

**kaspersky**

# **Kaspersky Endpoint Security voor Windows 11.9.0**

© 2024 AO Kaspersky Lab

# Inhoud

## [Kaspersky Endpoint Security voor Windows-help](#)

[Nieuwigheden](#)

[Veelgestelde vragen](#)

## [Kaspersky Endpoint Security voor Windows](#)

[Software pakket](#)

[Hardware- en softwarevereisten](#)

[Vergelijking van beschikbare programmafuncties naargelang het type besturingssysteem](#)

[Vergelijking van programmafuncties naargelang de beheertools](#)

[Compatibiliteit met andere programma's](#)

## [Het programma installeren en verwijderen](#)

[Implementatie via Kaspersky Security Center](#)

[Standaardinstallatie van het programma](#)

[Een installatiepakket maken](#)

[Databases in het installatiepakket updaten](#)

[Een taak voor een externe installatie maken](#)

[Het programma lokaal met de wizard installeren](#)

[Het programma op afstand installeren via System Center Configuration Manager](#)

[Beschrijving van de installatie-instellingen in het bestand 'setup.ini'](#)

[Programmaonderdelen wijzigen](#)

[Een upgrade voor een oude versie van het programma installeren](#)

[Programma verwijderen](#)

## [Licentie van het programma activeren](#)

[Over de Gebruiksrechtovereenkomst](#)

[Over de licentie](#)

[Over het licentiecertificaat](#)

[Over het abonnement](#)

[Over de licentiecode](#)

[Over de activeringscode](#)

[Over het licentiebestand](#)

[Vergelijking van programmafunctionaliteit afhankelijk van licentietype voor werkstations](#)

[Vergelijking van programmafunctionaliteit afhankelijk van licentietype voor servers](#)

[Programma activeren](#)

[Het programma activeren via Kaspersky Security Center](#)

[Activeringswizard gebruiken voor de activering van het programma](#)

[Licentie-informatie bekijken](#)

[Een licentie aanschaffen](#)

[Abonnement verlengen](#)

## [Gegevensverstrekking](#)

[Gegevensverstrekking onder de licentieovereenkomst voor eindgebruikers](#)

[Gegevensverstrekking tijdens het gebruik van Kaspersky Security Network](#)

[Gegevensverstrekking bij het gebruik van oplossingen voor Detection and Response](#)

[Kaspersky Endpoint Detection and Response](#)

[Kaspersky Sandbox](#)

[Naleving van de wetgeving van de Europese Unie \(AVG\)](#)

## [Aan de slag](#)

[Informatie over de beheerplug-in Kaspersky Endpoint Security voor Windows](#)

[Speciale aandachtspunten bij het werken met verschillende versies van beheerplug-ins](#)

[Bijzondere aandachtspunten bij het gebruik van geëncrypte protocollen voor interactie met externe services](#)

[Programma-interface](#)

[Programmapictogram in het systeemvak van de taakbalk](#)

[Vereenvoudigde programma-interface](#)

[De weergave van de programma-interface configureren](#)

[Aan de slag](#)

[Beleid beheren](#)

[Taakbeheer](#)

[Lokale programma-instellingen configureren](#)

[Kaspersky Endpoint Security starten en stoppen](#)

[Bescherming en controle van computer pauzeren en hervatten](#)

[Een configuratiebestand aanmaken en gebruiken](#)

[Standaardinstellingen van het programma herstellen](#)

[Virusscan van de computer](#)

[Computer scannen](#)

[Verwisselbare schijven scannen wanneer ze op de computer zijn aangesloten](#)

[Achtergrondscan](#)

[Scannen vanuit contextmenu](#)

[Controle van programma-integriteit](#)

[Scanbereik bewerken](#)

[Een geplande scan uitvoeren](#)

[Een scan uitvoeren namens een andere gebruiker](#)

[Scanoptimalisatie](#)

[Databases en softwaremodules van het programma bijwerken](#)

[Updatescenario's voor database en programmamodule](#)

[Updaten vanaf een opslagplaats op een server](#)

[Updaten vanaf een gedeelde map](#)

[Updaten met Kaspersky Update Utility](#)

[Updaten in mobiele modus](#)

[Een updatetaak starten en stoppen](#)

[Een updatetaak met de rechten van een ander gebruikersaccount starten](#)

[De uitvoermodus van de updatetaak selecteren](#)

[Een updatebron toevoegen](#)

[Bijwerken vanuit een gedeelde map configureren](#)

[Programmamodules updaten](#)

[Een proxyserver voor updates gebruiken](#)

[Laatste update terugdraaien](#)

[Werken met actieve dreigingen](#)

[Desinfectie van actieve dreigingen op werkstations](#)

[Desinfectie van actieve dreigingen op servers](#)

[Geavanceerde desinfectietechnologie inschakelen of uitschakelen](#)

[Verwerking van actieve dreigingen](#)

[Computerbescherming](#)

[File Threat Protection](#)

[File Threat Protection inschakelen en uitschakelen](#)

[File Threat Protection automatisch pauzeren](#)

[De actie wijzigen die het onderdeel File Threat Protection moet uitvoeren op geïnfecteerde bestanden](#)

[Het beschermd bereik van het onderdeel File Threat Protection instellen](#)

[Scanmethoden gebruiken](#)

[Scantechnologieën met het onderdeel File Threat Protection gebruiken](#)

[Het scannen van bestanden optimaliseren](#)

[Samengestelde bestanden scannen](#)

[De scanmodus wijzigen](#)

## [Web Threat Protection](#)

[Web Threat Protection inschakelen en uitschakelen](#)

[Methoden voor het detecteren van schadelijke webadressen configureren](#)

[Anti-Phishing](#)

[De lijst met vertrouwde webadressen aanmaken](#)

[De lijst met vertrouwde webadressen exporteren en importeren](#)

## [Mail Threat Protection](#)

[Mail Threat Protection inschakelen en uitschakelen](#)

[De uit te voeren actie op geïnfecteerde e-mailberichten wijzigen](#)

[Het beschermd bereik van het onderdeel Mail Threat Protection instellen](#)

[Samengestelde bestanden die zijn toegevoegd als bijlage aan e-mailberichten scannen](#)

[Filteren van bijlagen van e-mailberichten](#)

[Extensies exporteren en importeren voor het filteren van bijlagen](#)

[E-mails in Microsoft Office Outlook scannen](#)

## [Network Threat Protection](#)

[Network Threat Protection inschakelen en uitschakelen](#)

[Een aanvallende computer blokkeren](#)

[Adressen configureren die niet moeten worden geblokkeerd](#)

[De lijst met uitzonderingen voor blokkeren exporteren en importeren](#)

[Beveiliging tegen netwerkaanvallen configureren op type](#)

## [Firewall](#)

[Firewall inschakelen en uitschakelen](#)

[Status van de netwerkverbinding wijzigen](#)

[Regels voor netwerkpakketten beheren](#)

[Een regel voor netwerkpakketten maken](#)

[Een regel voor netwerkpakketten inschakelen of uitschakelen](#)

[De actie van Firewall voor een regel voor netwerkpakketten wijzigen](#)

[De prioriteit van een regel voor netwerkpakketten wijzigen](#)

[Netwerkpakketregels exporteren en importeren](#)

[Netwerkregels voor programma's beheren](#)

[Een netwerkregel voor programma's maken](#)

[Een netwerkregel voor programma's inschakelen en uitschakelen](#)

[De actie van Firewall voor een netwerkregel voor programma's wijzigen](#)

[De prioriteit van een netwerkregel voor programma's wijzigen](#)

[Netwerkmonitor](#)

## [BadUSB Attack Prevention](#)

[BadUSB Attack Prevention inschakelen en uitschakelen](#)

[Schermtoetsenbord gebruiken voor autorisatie van USB-apparaten](#)

## [AMSI-bescherming](#)

[AMSI-bescherming inschakelen en uitschakelen](#)

[AMSI-bescherming gebruiken om samengestelde bestanden te scannen](#)

## [Exploit-preventie](#)

[Exploit-preventie inschakelen en uitschakelen](#)

[Een actie selecteren die moet worden uitgevoerd wanneer een exploit wordt gedetecteerd](#)

[Bescherming voor systeempromessen in geheugen](#)

#### [Gedragsdetectie](#)

[Gedragsdetectie inschakelen en uitschakelen](#)

[De actie selecteren die moet worden genomen bij het detecteren van malwareactiviteit](#)

[Bescherming van gedeelde mappen tegen externe encryptie](#)

[Bescherming van gedeelde mappen tegen externe encryptie inschakelen en uitschakelen](#)

[De actie selecteren die u wilt uitvoeren bij de detectie van externe encryptie van gedeelde mappen](#)

[Een uitzondering voor bescherming van gedeelde mappen tegen externe encryptie maken:](#)

[Adressen van gedeelde mappen configureren die niet moeten worden beschermd tegen externe encryptie](#)

[Een lijst van uitzonderingen die niet moeten worden beschermd tegen externe encryptie exporteren en importeren:](#)

#### [Host Intrusion Prevention](#)

[Host Intrusion Prevention inschakelen en uitschakelen](#)

[Vertrouwensgroepen voor programma's beheren](#)

[De vertrouwensgroep van een programma wijzigen](#)

[Rechten van vertrouwensgroep configureren](#)

[Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security worden gestart](#)

[Een vertrouwensgroep selecteren voor onbekende programma's](#)

[Een vertrouwensgroep selecteren voor digitaal ondertekende programma's](#)

[Programmarechten beheren](#)

[Bronnen van het besturingssysteem en persoonsgegevens beschermen](#)

[Informatie over ongebruikte programma's verwijderen](#)

[Host Intrusion Prevention volgen](#)

[Toegang tot audio en video beveiligen](#)

#### [Remediation Engine](#)

##### [Kaspersky Security Network](#)

[Het gebruik van Kaspersky Security Network inschakelen en uitschakelen](#)

[Beperkingen van Privaat KSN](#)

[Cloudmodus voor beschermingsonderdelen inschakelen en uitschakelen](#)

[Instellingen voor KSN-proxy](#)

[De reputatie van een bestand in Kaspersky Security Network controleren](#)

##### [Versleutelde verbindingen scannen](#)

[Versleutelde verbindingen scannen inschakelen](#)

[Vertrouwde rootcertificaten installeren](#)

[Versleutelde verbindingen scannen met een niet-vertrouwd certificaat](#)

[Versleutelde verbindingen scannen in Firefox en Thunderbird](#)

[Versleutelde verbindingen uitsluiten van scannen](#)

##### [Gegevens wissen](#)

#### [Computerbeheer](#)

##### [Webcontrole](#)

[Webcontrole inschakelen en uitschakelen](#)

[Bewerkingen voor toegangsregels voor webbronnen](#)

[Een toegangsregel voor webbronnen toevoegen](#)

[Prioriteiten aan toegangsregels voor webbronnen toewijzen](#)

[Een toegangsregel voor webbronnen inschakelen en uitschakelen](#)

[De lijst met vertrouwde webadressen exporteren en importeren](#)

[Toegangsregels voor webbronnen testen](#)

[De lijst met adressen van webbronnen exporteren en importeren](#)  
[Activiteit van gebruikers op internet bewaken](#)  
[Berichtsjablonen van Webcontrole bewerken](#)  
[Maskers voor adressen van webbronnen bewerken](#)  
[Toegangsregels voor webbronnen migreren vanaf oudere versies van het programma](#)

#### [Apparaatcontrole](#)

[Apparaatcontrole inschakelen en uitschakelen](#)  
[Over toegangsregels](#)  
[Een regel voor toegang tot apparaten bewerken](#)  
[Een toegangsregel voor verbindingsbussen bewerken](#)  
[Een wifnetwerk toevoegen aan de lijst Vertrouwd](#)  
[Bewaking op het gebruik van verwisselbare schijven](#)  
[De cacheduur wijzigen](#)  
[Bewerkingen met vertrouwde apparaten](#)  
[Een apparaat vanuit de programma-interface toevoegen aan de lijst Vertrouwd](#)  
[Een apparaat vanuit Kaspersky Security Center toevoegen aan de Vertrouwde lijst](#)  
[Zo importeert en exporteert u de lijst met vertrouwde apparaten](#)  
[Toegang tot een geblokkeerd apparaat verkrijgen](#)  
[Online modus voor het verlenen van toegang](#)  
[Offline modus voor het verlenen van toegang](#)  
[Berichtsjablonen van Apparaatcontrole bewerken](#)  
[Anti-Bridging](#)  
[Anti-Bridging inschakelen](#)  
[De status van een verbidingsregel wijzigen](#)  
[De prioriteit van een verbidingsregel wijzigen](#)

#### [Adaptieve controle op afwijkingen](#)

[Adaptieve controle op afwijkingen inschakelen en uitschakelen](#)  
[Een regel van Adaptieve controle op afwijkingen inschakelen en uitschakelen](#)  
[Actie bij de activering van een regel van Adaptieve controle op afwijkingen wijzigen](#)  
[Een uitzondering maken voor een regel van Adaptieve controle op afwijkingen:](#)  
[Uitzonderingen voor regels van Adaptieve controle op afwijkingen exporteren en importeren:](#)  
[Updates voor regels van Adaptieve controle op afwijkingen toepassen](#)  
[Berichtsjablonen van Adaptieve controle op afwijkingen bewerken](#)  
[Rapporten van Adaptieve controle op afwijkingen bekijken](#)

#### [Programmacontrole](#)

[Beperkingen van de functionaliteit van Programmacontrole](#)  
[Programmacontrole inschakelen en uitschakelen](#)  
[De modus van Programmacontrole selecteren](#)  
[Werken met regels van programmacontrole in de applicatie-interface](#)  
[Een regel van programmacontrole toevoegen](#)  
[Een activeringsvoorwaarde voor een regel van Programmacontrole toevoegen](#)  
[De status van een regel van Programmacontrole wijzigen](#)  
[Regels van programmacontrole beheren in Kaspersky Security Center](#)  
[Informatie over geïnstalleerde programma's op computers van gebruikers ontvangen](#)  
[Programmacategorieën aanmaken](#)  
[Uitvoerbare bestanden uit de map Uitvoerbare bestanden toevoegen aan de programmacategorie](#)  
[Uitvoerbare bestanden die zijn gerelateerd aan gebeurtenissen toevoegen aan de programmacategorie](#)  
[Een regel van Programmacontrole toevoegen en wijzigen via Kaspersky Security Center](#)

[De status van een regel van Programmacontrole wijzigen via Kaspersky Security Center](#)

[Regels voor programma-beheer exporteren en importeren](#)

[Regels voor programmacontrole testen via Kaspersky Security Center](#)

[Gebeurtenissen die zich voordeden tijdens de geteste werking van het onderdeel Programmacontrole weergeven](#)

[Zo geeft u het rapport over geblokkeerde programma's in de testmodus weer](#)

[Gebeurtenissen die zich voordeden tijdens de werking van het onderdeel Programmacontrole weergeven](#)

[Een rapport over geblokkeerde programma's weergeven](#)

[Regels van Programmacontrole testen](#)

[Bewaking van programma-activiteit](#)

[Regels voor het maken van naammaskers voor bestanden of mappen](#)

[Berichtsjablonen van Programmacontrole bewerken](#)

[Best practices voor het implementeren van een lijst met toegestane programma's](#)

[Allowlist-modus configureren voor programma's](#)

[De allowlist-modus testen](#)

[Ondersteuning voor allowlist-modus](#)

[Netwerkpoothen bewaken](#)

[Bewaking van alle netwerkpoothen inschakelen](#)

[Een lijst met bewaakte netwerkpoothen aanmaken](#)

[Een lijst met programma's aanmaken waarvoor alle netwerkpoothen worden gemonitord](#)

[Lijsten met bewaakte poorten exporteren en importeren](#)

[Wachtwoordbeveiliging](#)

[Wachtwoordbeveiliging inschakelen](#)

[Machtigingen aan individuele gebruikers of groepen verlenen](#)

[Een tijdelijk wachtwoord gebruiken om machtigingen te verlenen](#)

[Aandachtspunten bij machtigingen met wachtwoordbeveiliging](#)

[Het KLAdmin-wachtwoord resetten](#)

