzonderingen voor programma** wordt geopend.
8. Schakel het selectievakje **Bewaak geen programma-activiteit** in.
9. Klik in het venster **Scanuitzonderingen voor programma** op **OK**.

   Het vertrouwde programma dat u hebt toegevoegd, wordt in de lijst met vertrouwde programma's weergegeven.
10. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Prestaties van Kaspersky Endpoint Security en compatibiliteit met andere programma's

In deze sectie vindt u informatie over de prestaties van Kaspersky Endpoint Security en de compatibiliteit met andere programma's. U vindt ook richtlijnen voor de selectie van de soorten detecteerbare objecten en de modus waarin u Kaspersky Endpoint Security kunt gebruiken.

Over de prestaties van Kaspersky Endpoint Security en de compatibiliteit met andere programma's

Prestaties van Kaspersky Endpoint Security

Onder de prestaties van Kaspersky Endpoint Security verstaan we het aantal detecteerbare soorten objecten die de computer schade kunnen berokkenen, alsook het energieverbruik en het gebruik van de computerbronnen.

Soorten detecteerbare objecten selecteren

Met Kaspersky Endpoint Security kunt u de bescherming van uw computer precies instellen en selecteren welke soorten objecten het programma moet detecteren. Kaspersky Endpoint Security scant het besturingssysteem altijd op virussen, wormen en Trojans. U kunt het scannen van deze soorten objecten niet uitschakelen. Die malware kan de computer immers grote schade toebrengen. Voor een nog betere beveiliging op uw computer kunt u het aantal detecteerbare soorten objecten uitbreiden door de monitoring in te schakelen voor legitieme software die criminelen kunnen gebruiken om uw computer of persoonlijke gegevens te beschadigen.

Energiebesparingsmodus gebruiken

Het energieverbruik door programma's is een zeer belangrijk aspect op draagbare computers. Geplande taken van Kaspersky Endpoint Security verbruiken doorgaans heel wat bronnen. Wanneer de batterij van de computer bijna leeg is, kunt u de energiebesparingsmodus gebruiken voor een zuiniger verbruik van de energie.

In de energiebesparingsmodus worden de volgende geplande taken automatisch uitgesteld:

- Updatetaak
- Volledige Scan
- Kritieke Gebiedenscan
- Aangepaste Scan
- Kwetsbaarheidsscan
- Integriteitscontrole

Ongeacht of de energiebesparingsmodus is ingeschakeld, Kaspersky Endpoint Security pauzeert encryptietaken wanneer een draagbare computer op batterijspanning werkt. Het programma hervat de encryptietaken wanneer de draagbare computer weer overschakelt van batterijspanning op netspanning.

Computerbronnen aan andere programma's afstaan

Het gebruik van computerbronnen door Kaspersky Endpoint Security kan de prestaties van andere programma's beïnvloeden. Om het probleem van de gelijktijdige werking tijdens een verhoogde belasting van de CPU en de subsystemen van harde schijven op te lossen, kan Kaspersky Endpoint Security geplande taken pauzeren en bronnen aan andere programma's afstaan.

Een aantal programma's worden echter onmiddellijk gestart wanneer CPU-bronnen beschikbaar worden en gaan op de achtergrond werken. Als u wilt voorkomen dat scans afhankelijk worden van de prestaties van andere programma's, is het beter om geen bronnen van het besturingssysteem aan die programma's af te staan.

Indien nodig kunt u die taken handmatig starten.

Geavanceerde desinfectietechnologie gebruiken

De kwaadaardige programma's van vandaag kunnen de laagste niveaus van een besturingssysteem binnendringen, waardoor ze vrijwel onmogelijk te elimineren zijn. Na de detectie van kwaadaardige activiteit in het besturingssysteem voert Kaspersky Endpoint Security een uitgebreide desinfectieprocedure uit die een speciale geavanceerde desinfectietechnologie gebruikt. De *geavanceerde desinfectietechnologie* dient om kwaadaardige programma's waarvan de processen al in het RAM zijn geladen en die Kaspersky Endpoint Security beletten om ze met andere methoden te verwijderen in het besturingssysteem te elimineren. De bedreiging wordt hierdoor onschadelijk gemaakt. Tijdens de geavanceerde desinfectie doet u er goed aan geen nieuwe processen te starten of het register van het besturingssysteem te bewerken. De geavanceerde desinfectietechnologie gebruikt heel wat bronnen van het besturingssysteem waardoor andere programma's mogelijk trager gaan werken.

Wanneer de geavanceerde desinfectie is voltooid op een computer met Microsoft Windows voor werkstations, vraagt Kaspersky Endpoint Security toestemming aan de gebruiker om de computer opnieuw op te starten. Na het opnieuw opstarten van het systeem verwijdert Kaspersky Endpoint Security de malwarebestanden en start het een "lichte" Volledige Scan van de computer.

Op computers met Microsoft Windows voor bestandsservers ziet de gebruiker geen vraag voor de herstart van de computer wegens de specifieke eigenschappen van Kaspersky Endpoint Security voor bestandsservers. Het ongepland opnieuw opstarten van een bestandsserver kan problemen veroorzaken (bijvoorbeeld gegevens op de bestandsserver die tijdelijk niet beschikbaar zijn of niet-opgeslagen gegevens die verloren gaan). U wordt aanbevolen een bestandsserver strikt volgens schema opnieuw op te starten. Om deze reden is de geavanceerde desinfectietechnologie standaard uitgeschakeld voor bestandsservers.

Als een actieve infectie op een bestandsserver is gevonden, wordt een gebeurtenis met informatie over een noodzakelijke geavanceerde desinfectie verstuurd naar Kaspersky Security Center. Om een geavanceerde infectie op een bestandsserver te desinfecteren, schakelt u de actieve desinfectietechnologie voor bestandsservers in en start u een *Virusscan* als groepstaak op een tijdstip dat de gebruikers van de bestandsserver goed uitkomt.

Soorten detecteerbare objecten selecteren

Zo selecteert u soorten detecteerbare objecten:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Antivirusbescherming**.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Objecten** op de knop **Instellingen**.

   Het venster **Te detecteren objecten** wordt geopend.
4. Schakel de selectievakjes naast de soorten objecten in die Kaspersky Endpoint Security moet detecteren:
   - **Schadelijke tools**
   - **Adware**
   - **Automatische inbelprogramma's**

- **Overige**
- **Ingepakte bestanden die mogelijk schadelijk zijn**
- **Meermaals ingepakte bestanden**

5. Klik op **OK**.

   Het venster **Te detecteren objecten** wordt gesloten. In het gedeelte **Objecten** worden de geselecteerde soorten objecten vermeld onder **De detectie van de volgende soorten objecten is ingeschakeld**.

6. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Geavanceerde desinfectietechnologie voor werkstations inschakelen of uitschakelen

Zo schakelt u de geavanceerde desinfectietechnologie voor werkstations in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Antivirusbescherming**.

   De instellingen van de antivirusbescherming worden rechts in het venster weergegeven.

3. Doe rechts in het venster één van het volgende:
   - Schakel het selectievakje **Geavanceerde desinfectietechnologie inschakelen** in om de geavanceerde desinfectietechnologie in te schakelen.
   - Schakel het selectievakje **Geavanceerde desinfectietechnologie inschakelen** uit om de geavanceerde desinfectietechnologie uit te schakelen.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Als de taak Geavanceerde desinfectie wordt gestart via het Kaspersky Security Center, zijn de meeste functies van het besturingssysteem niet beschikbaar voor de gebruiker. Het werkstation wordt opnieuw opgestart wanneer de taak is voltooid.

Geavanceerde desinfectietechnologie voor bestandsservers inschakelen of uitschakelen

Voer een van de volgende acties uit om de geavanceerde desinfectietechnologie voor bestandsservers in te schakelen:

- Schakel de geavanceerde desinfectietechnologie in de eigenschappen van het actieve Kaspersky Security Center-beleid in. Hiertoe doet u het volgende:
  a. Open het gedeelte **Algemene beschermingsinstellingen** in het venster met de beleidseigenschappen.
  b. Schakel het selectievakje **Geavanceerde desinfectietechnologie inschakelen** in.

c. Klik op **OK** in het venster met de beleidseigenschappen om de wijzigingen op te slaan.

- Schakel het selectievakje **Geavanceerde desinfectie direct uitvoeren** in de eigenschappen van de groepstaak Virusscan van Kaspersky Security Center in.

Doe een van het volgende om de geavanceerde desinfectietechnologie voor bestandsservers uit te schakelen:

- Schakel de geavanceerde desinfectietechnologie in de eigenschappen van het Kaspersky Security Center-beleid uit. Hiertoe doet u het volgende:

  a. Open het gedeelte **Algemene beschermingsinstellingen** in het venster met de beleidseigenschappen.

  b. Schakel het selectievakje **Geavanceerde desinfectietechnologie inschakelen** uit.

  c. Klik op **OK** in het venster met de beleidseigenschappen om de wijzigingen op te slaan.

- Schakel het selectievakje **Geavanceerde desinfectie direct uitvoeren** in de eigenschappen van de groepstaak Virusscan van Kaspersky Security Center uit.

Energiebesparingsmodus inschakelen of uitschakelen

Zo inschakelt u de energiebesparingsmodus in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Uitvoermodus** op de knop **Instellingen**.

   Het venster **Uitvoermodus** wordt geopend.
4. Voer de volgende acties in het venster **Uitvoermodus** uit:

   - Schakel het selectievakje **Stel geplande taken uit bij werking op accustroom** in om de energiebesparingsmodus in te schakelen.

     Wanneer de energiebesparingsmodus is ingeschakeld en de computer op batterijspanning werkt, worden de volgende taken niet gestart zelfs als ze zijn gepland:

     - Updatetaak
     - Volledige Scan
     - Kritieke Gebiedenscan
     - Aangepaste Scan
     - Kwetsbaarheidsscan
     - Integriteitscontrole

   - Schakel het selectievakje **Stel geplande taken uit bij werking op accustroom** uit als u de energiebesparingsmodus wilt uitschakelen. In dit geval voert Kaspersky Endpoint Security geplande taken uit ongeacht de energiebron van de computer.

5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Afstaan van bronnen aan andere programma's inschakelen of uitschakelen

Zo schakelt u het afstaan van bronnen aan andere programma's in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Uitvoermodus** op de knop **Instellingen**.

   Het venster **Uitvoermodus** wordt geopend.
4. Voer de volgende acties in het venster **Uitvoermodus** uit:

   - Als u de modus wilt inschakelen waarin bronnen aan andere programma's worden afgestaan, schakelt u het selectievakje **Bronnen aan andere programma's geven** in.

     Wanneer het afstaan van bronnen aan andere programma's is geconfigureerd, stelt Kaspersky Endpoint Security geplande taken die andere programma's vertragen uit:

     - Updatetaak
     - Volledige Scan
     - Kritieke Gebiedenscan
     - Aangepaste Scan
     - Kwetsbaarheidsscan
     - Integriteitscontrole
   - Als u de modus wilt uitschakelen waarin bronnen aan andere programma's worden afgestaan, schakelt u het selectievakje **Bronnen aan andere programma's geven** uit. In dit geval voert Kaspersky Endpoint Security geplande taken uit ongeacht de werking van andere programma's.

   Standaard is het programma geconfigureerd om bronnen aan andere programma's af te staan.
5. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Wachtwoordbeveiliging

In deze sectie vindt u informatie over de beveiliging van de toegang tot Kaspersky Endpoint Security met een wachtwoord.

Over de beperking van de toegang tot Kaspersky Endpoint Security

Meerdere gebruikers met een verschillende kennis van computers kunnen eenzelfde computer delen. Als gebruikers onbeperkte toegang tot Kaspersky Endpoint Security en de instellingen ervan hebben, is het algemene niveau van de computerbescherming mogelijk lager dan gewenst.