[Vertrouwde zone](#)

[Een scanuitzondering aanmaken](#)

[Een scanuitzondering inschakelen en uitschakelen](#)

[Soorten detecteerbare objecten selecteren](#)

[De lijst met vertrouwde programma's bewerken](#)

[Regels voor vertrouwde zone inschakelen en uitschakelen voor een programma in de lijst met vertrouwde programma's](#)

[Vertrouwde systeemcertificatenopslag gebruiken](#)

[Back-up beheren](#)

[De maximale opslagduur voor bestanden in Back-up configureren](#)

[De maximale grootte van Back-up configureren](#)

[Bestanden vanuit Back-up terugzetten](#)

[Back-ups van bestanden uit Back-up verwijderen](#)

[Service voor meldingen](#)

[Instellingen voor gebeurtenislogboeken configureren](#)

[Weergave en levering van meldingen configureren](#)

[Weergave van waarschuwingen over de status van het programma in het systeemvak configureren](#)

[Berichten tussen gebruikers en de beheerder](#)

[Rapporten beheren](#)

[Rapporten bekijken](#)

[Maximale opslagduur voor rapporten configureren](#)

[Maximale grootte van het rapportbestand configureren](#)

[Een rapport als een bestand opslaan](#)

[Rapporten wissen](#)

[Zelfbescherming van Kaspersky Endpoint Security](#)

[Zelfbescherming inschakelen en uitschakelen](#)

[Ondersteuning voor AM-PPL inschakelen en uitschakelen](#)

[Bescherming tegen extern beheer in- en uitschakelen](#)

[Ondersteuning voor programma's voor extern beheer](#)

[Prestaties van Kaspersky Endpoint Security en compatibiliteit met andere programma's](#)

[Energiebesparingsmodus inschakelen of uitschakelen](#)

[Afstaan van bronnen aan andere programma's inschakelen of uitschakelen](#)

[Best practices voor het optimaliseren van de prestaties van Kaspersky Endpoint Security](#)

[Gegevensencryptie](#)

[Beperkingen van de encryptiefunctie](#)

[Lengte van de encryptiesleutel wijzigen \(AES56 / AES256\)](#)

[Kaspersky Disk Encryption](#)

[Speciale kenmerken van SSD-schijfencryptie](#)

[Kaspersky Disk Encryption starten](#)

[Een lijst met harde schijven maken die niet moeten worden geëncrypt](#)

[Een lijst met harde schijven die niet moeten worden geëncrypt exporteren en importeren:](#)

[Enmalige aanmelding \(SSO\) inschakelen](#)

[Accounts voor Authenticatie-agent beheren](#)

[Een token en een smartcard met Authenticatie-agent gebruiken](#)

[Decryptie van harde schijven](#)

[Toegang herstellen tot een schijf beschermd met de Kaspersky Disk Encryption-technologie](#)

[Aanmelden met het service-account van de authenticatie-agent](#)

[Besturingssysteem updaten](#)

[Fouten na updaten van encryptiefunctie verhelpen](#)

[Het tracingniveau voor Authenticatie-agent selecteren](#)

[Helpteksten van Authenticatie-agent bewerken](#)

[Verwijderen van overgebleven objecten en gegevens na het testen van de werking van Authenticatie-agent](#)

[Beheer van BitLocker](#)

[BitLocker-stationsversleuteling starten](#)

[Een harde schijf die wordt beschermd door BitLocker decrypten](#)

[Toegang tot een met BitLocker beschermde schijf herstellen](#)

[BitLocker-bescherming pauzeren om software te updaten](#)

[File Level Encryption op lokale schijven van de computer](#)

[Bestanden op schijven van een lokale computer encrypten](#)

[Toegangsregels voor geëncrypte bestanden maken voor programma's](#)

[Bestanden die zijn gemaakt of gewijzigd door specifieke programma's encrypten](#)

[Een decryptieregel genereren](#)

[Bestanden op schijven van een lokale computer decrypten](#)

[Geëncrypte pakketten aanmaken](#)

[Toegang tot geëncrypte gegevens herstellen](#)

[Toegang tot geëncrypte gegevens herstellen na fout in besturingssysteem](#)

[Sjablonen van berichten voor toegang tot geëncrypte bestanden bewerken](#)

[Encryptie van verwisselbare schijven](#)

[Encryptie van verwisselbare schijven starten](#)

[Een encryptieregel voor verwisselbare schijven toevoegen](#)

[Een lijst met encryptieregels voor verwisselbare schijven exporteren en importeren](#)



[Portable modus voor toegang tot geëncrypte bestanden op verwisselbare schijven](#)

[Decryptie van verwisselbare schijven](#)

[Details van gegevensencryptie bekijken](#)

[De encryptiestatus bekijken](#)

[Encryptiestatistieken bekijken op dashboards van Kaspersky Security Center](#)

[Fouten tijdens bestandsencryptie op lokale schijven van de computer bekijken](#)

[Rapport over gegevensencryptie bekijken](#)

[Werken met geëncrypte apparaten als er geen toegang toe is](#)

[Gegevens herstellen met behulp van de FDERT Restore Utility](#)

[Een herstelschijf voor het besturingssysteem aanmaken](#)

[Detection and Response-oplossingen](#)

[Kaspersky Endpoint Agent beheren](#)

[Migratie van beleid en taken voor Kaspersky Endpoint Agent](#)

[De \[KES+KEA\]-configuratie migreren naar \[KES+built-in agent\]](#)

[Beheerde detectie en respons](#)

[Integratie met MDR](#)

[Migratie van Kaspersky Endpoint Agent](#)

[Endpoint Detection and Response](#)

[Integratie met Kaspersky Endpoint Detection and Response](#)

[Migratie van Kaspersky Endpoint Agent](#)

[Scannen op indicatoren van compromis \(standaard taak\).](#)

[Bestand in Quarantaine plaatsen](#)

[Bestand ophalen](#)

[Bestand verwijderen](#)

[Proces starten](#)

[Proces beëindigen](#)

[Preventie van uitvoering](#)

[Computer isoleren van netwerk](#)

[Appendix 1. Ondersteunde bestandsextensies voor Preventie van uitvoering](#)

[Appendix 2. Ondersteunde script interpreters](#)

[Appendix 3. IOC-scanbereik in het register \(RegistryItem\)](#)

[Appendix 4. IOC-bestandsvereisten](#)

[Kaspersky Sandbox](#)

[Integratie met Kaspersky Sandbox](#)

[Migratie van Kaspersky Endpoint Agent](#)

[Een TLS-certificaat toevoegen](#)

[Kaspersky Sandbox-servers toevoegen.](#)

[Scannen op indicatoren van compromis \(stand-alone taak\)](#)

[Server van Kaspersky Anti Targeted Attack Platform \(KATA EDR\)](#)

[Quarantaine beheren](#)

[De maximale quarantainegrootte configureren](#)

[Gegevens over in quarantaine geplaatste bestanden verzenden naar Kaspersky Security Center](#)

[Kaspersky Security for Windows Server](#)

[KES installeren bovenop KSWs](#)

[KES activeren met een KSWs-sleutel](#)

[Het beheren van het programma op een Core Mode server](#)

[Het programma vanaf de opdrachtregel beheren](#)

[Het programma installeren](#)

[Programma activeren](#)

[Programma verwijderen](#)

[AVP-opdrachten](#)

[SCAN. Virusscan](#)

[UPDATE. Databases en softwaremodules van het programma bijwerken](#)

[ROLLBACK. Laatste update terugdraaien](#)

[TRACES. Tracing](#)

[START. Start het profiel](#)

[STOP. Een profiel stoppen](#)

[STATUS. Profielstatus](#)

[STATISTICS. Statistieken over werking van profiel](#)

[RESTORE. Bestanden vanuit Back-up terugzetten](#)

[EXPORT. Programma-instellingen exporteren](#)

[IMPORT. Programma-instellingen importeren](#)

[ADDKEY. Een licentiebestand toepassen](#)

[LICENSE. Licentiebeheer](#)

[RENEW. Een licentie aanschaffen](#)

[PBATESTRESET. Reset de resultaten van de schijfcontrole voordat u de schijf encrypt](#)

[EXIT. Programma afsluiten](#)

[EXITPOLICY. Beleid uitschakelen](#)

[STARTPOLICY. Beleid inschakelen](#)

[DISABLE. Bescherming uitschakelen](#)

[SPYWARE. Detectie van spyware](#)

[KSN. Wereldwijde/privaat KSN-overgang](#)

[KESCLI-opdrachten](#)

[Scan. Virusscan](#)

[GetScanState. Status van voltooiing van scan](#)

[GetLastScanTime. De voltooiingstijd van de scan bepalen](#)

[GetThreats. Gegevens verkrijgen over gedetecteerde bedreigingen](#)

[UpdateDefinitions. Databases en softwaremodules van het programma bijwerken](#)

[GetDefinitionState. De voltooiingstijd van de update bepalen](#)

[EnableRTP. Beveiliging inschakelen](#)

[GetRealTimeProtectionState. Status van bescherming bestanden](#)

[Version. De versie van het programma bepalen](#)

[Opdrachten voor beheer van Detection and Response](#)

[SANDBOX. Kaspersky Sandbox beheren](#)

[PREVENTIE. Preventie van uitvoering beheren](#)

[ISOLATIE. Netwerkisolatie beheren](#)

[RESTORE. Bestanden terugzetten vanuit quarantaine](#)

[IOCSCAN. Scannen op IoC's \(Indicators of Compromise\)](#)

[MDRLICENSE. MDR-activering](#)

[Foutcodes](#)

[Appendix. Programmaprofielen](#)

[Het programma via de REST API beheren](#)

[Het programma installeren met de REST API](#)

[Werken met de API](#)

[Bronnen met informatie over het programma](#)

[Contact opnemen met de Technische Support](#)

[Inhoud en opslag van traceringsbestanden](#)

[Tracing van programmawerking](#)

[Tracing van programmaprestaties](#)

[Dump schrijven](#)

[Dump- en tracebestanden beschermen](#)

[Beperkingen en waarschuwingen](#)

[Woordenlijst](#)

[Actieve licentie](#)

[Antivirusdatabases](#)

[Archief](#)

[Authenticatie-agent](#)

[Beheergroep](#)

[Beschermd bereik](#)

[Database met phishing-webadressen](#)

[Database met schadelijke webadressen](#)

[Desinfectie](#)

[Extra licentie](#)

[Geïnfecteerd bestand](#)

[Genormaliseerde notatie van het adres van een webbron](#)

[Infecteerbaar bestand](#)

[IOC](#)

[IOC-bestand](#)

[Licentiecertificaat](#)

[Masker](#)

[Netwerkagent](#)

[OLE-object](#)

[OpenIOC](#)

[Portable bestandsbeheer](#)

[Scanbereik](#)

[Taak](#)

[Trusted Platform Module](#)

[Vals alarm](#)

[Verlener van certificaat](#)

[Bijlagen](#)

[Appendix 1. Programma-instellingen](#)

[File Threat Protection](#)

[Web Threat Protection](#)

[Mail Threat Protection](#)

[Network Threat Protection](#)

[Firewall](#)

[BadUSB Attack Prevention](#)

[AMSI-bescherming](#)

[Exploit-preventie](#)

[Gedragsdetectie](#)

[Host Intrusion Prevention](#)

[Remediation Engine](#)

[Kaspersky Security Network](#)

[Webcontrole](#)

[Apparaatcontrole](#)  
[Programmacontrole](#)  
[Adaptieve controle op afwijkingen](#)  
[Endpoint Sensor](#)  
[Kaspersky Sandbox](#)  
[Endpoint Detection and Response](#)  
[Full Disk Encryption](#)  
[File Level Encryption](#)  
[Encryptie van verwisselbare schijven](#)  
[Sjablonen \(gegevensencryptie\)](#)  
[Uitzonderingen](#)  
[Programma-instellingen](#)  
[Rapporten en Opslag](#)  
[Netwerkinstellingen](#)  
[Interface](#)  
[Instellingen beheren](#)  
[Databases en softwaremodules van het programma bijwerken](#)  
[Appendix 2. Vertrouwensgroepen voor programma's](#)  
[Appendix 3. Bestandsextensies voor snelle scan van verwisselbare schijven](#)  
[Appendix 4. Bestandstypen voor het bijlagefilter van Mail Threat Protection](#)  
[Appendix 5. Netwerkinstellingen voor interactie met externe services](#)  
[Appendix 6. Programma-gebeurtenissen](#)  
[Informatie over code van derden](#)  
[Kennisgevingen over handelsmerken](#)

# Kaspersky Endpoint Security voor Windows-help

## 🔍 Wat is er nieuw in 11.9.0

- [Nu kunt u een Authenticatie-agent-service-account maken voor Kaspersky Disk Encryption](#)
- [Verbeterde detectiedetailsinterface voor EDR Optimum](#)
- [Wat is er nieuw in elke versie van Kaspersky Endpoint Security voor Windows](#)

## 📁 Aan de slag

- [Implementatie van Kaspersky Endpoint Security voor Windows](#)
- [Eerste setup van Kaspersky Endpoint Security voor Windows](#)
- [Licentiebeheer van Kaspersky Endpoint Security voor Windows](#)

## 🛡️ Dreigingen elimineren

- [Op werkstations](#)
- [Op servers](#)
- Reageren op de detectie van een indicator of compromise ([Networkisolatie](#) → [Quarantaine](#) → [Preventie van uitvoering](#))

## 🔗 KES gebruiken als onderdeel van andere oplossingen

- [Kaspersky EDR](#)
- [Kaspersky Sandbox](#)
- [Kaspersky MDR](#)

## 📄 Gegevensverstrekking

- [Onder de Gebruiksrechtovereenkomst](#)
- [Wanneer de KSN gebruiken](#)

- [AVG](#)

## Nieuwigheden

### Update 11.9.0

Kaspersky Endpoint Security 11.9.0 voor Windows beschikt over de volgende functies en verbeteringen:

1. Nu kunt u [een service-account maken voor een authenticatie-agent](#) wanneer u Kaspersky Disk Encryption gebruikt. De service-account is nodig om toegang te krijgen tot de computer, bijvoorbeeld wanneer de gebruiker het wachtwoord vergeet. U kunt de service-account ook gebruiken als reserve-account.
2. Kaspersky Endpoint Agent distributiepakket maakt niet langer deel uit van de [programmadiistributiekit](#). Om oplossingen voor [Detection and Response](#) te ondersteunen, kunt u de ingebouwde agent van Kaspersky Endpoint Security gebruiken. U kunt indien nodig het Kaspersky Endpoint Agent-distributiepakket downloaden van de Kaspersky Anti Targeted Attack Platform-distributiekit.
3. De interface met detectedetails voor [Kaspersky Endpoint Detection and Response Optimum \(EDR Optimum\)](#) is verbeterd. Threat Response-functies hebben nu tooltips. Een stapsgewijze instructie om de beveiliging van de bedrijfsinfrastructuur te waarborgen wordt ook weergegeven wanneer er risico's worden gedetecteerd.
4. Nu kunt u Kaspersky Endpoint Security voor Windows activeren met een Kaspersky Hybrid Cloud Security-licentiecode.
5. Nieuwe evenementen toegevoegd over het [maken van verbinding met domeinen met niet-vertrouwde certificaten](#) en scanfouten van versleutelde verbindingen.

### Update 11.8.0

Kaspersky Endpoint Security 11.8.0 voor Windows beschikt over de volgende functies en verbeteringen:

1. [De ingebouwde agent voor de ondersteuning van de werking van de Kaspersky Endpoint Detection and Response Expert-oplossing is toegevoegd](#). *Kaspersky Endpoint Detection and Response Expert* is een oplossing die de IT-infrastructuur van het bedrijf beschermt tegen geavanceerde digitale dreigingen. De functionaliteit van de oplossing combineert de automatische detectie van dreigingen met de respons op deze dreigingen om geavanceerde aanvallen te neutraliseren, zoals nieuwe exploits, ransomware, bestandsloze aanvallen en methoden met legitieme hulpprogramma's van het systeem. EDR Expert biedt meer bewaking van dreigingen en reactie-functionaliteit dan EDR Optimum. Voor meer informatie over de oplossing raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Expert](#) <sup>12</sup>.
2. [De interface van de Netwerkmonitor](#) is nu verbeterd. De netwerkmonitor toont nu naast TCP ook het UDP-protocol.
3. De taak [Virusscan](#) is verbeterd. Als u de computer tijdens de scan opnieuw hebt opgestart, zet Kaspersky Endpoint Security automatisch de taak verder vanaf het punt waar de scan werd onderbroken.
4. Nu kunt u een limiet instellen voor de uitvoeringstijd van taken. U kunt de uitvoeringstijd beperken voor: *Virusscan* en *IOC-scantaken*. Na de opgegeven tijd stopt Kaspersky Endpoint Security de taak. Om de uitvoeringstijd van de *virusscan*-taak te verkorten, kunt u bijvoorbeeld [het scanbereik configureren](#) of [de scan optimaliseren](#).