U kunt de toegang tot Kaspersky Endpoint Security beperken door een gebruikersnaam en een wachtwoord in te stellen en de bewerkingen op te geven waarvoor de gebruiker deze gebruikersgegevens zal moeten invoeren:

Wanneer een oudere versie van het programma wordt geüpgraded naar Kaspersky Endpoint Security 10 Service Pack 2 voor Windows, wordt het wachtwoord behouden (als er een was ingesteld). Gebruik de standaard gebruikersnaam KLAdmin om de instellingen van de wachtwoordbeveiliging voor het eerst te bewerken.

Wachtwoordbeveiliging inschakelen en uitschakelen

Wij raden aan dat u voorzichtig te werk gaat wanneer u een wachtwoord gebruikt om de toegang tot het programma te beperken. Als u het wachtwoord vergeet, neemt u contact op met de Technische Support van Kaspersky voor instructies voor de uitschakeling van de wachtwoordbeveiliging.

Zo schakelt u de wachtwoordbeveiliging in:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Wachtwoordbeveiliging** op de knop **Instellingen**.

   Het venster **Wachtwoordbeveiliging** wordt geopend.
4. Schakel het selectievakje **Wachtwoordbeveiliging inschakelen** in.
5. Voer in het veld **Gebruikersnaam** de gebruikersnaam in die in het venster **Wachtwoordverificatie** moet worden opgegeven wanneer later bewerkingen worden uitgevoerd die met een wachtwoord zijn beveiligd.
6. Typ in het veld **Nieuw wachtwoord** een wachtwoord waarmee u toegang tot het programma krijgt.
7. Bevestig het wachtwoord in het veld **Bevestig wachtwoord**.
8. Als u de toegang voor alle bewerkingen met het programma wilt beperken, klikt u in het gedeelte **Wachtwoordbereik** op de knop **Alles selecteren**.
9. Als u de toegang van gebruikers selectief wilt beperken, schakelt u in het gedeelte **Wachtwoordbereik** de selectievakjes naast de namen van de relevante bewerkingen in:
   - **Programma-instellingen configureren**.
   - **Programma afsluiten**.
   - **Beschermingsonderdelen uitschakelen**.
   - **Controle-onderdelen uitschakelen**.

- **Code verwijderen**.
- **Programma verwijderen/wijzigen/herstellen**.
- **Toegang tot gegevens op geëncrypte schijven herstellen**.
- **Rapporten bekijken**.

10. Klik op de knop **OK**.

    Het programma controleert de ingevoerde wachtwoorden. Als de wachtwoorden overeenkomen, past het programma het wachtwoord toe. Als de wachtwoorden niet overeenkomen, wordt u door het programma gevraagd om het wachtwoord opnieuw te bevestigen in het veld **Bevestig wachtwoord**.

Nadat de wachtwoordbeveiliging is ingeschakeld, vraagt het programma het wachtwoord telkens als een bewerking wordt uitgevoerd die met het wachtwoord is beveiligd. Als u niet wilt dat het programma het wachtwoord vraagt telkens als u tijdens de huidige sessie een bewerking wilt uitvoeren die met het wachtwoord is beveiligd, kunt u het selectievakje **Onthoud wachtwoord voor deze sessie** in het venster **Wachtwoordverificatie** inschakelen.

Als het selectievakje **Onthoud wachtwoord voor deze sessie** is uitgeschakeld, wordt u bij elke bewerking die met het wachtwoord is beveiligd gevraagd om het wachtwoord in te voeren.

Zo schakelt u de wachtwoordbeveiliging uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Wachtwoordbeveiliging** op de knop **Instellingen**.

   Het venster **Wachtwoordbeveiliging** wordt geopend.
4. Schakel het selectievakje **Wachtwoordbeveiliging inschakelen** uit.

   U kunt Wachtwoordbeveiliging alleen uitschakelen als u bent aangemeld als KLAdmin. Wachtwoordbeveiliging kan niet worden uitgeschakeld als u een ander gebruikersaccount of een tijdelijk wachtwoord gebruikt.
5. Klik op de knop **OK**.

Nadat de wachtwoordbeveiliging is uitgeschakeld, wordt de verboden toegang tot het programma geannuleerd bij de volgende opstart van Kaspersky Endpoint Security.

Het wachtwoord voor de toegang tot Kaspersky Endpoint Security wijzigen

Zo wijzigt u het wachtwoord voor de toegang tot Kaspersky Endpoint Security:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.
3. Klik in het gedeelte **Wachtwoordbeveiliging** op de knop **Instellingen**.

Het venster **Wachtwoordbeveiliging** wordt geopend.

4. Voer de gebruikersnaam in het veld **Gebruikersnaam** in.
5. Typ in het veld **Nieuw wachtwoord** een nieuw wachtwoord waarmee u toegang tot het programma krijgt.
6. Voer in het veld **Bevestig wachtwoord** het nieuwe wachtwoord opnieuw in.
7. Klik op **OK**.

   Het programma controleert de ingevoerde wachtwoorden. Als de wachtwoorden overeenkomen, past het programma het nieuwe wachtwoord toe en wordt het venster **Wachtwoordbeveiliging** gesloten. Als de wachtwoorden niet overeenkomen, wordt u door het programma gevraagd om het wachtwoord opnieuw te bevestigen in het veld **Bevestig wachtwoord**.
8. Klik in het venster met de programma-instellingen op de knop **Opslaan** om de wijzigingen op te slaan.

Over het gebruik van een tijdelijk wachtwoord

Wanneer gebruikers werken op clientcomputers die door een Kaspersky Security Center-beleid worden beheerd, moet ze mogelijk bewerkingen met Kaspersky Endpoint Security uitvoeren die door het beleid zijn beveiligd met een wachtwoord. Als de wachtwoordbeveiliging is ingeschakeld, kan alleen de beheerder van Kaspersky Security Center de bewerkingen uitvoeren die in het wachtwoordbereik zijn opgegeven. Mocht de verbinding met Kaspersky Security Center echter worden verbroken (zoals wanneer de gebruiker zich buiten het bedrijfsnetwerk bevindt), dan zijn de functies voor het werken met de lokale interface van Kaspersky Security Center beperkt.

Om een gebruiker de noodzakelijke bewerkingen te laten uitvoeren zonder het wachtwoord te geven dat in de beleidsinstellingen is ingesteld, kan de beheerder van Kaspersky Security Center een tijdelijk wachtwoord aanmaken. Een tijdelijk wachtwoord heeft een beperkte geldigheidsduur en een beperkt actiebereik. Nadat de gebruiker het tijdelijke wachtwoord in de lokale interface van het programma heeft ingevoerd, worden de bewerkingen beschikbaar die door de beheerder van Kaspersky Security Center zijn toegestaan.

Wanneer het tijdelijke wachtwoord verloopt, blijft Kaspersky Endpoint Security werken volgens de instellingen van het Kaspersky Endpoint Security-beleid. Bewerkingen die door het beleid zijn beveiligd met een wachtwoord worden beschikbaar voor de gebruiker.

Een tijdelijk wachtwoord aanmaken via de Beheerconsole van Kaspersky Security Center

Zo maakt u een tijdelijk wachtwoord aan en stuurt u het naar een gebruiker:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de computer van de gebruiker behoort die het tijdelijke wachtwoord heeft aangevraagd.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer **Eigenschappen** in het contextmenu van de computer van de gebruiker die het tijdelijke wachtwoord heeft aangevraagd.

   Het venster **Eigenschappen: <Naam van computer>** wordt geopend.
5. Selecteer in het venster **Eigenschappen: <Naam van computer>** het gedeelte **Programma's**.

6. Selecteer Kaspersky Endpoint Security Service Pack 2 voor Windows en open het venster met de eigenschappen van het programma op een van de volgende manieren:

   - Klik op de knop **Eigenschappen** onder in het scherm.
   - Selecteer in het contextmenu van het programma de optie **Eigenschappen**.

   Hiermee opent u het venster **Programma-instellingen "<Naam van programma>"**.

7. In het venster **Programma-instellingen "<Naam van programma>"** selecteert u in het gedeelte **Geavanceerde instellingen** het subgedeelte **Programma-instellingen**.

8. Klik in het gedeelte **Wachtwoordbeveiliging** op de knop **Instellingen**.

   Het venster **Wachtwoordbeveiliging** wordt geopend.

9. In het venster **Wachtwoordbeveiliging** klikt u in het gedeelte **Tijdelijk wachtwoord** op de knop **Instellingen**.

   Deze knop is beschikbaar als de wachtwoordbeveiliging voor Kaspersky Security Center is ingeschakeld in het Kaspersky Security Center-beleid dat op de computer wordt uitgevoerd.

   Het venster **Tijdelijk wachtwoord aanmaken** wordt geopend.

10. Geef in het veld **Verloopdatum** de datum op waarop de gebruiker het tijdelijke wachtwoord niet meer kan gebruiken.

    Op deze datum wordt het tijdelijke wachtwoord ongeldig. Een nieuw tijdelijk wachtwoord moet worden aangemaakt om toegang te verlenen voor het uitvoeren van bewerkingen in de lokale interface van Kaspersky Endpoint Security.

11. Schakel in de tabel **Bereik tijdelijk wachtwoord** de selectievakjes in naast de bewerkingen die de gebruiker mag uitvoeren wanneer het tijdelijke wachtwoord geldig is.

12. Klik op de knop **Maken**.

    Hiermee opent u het venster **Tijdelijk wachtwoord** dat een geëncrypt bestand bevat.

13. Kopieer het wachtwoord en de instructies voor de toepassing ervan en verstuur ze naar de gebruiker.

Een tijdelijk wachtwoord in de interface van Kaspersky Endpoint Security toepassen

Deze instructies zijn bestemd voor gebruikers van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd.

Zo past u een tijdelijk wachtwoord toe:

1. Open het venster met de programma-instellingen.

2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De programma-instellingen worden rechts in het venster weergegeven.

3. Klik in het gedeelte **Wachtwoordbeveiliging** op de knop **Tijdelijk wachtwoord**.

   Het venster **Tijdelijk wachtwoord** wordt geopend.

4. Schakel het selectievakje **Tijdelijk wachtwoord inschakelen** in.

5. Geef in het invoerveld het wachtwoord op dat u van de beheerder van Kaspersky Security Center hebt gekregen.

6. Klik op **OK** om de wijzigingen op te slaan.

Wanneer het tijdelijke wachtwoord is toegepast, worden de bewerkingen die zijn opgegeven door de beheerder van Kaspersky Security Center beschikbaar. In het venster **Tijdelijk wachtwoord** ziet u de verloopdatum van het tijdelijke wachtwoord en de toegestane bewerkingen.

Extern beheer van het programma via Kaspersky Security Center

In deze sectie wordt beschreven hoe u Kaspersky Endpoint Security beheert via Kaspersky Security Center.

Over het beheer van het programma via Kaspersky Security Center

Met Kaspersky Security Center kunt u Kaspersky Endpoint Security op afstand installeren, verwijderen, starten en stoppen. U kunt ook op afstand de programma-instellingen configureren, de beschikbare programmaonderdelen wijzigen en update- en scantaken starten.

Voor aanvullende informatie over het beheer van het programma via Kaspersky Security Center die u niet in dit document vindt, raadpleegt u de *beheerdershandleiding van Kaspersky Security Center*.

Het programma kan via Kaspersky Security Center worden beheerd met behulp van de beheerplug-in van Kaspersky Endpoint Security.

De versie van de beheerplug-in verschilt mogelijk van de geïnstalleerde versie van Kaspersky Endpoint Security op de clientcomputer. Als de geïnstalleerde versie van de beheerplug-in minder functies heeft dan de geïnstalleerde versie van Kaspersky Endpoint Security, worden de instellingen van de ontbrekende functies niet beheerd door de beheerplug-in. Deze instellingen kunnen door de gebruiker worden gewijzigd in de lokale interface van Kaspersky Endpoint Security.