5. Beperkingen van serverplatforms worden opgeheven voor het programma geïnstalleerd op Windows 10 Enterprise multi-sessie. Kaspersky Endpoint Security beschouwt Windows 10 Enterprise multi-sessie nu als een workstation-besturingssysteem, niet als een serverbesturingssysteem. [Serverplatformbeperkingen](#) zijn dienovereenkomstig niet langer van toepassing op het programma op Windows 10 Enterprise multi-sessie. Het programma gebruikt ook een workstationlicentiecode voor activering in plaats van een serverlicentiecode.

## [Update 11.7.0](#)

Kaspersky Endpoint Security voor Windows 11.7.0 heeft de volgende nieuwe functies en verbeteringen:

1. De [interface van Kaspersky Endpoint Security voor Windows](#) is geüpdatet.

2. [Ondersteuning van Windows 11, Windows 10 21H2 en Windows Server 2022](#).

3. We hebben nieuwe onderdelen toegevoegd:

- [Er werd een ingebouwde agent voor integratie met Kaspersky Sandbox](#) toegevoegd. *De Kaspersky Sandbox-oplossing* detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Kaspersky Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Kaspersky Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Kaspersky Sandbox-servers). Voor meer informatie over de oplossing gaat u naar de [Help van Kaspersky Sandbox](#).

U hebt Kaspersky Endpoint Agent niet langer nodig om Kaspersky Sandbox te gebruiken. Kaspersky Endpoint Security kan alle functies van Kaspersky Endpoint Agent uitvoeren. Om Kaspersky Endpoint Agent-beleid te migreren, gebruikt u de [Migratiewizard](#). U hebt Kaspersky Security Center 13.2 nodig opdat alle functies van Kaspersky Sandbox zouden werken. Voor details over het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security voor Windows raadpleegt u de [help bij het programma](#).

- [De ingebouwde agent voor de ondersteuning van de werking van de Kaspersky Endpoint Detection and Response Optimum-oplossing is toegevoegd](#). *Kaspersky Endpoint Detection and Response Optimum* is een oplossing die de IT-infrastructuur van het bedrijf beschermt tegen geavanceerde digitale dreigingen. De functionaliteit van de oplossing combineert de automatische detectie van dreigingen met de respons op deze dreigingen om geavanceerde aanvallen te neutraliseren, zoals nieuwe exploits, ransomware, bestandsloze aanvallen en methoden met legitieme hulpprogramma's van het systeem. Voor meer informatie over de oplossing raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#).

U hebt Kaspersky Endpoint Agent niet langer nodig om Kaspersky Endpoint Detection and Response te gebruiken. Kaspersky Endpoint Security kan alle functies van Kaspersky Endpoint Agent uitvoeren. Om Kaspersky Endpoint Agent-beleid en taken te migreren, gebruikt u de [Migratiewizard](#). Kaspersky Endpoint Detection and Response Optimum vereist Kaspersky Security Center 13.2 om alle functies te gebruiken. Voor details over het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security voor Windows raadpleegt u de [help bij het programma](#).

4. De [Migratiewizard](#) voor Kaspersky Endpoint Agent-beleid en taken werd toegevoegd. De migratiewizard maakt nieuwe beleidsregels en taken voor Kaspersky Endpoint Security voor Windows. Met deze wizard kunt u Detection and Response-oplossingen overschakelen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security. Detection and Response-oplossingen zijn onder andere Kaspersky Sandbox, Kaspersky Managed Detection and Response (EDR Optimum) en Kaspersky Managed Detection and Response (MDR).

5. [Kaspersky Endpoint Agent](#), beschikbaar in het distributiepakket, is geüpdatet naar versie 3.11.

Wanneer u een upgrade van Kaspersky Endpoint Security uitvoert, detecteert het programma de versie en het specifieke doel van de Kaspersky Endpoint Agent. Als Kaspersky Endpoint Agent is aangewezen voor de werking van Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) en Kaspersky Endpoint Detection and Response Optimum (EDR Optimum), dan schakelt Kaspersky Endpoint Security de werking van deze oplossingen over naar de ingebouwde agent van het programma. Voor Kaspersky Sandbox en EDR Optimum verwijdert het programma Kaspersky Endpoint Agent automatisch. Voor MDR kunt u Kaspersky Endpoint Agent handmatig verwijderen. Als het programma is aangewezen voor de werking van Kaspersky Endpoint Detection and Response Expert (EDR Expert), voert Kaspersky Endpoint Security een upgrade uit van de versie van Kaspersky Endpoint Agent. Raadpleeg voor meer informatie over het programma de documentatie van Kaspersky-oplossingen die Kaspersky Endpoint Agent ondersteunen.



6. De BitLocker-encryptiefunctiefunctionaliteit is verbeterd:

- De geavanceerde pincode kan nu met [BitLocker-stationsversleuteling](#) worden gebruikt. Met *Geavanceerde pincode* kunt u naast cijfers ook andere tekens gebruiken: hoofdletters en kleine letters, speciale tekens en spaties.
- Er werd een functie toegevoegd om [BitLocker-verificatie uit te schakelen voor het upgraden van het besturingssysteem of het installeren van updatepakketten](#). Na de installatie van updates moet de computer mogelijk meermaals opnieuw worden opgestart. Voor de correcte installatie van updates kunt u de BitLocker-authenticatie tijdelijk uitschakelen en de authenticatie na de installatie van de updates opnieuw inschakelen.
- Nu kunt u [een vervaltijd instellen voor het wachtwoord of de pincode van de BitLocker-encryptie](#). Wanneer het wachtwoord of de pincode vervalt, wordt de gebruiker een nieuw wachtwoord gevraagd door Kaspersky Endpoint Security.

7. Nu kunt u het maximale aantal pogingen tot toetsenbordautorisatie instellen voor BadUSB Attack Prevention. Na het bereiken van [het ingestelde aantal verkeerde autorisatiecodes](#) wordt het USB-apparaat tijdelijk vergrendeld.

8. De functionaliteit van Firewall is verbeterd:

- Nu kunt u een bereik van IP-adressen configureren voor [Firewall-pakketregels](#). U kunt een bereik van adressen in de IPv4- of IPv6-structuur invoeren. Bijvoorbeeld 192.168.1.1-192.168.1.100 of 12:34::2-12:34::99.
- Nu kunt u DNS-namen voor [Firewall-pakketregels](#) in plaats van IP-adressen invoeren. U doet er goed aan om DNS-namen alleen te gebruiken voor computers in een netwerk of interne services. De interactie met cloudservices (zoals Microsoft Azure) en andere internetbronnen moet door het onderdeel Webcontrole gebeuren.

9. Het zoeken naar een [regel van Webcontrole](#) is verbeterd. Als u een toegangsregel voor webbronnen wilt zoeken, kunt u naast de naam van de regel ook de URL van de website, een gebruikersnaam, een inhoudscategorie of een gegevenstype gebruiken.

10. De taak *Virusscan* is verbeterd:

- De taak [Virusscan](#) in *inactieve modus* werd verbeterd. Als u de computer tijdens de scan opnieuw hebt opgestart, zet Kaspersky Endpoint Security automatisch de taak verder vanaf het punt waar de scan werd onderbroken.
- De taak [Virusscan](#) is geoptimaliseerd. Standaard start Kaspersky Endpoint Security de scan alleen als de computer inactief is. U kunt in de taakeigenschappen configureren wanneer de computerscan moet worden uitgevoerd.

11. Nu kunt u de gebruikerstoegang tot gegevens van [Bewaking van programma-activiteit](#) beperken. *Bewaking van programma-activiteit* is een tool ontworpen voor de realtime weergave van informatie over de activiteit van de computer van een gebruiker. De beheerder kan Bewaking van programma-activiteit verbergen voor de gebruiker in de beleidseigenschappen van het programma.

12. [De beveiliging van het programmabeheer via de REST API is verbeterd](#). Nu valideert Kaspersky Endpoint Security de handtekening van verzoeken die via de REST API worden verzonden. Om het programma te beheren, moet u een aanvraag-identificatiecertificaat installeren.

Kaspersky Endpoint Security 11.6.0 voor Windows beschikt over de volgende functies en verbeteringen:

1. [Ondersteuning voor Windows 10 21H1](#). Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows 10 raadpleegt u de [Knowledge Base van de Technische Support](#).
2. [Het onderdeel Managed Detection and Response werd toegevoegd](#). Dit onderdeel vergemakkelijkt de interactie met de oplossing die bekend staat als Kaspersky Managed Detection and Response. Kaspersky Managed Detection and Response (MDR) biedt 24 uur per dag bescherming tegen een groeiend aantal dreigingen die de geautomatiseerde beschermingsmechanismen kunnen omzeilen voor bedrijven die het moeilijk hebben om hooggekwalificeerde experts te vinden of die over beperkte interne middelen beschikken. Raadpleeg de Help van Kaspersky Managed Detection and Response voor gedetailleerde informatie over hoe de oplossing werkt.
3. [Kaspersky Endpoint Agent](#), opgenomen in de distributiekits, werd bijgewerkt naar versie 3.10. Kaspersky Endpoint Agent 3.10 biedt nieuwe functies, lost enkele eerdere problemen op en heeft een verbeterde stabiliteit. Raadpleeg voor meer informatie over het programma de documentatie van Kaspersky-oplossingen die Kaspersky Endpoint Agent ondersteunen.
4. Het biedt nu de mogelijkheid om bescherming tegen aanvallen te beheren zoals Network Flooding en Port scanning in [Network Threat Protection-instellingen](#).
5. Nieuwe methode toegevoegd voor het maken van netwerkregels voor Firewall. U kunt [pakketregels](#) en [programmaregels](#) toevoegen voor verbindingen die in het venster [Netwerkmonitor](#) worden weergegeven. Sommige verbindinginstellingen voor netwerkregels worden echter automatisch geconfigureerd.
6. [De interface van de Netwerkmonitor](#) is nu verbeterd. Informatie toegevoegd over netwerkactiviteit: proces-ID, die netwerkactiviteit start; netwerktype (lokaal netwerk of internet); lokale poorten. Standaard is de informatie over het netwerktype verborgen.
7. Er is nu de mogelijkheid om automatisch Authenticatie-agent-accounts aan te maken voor nieuwe Windows-gebruikers. Met de agent kan een gebruiker authenticatie voltooiën voor toegang tot schijven die zijn [versleuteld met Kaspersky Disk Encryption-technologie](#), en om het besturingssysteem te laden. Het programma controleert informatie over Windows-gebruikersaccounts op de computer. Als Kaspersky Endpoint Security een Windows-gebruikersaccount detecteert die geen Authenticatie-agent-account heeft, maakt het programma een nieuw account aan voor toegang tot geëncrypte schijven. Dit betekent dat u niet [handmatig Authenticatie-agent-accounts](#) hoeft toe te voegen voor computers met reeds versleutelde schijven.
8. Er is nu de mogelijkheid om het schijfversleutelingsproces te volgen in de programma-interface op de computers van gebruikers (Kaspersky Disk Encryption en BitLocker). U kunt de tool Versleutelingsmonitor uitvoeren vanuit het [hoofdvenster van het programma](#).

## [Update 11.5.0](#)

Kaspersky Endpoint Security 11.5.0 voor Windows beschikt over de volgende functies en verbeteringen:

1. [Ondersteuning voor Windows 10 20H2](#). Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows 10 raadpleegt u de [Knowledge Base van de Technische Support](#) <sup>2</sup>.
2. Bijgewerkt [interfaceprogramma](#). Ook het [programmapictogram in het vak meldingen](#), programmameldingen en dialoogvensters bijgewerkt.
3. Verbeterde interface van de Kaspersky Endpoint Security-webplug-in voor de componenten Programmacontrole, Apparaatbeheer en Adaptieve controle op afwijkingen.
4. Toegevoegde functionaliteit voor het importeren en exporteren van lijsten met regels en uitsluitingen in XML-indeling. Met de XML-indeling kunt u lijsten bewerken nadat ze zijn geëxporteerd. U kunt lijsten beheren met Webconsole van Kaspersky Security Center Console. De volgende lijsten zijn beschikbaar voor export/import:
  - [Gedragsdetectie \(lijst met uitzonderingen\)](#).
  - [Web Threat Protection \(lijst met vertrouwde webadressen\)](#).
  - [Mail Threat Protection \(lijst met filterextensies voor bijlagen\)](#).
  - [Network Threat Protection \(lijst met uitzonderingen\)](#).
  - [Firewall \(lijst met regels voor netwerkpakketten\)](#).
  - [Programmacontrole \(lijst met regels\)](#).
  - [Webcontrole \(lijst met regels\)](#).
  - [Netwerkpoortbewaking \(lijsten met poorten en programma's die worden gecontroleerd door Kaspersky Endpoint Security\)](#).
  - [Kaspersky Disk Encryption \(lijst met uitsluitingen\)](#).
  - [Encryptie van verwisselbare schijven \(lijst met regels\)](#).
5. Object MD5-informatie is toegevoegd aan het [dreigingsdetectierapport](#). In eerdere versies van het programma toonde Kaspersky Endpoint Security alleen de SHA256 van een object.
6. Mogelijkheid toegevoegd [om de prioriteit toe te wijzen voor apparaattoegangsregels](#) in de instellingen van apparaatcontrole. Prioriteitstoewijzing maakt een flexibelere configuratie van gebruikerstoegang tot apparaten mogelijk. Als een gebruiker aan meerdere groepen is toegevoegd, regelt Kaspersky Endpoint Security de apparaattoegang op basis van de regel met de hoogste prioriteit. U kunt bijvoorbeeld de machtiging alleen-lezen verlenen aan de groep ledereen en de machtiging lezen/schrijven aan de groep administrators. Om dit te doen, wijst u een prioriteit van 0 toe voor de groep administrators en een prioriteit van 1 voor de groep ledereen. U kunt de prioriteit alleen configureren voor apparaten met een bestandssysteem. Dit omvat harde schijven, verwisselbare schijven, disktestations, cd-/dvd-stations en draagbare apparaten (MTP).
7. Nieuwe functionaliteit toegevoegd:
  - [Beheer geluidsmeldingen](#).
  - Betaalbaar netwerken Kaspersky Endpoint Security beperkt zijn eigen netwerkverkeer als de internetverbinding beperkt is (bijvoorbeeld via een mobiele verbinding).