Speciale aandachtspunten bij het werken met verschillende versies van beheerplug-ins

U kunt een beheerplug-in gebruiken om de volgende items te wijzigen:

- Beleid
- Beleidsprofielen
- Groepstaken
- Lokale taken
- Lokale instellingen van Kaspersky Endpoint Security

U kunt Kaspersky Endpoint Security alleen via Kaspersky Security Center beheren als u een beheerplug-in hebt waarvan de versie gelijk is aan of nieuwer is dan de vermelde versie in de informatie over de compatibiliteit van Kaspersky Endpoint Security met de beheerplug-in. U kunt de minimale vereiste versie van de beheerplug-in bekijken in het bestand 'installer.ini' van het distributiepakket.

Als een onderdeel wordt geopend, controleert de beheerplug-in de informatie over de compatibiliteit ervan. Als de versie van de beheerplug-in gelijk is aan of nieuwer is dan de vermelde versie in de informatie over de compatibiliteit, kunt u de instellingen van dit onderdeel wijzigen. Anders kunt u de beheerplug-in niet gebruiken om de instellingen van het geselecteerde onderdeel te wijzigen. U wordt aanbevolen om de beheerplug-in bij te werken.

Eerder gedefinieerde instellingen wijzigen met een nieuwere versie van de beheerplug-in

U kunt een nieuwere versie van de beheerplug-in gebruiken om alle eerder gedefinieerde instellingen te wijzigen en om nieuwe instellingen te configureren die niet in de vorige versie van de beheerplug-in voorkwamen.

De nieuwe versie van de beheerplug-in wijst standaardwaarden aan de nieuwe instellingen toe wanneer een beleid, een beleidsprofiel of een taak voor het eerst wordt opgeslagen.

Na het wijzigen van de instellingen van een beleid, een beleidsprofiel of een groepstaak met een nieuwere versie van de beheerplug-in zijn deze onderdelen niet meer beschikbaar voor oudere versies van de beheerplug-in. De lokale instellingen van Kaspersky Endpoint Security en de instellingen van lokale taken zijn wel nog beschikbaar voor oudere versies van de beheerplug-in.

Kaspersky Endpoint Security starten en stoppen op een clientcomputer

Zo start of stopt u het programma op een clientcomputer:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer de computer waarop u het programma wilt starten of stoppen.
5. Klik rechts om het contextmenu van de clientcomputer weer te geven en selecteer **Eigenschappen**.

   Een venster met eigenschappen van de clientcomputer wordt geopend.
6. Selecteer het gedeelte **Programma's** in het venster met de eigenschappen van de clientcomputer.

   Een lijst met geïnstalleerde Kaspersky-programma's op de clientcomputer wordt rechts in het venster met de eigenschappen van de clientcomputer weergegeven.
7. Selecteer Kaspersky Endpoint Security 10 voor Windows.
8. Doe het volgende:

   - Als u het programma wilt starten, klikt u op de knop rechts van de lijst met Kaspersky-programma's of doet u het volgende:

     a. Selecteer **Eigenschappen** in het contextmenu van Kaspersky Endpoint Security of klik op de knop **Eigenschappen** onder de lijst met Kaspersky-programma's.

     Het venster **Instellingen van Kaspersky Endpoint Security 10 voor Windows** wordt geopend.

     b. Klik in het gedeelte **Algemeen** op de knop **Starten** rechts in het venster.

   - Als u het programma wilt stoppen, klikt u op de knop rechts van de lijst met Kaspersky-programma's of doet u het volgende:

     a. Selecteer **Eigenschappen** in het contextmenu van Kaspersky Endpoint Security of klik op de knop **Eigenschappen** onder de lijst met Kaspersky-programma's.

     Het venster **Instellingen van Kaspersky Endpoint Security 10 voor Windows** wordt geopend.

b. Klik in het gedeelte **Algemeen** op de knop **Stoppen** rechts in het venster.

Instellingen van Kaspersky Endpoint Security configureren

Zo configureert u de instellingen van Kaspersky Endpoint Security:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer de computer waarvoor u de instellingen van Kaspersky Endpoint Security wilt configureren.
5. Selecteer in het contextmenu van de clientcomputer de optie **Eigenschappen**.

   Een venster met eigenschappen van de clientcomputer wordt geopend.
6. Selecteer het gedeelte **Programma's** in het venster met de eigenschappen van de clientcomputer.

   Een lijst met geïnstalleerde Kaspersky-programma's op de clientcomputer wordt rechts in het venster met de eigenschappen van de clientcomputer weergegeven.
7. Selecteer het programma Kaspersky Endpoint Security 10 voor Windows.
8. Voer een van de volgende acties uit:

   - Selecteer **Eigenschappen** in het contextmenu van Kaspersky Endpoint Security 10 voor Windows.
   - Klik op de knop **Eigenschappen** onder de lijst met Kaspersky-programma's.

   Het venster **Instellingen van Kaspersky Endpoint Security 10 voor Windows** wordt geopend.
9. Configureer in het gedeelte **Geavanceerde instellingen** de instellingen voor Kaspersky Endpoint Security en de instellingen voor de rapporten en de opslag.

   De andere gedeelten van het venster **Instellingen van Kaspersky Endpoint Security 10 voor Windows** zijn dezelfde als in de standaard programmagedeelten van Kaspersky Security Center. Een beschrijving van deze gedeelten vindt u in de *beheerdershandleiding van Kaspersky Security Center*.

   Als een programma wordt beheerd door een beleid dat wijzigingen aan specifieke instellingen verbiedt, kunt u ze niet bewerken wanneer u programma-instellingen in het gedeelte **Geavanceerde instellingen** configureert.
10. Om de wijzigingen op te slaan, klikt u in het venster **Instellingen van Kaspersky Endpoint Security 10 voor Windows** op **OK**.

Taken beheren

In deze sectie wordt beschreven hoe u taken voor Kaspersky Endpoint Security beheert. Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het beheer van taken via Kaspersky Security Center.

Over taken voor Kaspersky Endpoint Security

Kaspersky Security Center beheert de activiteit van Kaspersky-programma's op clientcomputers door middel van taken. Via taken worden de primaire beheerfuncties uitgevoerd, zoals het installeren van codes, het scannen van de computer en het bijwerken van de databases en softwaremodules van het programma.

U kunt de volgende soorten taken aanmaken om Kaspersky Endpoint Security te beheren via Kaspersky Security Center:

- Lokale taken die voor een individuele clientcomputer zijn geconfigureerd.
- Groepstaken die voor clientcomputers in beheergroepen zijn geconfigureerd.
- Taken voor een reeks computers die niet tot beheergroepen behoren.

  Taken voor een reeks computers buiten beheergroepen zijn alleen van toepassing op de clientcomputers die in de taakinstellingen zijn opgegeven. Als nieuwe clientcomputers zijn toegevoegd aan een reeks computers waarvoor een taak is geconfigureerd, wordt deze taak niet toegepast op deze nieuwe computers. Om de taak op deze computers toe te passen, maakt u een nieuwe taak aan of bewerkt u de instellingen van de bestaande taak.

Voor het externe beheer van Kaspersky Endpoint Security kunt u de volgende soorten taken gebruiken:

- **Code toevoegen**. Kaspersky Endpoint Security voegt een code voor de activatie van het programma toe, waaronder een extra code.
- **Programma-onderdelen wijzigen**. Kaspersky Endpoint Security installeert of verwijdert onderdelen op clientcomputers volgens de lijst met onderdelen die in de taakinstellingen is opgegeven.
- **Inventaris**. Kaspersky Endpoint Security verzamelt informatie over alle uitvoerbare bestanden van programma's die op computers zijn opgeslagen.

  U kunt de inventarisatie van DLL-modules en scriptbestanden inschakelen. In dit geval ontvangt Kaspersky Security Center informatie over DLL-modules die zijn geladen op een computer waarop Kaspersky Endpoint Security is geïnstalleerd en over bestanden met scripts.

  Door het inschakelen van de inventarisatie van DLL-modules en scriptbestanden duurt de inventarisatietaak aanzienlijk langer en wordt de database veel groter.

- **Update**. Kaspersky Endpoint Security werkt de databases en programmamodules bij volgens de geconfigureerde update-instellingen.
- **Terugdraaien**. Kaspersky Endpoint Security draait de laatste update van de databases en de modules terug.
- **Virusscan**. Kaspersky Endpoint Security scant de in de taakinstellingen opgegeven computergebieden op virussen en andere bedreigingen.

- **Verbinding met KSN controleren**. Kaspersky Endpoint Security verstuurt een vraag over de beschikbaarheid van KSN-servers en werkt de status van de verbinding met KSN bij.
- **Integriteitscontrole**. Kaspersky Endpoint Security ontvangt gegevens over de geïnstalleerde programmamodules op de clientcomputer en scant de digitale handtekening van elke module.
- **Accounts in Verificatie-agent beheren**. Tijdens de uitvoering van deze taak genereert Kaspersky Endpoint Security opdrachten voor het verwijderen, toevoegen of wijzigen van accounts in Verificatie-agent.

U kunt de volgende acties met taken uitvoeren:

- Taken starten, stoppen, onderbreken en hervatten.
- Nieuwe taken aanmaken.
- Taakinstellingen bewerken.

De rechten voor de toegang tot de instellingen van Kaspersky Endpoint Security-taken (lezen, schrijven, uitvoeren) worden voor elke gebruiker die toegang heeft tot de Administration Server van Kaspersky Security Center gedefinieerd via de instellingen voor de toegang tot de functionele gebieden van Kaspersky Endpoint Security. Om de toegang tot de functionele gebieden van Kaspersky Endpoint Security te configureren, gaat u naar het gedeelte **Beveiliging** van het venster met de eigenschappen van de Administration Server van Kaspersky Security Center.

De modus voor taakbeheer configureren

Zo configureert u de modus voor het werken met taken in de lokale interface van Kaspersky Endpoint Security:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u de modus voor het werken met taken in de lokale interface van Kaspersky Endpoint Security wilt configureren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het gedeelte **Geavanceerde instellingen** het subgedeelte **Programma-instellingen**.
7. In het gedeelte **Uitvoermodus**:
   - Als u wilt toestaan dat gebruikers werken met lokale taken in de interface en via de opdrachtregel van Kaspersky Endpoint Security, schakelt u het selectievakje **Gebruik van lokale taken toestaan** in.

     Als het selectievakje is uitgeschakeld, wordt de werking van lokale taken gestopt. In deze modus worden de lokale taken niet volgens het schema uitgevoerd. Lokale taken kunnen ook niet worden gestart en bewerkt in de lokale interface van Kaspersky Endpoint Security en via de opdrachtregel.

- Schakel het selectievakje **Weergave van groepstaken toestaan** in als u wilt toestaan dat gebruikers de lijst met groepstaken bekijken.
- Schakel het selectievakje **Beheer van groepstaken toestaan** in als u wilt toestaan dat gebruikers de instellingen van groepstaken wijzigen.

8. Klik op **OK** om de wijzigingen op te slaan.
9. Pas het beleid toe.

   Raadpleeg de *beheerdershandleiding van Kaspersky Security Center* voor informatie over het toepassen van het Kaspersky Security Center-beleid.

Een lokale taak aanmaken

Zo maakt u een lokale taak aan:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer de computer waarvoor u een lokale taak wilt aanmaken.
5. Voer een van de volgende acties uit:
   - Selecteer in het contextmenu van de clientcomputer de optie **Alle taken** Taak aanmaken.
   - Selecteer in het contextmenu van de clientcomputer de optie **Eigenschappen**. In het geopende venster **Eigenschappen: <naam van computer>** klikt u op het tabblad **Taken** op de knop **Toevoegen**.
   - Selecteer in de vervolgkeuzelijst **Actie uitvoeren** de optie **Taak aanmaken**.

   De wizard Taak wordt gestart.
6. Volg de instructies van de wizard Taak.