- [Beheer de instellingen van Kaspersky Endpoint Security via vertrouwde externe beheertoepassingen](#) (zoals TeamViewer, LogMeln Pro en Remotely Anywhere). U kunt programma's voor extern beheer gebruiken om Kaspersky Endpoint Security te starten en instellingen te beheren in de programma-interface.
  - [Beheer de instellingen voor het scannen van beveiligd verkeer in Firefox en Thunderbird](#). U kunt de certificaatopslag selecteren die door Mozilla zal worden gebruikt: de Windows-certificaatopslag of de Mozilla-certificaatopslag. Deze functionaliteit is alleen beschikbaar voor computers waarop geen beleid wordt toegepast. Als een beleid wordt toegepast op een computer, dan schakelt Kaspersky Endpoint Security automatisch het gebruik in van de Windows-certificaatopslag in Firefox en Thunderbird.
8. Mogelijkheid toegevoegd om [de scanmodus voor veilig verkeer te configureren](#): scan verkeer altijd, zelfs als beschermingsonderdelen uitgeschakeld zijn, of scan verkeer wanneer daarom wordt gevraagd door beschermingsonderdelen.
  9. Herziene procedure voor het [verwijderen van informatie uit rapporten](#). Een gebruiker kan alleen alle rapporten verwijderen. In eerdere versies van het programma kon een gebruiker specifieke onderdelen selecteren waarvan de informatie uit rapporten zou worden verwijderd.
  10. Herziene procedure voor het [importeren van een configuratiebestand met Kaspersky Endpoint Security-instellingen](#), en herziene procedure voor het [herstellen van programma-instellingen](#). Voorafgaand aan het importeren of herstellen toont Kaspersky Endpoint Security alleen een waarschuwing. In eerdere versies van het programma kon u de waarden van de nieuwe instellingen bekijken voordat ze werden toegepast.
  11. Vereenvoudigde [procedure voor het herstellen van de toegang tot een station dat is gecodeerd door BitLocker](#). Na het voltooiën van de procedure voor toegangsherstel, vraagt Kaspersky Endpoint Security de gebruiker om een nieuw wachtwoord of nieuwe pincode in te stellen. Nadat u een nieuw wachtwoord hebt ingesteld, encrypt BitLocker de schijf. In de vorige versie van het programma moest de gebruiker het wachtwoord handmatig opnieuw instellen in de BitLocker-instellingen.
  12. Gebruikers hebben nu de mogelijkheid om hun eigen lokale [vertrouwde zone](#) voor een specifieke computer te creëren. Op deze manier kunnen gebruikers hun eigen lokale lijsten met [uitzonderingen](#) en [vertrouwde programma's maken](#) naast de algemene vertrouwde zone in een beleid. Een beheerder kan het gebruik van lokale uitzonderingen of lokale vertrouwde programma's toestaan of blokkeren. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.
  13. Mogelijkheid toegevoegd [om opmerkingen in te voeren in de eigenschappen van vertrouwde programma's](#). Opmerkingen helpen het zoeken en sorteren van vertrouwde applicaties te vereenvoudigen.
  14. [Het programma via de REST API beheren](#):
    - Het is nu mogelijk om de instellingen te configureren van de Mail Threat Protection-extensie voor Outlook.
    - Het is verboden om de detectie van virussen, wormen en Trojaanse paarden uit te schakelen.

## [Update 11.4.0](#)

Kaspersky Endpoint Security 11.4.0 voor Windows beschikt over de volgende functies en verbeteringen:

1. Nieuwe ontwerp van het [programmapictogram in het systeemvak](#). Het nieuwe  wordt nu weergegeven in plaats van het oude -pictogram. Als de gebruiker een actie moet uitvoeren (bijvoorbeeld de computer opnieuw opstarten na het updaten van de applicatie), dan verandert het pictogram in . Als de beschermingsonderdelen van het programma uitgeschakeld of defect zijn, dan verandert het pictogram in  of . Als u met de muis over het pictogram beweegt, geeft Kaspersky Endpoint Security een beschrijving van het probleem met computerbeveiliging weer.
2. Kaspersky Endpoint Agent, beschikbaar in het distributiepakket, is geüpdatet naar versie 3.9. Kaspersky Endpoint Agent 3.9 ondersteunt integratie met nieuwe Kaspersky-oplossingen. Raadpleeg voor meer informatie over het programma de documentatie van Kaspersky-oplossingen die Kaspersky Endpoint Agent ondersteunen.
3. De status *Niet ondersteund door licentie* voor Kaspersky Endpoint Security-onderdelen. U kunt de status van componenten bekijken in het [hoofdenster van het programma](#).
4. Nieuwe gebeurtenissen uit [Exploit-preventie](#) zijn toegevoegd aan [rapporten](#).
5. Stuurprogramma's voor [Kaspersky Disk Encryption-technologie](#) worden nu automatisch toegevoegd aan de Windows Recovery-omgeving (WinRE) wanneer de encryptie van schijven wordt gestart. De vorige versie van Kaspersky Endpoint Security heeft stuurprogramma's toegevoegd tijdens de installatie van het programma. Het toevoegen van stuurprogramma's aan WinRE kan de stabiliteit van het programma verbeteren bij het herstellen van het besturingssysteem op computers die worden beschermd door Kaspersky Disk Encryption-technologie.

Het onderdeel Endpoint Sensor is verwijderd uit Kaspersky Endpoint Security. U kunt Endpoint Sensor-instellingen nog altijd in een beleid configureren op voorwaarde dat versie 11.0.0 tot 11.3.0 van Kaspersky Endpoint Security op de computer geïnstalleerd is.

## Veelgestelde vragen



### ALGEMEEN

[Op welke computers werkt Kaspersky Endpoint Security?](#)

[Wat is er veranderd sinds de laatste versie?](#)

[Met welke andere Kaspersky-programma's is Kaspersky Endpoint Security compatibel?](#)

[Hoe kan ik het gebruik van computerbronnen herleiden tot een minimum wanneer Kaspersky Endpoint Security actief is?](#)



### IMPLEMENTATIE

[Hoe installeer ik Kaspersky Endpoint Security op alle computers binnen een bedrijf?](#)



### INTERNET

[Scant Kaspersky Endpoint Security ook geëncrypte verbindingen \(HTTPS\)?](#)

[Hoe zorg ik ervoor dat gebruikers alleen met vertrouwde wifinetwerken verbinding maken?](#)

[Hoe blokkeer ik bezoeken aan sociale netwerken?](#)



### PROGRAMMA'S

[Hoe achterhaal ik welke programma's zijn geïnstalleerd op de computer van een gebruiker \(inventaris\)?](#)

[Hoe belet ik dat computergames worden gestart?](#)

[Hoe controleer ik of Programmacontrole juist is geconfigureerd?](#)

[Welke installatie-instellingen kan ik configureren met de opdrachtregel?](#)

[Hoe kan ik Kaspersky Endpoint Security op afstand verwijderen?](#)



#### UPDATE

[Hoe kan ik de databases updaten?](#)

[Wat moet ik doen als er na een update problemen optreden?](#)

[Hoe kan ik databases updaten als ik me buiten het bedrijfsnetwerk bevind?](#)

[Kan ik een proxyserver voor updates gebruiken?](#)



#### BEVEILIGING

[Hoe scant Kaspersky Endpoint Security e-mail?](#)

[Hoe zorg ik ervoor dat een vertrouwd bestand niet wordt gescand?](#)

[Hoe bescherm ik een computer tegen virussen op USB-sticks?](#)

[Hoe kan ik een virusscan uitvoeren zonder dat de gebruiker het weet?](#)

[Hoe kan ik de bescherming van Kaspersky Endpoint Security tijdelijk pauzeren?](#)

[Hoe kan ik een bestand terugzetten dat Kaspersky Endpoint Security per vergissing heeft verwijderd?](#)

[Hoe zorg ik ervoor dat Kaspersky Endpoint Security niet kan worden verwijderd door een gebruiker?](#)

[Hoe voeg ik een programma toe aan de lijst met vertrouwde programma's?](#)



#### APPARATEN

[Hoe blokkeer ik het gebruik van USB-sticks?](#)

[Hoe voeg ik een apparaat toe aan de lijst met vertrouwde apparaten?](#)

[Kan ik toegang tot een geblokkeerd apparaat krijgen?](#)



#### ENCRYPTIE

[Wanneer is encryptie mogelijk?](#)

[Hoe gebruik ik een wachtwoord om de toegang tot een archief beperken?](#)

[Kan ik smartcards en tokens met encryptie gebruiken?](#)

[Kan ik toegang tot geëncrypte gegevens krijgen als er geen verbinding met Kaspersky Security Center is?](#)

[Wat moet ik doen als het besturingssysteem van de computer fouten vertoont maar de gegevens geëncrypt blijven?](#)



#### ONDERSTEUNING

[Waar kan ik het rapportbestand vinden?](#)







[Hoe maak ik een tracebestand?](#)

[Hoe schakel ik het schrijven naar een dump in?](#)

# Kaspersky Endpoint Security voor Windows

Kaspersky Endpoint Security voor Windows (hierna ook Kaspersky Endpoint Security genoemd) biedt een uitgebreide computerbescherming tegen verschillende soorten dreigingen en netwerk- en phishingaanvallen.


## Technologieën voor detectie van dreigingen

|  |   |
|--|---|
| <p> <b>Machine learning</b></p> <p>Kaspersky Endpoint Security gebruikt een model gebaseerd op machine learning. Het model is ontwikkeld door experts van Kaspersky. Gegevens over dreigingen worden continu aan het model toegevoegd vanaf KSN (modeltraining).</p> <p> <b>Cloud- analyse</b></p> <p>Kaspersky Endpoint Security krijgt van het <a href="#">Kaspersky Security Network</a> gegevens over dreigingen. <i>Kaspersky Security Network (KSN)</i> 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.</p> <p> <b>Geavanceerde analyse</b></p> <p>Kaspersky Endpoint Security gebruikt gegevens over dreigingen toegevoegd door virusanalisten van Kaspersky. Virusanalisten evalueren objecten als de reputatie van een object niet automatisch kan worden bepaald.</p> | <p> <b>Gedrags- analyse</b></p> <p>Kaspersky Endpoint Security analyseert de activiteit van een object in realtime.</p> <p> <b>Automatische analyse</b></p> <p>Kaspersky Endpoint Security krijgt gegevens van een systeem dat objecten automatisch analyseert. Het systeem verwerkt alle objecten die naar Kaspersky worden verstuurd. Vervolgens bepaalt het systeem de reputatie van het object en voegt het de gegevens aan de antivirusdatabases toe. Als het systeem de reputatie van het object niet kan bepalen, stuurt het systeem een verzoek naar de Kaspersky-virusanalisten.</p> <p> <b>Kaspersky Sandbox</b></p> <p>Kaspersky Endpoint Security verwerkt het object in een virtuele machine. Kaspersky Sandbox analyseert het gedrag van het object en neemt een beslissing over de reputatie. Deze technologie is alleen beschikbaar als u de <a href="#">Kaspersky Sandbox-oplossing</a> gebruikt.</p> |
|--|---|

## Keuzelijst

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

Keuzelijst

| Gedeelte   | Onderdeel   |
|--|---|
| <p><b>Essential Threat Protection</b></p> <p></p> | <p><b>File Threat Protection</b></p> <p>Met het onderdeel File Threat Protection voorkomt u dat het bestandssysteem van de computer geïnfecteerd raakt. Standaard bevindt het onderdeel File Threat Protection zich permanent in het RAM van de computer. Het onderdeel scant bestanden op alle schijven van de computer, evenals op aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de <a href="#">Kaspersky Security Network-cloudservice</a> en heuristische analyse.</p> <p><b>Web Threat Protection</b></p> |



Het onderdeel Web Threat Protection voorkomt downloads van schadelijke bestanden vanaf het internet en blokkeert ook schadelijke en phishingwebsites. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

### Mail Threat Protection

Het onderdeel Mail Threat Protection scant de bijlagen van inkomende en uitgaande e-mailberichten op virussen en andere dreigingen. Dit onderdeel scant ook berichten op schadelijke links en phishinglinks. Het onderdeel Mail Threat Protection bevindt zich standaard permanent in het RAM van de computer en scant alle berichten die worden ontvangen of verzonden met de protocollen POP3, SMTP, IMAP of NNTP of de Microsoft Office Outlook-mailclient (MAPI). Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

### Network Threat Protection

Het onderdeel Network Threat Protection scant inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Wanneer Kaspersky Endpoint Security een poging tot netwerkaanval op de computer van een gebruiker detecteert, blokkeert het de netwerkverbinding met de aanvallende computer. 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 Threat Protection wordt bijgewerkt wanneer [de databases en de modules van het programma worden bijgewerkt](#).

### Firewall

De Firewall blokkeert ongeautoriseerde verbindingen met de computer tijdens het werken op internet of een lokaal netwerk. De Firewall controleert ook de netwerkactiviteit van programma's op de computer. Hierdoor kunt u uw bedrijfs-LAN beschermen tegen identiteitsdiefstal en andere aanvallen. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en vooraf gedefinieerde *netwerkregels*.

### BadUSB Attack Prevention

Het onderdeel BadUSB Attack Prevention voorkomt dat geïnfecteerde USB-apparaten zich voordoen als een toetsenbord wanneer ze op de computer worden aangesloten.

### AMSI-bescherming

AMSI-beschermingsonderdeel is ontwikkeld als ondersteuning voor de Antimalware Scan Interface van Microsoft. Dankzij de *Antimalware Scan Interface (AMSI)* kunnen programma's van andere leveranciers met AMSI-ondersteuning objecten (bijvoorbeeld PowerShell-scripts) versturen naar Kaspersky Endpoint Security om ze te laten scannen en om vervolgens de resultaten van de scans voor deze objecten te ontvangen.

## Advanced Threat Protection



### Kaspersky Security Network

*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 dreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. Als u deelneemt aan Kaspersky Security Network, ontvangt Kaspersky Endpoint Security van de KSN-services informatie over de categorie en reputatie van gescande bestanden, alsook informatie over de reputatie van gescande webadressen.



## **Gedragsdetectie**

Het onderdeel Gedragsdetectie ontvangt gegevens over de acties van programma's op de computer en geeft deze gegevens door aan andere beschermingsonderdelen om hun prestaties te verbeteren. Het onderdeel Gedragsdetectie gebruikt definities van gedragspatronen (BSS) voor programma's. Als een programma-activiteit overeenkomt met een behavior stream signature, voert Kaspersky Endpoint Security de geselecteerde responsieve actie uit. De functionaliteit van Kaspersky Endpoint Security op basis van de definities van gedragspatronen levert een proactieve bescherming voor de computer.

## **Exploit-preventie**

Het onderdeel Exploit-preventie detecteert programmacode die kwetsbaarheden op de computer uitbuit om bevoegdheden van beheerders te misbruiken of om schadelijke activiteit uit te voeren. Exploits kunnen bijvoorbeeld aanvallen met bufferoverschrijdingen gebruiken. Hiervoor verstuurt de exploit een grote hoeveelheid gegevens naar een kwetsbaar programma. Wanneer deze gegevens worden verwerkt, voert het kwetsbare programma schadelijke code uit. Door deze aanval kan de exploit een onbevoegde installatie van malware starten. Wanneer er zonder medeweten van de gebruiker wordt geprobeerd om een uitvoerbaar bestand te starten met een kwetsbaar programma, belet Kaspersky Endpoint Security dat het bestand wordt gestart en brengt het de gebruiker op de hoogte.

## **Host Intrusion Prevention**

Het onderdeel Host Intrusion Prevention voorkomt dat programma's acties uitvoeren die mogelijk gevaarlijk zijn voor het besturingssysteem en controleert de toegang tot bronnen van het besturingssysteem en persoonlijke gegevens. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases en de Kaspersky Security Network-cloudservice.

## **Remediation Engine**

Via Remediation Engine kan Kaspersky Endpoint Security acties van malware in het besturingssysteem terugdraaien.

## **Security Controls**



### **Programmacontrole**

Programmacontrole beheert het opstarten van applicaties op de computers van gebruikers. Hiermee kunt u een bedrijfsbeveiligingsbeleid implementeren bij het gebruik van programma's. Programmacontrole vermindert ook het risico op computerinfectie door de toegang tot programma's te beperken.

### **Apparaatcontrole**

Apparaatcontrole beheert de toegang van gebruikers tot apparaten die zijn geïnstalleerd in of aangesloten op de computer (bijvoorbeeld harde schijven, camera's of wifi-apparaten). Met dit onderdeel kunt u de computer beschermen tegen infecties en datalekken voorkomen wanneer zulke apparaten worden aangesloten.

### **Webcontrole**

Webcontrole beheert de toegang van gebruikers tot webbronnen. Het onderdeel helpt zo het verkeersvolume en het misbruik van werkuren verminderen. Als een gebruiker een website probeert te openen die is beperkt door Webcontrole, blokkeert Kaspersky Endpoint Security de toegang of toont het een waarschuwing.