Een groepstaak aanmaken

Zo maakt u een groepstaak aan:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Voer een van de volgende acties uit:
   - Selecteer de map **Beheerde apparaten** in de structuur van de Beheerconsole om een groepstaak voor alle computers beheerd door Kaspersky Security Center aan te maken.
   - Selecteer in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.

3. Selecteer het tabblad **Taken** in de werkruimte.
4. Klik op de knop **Taak aanmaken**.

   De wizard Taak wordt gestart.
5. Volg de instructies van de wizard Taak.

Een taak voor een selectie van apparaten aanmaken

Doe het volgende om een taak voor een selectie van apparaten aan te maken:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer de map **Taken** in de structuur van de Beheerconsole.
3. Klik op de knop **Taak aanmaken**.

   De wizard Taak wordt gestart.
4. Volg de instructies van de wizard Taak.
5. Klik in het venster **Selecteer de apparaten waaraan de taak wordt toegewezen** van de wizard op de knop **Taak aan een selectie van apparaten toewijzen**.
6. Klik in het volgende venster van de wizard op de knop **Selecteren**.

   Het venster **Selectie van apparaten** wordt geopend.
7. Selecteer de noodzakelijke apparaten.
8. Klik op **OK** in het venster **Selectie van apparaten**.
9. Volg de instructies van de wizard Taak.

Een taak starten, stoppen, onderbreken en hervatten

Als Kaspersky Endpoint Security wordt uitgevoerd op een clientcomputer, kunt u via Kaspersky Security Center een taak starten, stoppen, onderbreken en hervatten op deze clientcomputer. Als Kaspersky Endpoint Security wordt onderbroken, worden alle actieve taken onderbroken en kunt u geen taken starten, stoppen, onderbreken of hervatten via Kaspersky Security Center.

Zo start, stopt, onderbreekt of hervat u een lokale taak:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.

4. Selecteer de computer waarop u een lokale taak wilt starten, stoppen, pauzeren of hervatten.

5. Klik rechts om het contextmenu van de clientcomputer weer te geven en selecteer **Eigenschappen**.

   Een venster met eigenschappen van de clientcomputer wordt geopend.

6. Selecteer het gedeelte **Taken**.

   Een lijst met lokale taken wordt rechts in het venster weergegeven.

7. Selecteer een lokale taak die u wilt starten, stoppen, onderbreken of hervatten.

8. Voer de noodzakelijke actie op de taak uit door een van de volgende methoden te gebruiken:

   - Klik rechts om het contextmenu van de lokale taak te openen en selecteer **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.
   - Om een lokale taak te starten of te stoppen, klikt u op de knop / rechts van de lijst met lokale taken.
   - Doe het volgende:

     a. Klik op de knop **Eigenschappen** onder de lijst met lokale taken of selecteer **Eigenschappen** in het contextmenu van de taak.

        Het venster **Eigenschappen: <naam van taak>** wordt geopend.

     b. Klik op het tabblad **Algemeen** op de knop **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.

Zo start, stopt, pauzeert of hervat u een groepstaak:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waarvoor u een groepstaak wilt starten, stoppen, pauzeren of hervatten.

3. Selecteer het tabblad **Taken** in de werkruimte.

   De groepstaken worden rechts in het venster weergegeven.

4. Selecteer een groepstaak die u wilt starten, stoppen, pauzeren of hervatten.

5. Voer de noodzakelijke actie op de taak uit door een van de volgende methoden te gebruiken:

   - Selecteer in het contextmenu van de groepstaak de optie **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.
   - Klik op de knop / rechts in het venster om een groepstaak te starten of te stoppen.
   - Doe het volgende:

     a. Klik op de koppeling **Taakinstellingen** rechts in de werkruimte van de Beheerconsole of selecteer **Eigenschappen** in het contextmenu van de taak.

        Het venster **Eigenschappen: <naam van taak>** wordt geopend.

     b. Klik op het tabblad **Algemeen** op de knop **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.

Zo start, stopt, pauzeert of hervat u een taak voor een selectie van computers:

1. Open de Beheerconsole van Kaspersky Security Center.

2. Selecteer in de map **Taken** in de structuur van de Beheerconsole de taak voor de selectie van computers die u wilt starten, stoppen, pauzeren of hervatten.
3. Voer een van de volgende acties uit:
   - Selecteer in het contextmenu van de taak de optie **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.
   - Klik op de knop / rechts in het venster om de taak voor specifieke computers te starten of te stoppen.
   - Doe het volgende:
     a. Klik op de koppeling **Taakinstellingen** rechts in de werkruimte van de Beheerconsole of selecteer **Eigenschappen** in het contextmenu van de taak.
     Het venster **Eigenschappen: <naam van taak>** wordt geopend.
     b. Klik op het tabblad **Algemeen** op de knop **Starten** / **Stoppen** / **Pauzeren** / **Hervatten**.

Taakinstellingen bewerken

Zo bewerkt u de instellingen van een lokale taak:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputer behoort.
3. Selecteer in de werkruimte het tabblad **Apparaten**.
4. Selecteer de computer waarvoor u programma-instellingen wilt configureren.
5. Klik rechts om het contextmenu van de clientcomputer weer te geven en selecteer **Eigenschappen**.
   Een venster met eigenschappen van de clientcomputer wordt geopend.
6. Selecteer het gedeelte **Taken**.
   Een lijst met lokale taken wordt rechts in het venster weergegeven.
7. Selecteer de noodzakelijke lokale taak in de lijst met lokale taken.
8. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
9. Selecteer in het venster **Eigenschappen:<naam van lokale taak>** het gedeelte **Instellingen**.
10. Bewerk de instellingen van de lokale taak.
11. Klik in het venster **Eigenschappen: <naam van lokale taak>** op **OK** om de wijzigingen op te slaan.
12. Klik in het venster **Eigenschappen: <naam van computer>** op **OK** om de wijzigingen op te slaan.

Zo bewerkt u de instellingen van een groepstaak:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** de map met de naam van de relevante beheergroep.
3. Selecteer het tabblad **Taken** in de werkruimte.
   Groepstaken worden in de werkruimte van de Beheerconsole weergegeven.
4. Selecteer de noodzakelijke groepstaak.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
6. Selecteer in het venster **Eigenschappen:<naam van groepstaak>** het gedeelte **Instellingen**.
7. Bewerk de instellingen van de groepstaak.
8. Klik in het venster **Eigenschappen: <naam van groepstaak>** op **OK** om de wijzigingen op te slaan.

Zo bewerkt u de instellingen van een taak voor een selectie van computers:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de map **Taken** in de structuur van de Beheerconsole de taak voor de selectie van computers waarvan u de instellingen wilt bewerken.
3. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.
4. Selecteer in het venster **Eigenschappen: <naam van de taak voor de selectie van computers>** het gedeelte **Instellingen**.
5. Bewerk de taakinstellingen voor de selectie van computers.
6. Klik in het venster **Eigenschappen: <naam van de taak voor de selectie van computers>** op **OK** om de wijzigingen op te slaan.

Met uitzondering van het gedeelte **Instellingen** zijn alle gedeelten in het venster met de taakeigenschappen identiek aan deze die in Kaspersky Security Center worden gebruikt. Voor een gedetailleerde beschrijving ervan raadpleegt u de *beheerdershandleiding van Kaspersky Security Center*. In het gedeelte **Instellingen** vindt u de specifieke instellingen van Kaspersky Endpoint Security 10 voor Windows. De inhoud ervan hangt af van de geselecteerde taak of het type van de taak.

Beleid beheren

In deze sectie wordt de aanmaak en de configuratie van een beleid voor Kaspersky Endpoint Security besproken. Voor meer gedetailleerde informatie over het beheer van Kaspersky Endpoint Security via een Kaspersky Security Center-beleid raadpleegt u de *beheerdershandleiding van Kaspersky Security Center*.

Over het beleid

U kunt een beleid gebruiken om identieke instellingen van Kaspersky Endpoint Security toe te passen op alle clientcomputers in een beheergroep.

U kunt de opgegeven waarden van instellingen in een beleid voor individuele computers in een beheergroep lokaal wijzigen via Kaspersky Endpoint Security. Alleen de instellingen die volgens het beleid mogen worden gewijzigd kunt u lokaal wijzigen.

De mogelijke bewerking van een programma-instelling op een clientcomputer wordt bepaald aan de hand van de "vergrendelde" status van de instelling in een beleid:

- Als een instelling is "vergrendeld" (), kunt u de waarde van deze instelling niet lokaal bewerken. De in het beleid opgegeven waarde van de instelling wordt voor alle clientcomputers in de beheergroep gebruikt.
- Als een instelling is "ontgrendeld" (), kunt u de instelling lokaal bewerken. Een lokaal geconfigureerde instelling wordt op alle clientcomputers in de beheergroep toegepast. De instelling die in het beleid is geconfigureerd wordt niet toegepast.

Wanneer het beleid voor het eerst is toegepast, worden de lokale programma-instellingen volgens de beleidsinstellingen gewijzigd.

De rechten voor de toegang tot de beleidsinstellingen (lezen, schrijven, uitvoeren) worden voor elke gebruiker die toegang heeft tot de Administration Server van Kaspersky Security Center opgegeven, en ook apart voor elk functioneel bereik van Kaspersky Endpoint Security. Om de rechten voor de toegang tot de beleidsinstellingen te configureren, gaat u naar het gedeelte **Beveiliging** van het venster met de eigenschappen van de Administration Server van Kaspersky Security Center.

De volgende functionele bereiken van Kaspersky Endpoint Security worden onderscheiden:

- Antivirusbescherming. Het functionele bereik omvat Anti-Virus voor bestanden, Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Kwetsbaarheidsscan en scantaken.
- Programma-opstartcontrole. Het functionele bereik omvat het onderdeel Programma-opstartcontrole.
- Apparaatcontrole. Het functionele bereik omvat het onderdeel Apparaatcontrole.
- Encryptie. Het functionele bereik omvat de onderdelen voor de encryptie van harde schijven, bestanden en mappen.
- Vertrouwde zone. Het functionele bereik omvat de Vertrouwde zone.
- Webcontrole. Het functionele bereik omvat het onderdeel Webcontrole.
- Host Intrusion Prevention. Dit functionele bereik omvat Programma-activiteitenbewaking, Kwetsbaarheidsbewaking, Firewall, Network Attack Blocker en Controle van programmabevoegdheden.
- Basisfunctionaliteit. Dit functionele bereik omvat algemene programma-instellingen die niet voor andere functionele bereiken zijn opgegeven, zoals: licentiebeheer, instellingen voor KSN, inventarisaties, updatetaken

voor databases en modules, Zelfbescherming, geavanceerde programma-instellingen, rapporten en opslag, instellingen voor wachtwoordbeveiliging en instellingen voor de programma-interface.

U kunt de volgende bewerkingen uitvoeren voor een beleid:

- Maak een beleid aan.
- Bewerk beleidsinstellingen.

  Als het gebruikersaccount waarmee u toegang tot de Administration Server hebt gekregen geen rechten voor de bewerking van instellingen van bepaalde functionele bereiken heeft, kunnen de instellingen van deze functionele bereiken niet worden bewerkt.

- Verwijder een beleid.
- Wijzig de status van een beleid.

Voor informatie over het gebruik van een beleid waarvoor geen interactie met Kaspersky Endpoint Security is vereist, raadpleegt u de *beheerdershandleiding van Kaspersky Security Center*.

Een beleid aanmaken

Zo maakt u een beleid aan:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Voer een van de volgende acties uit:
   - Selecteer de map **Beheerde apparaten** in de structuur van de Beheerconsole als u een beleid voor alle computers beheerd door Kaspersky Security Center wilt aanmaken.
   - Selecteer in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Voer een van de volgende acties uit:
   - Klik op de knop **Beleid aanmaken**.
   - Klik rechts om het contextmenu te openen en selecteer Beleid **maken** .

   De wizard Beleid wordt gestart.
5. Volg de instructies van de wizard Beleid.