### **Adaptieve controle op afwijkingen**

Het onderdeel Adaptieve controle op afwijkingen bewaakt en blokkeert acties die niet kenmerkend zijn voor de computers in het bedrijfsnetwerk. Adaptieve controle op afwijkingen gebruikt een aantal regels om afwijkend gedrag bij te houden (bijvoorbeeld de regel *Start van Windows PowerShell via Office-programma*). Regels worden door Kaspersky-experts gemaakt op basis van kenmerkende scenario's van malware-activiteit. U kunt configureren hoe Adaptieve controle op afwijkingen elke regel moet gebruiken en bijvoorbeeld toestaan dat PowerShell-scripts voor de automatisering van bepaalde workflows worden uitgevoerd. Kaspersky Endpoint Security updatet de reeks regels samen met de programmadatabases.

## Taken



### Virusscan

Kaspersky Endpoint Security scant de computer op virussen en andere bedreigingen. De virusscan helpt malware te vermijden die niet is gedetecteerd door beschermingsonderdelen, bijvoorbeeld wegens een laag ingesteld beveiligingsniveau.

### Update

Kaspersky Endpoint Security downloadt bijgewerkte databases en programmamodules. Updates houden de computer beschermd tegen de nieuwste virussen en andere dreigingen. Het programma wordt standaard automatisch bijgewerkt maar u kunt indien nodig de databases en de programmamodules handmatig bijwerken.

### Laatste update terugdraaien

Kaspersky Endpoint Security draait de laatste update van de databases en de modules terug. Zo kunt u indien nodig de databases en de programmamodules terugdraaien naar hun vorige versies wanneer de nieuwe databaseversie bijvoorbeeld een ongeldige definitie bevat waardoor Kaspersky Endpoint Security een veilig programma blokkeert.

### 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.

## Gegevensencryptie



### File Level Encryption

Met dit onderdeel kunt u encryptieregels voor bestanden maken. U kunt vooraf gedefinieerde mappen selecteren die u wilt encrypten, een map handmatig selecteren of individuele bestanden volgens extensie selecteren.

### Full Disk Encryption

Met dit onderdeel kunt u de harde schijf encrypten met Kaspersky Disk Encryption of BitLocker-stationsversleuteling.

### Encryption of removable drives

Met dit onderdeel kunt u gegevens op verwisselbare schijven beschermen. U kunt Full Disk Encryption (FDE) of File Level Encryption (FLE) gebruiken.

## Detection and Response



### Endpoint Detection and Response Optimum

Ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing (hierna ook "EDR Optimum" genoemd). *Kaspersky Endpoint Detection and Response Expert* is een oplossing die de IT-infrastructuur van het bedrijf beschermt tegen geavanceerde digitale dreigingen. De functionaliteit van de oplossing combineert de automatische detectie van dreigingen met de respons op deze dreigingen om geavanceerde aanvallen te neutraliseren, zoals nieuwe exploits, ransomware, bestandsloze aanvallen en methoden met legitieme hulpprogramma's van het systeem. Voor meer informatie over de oplossing raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#).

## Endpoint Detection and Response Expert

Ingebouwde agent voor de Kaspersky Endpoint Detection and Response Expert-oplossing (hierna ook "EDR Expert" genoemd). EDR Expert biedt meer bewaking van dreigingen en reactie-functionaliteit dan EDR Optimum. Voor meer informatie over de oplossing raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Expert](#).

## Kaspersky Sandbox

Ingebouwde agent voor de Kaspersky Sandbox-oplossing. De *Kaspersky Sandbox-oplossing* detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Kaspersky Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Kaspersky Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Kaspersky Sandbox-servers). Voor meer informatie over de oplossing gaat u naar de [Help van Kaspersky Sandbox](#).

## Managed Detection and Response

Ingebouwde agent voor de ondersteuning van de werking van de Kaspersky Managed Detection and Response-oplossing is toegevoegd. De *Kaspersky Managed Detection and Response (MDR)*-oplossing detecteert en analyseert automatisch beveiligingsincidenten in uw bedrijf. Hiertoe gebruikt MDR telemetriegegevens van eindpunten en machine learning. MDR stuurt incidentgegevens naar Kaspersky-experts. De experts kunnen vervolgens het incident verwerken en bijvoorbeeld een nieuwe vermelding toevoegen aan de antivirusdatabases. Of de experts kunnen aanbevelingen geven voor de verwerking van het incident en bijvoorbeeld voorstellen om de computer te isoleren van het netwerk. Voor gedetailleerde informatie over de werking van de oplossing raadpleegt u de [Help van Kaspersky Managed Detection and Response](#).

## Onderhoudsfuncties van het programma

Kaspersky Endpoint Security beschikt over een aantal onderhoudsfuncties. De onderhoudsfuncties zijn meegeleverd 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 bij. U kunt rapporten ook gebruiken om de resultaten van voltooide taken bij te houden. De rapporten bevatten lijsten met gebeurtenissen die zich tijdens de werking van Kaspersky Endpoint Security voordeden 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.
- **Back-up.** Als het programma geïnfecteerde bestanden vindt tijdens het scannen van de computer op virussen en andere dreigingen, blokkeert het die bestanden. 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 actieve dreigingen*. U kunt bestanden scannen, bestanden in hun originele map terugzetten en de gegevensopslag legen.
- **Meldingen.** Via de service voor meldingen kan de gebruiker gebeurtenissen bijhouden die van invloed zijn op de status van de computerbescherming en 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 efficiëntie van de computerbescherming via het realtime gebruik van informatie over de reputatie van bestanden, webbronnen en software die van gebruikers wereldwijd wordt ontvangen.

- **Licentie.** Door de aanschaf van een licentie kunt u de functionaliteit van het programma ontgrendelen, updates voor de programmadatabases en -modules installeren en ondersteuning via 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 naar de Technische Support van Kaspersky versturen via de Kaspersky CompanyAccount-portal of u kunt bellen naar de Technische Support.

## Software pakket

Het softwarepakket bevat de volgende distributiepakketten:

- **Sterke encryptie (AES256)**

Dit distributiepakket bevat cryptografische tools die het AES-encryptiealgoritme (Advanced Encryption Standard) met een effectieve sleutellengte van 256 bits implementeren.

- **Normale encryptie (AES56)**

Dit distributiepakket bevat cryptografische tools die het AES-encryptiealgoritme met een effectieve sleutellengte van 56 bits implementeren.

Elk distributiepakket bevat de volgende bestanden:

|                       |   |
|-----------------------|---|
| kes_win.msi           | Installatiepakket van Kaspersky Endpoint Security   |
| setup_ks.exe          | Benodigde bestanden voor <a href="#">de installatie van het programma</a> via een van de beschikbare methoden.        |
| kes_win.kud           | Bestand voor het <a href="#">maken van installatiepakketten voor Kaspersky Endpoint Security</a> .                    |
| klcfginst.msi         | Installatiepakket voor de Kaspersky Endpoint Security-beheerplug-in voor Kaspersky Security Center.                   |
| bases.cab             | Bestanden van het updatepakket die tijdens de installatie worden gebruikt.  |
| cleaner.cab           | Bestanden voor de verwijdering van incompatibele software.  |
| incompatible.txt      | Bestand dat een lijst met incompatibele software bevat.   |
| ksn_<language_ID>.txt | Bestand waarin u de voorwaarden voor deelname aan Kaspersky Security Network kunt lezen.                              |
| license.txt           | Bestand waarin u de <a href="#">Gebruiksrechtsovereenkomst</a> en het Privacybeleid kunt lezen.                       |
| installer.ini         | Bestand met de interne instellingen van het distributiepakket.  |
| keswin_web_plugin.zip | Archief met de bestanden vereist voor het installeren van de <a href="#">Kaspersky Endpoint Security-webplug-in</a> . |

U wordt aanbevolen om de waarden van de instellingen niet te wijzigen. Gebruik het bestand [setup.ini](#) als u de installatieopties wilt wijzigen.

## Hardware- en softwarevereisten

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

Minimale algemene vereisten:

- 2 GB vrije ruimte op de harde schijf
- CPU:
  - Werkstation: 1 GHz
  - Server: 1.4 GHz
  - Support voor de SSE2-instructieset
- RAM:
  - Werkstation (x86): 1 GB
  - Werkstation (x64): 2 GB
  - Server: 2 GB

### Werkstations

Ondersteunde besturingssystemen voor werkstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 of hoger;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessie;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise.

Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows 10 raadpleegt u de [Knowledge Base van de Technische Support](#).

Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows 11 raadpleegt u de [Knowledge Base van de Technische Support](#).

### Servers

Kaspersky Endpoint Security ondersteunt hoofdonderdelen van het programma op computers met het Windows-besturingssysteem voor servers. U kunt Kaspersky Endpoint Security voor Windows gebruiken in plaats van Kaspersky Security voor Windows Server op servers en clusters van uw organisatie. De Core-modus wordt ondersteund met [beperkingen](#).

Ondersteunde besturingssystemen voor servers:

- Windows Small Business Server 2011 Essentials / Standard (64-bits);

Microsoft Small Business Server 2011 Standard (64-bits) wordt alleen ondersteund als Service Pack 1 voor Microsoft Windows Server 2008 R2 geïnstalleerd is.

- Windows MultiPoint Server 2011 (64-bits);
- 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;
- Windows Server 2022.

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

Voor informatie over de ondersteuning voor het besturingssysteem Microsoft Windows Server 2022 raadpleegt u de [Knowledge Base van de Technische Support](#).

## Terminalservers

Ondersteunde servertypes terminal:

- Microsoft Remote Desktop Services gebaseerd op Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2012;
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2012 R2;
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2016;
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2019;

## Virtuele platforms

Ondersteunde virtuele platforms:

- VMware Workstation 16.2.2 Pro;
- VMware ESXi 7.0 Update 3b;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2112;
- Citrix Provisioning 2112;
- Citrix Hypervisor 8.2.

Kaspersky Endpoint Security ondersteunt werking met de volgende versies van Kaspersky Security Center:

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

## Vergelijking van beschikbare programmafuncties naargelang het type besturingssysteem

Welke functies van Kaspersky Endpoint Security beschikbaar zijn, hangt af van het type besturingssysteem: werkstation of server (zie onderstaande tabel).

Vergelijking van Kaspersky Endpoint Security-functies

| Functie                            | Werkstation | Server |
|------------------------------------|-------------|--------|
| <b>Advanced Threat Protection</b>  |             |        |
| Kaspersky Security Network         | ✓           | ✓      |
| Gedragsdetectie                    | ✓           | ✓      |
| Exploit-preventie                  | ✓           | ✓      |
| Host Intrusion Prevention          | ✓           | –      |
| Remediation Engine                 | ✓           | ✓      |
| <b>Essential Threat Protection</b> |             |        |
| File Threat Protection             | ✓           | ✓      |
| Web Threat Protection              | ✓           | ✓      |

|   |   |   |
|---|---|---|
| Mail Threat Protection                  | ✓ | ✓ |
| Firewall                                | ✓ | ✓ |
| Network Threat Protection               | ✓ | ✓ |
| BadUSB Attack Prevention                | ✓ | ✓ |
| AMSI-bescherming                        | ✓ | ✓ |
| <b>Security Controls</b>                |   |   |
| Programmacontrole                       | ✓ | ✓ |
| Apparaatcontrole                        | ✓ | ✓ |
| Webcontrole                             | ✓ | ✓ |
| Adaptieve controle op afwijkingen       | ✓ | – |
| <b>Gegevensencryptie</b>                |   |   |
| Kaspersky Disk Encryption               | ✓ | – |
| BitLocker-stationsversleuteling         | ✓ | ✓ |
| File Level Encryption                   | ✓ | – |
| Encryptie van verwisselbare schijven    | ✓ | – |
| <b>Detection and Response</b>           |   |   |
| Endpoint Detection and Response Optimum | ✓ | ✓ |
| Endpoint Detection and Response Expert  | ✓ | ✓ |
| Kaspersky Sandbox                       | ✓ | ✓ |
| Managed Detection and Response (MDR)    | ✓ | ✓ |

## Vergelijking van programmafuncties naargelang de beheertools

De beschikbare functionaliteit in Kaspersky Endpoint Security hangt af van de beheertools (zie onderstaande tabel).

U kunt het programma beheren met de volgende consoles van Kaspersky Security Center:

- Beheerconsole. Microsoft Management Console (MMC)-module geïnstalleerd op het werkstation van de beheerder.
- Webconsole. Onderdeel van Kaspersky Security Center dat in Administration Server is geïnstalleerd. U kunt werken in de Webconsole via een browser op computers met toegang tot Administration Server.

U kunt het programma ook beheren met Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* is de cloudversie van Kaspersky Security Center. Dit betekent dat de Administration Server en andere onderdelen van Kaspersky Security Center worden geïnstalleerd in de cloudinfrastructuur van Kaspersky. Voor informatie over het beheer van het programma via de Cloudconsole van Kaspersky Security Center raadpleegt u de [Help van de Kaspersky Security Center Cloud Console](#).

Vergelijking van Kaspersky Endpoint Security-functies

| Functie | Kaspersky Security Center | Kaspersky Security Center |
|---------|---------------------------|---------------------------|
|---------|---------------------------|---------------------------|



|   | Beheerconsole | Webconsole | Cloudconsole |
|---|---------------|------------|--------------|
| <b>Advanced Threat Protection</b>       |               |            |              |
| Kaspersky Security Network              | ✓             | ✓          | ✓            |
| Kaspersky Private Security Network      | ✓             | ✓          | –            |
| Gedragdetectie                          | ✓             | ✓          | ✓            |
| Exploit-preventie                       | ✓             | ✓          | ✓            |
| Host Intrusion Prevention               | ✓             | ✓          | ✓            |
| Remediation Engine                      | ✓             | ✓          | ✓            |
| <b>Essential Threat Protection</b>      |               |            |              |
| File Threat Protection                  | ✓             | ✓          | ✓            |
| Web Threat Protection                   | ✓             | ✓          | ✓            |
| Mail Threat Protection                  | ✓             | ✓          | ✓            |
| Firewall                                | ✓             | ✓          | ✓            |
| Network Threat Protection               | ✓             | ✓          | ✓            |
| BadUSB Attack Prevention                | ✓             | ✓          | ✓            |
| AMSI-bescherming                        | ✓             | ✓          | ✓            |
| <b>Security Controls</b>                |               |            |              |
| Programmacontrole                       | ✓             | ✓          | ✓            |
| Apparaatcontrole                        | ✓             | ✓          | ✓            |
| Webcontrole                             | ✓             | ✓          | ✓            |
| Adaptieve controle op afwijkingen       | ✓             | ✓          | ✓            |
| <b>Gegevensencryptie</b>                |               |            |              |
| Kaspersky Disk Encryption               | ✓             | ✓          | –            |
| BitLocker-stationsversleuteling         | ✓             | ✓          | ✓            |
| File Level Encryption                   | ✓             | ✓          | –            |
| Encryptie van verwisselbare schijven    | ✓             | ✓          | –            |
| <b>Detection and Response</b>           |               |            |              |
| Endpoint Detection and Response Optimum | –             | ✓          | ✓            |
| Endpoint Detection and Response Expert  | –             | –          | ✓            |
| Kaspersky Sandbox                       | –             | ✓          | –            |
| Managed Detection and Response (MDR)    | ✓             | ✓          | ✓            |
| <b>Taken</b>                            |               |            |              |
| Licentie toevoegen                      | ✓             | ✓          | ✓            |
| Programmaonderdelen wijzigen            | ✓             | ✓          | ✓            |
| Inventaris                              | ✓             | ✓          | ✓            |
| Update                                  | ✓             | ✓          | ✓            |

|   |   |   |   |
|---|---|---|---|
| Update terugdraaien   | ✓ | ✓ | ✓ |
| Virusscan   | ✓ | ✓ | ✓ |
| Integriteitscontrole  | ✓ | ✓ | – |
| Gegevens wissen   | ✓ | ✓ | ✓ |
| Accounts voor Authenticatie-agent beheren (Kaspersky Disk Encryption) | ✓ | ✓ | – |
| IOC-scan (EDR)  | – | ✓ | ✓ |
| Bestand in Quarantaine plaatsen (EDR)                                 | – | ✓ | ✓ |
| Bestand ophalen (EDR)   | – | ✓ | ✓ |
| Bestand verwijderen (EDR)   | – | ✓ | ✓ |
| Proces starten (EDR)  | – | ✓ | ✓ |
| Proces beëindigen (EDR)   | – | ✓ | ✓ |

## Compatibiliteit met andere programma's

Alvorens de installatie begint, controleert Kaspersky Endpoint Security of er andere Kaspersky-programma's op de computer zijn geïnstalleerd. Het programma controleert ook de computer op incompatibele software. De lijst met incompatibele software vindt u in het bestand incompatible.txt in het [distributiepakket](#).