Beleidsinstellingen bewerken

Zo bewerkt u de beleidsinstellingen:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Beheerde apparaten** in de structuur van de Beheerconsole de map met de naam van de relevante beheergroep waarvoor u beleidsinstellingen wilt bewerken.
3. Selecteer in de werkruimte het tabblad **Beleid**.
4. Selecteer het noodzakelijke beleid.
5. Open het venster **Eigenschappen: <naam van beleid>** op een van de volgende manieren:
   - Selecteer in het contextmenu van het beleid de optie **Eigenschappen**.
   - Klik op de koppeling **Beleid configureren** rechts in de werkruimte van de Beheerconsole.

   De beleidsinstellingen voor Kaspersky Endpoint Security 10 voor Windows omvatten de instellingen van onderdelen en de programma-instellingen. In de gedeelten **Antivirusbescherming** en **Endpoint-controle** van het venster **Eigenschappen: <naam van beleid>** ziet u de instellingen van de beschermings- en controle-onderdelen terwijl u in het gedeelte **Gegevensencryptie** de encryptie-instellingen voor bestanden en mappen en in het gedeelte **Geavanceerde instellingen** de programma-instellingen ziet.

   Als u de weergave van de instellingen voor gegevensencryptie en de instellingen van controle-onderdelen in de beleidsinstellingen wilt inschakelen, moet u de overeenkomstige selectievakjes in het venster **Interface-instellingen** van Kaspersky Security Center inschakelen.
6. Bewerk de beleidsinstellingen.
7. Klik in het venster **Eigenschappen: <naam van beleid>** op **OK** om uw wijzigingen op te slaan.

Instellingen selecteren die in het Kaspersky Security Center-beleid moeten worden weergegeven

Zo selecteert u de instellingen die in het Kaspersky Security Center-beleid moeten worden weergegeven

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in het contextmenu van het knooppunt **Administration Server – <Naam van computer>** in de structuur van de Beheerconsole achtereenvolgens Weergave → **Interface-instellingen**.

   Het venster **Interface-instellingen** wordt geopend.
3. Schakel in het venster **Interface-instellingen** de selectievakjes naast de instellingen in die u in de instellingen voor het aanmaken van het Kaspersky Security Center-beleid en in de eigenschappen van het beleid wilt weergeven:
   - Schakel het selectievakje **Onderdelen van Endpoint-controle weergeven** in om de weergave van de instellingen van controle-onderdelen in het venster van de wizard Nieuw beleid van Kaspersky Security Center en in de eigenschappen van het beleid in te schakelen.
   - Schakel het selectievakje **Encryptie en gegevensbescherming tonen** in om de weergave van de instellingen voor gegevensencryptie in de wizard Nieuw beleid van Kaspersky Security Center en in de eigenschappen van het beleid in te schakelen.
4. Klik op **OK**.

Gebruikersberichten naar de server van Kaspersky Security Center sturen

In de volgende gevallen moet een gebruiker mogelijk een bericht naar de beheerder van het bedrijfsnetwerk sturen:

- Apparaatcontrole heeft de toegang tot het apparaat geblokkeerd.

  De berichtsjabloon voor een aanvraag voor toegang tot een geblokkeerd apparaat is beschikbaar in het gedeelte Apparaatcontrole in de interface van Kaspersky Endpoint Security.

- Programma-opstartcontrole heeft de opstart van een programma geblokkeerd.

  De berichtsjabloon voor een aanvraag voor het toestaan van de opstart van een geblokkeerd programma vindt u in het gedeelte Programma-opstartcontrole in de interface van Kaspersky Endpoint Security.

- Webcontrole heeft de toegang tot een webbron geblokkeerd.

  De berichtsjabloon voor een aanvraag voor toegang tot een geblokkeerde webbron is beschikbaar in het gedeelte Webcontrole in de interface van Kaspersky Endpoint Security.

De methode voor de verzending van berichten en de gebruikte sjabloon hangen af van het eventuele gebruik van een Kaspersky Security Center-beleid op de computer waarop Kaspersky Endpoint Security is geïnstalleerd en van een eventuele verbinding met de Administration Server van Kaspersky Security Center. De volgende scenario's zijn mogelijk:

- Als geen Kaspersky Security Center-beleid actief is op de computer waarop Kaspersky Endpoint Security is geïnstalleerd, wordt een bericht van de gebruiker per e-mail verstuurd naar de netwerkbeheerder.

  De velden van het bericht worden ingevuld met de waarden van de velden uit de gedefinieerde sjabloon in de lokale interface van Kaspersky Endpoint Security.

- Als een Kaspersky Security Center-beleid actief is op de computer waarop Kaspersky Endpoint Security is geïnstalleerd, wordt het standaardbericht verstuurd naar de Administration Server van Kaspersky Security Center.

  In dit geval kunnen de berichten van de gebruiker worden bekeken in de gebeurtenissenopslag van Kaspersky Security Center. De velden van het bericht worden ingevuld met de waarden van de velden uit de gedefinieerde sjabloon in het Kaspersky Endpoint Security-beleid.

- Als een Kaspersky Security Center-afwezigheidsbeleid actief is op de computer waarop Kaspersky Endpoint Security is geïnstalleerd, hangt de gebruikte methode voor de verzending van berichten af van de eventuele verbinding met Kaspersky Security Center.

  - In het geval van een verbinding met Kaspersky Security Center verstuurt Kaspersky Endpoint Security het standaardbericht naar de Administration Server van Kaspersky Security Center.

  - Mocht er geen verbinding met Kaspersky Security Center zijn, dan wordt het bericht van de gebruiker per e-mail verstuurd naar de netwerkbeheerder.

  In beide gevallen worden de velden van het bericht ingevuld met de waarden van de velden uit de gedefinieerde sjabloon in het Kaspersky Endpoint Security-beleid.

Gebruikersberichten in de gebeurtenissenopslag van Kaspersky Security Center bekijken

Dankzij de onderdelen Programma-opstartcontrole, Apparaatcontrole en Webcontrole kunnen netwerkgebruikers met computers waarop Kaspersky Endpoint Security is geïnstalleerd berichten naar de beheerder versturen.

Een gebruiker kan op twee manieren berichten naar de beheerder versturen:

- Als een gebeurtenis in de gebeurtenissenopslag van Kaspersky Security Center.

  De gebeurtenis van de gebruiker wordt naar de gebeurtenissenopslag van Kaspersky Security Center verstuurd als Kaspersky Endpoint Security op de computer van de gebruiker wordt uitgevoerd onder een actief beleid.

- Als een e-mailbericht.

  De informatie van de gebruiker wordt per e-mail verstuurd als Kaspersky Endpoint Security op de computer van de gebruiker niet wordt uitgevoerd onder een beleid of onder een afwezigheidsbeleid wordt uitgevoerd.

Zo bekijkt u een bericht van een gebruiker in de gebeurtenissenopslag van Kaspersky Security Center:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Gebeurtenissen**.

   In de werkruimte van Kaspersky Security Center ziet u alle gebeurtenissen die zich tijdens de werking van Kaspersky Endpoint Security voordoen, inclusief berichten die netwerkgebruikers naar de beheerder hebben verstuurd.
3. Als u de filter voor gebeurtenissen wilt configureren, selecteert u in de vervolgkeuzelijst **Selectie van gebeurtenissen** de optie **Gebruikersaanvragen**.
4. Selecteer het bericht dat u naar de beheerder wilt versturen.
5. Open het venster **Instellingen van gebeurtenis** op een van de volgende manieren:

   - Klik rechts op de gebeurtenis. Selecteer in het geopende contextmenu de optie **Eigenschappen**.
   - Klik op de knop **Venster met eigenschappen van gebeurtenis openen** rechts in de werkruimte van de Beheerconsole.

Deelnemen aan het Kaspersky Security Network

In deze sectie vindt u informatie over de deelname aan Kaspersky Security Network en instructies voor de in- en uitschakeling van het gebruik van Kaspersky Security Network.

Over de deelname aan Kaspersky Security Network

Voor een effectievere bescherming van uw computer gebruikt Kaspersky Endpoint Security gegevens die het van gebruikers over de hele wereld verzamelt. *Kaspersky Security Network* is ontworpen om zulke gegevens te verzamelen.

Kaspersky Security Network (KSN) is een infrastructuur van cloudservices die toegang biedt tot de online Knowledge Base van Kaspersky. Deze Knowledge Base bevat informatie over de reputatie van bestanden, webbronnen en software. Het gebruik van gegevens uit Kaspersky Security Network zorgt niet alleen voor een snellere respons door Kaspersky Endpoint Security bij nieuwe bedreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives.

Afhankelijk van de locatie van de infrastructuur is er een Wereldwijde KSN-service (de infrastructuur wordt door de Kaspersky-servers gehost) of een Private KSN-service (de infrastructuur wordt door servers van derden gehost, bijvoorbeeld in het netwerk van de internetprovider).

Na het wijzigen van de licentie verstuurt u de gegevens van de nieuwe code naar de serviceprovider om het Privaat KSN te kunnen gebruiken. Anders is er geen gegevensuitwisseling met KSN mogelijk.

Dankzij de gebruikers die deelnemen aan KSN kan Kaspersky snel informatie over de soorten bedreigingen en hun bronnen verzamelen, oplossingen ontwikkelen om ze onschadelijk te maken en het aantal false positives van programmaonderdelen minimaliseren.

Tijdens de deelname aan KSN stuurt het programma automatisch statistieken die tijdens de werking van het programma zijn gegenereerd naar KSN. Het programma kan ook bepaalde bestanden (of delen van bestanden) die hackers kunnen gebruiken om de computer of gegevens schade te berokkenen versturen naar Kaspersky voor aanvullend onderzoek.

Er worden geen persoonlijke gegevens verzameld, verwerkt of opgeslagen. Voor meer gedetailleerde informatie over de verzending van statistieken tijdens de deelname aan KSN en over de opslag en de vernietiging van zulke informatie raadpleegt u de Kaspersky Security Network-verklaring en de website van Kaspersky. Het bestand ksn_<taalcode>.txt met de tekst van de Verklaring van Kaspersky Security Network wordt bij het distributiepakket van het programma meegeleverd.

Om de belasting van de KSN-servers te verminderen, kan Kaspersky antivirusdatabases voor het programma beschikbaar maken die verzoeken aan Kaspersky Security Network tijdelijk uitschakelen of deels beperken. In dit geval wordt de status van de verbinding met KSN weergegeven als *Ingeschakeld met beperkingen*.

Computers van gebruikers die worden beheerd door de Administration Server van Kaspersky Security Center kunnen gegevens uitwisselen met KSN via de service KSN-proxy.

De service KSN-proxy verleent de volgende functionaliteit:

- De computer van de gebruiker kan verzoeken en informatie naar KSN sturen, zelfs zonder directe toegang tot het internet.
- KSN-proxy plaatst verwerkte gegevens in de cache waardoor de externe netwerkverbinding minder belast wordt en de informatie gevraagd door de computer van de gebruiker sneller wordt ontvangen.

Meer informatie over de service KSN-proxy vindt u in de *beheerdershandleiding van Kaspersky Security Center*.

De instellingen van de service KSN-proxy kunnen in de eigenschappen van het *Kaspersky Security Center*-beleid worden geconfigureerd.

Deelname aan Kaspersky Security Network is vrijwillig. De gebruiker wordt tijdens de initiële configuratie van het programma uitgenodigd om aan KSN deel te nemen. Gebruikers kunnen hun deelname aan KSN op elk moment starten of stoppen.

Het gebruik van Kaspersky Security Network inschakelen en uitschakelen

Zo schakelt u het gebruik van Kaspersky Security Network in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer in het gedeelte **Geavanceerde instellingen** links in het venster het subgedeelte **Instellingen voor KSN**.

   De instellingen van Kaspersky Security Network worden rechts in het venster weergegeven.
3. Voer een van de volgende acties uit:
   - Als u het gebruik van Kaspersky Security Network wilt inschakelen, schakelt u het selectievakje **Ik ga akkoord met de KSN-verklaring en de voorwaarden voor deelname** in.
   - Als u het gebruik van Kaspersky Security Network wilt uitschakelen, schakelt u het selectievakje **Ik ga akkoord met de KSN-verklaring en de voorwaarden voor deelname** uit.
4. Klik op de knop **Opslaan** om de wijzigingen op te slaan.

Verbinding met Kaspersky Security Network testen

Zo test u de verbinding met Kaspersky Security Network:

1. Open het hoofdvenster van het programma.
2. Klik boven in het venster op de knop **Kaspersky Security Network**.

   Het venster **Kaspersky Security Network** wordt geopend.

   Links in het venster **Kaspersky Security Network** ziet u de modus van de verbinding met Kaspersky Security Network in de vorm van een ronde **KSN**-knop:
   - Als Kaspersky Endpoint Security niet is verbonden met Kaspersky Security Network, is de **KSN**-knop grijs. De weergegeven status onder de **KSN**-knop geeft *Uitgeschakeld* aan.
   - Als Kaspersky Endpoint Security is verbonden met Kaspersky Security Network en de KSN-servers beschikbaar zijn, is de **KSN**-knop groen. De volgende informatie verschijnt onder de **KSN**-knop: de status

Ingeschakeld, het type van het gebruikte KSN (**Privaat KSN** of **Wereldwijd KSN**) en de datum en tijd van de laatste synchronisatie met de KSN-servers. Rechts in het venster ziet u statistieken over de reputatie van bestanden, webbronnen en software.

Kaspersky Endpoint Security verzamelt statistische gegevens over het gebruik van KSN wanneer u het venster **Kaspersky Security Network** opent. De statistieken worden niet in real time bijgewerkt.

- Als Kaspersky Endpoint Security is verbonden met Kaspersky Security Network maar de KSN-servers niet beschikbaar zijn, is de **KSN**-knop rood. De weergegeven status onder de **KSN**-knop geeft *Ingeschakeld* aan.

  Als de laatste synchronisatie met de KSN-servers meer dan 15 minuten geleden is of de status *Onbekend* heeft, betekent dit dat de KSN-servers niet beschikbaar zijn. In dit geval wordt u aanbevolen om contact op te nemen met de Technische Support of uw serviceprovider.

  Mogelijk bent u niet verbonden met de Kaspersky Security Network-servers omwille van de volgende redenen:

  - De computer is niet verbonden met het internet.
  - Het programma is niet geactiveerd of de licentie is verlopen.
  - Er zijn problemen met de code gevonden (de code staat bijvoorbeeld op de blacklist).

De reputatie van een bestand in Kaspersky Security Network controleren

Met de KSN-service kunt u informatie opvragen over programma's die in de reputatiedatabases van Kaspersky zijn opgenomen. Dit is handig om het bedrijfsbeleid voor het starten van programma's flexibel te beheren. Op deze manier kunt u voorkomen dat adware en andere programma's die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen worden gestart.

Zo controleert u de reputatie van een bestand in Kaspersky Security Network:

1. Klik rechts om het contextmenu te openen voor het bestand waarvan u de reputatie wilt controleren.
2. Selecteer de optie **Reputatie in KSN controleren**.

Deze optie is beschikbaar als u de voorwaarden van de Verklaring van Kaspersky Security Network hebt aanvaard.

Hiermee opent u het venster **<Bestandsnaam> - Reputatie in KSN**. In het venster <Bestandsnaam> - **Reputatie in KSN** ziet u de volgende informatie over het bestand dat wordt gecontroleerd:

- **Pad**. Pad waar het bestand op een schijf is opgeslagen.
- **Versie**. Versie van het programma (informatie wordt alleen voor uitvoerbare bestanden weergegeven).
- **Digitale handtekening**. Aanwezigheid van een digitale handtekening voor het bestand.
- **Ondertekend**. Datum waarop het certificaat is ondertekend met een digitale handtekening.

- **Gemaakt**. Aanmaakdatum van het bestand.
- **Aangepast**. Datum van laatste aanpassing van het bestand.
- **Grootte**. Ruimte die het bestand op de schijf inneemt.
- Informatie over het aantal gebruikers die het bestand vertrouwen of blokkeren.

Geavanceerde bescherming met Kaspersky Security Network

Kaspersky biedt het Kaspersky Security Network aan om gebruikers nog beter te beschermen. Deze beschermingsmethode is ontworpen om geavanceerde permanente bedreigingen en zero-day-aanvallen te bestrijden. De geïntegreerde cloudtechnologieën en de ervaring van Kaspersky-virusanalisten maken van Kaspersky Endpoint Security een uitstekende keuze voor uw bescherming tegen de meest geavanceerde digitale dreigingen.

Op de website van Kaspersky vindt u informatie over de uitgebreide bescherming van Kaspersky Endpoint Security.

Bronnen met informatie over het programma

De pagina van Kaspersky Endpoint Security op de website van Kaspersky

Op de pagina van Kaspersky Endpoint Security vindt u algemene informatie over het programma en de functies en kenmerken ervan.

Op de pagina van Kaspersky Endpoint Security staat een koppeling naar de online shop. Daar kunt u het programma aanschaffen of verlengen.

De pagina van Kaspersky Endpoint Security in de Knowledge Base

De *Knowledge Base* is een onderdeel van de website van de Technische Support.

Op de pagina van Kaspersky Endpoint Security in de Knowledge Base kunt u artikelen lezen die nuttige informatie, aanbevelingen en antwoorden op veelgestelde vragen over de aanschaf, de installatie en het gebruik van het programma bevatten.

Knowledge Base-artikelen beantwoorden mogelijk niet alleen vragen over Kaspersky Endpoint Security maar ook vragen over andere Kaspersky-programma's. Artikelen in de Knowledge Base bevatten mogelijk ook nieuws van de Technische Support.

Kaspersky-programma's bespreken op het forum

Als uw vraag niet dringend is, kunt u uw vraag bespreken met de experts van Kaspersky en andere gebruikers op ons forum.

Op dit forum kunt u bestaande discussies bekijken, commentaar leveren en nieuwe discussies starten.

Contact opnemen met de Technische Support

In deze sectie leest u hoe u technische ondersteuning verkrijgt en welke voorwaarden hieraan zijn verbonden.

Technische ondersteuning verkrijgen

Als u geen oplossing voor uw probleem vindt in de documentatie van het programma of in één van de informatiebronnen over het programma, raden we aan dat u contact opneemt met de Technische Support. De experts van de Technische Support beantwoorden graag al uw vragen over de installatie en het gebruik van het programma.

Technische ondersteuning is alleen beschikbaar voor gebruikers die een commerciële licentie hebben aangeschaft. Er wordt geen technische ondersteuning verleend aan gebruikers met een evaluatielicentie.

Lees eerst de regels voor ondersteuning voordat u contact opneemt met de Technische Support.

U kunt contact opnemen met de Technische support op één van de volgende manieren:

- Door telefonisch contact op te nemen met de Technische Support
- Door een verzoek naar de Technische Support van Kaspersky te sturen via de Kaspersky CompanyAccount-portal

Telefonische Technische Support

In de meeste regio's over de hele wereld kunt u telefonisch contact opnemen met de experts van de Technische Support. Op de website van de Technische Support van Kaspersky leest u hoe u technische ondersteuning in uw regio kunt krijgen en vindt u de contactgegevens van de Technische Support.

Lees eerst de regels voor ondersteuning voordat u contact opneemt met de Technische Support.

Technische ondersteuning via Kaspersky CompanyAccount

Kaspersky CompanyAccount is een portal voor bedrijven die Kaspersky-programma's gebruiken. De Kaspersky CompanyAccount-portal is ontworpen voor de interactie tussen gebruikers en de Kaspersky-experts via elektronische verzoeken. U kunt de Kaspersky CompanyAccount-portal gebruiken om de status van uw elektronische verzoeken op te volgen en om een geschiedenis van die verzoeken bij te houden.

U kunt alle werknemers van uw bedrijf registreren onder een enkel account voor Kaspersky CompanyAccount. Met een enkel account kunt u elektronische verzoeken van geregistreerde werknemers aan Kaspersky op één plaats beheren en kunt u ook de bevoegdheden van deze werknemers via Kaspersky CompanyAccount beheren.

De Kaspersky CompanyAccount-portal is beschikbaar in de volgende talen:

- Engels

- Spaans
- Italiaans
- Duits
- Pools
- Portugees
- Russisch
- Frans
- Japans

Voor meer informatie over Kaspersky CompanyAccount bezoekt u de website van de Technische Support.

Gegevens verzamelen voor Technische Support

Wanneer u de experts van de Technische Support van Kaspersky op de hoogte hebt gebracht van uw probleem, kunnen ze u vragen een *tracebestand* aan te maken. Met het tracebestand kunt u de uitvoering van programmaopdrachten stapsgewijs bijhouden en bepalen in welke fase van de programmawerking de fout optreedt.

Mogelijk vragen de experts van de Technische Support ook aanvullende informatie over het besturingssysteem, actieve processen op de computer, gedetailleerde rapporten over de werking van programmaonderdelen en crashdumps van het programma.

U kunt de noodzakelijke informatie met behulp van Kaspersky Endpoint Security verzamelen. De verzamelde informatie kan op de harde schijf worden opgeslagen en later worden geüpload wanneer u dat goed uitkomt.

Wanneer de diagnostische testen worden uitgevoerd, kunnen de experts van de Technische Support u vragen om programma-instellingen te wijzigen door:

- De functie voor de verzameling van uitgebreide diagnostische informatie te activeren.
- De instellingen van individuele programmaonderdelen, die niet beschikbaar zijn via de standaardelementen in de gebruikersinterface, precies te configureren.
- De instellingen voor de opslag en de verzending van de verzamelde diagnostische informatie te wijzigen.
- De onderschepping en de registratie van netwerkverkeer te configureren.

Experts van de Technische Support geven alle noodzakelijke informatie om deze handelingen uit te voeren (beschrijving van de te volgen stappen, de te wijzigen instellingen, configuratiebestanden, scripts, aanvullende functionaliteit voor de opdrachtregel, modules voor foutopsporing, speciale hulpprogramma's, enzovoort) en zeggen u welke gegevens er worden verzameld om de fout op te sporen en te corrigeren. De uitgebreide diagnostische informatie wordt op de computer van de gebruiker opgeslagen. De verzamelde gegevens worden niet automatisch verstuurd naar Kaspersky.

De gebruikte instellingen voor de bepaling van het adres van de dumpserver voor de verzending van de dumpbestanden naar Kaspersky worden op de computer van de gebruiker opgeslagen. De waarden van deze instellingen kunnen indien nodig worden bewerkt in de volgende registersleutel van het besturingssysteem: `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

De eerder vermelde handleidingen mogen alleen onder het toezicht van experts van de Technische Support worden uitgevoerd en hun instructies moeten strikt worden opgevolgd. Wijzigingen aan programma-instellingen zonder het toezicht van de experts en die op een andere manier worden uitgevoerd dan beschreven in de beheerdershandleiding of de instructies van de experts van de Technische Support kunnen het besturingssysteem vertragen of doen crashen, de beveiliging van de computer aantasten of de beschikbaarheid en de integriteit van de te verwerken gegevens in gevaar brengen.

Een tracebestand aanmaken

Zo maakt u een tracebestand aan:

1. Open het hoofdvenster van het programma.
2. Klik in het hoofdvenster van het programma op de knop .

   Het venster **Support** wordt geopend.
3. Klik in het venster **Support** op de knop **Systeemtracing**.

   Het venster **Informatie voor Technische Support** wordt geopend.
4. Schakel het selectievakje **Tracing inschakelen** in om de tracing te beginnen.
5. Selecteer in de vervolgkeuzelijst **Niveau** het traceniveau.