[DOWNLOAD HET BESTAND SETUP.INI](#)

Kaspersky Endpoint Security is niet compatibel met de volgende Kaspersky-programma's:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (inclusief het Endpoint Sensor-onderdeel).
- Kaspersky Sandbox (inclusief Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (inclusief het Endpoint Sensor-onderdeel).

Als het Endpoint Agent-onderdeel op een computer is geïnstalleerd met behulp van de implementatietools van andere Kaspersky-programma's, wordt het onderdeel automatisch verwijderd tijdens de installatie van Kaspersky Endpoint Security. Kaspersky Endpoint Security kan ook het onderdeel Endpoint Sensor/Kaspersky Endpoint Agent bevatten als u Endpoint Agent hebt geselecteerd in de lijst met programmaonderdelen.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server.
- Kaspersky Embedded Systems Security.

Als Kaspersky-programma's uit deze lijst zijn geïnstalleerd op de computer, verwijdert Kaspersky Endpoint Security deze programma's. Wacht tot de verwijdering is voltooid voordat u met de installatie van Kaspersky Endpoint Security doorgaat.

# Het programma installeren en verwijderen

U kunt Kaspersky Endpoint Security op een computer installeren op de volgende manieren:

- lokaal, met behulp van de [Installatiewizard](#).
- lokaal, via de [opdrachtregel](#).
- op afstand via [Kaspersky Security Center](#).
- op afstand via de Editor voor groepsbeleidsbeheer van Microsoft Windows (ga voor meer informatie naar de [website van de Technische ondersteuning van Microsoft](#) <sup>2</sup>).
- op afstand, met behulp van de [System Center Configuration Manager](#).

U kunt de instellingen voor de installatie van het programma configureren op verschillende manieren. Als u meerdere methoden voor de configuratie van instellingen tegelijk gebruikt, past Kaspersky Endpoint Security de instellingen met de hoogste prioriteit toe. Kaspersky Endpoint Security gebruikt de volgende volgorde van prioriteiten:

1. Instellingen uit het bestand [setup.ini](#).
2. Instellingen uit het bestand 'installer.ini'.
3. Instellingen die worden ontvangen vanaf de [opdrachtregel](#).

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

## Implementatie via Kaspersky Security Center

Kaspersky Endpoint Security kan op verschillende manieren worden geïmplementeerd op computers in een bedrijfsnetwerk. U kunt het meest geschikte implementatiescenario voor uw bedrijf kiezen of verschillende implementatiescenario's tegelijk combineren. Kaspersky Security Center ondersteunt de volgende voornaamste implementatiemethoden:

- Installeer het programma met de wizard Bescherming implementeren.  
De [standaard installatiemethode](#) is handig als u tevreden bent met de standaardinstellingen van Kaspersky Endpoint Security en uw bedrijf een eenvoudige infrastructuur heeft die geen speciale configuratie vereist.
- Installeer het programma met een taak voor een externe installatie.  
Met deze universele installatiemethode kunt u de instellingen van Kaspersky Endpoint Security configureren en taken voor externe installaties flexibel beheren. De installatie van Kaspersky Endpoint Security bestaat uit de volgende stappen:
  1. [Een installatiepakket maken](#).
  2. [Een taak voor een externe installatie maken](#).

Kaspersky Security Center ondersteunt ook andere methoden voor de installatie van Kaspersky Endpoint Security, zoals een implementatie in een image van een besturingssysteem. Voor informatie over andere implementatiemethoden raadpleegt u de [Help van Kaspersky Security Center](#).

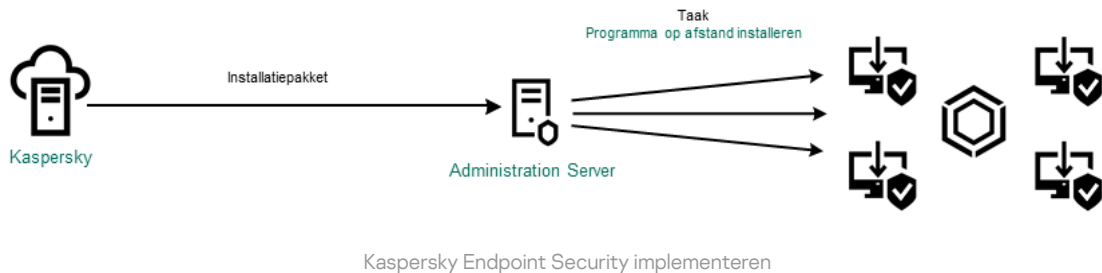
## Standaardinstallatie van het programma

Kaspersky Security Center beschikt over de wizard Bescherming implementeren die het programma op de computers van uw bedrijf installeert. De wizard Bescherming implementeren voert de volgende hoofdbewerkingen uit:

1. Een installatiepakket voor Kaspersky Endpoint Security selecteren.

Een *installatiepakket* is een reeks bestanden waarmee u een Kaspersky-programma op afstand kunt installeren via Kaspersky Security Center. Het installatiepakket bevat een aantal instellingen die vereist zijn om het programma te installeren en om het meteen na de installatie te starten. Het installatiepakket wordt gemaakt met KPD- en KUD-bestanden die bij het distributiepakket van het programma worden meegeleverd. Het installatiepakket van Kaspersky Endpoint Security werkt met alle ondersteunde Windows-versies en soorten processors.

2. De taak *Programma op afstand installeren* maken in de Administration Server van Kaspersky Security Center.



[De wizard Bescherming implementeren uitvoeren in de Beheerconsole \(MMC\)](#)

1. Ga in de Beheerconsole naar de map **Administration Server** → **Additional** → **Remote installation**.
2. Klik op de link **Installatiepakket implementeren op beheerde apparaten (werkstations)**.

Op deze manier start u de wizard Bescherming implementeren. Volg de instructies van de wizard.

TCP-poorten 139 en 445 en UDP-poorten 137 en 138 moeten worden geopend op een clientcomputer.

## Stap 1. Een installatiepakket selecteren

Selecteer het installatiepakket voor Kaspersky Endpoint Security in de lijst. Als u geen installatiepakket voor Kaspersky Endpoint Security in de lijst ziet, kunt u het pakket maken in de wizard.

U kunt de [instellingen van het installatiepakket](#) configureren in Kaspersky Security Center. Zo kunt u bijvoorbeeld de programmaonderdelen selecteren die op een computer moeten worden geïnstalleerd.

Netwerkagent wordt samen met Kaspersky Endpoint Security geïnstalleerd. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een clientcomputer. Als de netwerkagent al op de computer is geïnstalleerd, wordt deze niet opnieuw geïnstalleerd.

## Stap 2. Kiezen op welke apparaten de installatie moet worden uitgevoerd

Selecteer de computers waarop u Kaspersky Endpoint Security wilt installeren. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De netwerkagent wordt niet geïnstalleerd op niet-toegewezen apparaten. In dit geval wordt de taak toegewezen aan specifieke apparaten. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 3: Instellingen voor installatietaken op afstand definiëren

Configureer de volgende aanvullende programma-instellingen:

- **Download van installatiepakket forceren.** Selecteer de installatiemethode voor het programma:
  - **Met behulp van een netwerkagent.** Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
  - **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten.** Met tools van besturingssysteem wordt het installatiepakket aan clientcomputers geleverd via distributiepunten. U

kunt deze optie selecteren als het netwerk ten minste één distributiepunt heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).

- **Met tools van het besturingssysteem via Administration Server.** Met tools van het besturingssysteem worden bestanden aan clientcomputers geleverd via Administration Server. U kunt deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.
- **Gedrag voor apparaten beheerd door andere Administration Servers.** Selecteer de installatiemethode voor Kaspersky Endpoint Security. Als in het netwerk meer dan één Administration Server is geïnstalleerd, kunnen deze Administration Servers dezelfde clientcomputers zien. Dit kan er bijvoorbeeld voor zorgen dat verschillende Administration Servers een programma meer dan één keer op afstand installeren op dezelfde clientcomputer, of andere conflicten.
- **Installeer het programma niet opnieuw als het al geïnstalleerd is.** Schakel dit selectievakje uit als u bijvoorbeeld een oudere versie van het programma wilt installeren.
- **Wijs de installatie van Netwerkagent in een Active Directory-groepsbeleid toe.** Netwerkagent handmatig installeren met behulp van Active Directory-bronnen. Voor de installatie van een netwerkagent moet de taak voor de externe installatie worden uitgevoerd met de bevoegdheden van de domeinbeheerder.

#### Stap 4: Een licentiesleutel selecteren

Voeg een licentie toe aan het installatiepakket toe waarmee u het programma wilt activeren. Deze stap is optioneel. Als de Administration Server een licentie met automatische distributiefunctie heeft, wordt de licentie later automatisch toegevoegd. U kunt ook later [het programma activeren](#) met de taak *Licentie toevoegen*.

#### Stap 5: De instelling voor herstart van het besturingssysteem selecteren

Selecteer de actie die moet worden uitgevoerd als de computer opnieuw moet worden opgestart. 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.

#### Stap 6: Incompatibele programma's verwijderen voordat u het programma installeert

Neem de lijst met incompatibele programma's zorgvuldig door en sta de verwijdering van deze programma's toe. Als incompatibele programma's op de computer zijn geïnstalleerd, eindigt de installatie van Kaspersky Endpoint Security met een fout.

#### Stap 7. Een account voor toegang tot apparaten selecteren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security installeert met de tools van de netwerkagent, hoeft u geen account te selecteren.

#### Stap 8. De installatie starten

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

[De Wizard Bescherming implementeren starten in de Webconsole en Cloudconsole](#) 



Selecteer in het hoofdvenster van de webconsole **Discovery & Deployment** → **DEPLOYMENT & ASSIGNMENT** → **Protection Deployment Wizard**.

Op deze manier start u de wizard Bescherming implementeren. Volg de instructies van de wizard.

TCP-poorten 139 en 445 en UDP-poorten 137 en 138 moeten worden geopend op een clientcomputer.

## Stap 1. Een installatiepakket selecteren

Selecteer het installatiepakket voor Kaspersky Endpoint Security in de lijst. Als u geen installatiepakket voor Kaspersky Endpoint Security in de lijst ziet, kunt u het pakket maken in de wizard. Voor het maken van het installatiepakket hoeft u het distributiepakket niet te zoeken en op de computer op te slaan. In Kaspersky Security Center kunt u de lijst met distributiepakketten op Kaspersky-servers zien. Het installatiepakket wordt automatisch gemaakt. Kaspersky updatet de lijst na de release van nieuwe versies van programma's.

U kunt de [instellingen van het installatiepakket](#) configureren in Kaspersky Security Center. Zo kunt u bijvoorbeeld de programmaonderdelen selecteren die op een computer moeten worden geïnstalleerd.

## Stap 2: Een licentiesleutel selecteren

Voeg een licentie toe aan het installatiepakket toe waarmee u het programma wilt activeren. Deze stap is optioneel. Als de Administration Server een licentie met automatische distributiefunctie heeft, wordt de licentie later automatisch toegevoegd. U kunt ook later [het programma activeren](#) met de taak *Licentie toevoegen*.

## Stap 3. Een netwerkagent selecteren

Selecteer de versie van Netwerkagent die u samen met Kaspersky Endpoint Security wilt installeren. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een clientcomputer. Als de netwerkagent al op de computer is geïnstalleerd, wordt deze niet opnieuw geïnstalleerd.

## Stap 4. Kiezen op welke apparaten de installatie moet worden uitgevoerd

Selecteer de computers waarop u Kaspersky Endpoint Security wilt installeren. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De netwerkagent wordt niet geïnstalleerd op niet-toegewezen apparaten. In dit geval wordt de taak toegewezen aan specifieke apparaten. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 5. Geavanceerde instellingen configureren

Configureer de volgende aanvullende programma-instellingen:

- **Download van installatiepakket forceren.** Selecteer de installatiemethode voor het programma:
  - **Met behulp van een netwerkagent.** Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
  - **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten.** Met tools van besturingssysteem wordt het installatiepakket aan clientcomputers geleverd via distributiepunten. U kunt deze optie selecteren als het netwerk ten minste één distributiepunt heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).
  - **Met tools van het besturingssysteem via Administration Server.** Met tools van het besturingssysteem worden bestanden aan clientcomputers geleverd via Administration Server. U kunt deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.
- **Installeer het programma niet opnieuw als het al geïnstalleerd is.** Schakel dit selectievakje uit als u bijvoorbeeld een oudere versie van het programma wilt installeren.
- **Wijs de installatie van het pakket in een Active Directory-groepsbeleid toe.** Kaspersky Endpoint Security wordt geïnstalleerd met behulp van een netwerkagent of handmatig via Active Directory. Voor de installatie van een netwerkagent moet de taak voor de externe installatie worden uitgevoerd met de bevoegdheden van de domeinbeheerder.

## Stap 6: De instelling voor herstart van het besturingssysteem selecteren

Selecteer de actie die moet worden uitgevoerd als de computer opnieuw moet worden opgestart. 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.

## Stap 7: Incompatibele programma's verwijderen voordat u het programma installeert

Neem de lijst met incompatibele programma's zorgvuldig door en sta de verwijdering van deze programma's toe. Als incompatibele programma's op de computer zijn geïnstalleerd, eindigt de installatie van Kaspersky Endpoint Security met een fout.

## Stap 8. Toewijzen aan een beheergroep

Selecteer de beheergroep waarnaar de computers worden verplaatst nadat Networkagent is geïnstalleerd. Computers moeten naar een beheergroep worden verplaatst zodat [beleid](#) en [groepstaken](#) kunnen worden toegepast. Als een computer al een toegewezen beheergroep heeft, wordt de computer niet verplaatst. Als u geen beheergroep selecteert, worden de computers toegevoegd aan de groep **Niet-toegewezen apparaten**.

## Stap 9. Een account voor toegang tot apparaten selecteren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security installeert met de tools van de netwerkagent, hoeft u geen account te selecteren.

## Stap 10. Installatie starten

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

## Een installatiepakket maken

Een *installatiepakket* is een reeks bestanden waarmee u een Kaspersky-programma op afstand kunt installeren via Kaspersky Security Center. Het installatiepakket bevat een aantal instellingen die vereist zijn om het programma te installeren en om het meteen na de installatie te starten. Het installatiepakket wordt gemaakt met KPD- en KUD-bestanden die bij het distributiepakket van het programma worden meegeleverd. Het installatiepakket van Kaspersky Endpoint Security werkt met alle ondersteunde Windows-versies en soorten processors.

[Een installatiepakket maken in de Beheerconsole \(MMC\)](#) 

1. Ga in de Beheerconsole naar de map **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.

2. Klik op de knop **Installatiepakket maken**.

De wizard Nieuw pakket wordt gestart. Volg de instructies van de wizard.

### Stap 1. Het type installatiepakket selecteren

Selecteer de optie **Installatiepakket voor een Kaspersky-programma maken**.

### Stap 2. De naam van het installatiepakket definiëren

Voer de naam van het installatiepakket in, bijvoorbeeld *Kaspersky Endpoint Security voor Windows 11.9.0*.

### Stap 3: Het distributiepakket voor installatie selecteren

Klik op de knop **Bladeren** en selecteer het bestand `kes_win.kud` dat in het [distributiepakket](#) zit.

Werk indien nodig de antivirusdatabases in het installatiepakket bij met behulp van het selectievakje **Updates kopiëren van opslagplaats naar installatiepakket**.

### Stap 4: Gebruiksrechtovereenkomst en Privacybeleid

Lees en accepteer de voorwaarden van de Gebruiksrechtovereenkomst en het Privacybeleid.