   U wordt aanbevolen om het vereiste traceniveau met een expert van de Technische Support te bespreken. Zonder begeleiding van de Technische Support stelt u het traceniveau in op **Normaal (500)**.
6. Herhaal de situatie waarin het probleem optrad.
7. Om de tracing te stoppen, gaat u terug naar het venster **Informatie voor Technische Support** en schakelt u het selectievakje **Tracing inschakelen** uit.

Wanneer het tracebestand is aangemaakt, kunt u de traceresultaten naar de Kaspersky-server uploaden.

Inhoud en opslag van traceringsbestanden

De gebruiker is persoonlijk verantwoordelijk voor de veiligheid van de verzamelde gegevens, in het bijzonder voor de monitoring en beperking van de toegang tot de verzamelde gegevens op de computer, totdat ze naar Kaspersky worden verzonden.

Tracebestanden worden in gewijzigde vorm opslagen op de computer zodat ze niet kunnen worden gelezen zolang het programma actief is en worden permanent verwijderd wanneer het programma wordt verwijderd.

Traceringsbestanden worden in de map ProgramData\Kaspersky Lab folder bewaard.

De naam van het tracebestand heeft de volgende structuur:
`KES<versienummer_datumXX.XX_tijdXX.XX_pidXXX.><type tracebestand>.log.enc1`.

Het tracebestand van Verificatie-agent is in de map met informatie over systeemvolumes opgeslagen en heeft de volgende naam: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

U kunt opgeslagen gegevens in tracebestanden bekijken. Neem contact op met de Technische Support van Kaspersky voor advies om de gegevens te bekijken.

Alle traceringsbestanden bevatten de volgende algemene gegevens:

- Het tijdstip van de gebeurtenis.
- Het nummer van de uitvoeringsthread.

  Het tracebestand van Verificatie-agent bevat deze informatie niet.

- Het programmaonderdeel dat de gebeurtenis heeft veroorzaakt.
- De ernst van de gebeurtenis (informatieve gebeurtenis, waarschuwing, kritieke gebeurtenis, fout).
- Een beschrijving van de gebeurtenis die de uitvoering van een opdracht door een programmaonderdeel inhoudt en het resultaat van de uitvoering van deze opdracht.

Inhoud van de tracebestanden SRV.log, GUI.log en ALL.log

De tracebestanden SRV.log, GUI.log en ALL.log bevatten naast de algemene gegevens mogelijk ook de volgende gegevens:

- Persoonlijke gegevens, waaronder achternaam, voornaam en tweede voornaam, als die gegevens deel uitmaken van het pad naar bestanden op de lokale computer.
- De gebruikersnaam en het wachtwoord als die openbaar zijn verzonden. Deze gegevens kunnen tijdens het scannen van het internetverkeer worden geregistreerd in tracebestanden. Het verkeer wordt alleen vanaf trafmon2.ppl geregistreerd in tracebestanden.
- De gebruikersnaam en het wachtwoord als ze in HTTP-headers zijn opgenomen.
- De naam van het Microsoft Windows-account als de accountnaam deel uitmaakt van de bestandsnaam.
- Uw e-mailadres of een webadres met de naam van uw account en het wachtwoord als deze deel uitmaken van de naam van het gevonden object.
- Websites die u bezoekt en omleidingen van deze websites. Deze gegevens worden naar tracebestanden geschreven wanneer het programma websites scant.
- Adres van proxyserver, naam van computer, IP-adres en gebruikersnaam om bij de proxyserver aan te melden. Deze gegevens worden naar tracebestanden geschreven als het programma een proxyserver gebruikt.
- Externe IP-adressen waarmee de computer verbinding heeft gemaakt.
- Onderwerp van het bericht, ID, naam van afzender en adres van de webpagina van de afzender van het bericht in het sociale netwerk. Deze gegevens worden naar tracebestanden geschreven als het onderdeel Webcontrole is ingeschakeld.

Inhoud van de tracebestanden HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Naast de algemene gegevens bevat het tracebestand HST.log ook gegevens over de uitvoering van een updatetaak voor de databases en programmamodules.

Naast de algemene gegevens bevat het tracebestand BL.log ook gegevens over gebeurtenissen die zich tijdens de werking van het programma voordoen, alsook benodigde gegevens om fouten in het programma op te lossen. Dit bestand wordt aangemaakt als het programma met de parameter avp.exe –bl is gestart.

Naast de algemene gegevens bevat het tracebestand Dumpwriter.log ook benodigde servicegegevens voor het oplossen van fouten die zich voordoen wanneer het dumpbestand van het programma wordt geschreven.

Naast de algemene gegevens bevat het tracebestand WD.log ook gegevens over gebeurtenissen die zich tijdens de werking van de avpsus-service voordoen, waaronder updates van programmamodules.

Naast de algemene gegevens bevat het tracebestand AVPCon.dll.log ook gegevens over gebeurtenissen die zich tijdens de werking van de verbindingsmodule van Kaspersky Security Center voordoen.

Inhoud van de tracebestanden van programmaplug-ins

Tracebestanden van programmaplug-ins bevatten naast de algemene gegevens ook de volgende gegevens:

- Het tracebestand shellex.dll.log van de plug-in die de scantaak start vanuit het contextmenu bevat informatie over de uitvoering van de scantaak en noodzakelijke gegevens voor de opsporing van fouten in de plug-in.
- Het tracebestand mcou.OUTLOOK.EXE van de Mail Anti-Virus-plug-in bevat mogelijk delen van e-mailberichten, waaronder e-mailadressen.

Inhoud van het tracebestand van Verificatie-agent

Naast de algemene gegevens bevat het tracebestand van Verificatie-agent ook gegevens over de werking van Verificatie-agent en de acties die de gebruiker met Verificatie-agent uitvoert.

De verzending van dumpbestanden en tracebestanden naar Kaspersky inschakelen of uitschakelen

Zo schakelt u de verzending van dumpbestanden en tracebestanden naar Kaspersky in of uit:

1. Open het venster met de programma-instellingen.
2. Selecteer links in het venster het gedeelte **Geavanceerde instellingen**.

   De geavanceerde programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Uitvoermodus** op de knop **Instellingen**.

   Het venster **Uitvoermodus** wordt geopend.
4. Schakel in het venster **Uitvoermodus** het selectievakje **Schrijven naar dump inschakelen** in om het programma naar dumpbestanden van het programma te laten schrijven.
5. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Dump- en tracebestanden naar Kaspersky versturen** in als u wilt dat het programma een vraag in het venster **Informatie voor Technische Support uploaden naar server** toont om bij de volgende opstart van het programma dump- en tracebestanden naar Kaspersky te sturen voor de analyse van de oorzaken van de fout in het programma.

- In het andere geval schakelt u het selectievakje **Dump- en tracebestanden naar Kaspersky versturen** uit.

6. Klik op **OK** in het venster **Uitvoermodus**.

7. Klik in het hoofdvenster van het programma op de knop **Opslaan** om de wijzigingen op te slaan.

Bestanden naar de server van de Technische Support versturen

Bestanden met informatie over het besturingssysteem, tracebestanden en dumpbestanden moeten naar experts van de Technische Support van Kaspersky worden verstuurd.

Zo verstuurt u bestanden naar de server van de Technische Support:

1. Herstart Kaspersky Endpoint Security na een fout in de werking ervan.

   Hiermee opent u het venster **Vorige start van het programma is mislukt**.

   Het venster **Vorige start van het programma is mislukt** wordt geopend telkens als Kaspersky Endpoint Security wordt gestart (inclusief na het opnieuw opstarten van de computer) totdat u de dump- of tracebestanden naar de Technische Support verstuurt of totdat u op de knop **Niet versturen** klikt.

2. Open in het venster **Vorige start van het programma is mislukt** de lijst met gegenereerde bestanden door **hier** te klikken.

3. Selecteer de selectievakjes naast de bestanden die u naar de Technische Support wilt versturen.

4. Klik op de knop **Verklaring weergeven**.

   Het venster **Verklaring inzake gegevensverstrekking** wordt geopend.

5. Lees de tekst van de Verklaring inzake gegevensverstrekking en klik op de knop **Sluiten**.

6. Schakel in het venster **Verklaring inzake gegevensverstrekking** het selectievakje **Ik ga akkoord met de Verklaring inzake gegevensverstrekking** uit.

7. Klik op de knop **Verzenden**.

   Hiermee opent u het venster **Aanvraagnummer**.

8. Geef in het venster **Aanvraagnummer** het nummer op dat aan uw aanvraag is toegewezen wanneer u via Kaspersky CompanyAccount contact hebt opgenomen met de Technische Support.

9. Klik op **OK**.

De geselecteerde gegevensbestanden worden ingepakt en naar de server van de Technische Support verstuurd.

De bescherming van dumpbestanden en tracebestanden inschakelen en uitschakelen

Dump- en tracebestanden bevatten informatie over het besturingssysteem en vertrouwelijke gegevens van de gebruiker. Om de onbevoegde toegang tot zulke gegevens te voorkomen, kunt u de bescherming van dump- en tracebestanden inschakelen.

Als de bescherming van dump- en tracebestanden is ingeschakeld, kunnen de bestanden worden geopend door de volgende gebruikers:

- Dumpbestanden kunnen worden geopend door de systeembeheerder en de lokale beheerder, alsook door de gebruiker die het schrijven van informatie naar dump- en tracebestanden heeft ingeschakeld.
- Tracebestanden kunnen alleen worden geopend door de systeembeheerder en de lokale beheerder.

Zo schakelt u de bescherming van dump- en tracebestanden in:

1. Open het venster met de programma-instellingen.
2. Selecteer het gedeelte **Geavanceerde instellingen** aan de linkerkant.

   De programma-instellingen worden rechts in het venster weergegeven.
3. Klik in het gedeelte **Uitvoermodus** op de knop **Instellingen**.

   Het venster **Uitvoermodus** wordt geopend.
4. Voer een van de volgende acties uit:

   - Schakel het selectievakje **Bescherming voor dump- en tracebestanden inschakelen** in als u de bescherming wilt inschakelen.
   - Schakel het selectievakje **Bescherming voor dump- en tracebestanden inschakelen** uit als u de bescherming wilt uitschakelen.
5. Klik op **OK** in het venster **Uitvoermodus**.
6. Klik in het hoofdvenster van het programma op de knop **Opslaan** om de wijzigingen op te slaan.

Dump- en tracebestanden waarnaar informatie is geschreven wanneer de bescherming actief was blijven zelfs na de uitschakeling van deze functie beschermd.

Woordenlijst

Actieve code

Een code die momenteel door het programma wordt gebruikt.

Administration Server

Een onderdeel van Kaspersky Security Center waar informatie over alle geïnstalleerde Kaspersky-programma's in het bedrijfsnetwerk wordt bewaard. Het kan ook worden gebruikt om deze programma's te beheren.

Analyse op basis van definities

Een technologie voor bedreigingsdetectie die de databases van Kaspersky Endpoint Security gebruikt. Deze databases bevatten beschrijvingen van bekende bedreigingen en methoden om ze onschadelijk te maken. Een bescherming met een analyse op basis van definities biedt een minimaal beveiligingsniveau. Op advies van de Kaspersky-experts is deze methode altijd ingeschakeld.

Antivirusdatabases

Databases met informatie over gevaren voor de beveiliging van computers die op het moment van de uitgave van de antivirusdatabases zijn gekend door Kaspersky. De definities in de antivirusdatabases helpen kwaadaardige code in gescande objecten te vinden. De antivirusdatabases worden door experts van Kaspersky gemaakt en worden elk uur bijgewerkt.

Archief

Een of meerdere bestanden die in een enkel gecomprimeerd bestand zijn ingepakt. U hebt een speciaal programma (een 'archiver') nodig om gegevens in en uit te pakken.

Back-up

Een speciale opslag voor back-ups van bestanden die vóór de desinfectie of de verwijdering worden gemaakt.