Het installatiepakket wordt gemaakt en toegevoegd aan Kaspersky Security Center. Met het installatiepakket kunt u Kaspersky Endpoint Security installeren op computers in het bedrijfsnetwerk of de programmaversie updaten. In de instellingen van het installatiepakket kunt u de programmaonderdelen selecteren en de instellingen voor de installatie van het programma configureren (zie onderstaande tabel). Het installatiepakket bevat antivirusdatabases uit de Administration Server-opslagplaats. U kunt [de databases in het installatiepakket updaten](#) om minder verkeer te verbruiken wanneer u de databases wilt updaten nadat Kaspersky Endpoint Security is geïnstalleerd.

[Een installatiepakket maken in de Webconsole en Cloudconsole](#) 

1. Aselecteer in het hoofdvenster van de webconsole **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages**.

Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.

2. Klik op de knop **Add**.

De wizard Nieuw pakket wordt gestart. Volg de instructies van de wizard.

## Stap 1. Het type installatiepakket selecteren

Selecteer de optie **Installatiepakket voor een Kaspersky-programma maken**.

De wizard maakt een installatiepakket met behulp van het distributiepakket dat zich op de Kaspersky-servers bevindt. De lijst wordt automatisch geüpdatet wanneer nieuwe versies worden gereleased. U wordt aanbevolen deze optie voor de installatie van Kaspersky Endpoint Security te selecteren.

U kunt ook een installatiepakket met behulp van een bestand maken.

## Stap 2. Installatiepakketten

Selecteer het installatiepakket voor Kaspersky Endpoint Security voor Windows. De aanmaak van het installatiepakket wordt gestart. Tijdens het maken van het installatiepakket moet u de voorwaarden van de Gebruiksrechtovereenkomst en het Privacybeleid accepteren.

Het installatiepakket wordt gemaakt en toegevoegd aan Kaspersky Security Center. Met het installatiepakket kunt u Kaspersky Endpoint Security installeren op computers in het bedrijfsnetwerk of de programmaversie updaten. In de instellingen van het installatiepakket kunt u de programmaonderdelen selecteren en de instellingen voor de installatie van het programma configureren (zie onderstaande tabel). Het installatiepakket bevat antivirusdatabases uit de Administration Server-opslagplaats. U kunt [de databases in het installatiepakket updaten](#) om minder verkeer te verbruiken wanneer u de databases wilt updaten nadat Kaspersky Endpoint Security is geïnstalleerd.

Instellingen van het installatiepakket

| Gedeelte                     | Beschrijving  |
|------------------------------|---|
| <b>Protection components</b> | <p>In dit gedeelte kunt u selecteren welke programmaonderdelen beschikbaar zullen zijn. U kunt later <a href="#">de selectie van programmaonderdelen wijzigen</a> met de taak <i>Programmaonderdelen wijzigen</i>. De onderdelen BadUSB Attack Prevention, Detection and Response en gegevensversleutelingsonderdelen worden standaard niet geïnstalleerd. Deze onderdelen kunnen in de instellingen van het installatiepakket worden toegevoegd.</p> <p>Als u onderdelen voor detectie en reactie moet installeren, ondersteunt Kaspersky Endpoint Security de volgende configuraties:</p> <ul style="list-style-type: none"><li>• Alleen Endpoint Detection and Response Optimum</li><li>• Alleen Endpoint Detection and Response Expert</li><li>• Alleen Kaspersky Sandbox</li><li>• Endpoint Detection and Response Optimum en Kaspersky Sandbox</li><li>• Endpoint Detection and Response Expert en Kaspersky Sandbox.</li></ul> |

|                                  |  |
|----------------------------------|--|
|                                  | Kaspersky Endpoint Security controleert de selectie van componenten alvorens de toepassing te installeren. Als de geselecteerde configuratie van Detection and Response-onderdelen niet wordt ondersteund kan Kaspersky Endpoint Security niet geïnstalleerd worden.   |
| <b>Licentiecode</b>              | In deze sectie kunt u het programma activeren. Om het programma te activeren, moet u een licentiecode selecteren. Voordat u dat doet, moet u de code toevoegen aan de Administration Server. Voor meer informatie over het toevoegen van codes aan de Administration Server van Kaspersky Security Center raadpleegt u de <a href="#">Help van Kaspersky Security Center</a> .   |
| <b>Incompatibele programma's</b> | Neem de lijst met incompatibele programma's zorgvuldig door en sta de verwijdering van deze programma's toe. Als incompatibele programma's op de computer zijn geïnstalleerd, eindigt de installatie van Kaspersky Endpoint Security met een fout.   |
| <b>Installation settings</b>     | <p><b>Add application location to environment variable %PATH%.</b> U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de <a href="#">opdrachtregel-interface</a> eenvoudig te gebruiken.</p> <p><b>Do not protect the installation process.</b> De bescherming van de installatie voorkomt de vervanging van het distributiepakket door schadelijke programma's, 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.</p> <p><b>Ensure compatibility with Citrix PVS (this is only necessary when working with Citrix PVS).</b> U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.</p> <p><b>Path to application installation folder.</b> U kunt het pad voor de installatie van Kaspersky Endpoint Security op een clientcomputer wijzigen. Standaard wordt het programma geïnstalleerd in de map %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.</p> <p><b>Configuration file.</b> U kunt een bestand uploaden dat de instellingen van Kaspersky Endpoint Security definieert. U kunt <a href="#">een configuratiebestand in de lokale interface van het programma maken</a>.</p> |

## Databases in het installatiepakket updaten

Het installatiepakket bevat antivirusdatabases uit de Administration Server-opslagplaats die up-to-date zijn wanneer het installatiepakket wordt gemaakt. Nadat het installatiepakket is gemaakt, kunt u de antivirusdatabases in het installatiepakket updaten. Zo verbruikt u minder verkeer wanneer u de antivirusdatabases updatet nadat u Kaspersky Endpoint Security hebt geïnstalleerd.

Voor het updaten van de antivirusdatabases in de Administration Server-opslagplaats gebruikt u de taak *Updates downloaden naar de Administration Server-opslagplaats* van de Administration Server. Voor meer informatie over het updaten van de antivirusdatabases in het Administration Server-archief raadpleegt u de [Help van Kaspersky Security Center](#).

U kunt de databases in het installatiepakket alleen updaten in de Beheerconsole en Webconsole van Kaspersky Security Center. Het is niet mogelijk om de databases in het installatiepakket te updaten in Kaspersky Security Center Cloud Console.

[De antivirusdatabases in het installatiepakket bijwerken via de Beheerconsole \(MMC\)](#)

1. Ga in de Beheerconsole naar de map **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.

2. Open de eigenschappen van het installatiepakket.
3. Klik in het gedeelte **Algemeen** op de knop **Databases updaten**.

De antivirusdatabases in het installatiepakket worden nu geüpdatet via de Administration Server-opslagplaats. Het bestand `bases . cab` in het [distributiepakket](#) wordt vervangen door de map `bases .` De bestanden van het updatepakket zullen zich in de map bevinden.

### [Antivirusdatabases in een installatiepakket updaten via de Webconsole](#)

1. Aselecteer in het hoofdvenster van de webconsole **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages**.

U ziet nu een lijst met installatiepakketten die naar Webconsole zijn gedownload.

2. Klik op de naam van het Kaspersky Endpoint Security-installatiepakket waarvan u de antivirusdatabases wilt updaten.

U ziet nu het venster met eigenschappen van het installatiepakket.

3. Klik op het tabblad **Algemene informatie** op de koppeling **Databases updaten**.

De antivirusdatabases in het installatiepakket worden nu geüpdatet via de Administration Server-opslagplaats. Het bestand `bases . cab` in het [distributiepakket](#) wordt vervangen door de map `bases .` De bestanden van het updatepakket zullen zich in de map bevinden.

## Een taak voor een externe installatie maken

De taak *Programma op afstand installeren* is bedoeld om Kaspersky Endpoint Security op afstand te installeren. Met de taak *Programma op afstand installeren* kunt u het [installatiepakket van het programma](#) op alle computers in de organisatie implementeren. Voordat u het installatiepakket implementeert, kunt u [de antivirusdatabases in het pakket bijwerken](#) en de beschikbare programmaonderdelen selecteren in de eigenschappen van het installatiepakket.

### [Een taak voor installatie op afstand maken in de Beheerconsole \(MMC\)](#)

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Security Center Administration Server** → **Programma op afstand installeren**.

## Stap 2. Een installatiepakket selecteren

Selecteer het installatiepakket voor Kaspersky Endpoint Security in de lijst. Als u geen installatiepakket voor Kaspersky Endpoint Security in de lijst ziet, kunt u het pakket maken in de wizard.

U kunt de [instellingen van het installatiepakket](#) configureren in Kaspersky Security Center. Zo kunt u bijvoorbeeld de programmaonderdelen selecteren die op een computer moeten worden geïnstalleerd.

Netwerkagent wordt samen met Kaspersky Endpoint Security geïnstalleerd. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een clientcomputer. Als de netwerkagent al op de computer is geïnstalleerd, wordt deze niet opnieuw geïnstalleerd.

## Stap 3. Extra

Selecteer het installatiepakket voor de netwerkagent. De geselecteerde versie van Netwerkagent wordt samen met Kaspersky Endpoint Security geïnstalleerd.

## Stap 4. Instellingen

Configureer de volgende aanvullende programma-instellingen:

- **Download van installatiepakket forceren.** Selecteer de installatiemethode voor het programma:
  - **Met behulp van een netwerkagent.** Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
  - **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten.** Met tools van besturingssysteem wordt het installatiepakket aan clientcomputers geleverd via distributiepunten. U kunt deze optie selecteren als het netwerk ten minste één distributiepunt heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).
  - **Met tools van het besturingssysteem via Administration Server.** Met tools van het besturingssysteem worden bestanden aan clientcomputers geleverd via Administration Server. U kunt deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.
- **Gedrag voor apparaten beheerd door andere Administration Servers.** Selecteer de installatiemethode voor Kaspersky Endpoint Security. Als in het netwerk meer dan één Administration Server is geïnstalleerd,



kunnen deze Administration Servers dezelfde clientcomputers zien. Dit kan er bijvoorbeeld voor zorgen dat verschillende Administration Servers een programma meer dan één keer op afstand installeren op dezelfde clientcomputer, of andere conflicten.

- **Installeer het programma niet opnieuw als het al geïnstalleerd is.** Schakel dit selectievakje uit als u bijvoorbeeld een oudere versie van het programma wilt installeren.

## Stap 5: De instelling voor herstart van het besturingssysteem selecteren

Selecteer de actie die moet worden uitgevoerd als de computer opnieuw moet worden opgestart. 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.

## Stap 6: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop u Kaspersky Endpoint Security wilt installeren. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De netwerkagent wordt niet geïnstalleerd op niet-toegewezen apparaten. In dit geval wordt de taak toegewezen aan specifieke apparaten. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 7: Het account selecteren om de taak uit te voeren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security installeert met de tools van de netwerkagent, hoeft u geen account te selecteren.



## Stap 8. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of wanneer de computer niet actief is.

## Stap 9. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Kaspersky Endpoint Security voor Windows 11.9.0 installeren*.

## Stap 10. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. Het programma wordt in de stille modus geïnstalleerd. Na de installatie wordt het pictogram  toegevoegd aan het systeemvak van de computer van de gebruiker. Als u het pictogram  ziet, controleert u of u [het pictogram hebt geactiveerd](#).

[Een taak voor installatie op afstand maken in de Webconsole en de Cloudconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Programma** de optie **Kaspersky Security Center**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Programma op afstand installeren**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Installatie van Kaspersky Endpoint Security voor managers*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

## Stap 2. Kiezen op welke computers de installatie moet worden uitgevoerd

Selecteer tijdens deze stap de computers waarop u Kaspersky Endpoint Security wilt installeren volgens de geselecteerde optie voor het taakbereik.

## Stap 3. Een installatiepakket configureren

Configureer tijdens deze stap het installatiepakket:

1. Selecteer het installatiepakket voor Kaspersky Endpoint Security voor Windows (11.9.0).

2. Selecteer het installatiepakket voor de netwerkagent.

De geselecteerde versie van Netwerkagent wordt samen met Kaspersky Endpoint Security geïnstalleerd. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een clientcomputer. Als de netwerkagent al op de computer is geïnstalleerd, wordt deze niet opnieuw geïnstalleerd.

3. Selecteer in het blok **Download van installatiepakket forceren** de installatiemethode voor het programma:

- **Met behulp van een netwerkagent.** Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
- **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten.** Met tools van besturingssysteem wordt het installatiepakket aan clientcomputers geleverd via distributiepunten. U kunt deze optie selecteren als het netwerk ten minste één distributiepunt heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).
- **Met tools van het besturingssysteem via Administration Server.** Met tools van het besturingssysteem worden bestanden aan clientcomputers geleverd via Administration Server. U kunt

deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.

4. Stel in het veld **Maximum aantal gelijktijdige downloads** een limiet in voor het aantal verzoeken voor de download van het installatiepakket dat naar Administration Server wordt verstuurd. Een limiet voor het aantal verzoeken helpt te voorkomen dat het netwerk overbelast raakt.
5. Stel in het veld **Maximum aantal installatiepogingen** een limiet in voor het aantal pogingen dat mag worden gedaan om het programma te installeren. Als de installatie van Kaspersky Endpoint Security eindigt met een fout, start de taak automatisch de installatie weer.
6. Schakel indien nodig het selectievakje **Installeer het programma niet opnieuw als het al geïnstalleerd is** uit. Op deze manier kunt u bijvoorbeeld een oudere versie van het programma installeren.
7. Schakel indien nodig het selectievakje **Controleer het type besturingssysteem vóór de download** uit. Zo voorkomt u dat het distributiepakket voor het programma wordt gedownload als het besturingssysteem van de computer niet voldoet aan de softwarevereisten. Als u zeker weet dat het besturingssysteem van de computer voldoet aan de softwarevereisten, kunt u deze controle overslaan.
8. Schakel indien nodig het selectievakje **Wijs de installatie van het pakket in een Active Directory-groepsbeleid toe** in. Kaspersky Endpoint Security wordt geïnstalleerd met behulp van een netwerkagent of handmatig via Active Directory. Voor de installatie van een netwerkagent moet de taak voor de externe installatie worden uitgevoerd met de bevoegdheden van de domeinbeheerder.
9. Schakel indien nodig het selectievakje **Vraag gebruikers om actieve programma's te sluiten** in. Voor de installatie van Kaspersky Endpoint Security zijn heel wat computerbronnen vereist. Voor het gemak van de gebruiker wordt u door de wizard Programma installeren gevraagd om actieve programma's af te sluiten voordat u de installatie start. Op deze manier voorkomt u onderbrekingen in de werking van andere programma's en mogelijke fouten op de computer.
10. Selecteer in het blok **Gedrag voor apparaten beheerd door andere Administration Servers** de installatiemethode voor Kaspersky Endpoint Security. Als in het netwerk meer dan één Administration Server is geïnstalleerd, kunnen deze Administration Servers dezelfde clientcomputers zien. Dit kan er bijvoorbeeld voor zorgen dat verschillende Administration Servers een programma meer dan één keer op afstand installeren op dezelfde clientcomputer, of andere conflicten.

#### Stap 4: Het account selecteren om de taak uit te voeren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security installeert met de tools van de netwerkagent, hoeft u geen account te selecteren.

#### Stap 5. Aanmaak van de taak voltooien

Voltooi de wizard door op de knop **Finish** te klikken. U ziet een nieuwe taak in de lijst met taken. Start een taak door het selectievakje naast de taak in te schakelen en op de knop **Starten** te klikken. Het programma wordt in de stille modus geïnstalleerd. Na de installatie wordt het pictogram  toegevoegd aan het systeemvak van de computer van de gebruiker. Als u het pictogram  ziet, controleert u of u [het pictogram hebt geactiveerd](#).

De interface van de Installatiewizard van het programma bestaat uit een reeks vensters die de installatiestappen van het programma voorstellen.

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

1. Kopieer de [distributiekits](#)map naar de computer van de gebruiker.
2. Voer setup\_ks.exe uit.

De Installatiewizard wordt gestart.