Beheergroep

Een reeks apparaten met dezelfde algemene functies en een aantal geïnstalleerde Kaspersky-programma's. De apparaten zijn gegroepeerd zodat ze handig als een enkele eenheid kunnen worden beheerd. Een groep kan andere groepen bevatten. U kunt een groepsbeleid en groepstaken voor elk geïnstalleerd programma in de groep maken.

Beschermd bereik

Objecten die voortdurend worden gescand door de antivirusbescherming wanneer die actief is. De beschermde bereiken van de verschillende onderdelen hebben verschillende eigenschappen.

Bestanden in Quarantaine plaatsen

Een methode voor de verwerking van een waarschijnlijk geïnfecteerd bestand waarbij de toegang tot het bestand wordt geblokkeerd en het bestand vanaf de originele locatie wordt verplaatst naar de Quarantaine-map, waar het geëncrypt wordt opgeslagen om mogelijke infecties te voorkomen.

Bestandsmasker

Voorstelling van een bestandsnaam en extensie met behulp van jokertekens.

Bestandsmaskers kunnen alle tekens bevatten die in bestandsnamen zijn toegestaan, inclusief jokertekens:

- ***** – Vervangt een willekeurig aantal tekens.
- **?** – Vervangt één willekeurig teken.

De bestandsnaam en de extensie worden altijd door een punt gescheiden.

Blacklist van adressen

Een lijst met e-mailadressen waarvoor alle inkomende berichten worden geblokkeerd door het Kaspersky-programma, ongeacht de inhoud van het bericht.

Certificaat

Elektronisch document met de private sleutel en informatie over de eigenaar en het bereik van de sleutel en dat bevestigt dat de openbare sleutel aan de eigenaar toebehoort. Het certificaat moet ondertekend zijn door de certificeringsinstantie die het certificaat heeft verleend.

Certificaathouder

Houder van een private sleutel gekoppeld aan een certificaat. Dit kan een gebruiker, een programma, een virtueel object, een computer of een service zijn.

Database met kwaadaardige webadressen

Een lijst met webadressen waarvan de inhoud mogelijk gevaarlijk is. De lijst is door experts van Kaspersky gemaakt. Ze wordt periodiek geüpdatet en is een onderdeel van het distributiepakket van het Kaspersky-programma.

Database met phishingwebadressen

Een lijst met webadressen die volgens experts van Kaspersky phishingadressen zijn. De database wordt periodiek geüpdatet en is een onderdeel van het distributiepakket van het Kaspersky-programma.

Desinfectie

Een methode voor de verwerking van geïnfecteerde objecten die resulteert in een compleet of gedeeltelijk herstel van de gegevens. Niet alle geïnfecteerde gegevens kunnen worden gedesinfecteerd.

Exploits

Programmacode die een bepaalde kwetsbaarheid in het systeem of de software gebruikt. Exploits worden vaak gebruikt om malware op de computer te installeren zonder medeweten van de gebruiker.

Extra code

Een code die het recht op het gebruik van het programma certificeert maar momenteel niet wordt gebruikt.

Geïnfecteerd bestand

Een bestand dat kwaadaardige code bevat (code van bekende malware die tijdens het scannen van het bestand is gedetecteerd). Kaspersky raadt het gebruik van zulke bestanden af omdat ze uw computer kunnen infecteren.

Genormaliseerde notatie van het adres van een webbron

De genormaliseerde notatie van het adres van een webbron is een tekstuele voorstelling van een webadres dat door normalisatie wordt verkregen. Normalisatie is een proces waarbij de tekstuele voorstelling van een webadres wijzigt volgens specifieke regels (bijvoorbeeld de weglating van de HTTP-gebruikersnaam, wachtwoord en poort voor verbinding in de tekstuele voorstelling van het adres van de webbron; de hoofdletters van het adres van de webbron worden gewijzigd in kleine letters).

In de context van antivirusbescherming worden adressen van webbronnen genormaliseerd om te vermijden dat de webadressen, die mogelijk verschillen in syntaxis terwijl ze fysiek identiek zijn, meer dan eens worden gescand.

Voorbeeld:

Niet-genormaliseerde notatie van een adres: www.Voorbeeld.nl\.

Genormaliseerde notatie van een adres: www.voorbeeld.nl.

Heuristische analyse

De technologie is ontworpen om dreigingen te detecteren die niet met de huidige versie van de databases van het Kaspersky-programma kunnen worden gedetecteerd. De technologie detecteert bestanden die mogelijk geïnfecteerd zijn met een onbekend virus of een nieuwe variëteit van een bekend virus.

Infecteerbaar bestand

Een bestand dat, wegens de structuur of de indeling ervan, door criminelen kan worden gebruikt als een "container" om kwaadaardige code op te slaan en te verspreiden. Doorgaans zijn deze bestanden uitvoerbare bestanden met bestandsextensies zoals .com, .exe en .dll. Het risico op indringing van kwaadaardige code in zulke bestanden is vrij hoog.

Licentiecertificaat

Een document dat Kaspersky samen met het licentiebestand of de activatiecode verstrekt aan de gebruiker. Het bevat informatie over de licentie die aan de gebruiker is verleend.

Netwerkagent

Een Kaspersky Security Center-onderdeel voor de interactie tussen Administration Server en Kaspersky-programma's die op een specifiek netwerkknooppunt zijn geïnstalleerd (werkstation of server). Alle Kaspersky-programma's voor Windows hebben dit onderdeel. Speciale versies van Netwerkagent zijn bedoeld voor programma's die met andere besturingssystemen werken.

Netwerkservice

Reeks parameters die netwerkactiviteit definiëren. Voor deze netwerkactiviteit kunt u een netwerkregel aanmaken die de werking van Firewall regelt.

Network Agent Connector

Een functie van het programma dat het met de Netwerkagent verbindt. De Network Agent Connector maakt het externe beheer van het programma via Kaspersky Security Center mogelijk.

OLE-object

Een toegevoegd bestand of een bestand dat in een ander bestand is ingesloten. Kaspersky-programma's kunnen OLE-objecten scannen op virussen. Als u bijvoorbeeld een Microsoft Office Excel®-tabel in een Microsoft Office Word-document invoegt, wordt de tabel als een OLE-object gescand.

Patch

Een kleine toevoeging aan het programma die fouten verhelpt die tijdens de werking van het programma zijn ontdekt, of die updates installeert.

Phishing

Een soort internetfraude waarbij e-mailberichten worden verstuurd om vertrouwelijke gegevens te stelen (heel vaak financiële gegevens).

Portable bestandsbeheer

Dit is een programma met een interface die u kunt gebruiken om met geëncrypte bestanden op verwisselbare schijven te werken als er geen encryptiefunctionaliteit op de computer beschikbaar is.

Programma-instellingen

Programma-instellingen die bij alle typen taken voorkomen en de algemene werking van het programma bepalen. Voorbeelden: instellingen voor de werking van het programma, instellingen voor rapporten en instellingen voor back-ups.

Programmamodules

Bestanden die een onderdeel van het installatiebestand van het programma zijn en de belangrijkste functionaliteit van het programma voorstellen. Er is een aparte uitvoerbare module voor elk type taak die door het programma wordt uitgevoerd (Realtime bescherming, scan op verzoek en Update). Wanneer een volledige scan van de computer wordt gestart vanuit het hoofdvenster van het programma, zet u de module van deze taak in werking.

Quarantaine

Kaspersky Endpoint Security plaatst waarschijnlijk geïnfecteerde bestanden in deze map. Bestanden in Quarantaine worden in geëncrypte vorm opgeslagen.

Scanbereik

Objecten die Kaspersky Endpoint Security scant wanneer het een scantaak uitvoert.

Taak

Functies die door het Kaspersky-programma als taken worden uitgevoerd, zoals: realtime bestandsbescherming, volledige scan van apparaten, database-updates.

Taakinstellingen

Specifieke programma-instellingen voor elk type taak.

Trusted Platform Module

Een microchip die is ontwikkeld om basisfuncties voor beveiliging te leveren (bijvoorbeeld de opslag van encryptiesleutels). Een Trusted Platform Module wordt doorgaans geïnstalleerd op de systeemkaart van de computer en communiceert met alle andere systeemcomponenten via de hardwarebus.

Update

Het vervangen of toevoegen van nieuwe bestanden (databases of programmamodules) die vanaf Kaspersky-updateservers worden opgehaald.

Vals alarm

Er is sprake van een vals alarm wanneer het Kaspersky-programma aangeeft dat een bestand geïnfecteerd is terwijl dat niet het geval is. Dit gebeurt als de definitie van het bestand erg gelijkt op de definitie van een virus.

Verificatie-agent

Een interface voor de verificatie van de identiteit om toegang tot geëncrypte harde schijven te krijgen en het besturingssysteem te laden nadat de harde schijf van het systeem is geëncrypt.

Verlener van certificaat

Certificeringsinstantie die het certificaat heeft verleend.

Vingerafdruk van certificaat

Gebruikte informatie om een certificaatsleutel te identificeren. Een vingerafdruk wordt aangemaakt door een cryptografische hash-functie toe te passen op de waarde van de sleutel.

Waarschijnlijk geïnfecteerd bestand

Een bestand met aangepaste code van een bekend virus of code die gelijkt op deze van een virus maar nog niet door Kaspersky is gekend. Waarschijnlijk geïnfecteerde bestanden worden door de heuristische scanner gevonden.

Informatie over code van derden

Informatie over code van derden bevindt zich in het bestand legal_notices.txt in de installatiemap van het programma.

Kennisgevingen over handelsmerken

Gedeponeerde handelsmerken en dienstmerken zijn de eigendom van hun respectieve eigenaar.

Adobe, Acrobat en Shockwave zijn de handelsmerken of gedeponeerde handelsmerken van Adobe Systems Incorporated in de Verenigde Staten en/of andere landen.

Mac en FireWire zijn gedeponeerde handelsmerken van Apple Inc. in de Verenigde Staten en andere landen.

AutoCAD is een handelsmerk of een gedeponeerd handelsmerk van Autodesk, Inc. en/of diens dochterondernemingen/gelieerde ondernemingen in de Verenigde Staten en andere landen.

Het woordmerk Bluetooth en het logo ervan zijn het eigendom van Bluetooth SIG, Inc.

Borland is een handelsmerk of een gedeponeerd handelsmerk van Borland Software Corporation in de Verenigde Staten en andere landen.

Citrix en Citrix Provisioning Services zijn gedeponeerde handelsmerken van Citrix Systems, Inc. en/of diens dochterondernemingen in het octrooibureau van de Verenigde Staten en andere landen.

dBase is een handelsmerk van dataBased Intelligence, Inc.

EMC en SecurID zijn handelsmerken of gedeponeerde handelsmerken van EMC Corporation in de Verenigde Staten en andere landen.

ICQ is een handelsmerk en / of dienstmerk van ICQ LLC.

Intel en Pentium zijn de gedeponeerde handelsmerken van Intel Corporation in de Verenigde Staten en andere landen.

Logitech is een handelsmerk of gedeponeerd handelsmerk van Logitech Company in de Verenigde Staten en andere landen.

Mail.ru is een gedeponeerd handelsmerk van Mail.Ru, LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell en Surface zijn de gedeponeerde handelsmerken van Microsoft Corporation in de Verenigde Staten en andere landen.

Mozilla en Thunderbird zijn de handelsmerken van Mozilla Foundation.

Novell is een gedeponeerd handelsmerk van Novell Inc. in de Verenigde Staten en andere landen.

Java en JavaScript zijn gedeponeerde handelsmerken van Oracle Corporation en/of diens gelieerde ondernemingen.

SafeNet is het gedeponeerde handelsmerk van SafeNet, Inc.

UNIX is een gedeponeerd handelsmerk in de Verenigde Staten en andere landen en wordt gebruikt onder licentie van X/Open Company Limited.