## Installatie voorbereiden

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

- Aanwezigheid van geïnstalleerde incompatibele software (de lijst met incompatibele software vindt u in het bestand 'incompatible.txt' in het [distributiepakket](#)).
- 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 activeringsgegevens en programma-instellingen) behouden en gebruikt tijdens de installatie van Kaspersky Endpoint Security 11.9.0 voor Windows. De vorige versie van het programma wordt automatisch verwijderd. Dit is van toepassing op de volgende programmaversies:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 voor Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 voor Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 voor Windows (build 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 voor Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 voor Windows CF1 (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 voor Windows (build 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 voor Windows (build 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 voor Windows (build 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 voor Windows (build 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 voor Windows (build 11.7.0.669).

- Kaspersky Endpoint Security 11.8.0 voor Windows (build 11.8.0.384).

## Kaspersky Endpoint Security-onderdelen

Tijdens de installatie kunt u de onderdelen van Kaspersky Endpoint Security selecteren die u wilt installeren. De installatie van het onderdeel File Threat Protection is verplicht. U kunt de installatie ervan niet annuleren.

Standaard zijn alle programmaonderdelen voor installatie geselecteerd behalve de volgende:

- [BadUSB Attack Prevention](#).
- [Onderdelen voor gegevensencryptie](#).
- Detection and Response-onderdelen.

U kunt [de beschikbare programmaonderdelen wijzigen nadat het programma geïnstalleerd is](#). Om dit te doen, moet u de installatiewizard opnieuw uitvoeren en ervoor kiezen om de beschikbare componenten te wijzigen.

Als u onderdelen voor detectie en reactie moet installeren, ondersteunt Kaspersky Endpoint Security de volgende configuraties:

- Alleen Endpoint Detection and Response Optimum
- Alleen Endpoint Detection and Response Expert
- Alleen Kaspersky Sandbox
- Endpoint Detection and Response Optimum en Kaspersky Sandbox
- Endpoint Detection and Response Expert en Kaspersky Sandbox.

Kaspersky Endpoint Security controleert de selectie van componenten alvorens de toepassing te installeren. Als de geselecteerde configuratie van Detection and Response-onderdelen niet wordt ondersteund kan Kaspersky Endpoint Security niet geïnstalleerd worden.

## Geavanceerde instellingen

**Bescherm het installatieproces van het programma.** De bescherming van de installatie voorkomt de vervanging van het distributiekpakket door schadelijke programma's, 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.

**Ensure compatibility with Citrix PVS (this is only necessary when working with Citrix PVS).** U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.

**Add application location to environment variable %PATH%.** U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de [opdrachregel-interface](#) eenvoudig te gebruiken.

## Het programma op afstand installeren via System Center Configuration Manager

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

1. Open de console Configuratiebeheer.
  2. Selecteer in het blok **App management** rechts in de console de optie **Packages**.
  3. Klik boven in de console van het configuratiescherm op de knop **Create package**.  
Hiermee start u de *New Package and Application Wizard*.
  4. In de wizard Nieuw pakket en programma:
    - a. In het gedeelte **Package**:
      - Voer in het veld **Name** de naam van het installatiepakket in.
      - Geef in het veld **Source folder** het pad op naar de map met het distributiepakket van Kaspersky Endpoint Security.
    - b. Selecteer in het gedeelte **Application type** de optie **Standard program**.
    - c. In het gedeelte **Standard program**:
      - Voer in het veld **Name** de unieke naam voor het installatiepakket in (bijvoorbeeld de naam van het programma met de versie).
      - Geef in het veld **Command line** de installatieopties van Kaspersky Endpoint Security op vanaf de opdrachtregel.
      - Klik op de knop **Browse** om het pad naar het uitvoerbare bestand van het programma op te geven.
      - Zorg ervoor dat in de lijst **Run mode** de optie **Run with administrative rights** is ingeschakeld.
    - d. In het gedeelte **Requirements**:
      - Schakel het selectievakje **Run another program first** in als u een ander programma wilt starten voordat u Kaspersky Endpoint Security installeert.  
Selecteer het programma in de vervolgkeuzelijst **Application** of geef het pad naar het uitvoerbare bestand van dit programma op door te klikken op de knop **Browse**.
      - Selecteer de optie **This program can run only on specified platforms** in het blok **Platform requirements** 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 **Summary** alle ingevoerde waarden van de instellingen en klik op **Next**.

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

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

Hiermee start u de *Deployment Wizard*.

6. In de wizard Implementatie:

a. In het gedeelte **General**:

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

b. Voeg in het gedeelte **Contains** 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 **Summary** alle ingevoerde waarden van de instellingen en klik op **Next**.

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 vanaf de opdrachtregel wordt geïnstalleerd of wanneer de Editor voor lokaal groepsbeleid van Microsoft Windows wordt gebruikt. 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.



[DOWNLOAD HET BESTAND SETUP.INI](#)

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

- **[Setup]** – algemene instellingen 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. File Threat Protection is een verplicht onderdeel en wordt op de computer geïnstalleerd ongeacht de geconfigureerde instellingen in dit gedeelte. Het onderdeel Managed Detection and Response ontbreekt ook in deze sectie. Om dit onderdeel te installeren, moet u [Beheerde detectie en respons activeren in de Kaspersky Security Center Console](#).
- **[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**.



| Gedeelte | Parameter       | Beschrijving   |
|----------|-----------------|--|
| [Setup]  | InstallDir      | Pad naar de installatiemap van het programma.  |
|          | ActivationCode  | Activeringscode van Kaspersky Endpoint Security.   |
|          | EULA=1          | <p>Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het <a href="#">distributiepakket van Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.</p> </div>  |
|          | PrivacyPolicy=1 | <p>Aanvaarding van het Privacybeleid. De tekst van het Privacybeleid wordt bij het <a href="#">distributiepakket van Kaspersky Endpoint Security</a> meegeleverd.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.</p> </div>   |
|          | KSN             | <p>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:</p> <ul style="list-style-type: none"> <li>• 1 – Aanvaarding van de deelname aan KSN.</li> <li>• 0 – Weigering van de deelname aan KSN (standaardwaarde).</li> </ul> <p>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.</p> |
|          | Login           | Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel <a href="#">Wachtwoordbeveiliging</a> ). De gebruikersnaam wordt samen met de parameters Password en PasswordArea ingesteld. De gebruikersnaam 'KLAdmin' wordt standaard gebruikt.  |
|          | Wachtwoord      | 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   | <p>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, vraagt Kaspersky Endpoint Security de accountgegevens van de gebruiker (de parameters Gebruikersnaam en Wachtwoord). Gebruik het teken ';' om meerdere waarden op te geven.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• SET – voor het wijzigen van de programma-instellingen.</li> <li>• EXIT – voor het afsluiten van het programma.</li> <li>• DISPROTECT – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken.</li> <li>• DISPOLICY – voor het uitschakelen van het Kaspersky Security Center-beleid.</li> <li>• UNINST – voor het verwijderen van het programma op de computer.</li> <li>• DISCTRL – voor het uitschakelen van de controleonderdelen.</li> <li>• REMOVELIC – voor het verwijderen van de licentie.</li> <li>• REPORTS – voor het bekijken van rapporten.</li> </ul> |
|  | SelfProtection | <p>Schakel het beschermingsmechanisme voor de installatie van het programma in of uit. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – Het beschermingsmechanisme voor de installatie van het programma is ingeschakeld (standaardwaarde).</li> <li>• 0 – Het beschermingsmechanisme voor de installatie van het programma is uitgeschakeld.</li> </ul> <p>De bescherming van de installatie voorkomt de vervanging van het distributiekpakket door schadelijke programma's, 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.</p>   |
|  | Reboot=1       | Computer automatisch opnieuw opstarten, indien nodig  |

|  |                |  |
|--|----------------|--|
|  |                | <p>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.</p> <p>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.</p>  |
|  | AddEnvironment | <p>Voeg het pad naar de uitvoerbare bestanden in de installatiemap van Kaspersky Endpoint Security toe aan de systeemvariabele %PATH%. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – De systeemvariabele %PATH% wordt toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden.</li> <li>• 0 – De systeemvariabele %PATH% wordt niet toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden.</li> </ul>  |
|  | AMPPL          | <p>Schakelt de bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie (Antimalware Protected Process Light) in of uit. Voor meer informatie over AM-PPL-technologie gaat u naar de <a href="#">website van Microsoft</a>.</p> <p>AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is ingeschakeld.</li> <li>• 0 – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is uitgeschakeld.</li> </ul> |
|  | SetupReg       | <p>Schakel het schrijven van registersleutels vanuit het bestand 'setup.reg' naar het register in. Waarde van de parameter SetupReg: setup.reg.</p>  |
|  | EnableTraces   | <p>Programmatracing inschakelen of uitschakelen. Nadat Kaspersky Endpoint Security is gestart, worden de tracebestanden opgeslagen in de map %ProgramData%/Kaspersky Lab\KES\Traces.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – tracing is ingeschakeld.</li> <li>• 0 – tracing is uitgeschakeld (standaardwaarde).</li> </ul>   |
|  |                |  |

|                     |  |   |
|---------------------|--|---|
| TracesLevel         |  | <p>Detailniveau van tracing. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• <b>100</b> (kritiek). Alleen berichten over onherstelbare fouten.</li> <li>• <b>200</b> (hoog). Berichten over alle fouten, inclusief onherstelbare fouten.</li> <li>• <b>300</b> (diagnostisch). Berichten over alle fouten, alsook waarschuwingen.</li> <li>• <b>400</b> (belangrijk). Alle foutberichten, waarschuwingen en aanvullende informatie.</li> <li>• <b>500</b> (normaal). Berichten over alle fouten en waarschuwingen, alsook gedetailleerde informatie over de werking van het programma in de normale modus (standaard).</li> <li>• <b>600</b> (laag). Alle berichten.</li> </ul> |
| RESTAPI             |  | <p>Het programma via de REST API beheren. Voor het beheer van het programma via de REST API moet u de gebruikersnaam opgeven (parameter RESTAPI_User).</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• <b>1</b> – Beheer via de REST API is toegestaan.</li> <li>• <b>0</b> – Beheer via de REST API is niet toegestaan (standaardwaarde).</li> </ul> <p>Voor het beheer van het programma via de REST API moet het beheer met beheersystemen toegestaan zijn. Hiervoor stelt u de parameter AdminKitConnector=1 in. Als u het programma via de REST API beheert, is het niet mogelijk om het programma via de beheersystemen van Kaspersky te beheren.</p>              |
| RESTAPI_User        |  | <p>Gebruikersnaam van het Windows-domeinaccount dat wordt gebruikt voor het beheer van het programma via de REST API. Alleen deze gebruiker kan het programma via de REST API beheren. Voer de gebruikersnaam in de structuur &lt;DOMEIN&gt;\&lt;Gebruikersnaam&gt; in (bijvoorbeeld, RESTAPI_User=BEDRIJF\Beheerder). U kunt slechts één gebruiker kiezen die met de REST API mag werken.</p> <p>Een gebruikersnaam toevoegen is een vereiste voor het beheer van het programma via de REST API.</p>   |
| RESTAPI_Port        |  | <p>Poort die wordt gebruikt voor het beheer van het programma via de REST API. Poort 6782 wordt standaard gebruikt.</p>   |
| RESTAPI_Certificate |  | <p>Certificaat voor de identificatie van verzoeken (bijvoorbeeld RESTAPI_Certificate=C:\cert.pem). Voor de beveiligde interactie tussen Kaspersky Endpoint Security en de REST-client moet de identificatie van verzoeken worden geconfigureerd.</p>  |

|              |                          |  |
|--------------|--------------------------|--|
|              |                          | Hiervoor moet u een certificaat installeren en vervolgens de payload van elk verzoek ondertekenen.   |
| [Components] | ALL                      | <p>Installatie van alle onderdelen. Als parameterwaarde 1 is opgegeven, worden alle onderdelen geïnstalleerd ongeacht de installatie-instellingen van individuele onderdelen.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Vanwege de manier waarop Detection and Response-oplossingen worden ondersteund, worden de onderdelen Endpoint Detection and Response Optimum en Kaspersky Sandbox op de computer geïnstalleerd. Het onderdeel Endpoint Detection and Response is niet compatibel met deze configuratie.</p> </div> |
|              | MailThreatProtection     | Mail Threat Protection.  |
|              | WebThreatProtection      | Web Threat Protection.   |
|              | AMSI                     | AMSI-bescherming.  |
|              | HostIntrusionPrevention  | Host Intrusion Prevention.   |
|              | BehaviorDetection        | Gedragsdetectie.   |
|              | ExploitPrevention        | Exploit-preventie.   |
|              | RemediationEngine        | Remediation Engine.  |
|              | Firewall                 | Firewall.  |
|              | NetworkThreatProtection  | Network Threat Protection.   |
|              | WebControl               | Webcontrole.   |
|              | DeviceControl            | Apparaatcontrole.  |
|              | ApplicationControl       | Programmacontrole.   |
|              | AdaptiveAnomaliesControl | Adaptieve controle op afwijkingen.   |
|              | FileEncryption           | File Level Encryption-bibliotheken.  |
|              | DiskEncryption           | Full Disk Encryption-bibliotheken.   |
|              | BadUSBAttackPrevention   | BadUSB Attack Prevention.  |
|              | EDR                      | <p>Endpoint Detection and Response Optimum (EDR Optimum).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Het onderdeel is niet compatibel met het onderdeel EDR Expert (EDRCloud).</p> </div>   |
|              | EDRCloud                 | <p>Endpoint Detection and Response Expert (EDR Expert).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Het onderdeel is niet compatibel met het onderdeel EDR Optimum (EDR).</p> </div>   |

|         |                   |   |
|---------|-------------------|---|
|         | SB                | Kaspersky Sandbox.  |
|         | AdminKitConnector | <p>Programmabeheer met beheersystemen. Kaspersky Security Center is bijvoorbeeld een beheersysteem. Naast de Kaspersky-beheersystemen kunt u ook oplossingen van andere leveranciers gebruiken. Kaspersky Endpoint Security heeft hiervoor een API.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – Programmabeheer met behulp van beheersystemen is toegestaan (standaardwaarde).</li> <li>• 0 – Programmabeheer is alleen via de lokale interface toegestaan.</li> </ul> |
| [Tasks] | ScanMyComputer    | <p>De taak Volledige Scan. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> <li>• 0 – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> </ul>   |
|         | ScanCritical      | <p>De taak Kritieke Gebiedenscan. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> <li>• 0 – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> </ul>  |
|         | Updater           | <p>Updatetaak. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> <li>• 0 – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.</li> </ul>   |

## Programmaonderdelen wijzigen

Tijdens de installatie van het programma kunt u de onderdelen selecteren die beschikbaar zullen zijn. U kunt op de volgende manieren wijzigen welke programmaonderdelen beschikbaar zullen zijn:

- Lokaal, met behulp van de Installatiewizard.

Programmaonderdelen worden verwijderd met de normale methode van een Windows-besturingssysteem: via het Configuratiescherm. Start de Installatiewizard en selecteer de optie voor het wijzigen van beschikbare programmaonderdelen. Volg de instructies op het scherm.

- Op afstand via Kaspersky Security Center.

Met de taak *Programmaonderdelen wijzigen* kunt u na de installatie van Kaspersky Endpoint Security de onderdelen van het programma wijzigen.

Houd rekening met het volgende wanneer u de programmaonderdelen wijzigt:

- Op computers met Windows Server kunt u niet [alle onderdelen van Kaspersky Endpoint Security installeren](#) (het onderdeel Adaptieve controle op afwijkingen is bijvoorbeeld niet beschikbaar).
- Als de harde schijven op de computer beveiligd zijn met [Full Disk Encryption \(FDE\)](#), kunt u het onderdeel Full Disk Encryption niet verwijderen. Voor de verwijdering van het onderdeel Full Disk Encryption decrypt u alle harde schijven van de computer.
- Als de computer [geëncrypte bestanden \(FLE\)](#) heeft of als de gebruiker [geëncrypte verwisselbare schijven \(FDE of FLE\)](#) gebruikt, is het na de verwijdering van de onderdelen voor gegevensencryptie niet mogelijk om toegang tot de bestanden en verwisselbare schijven te krijgen. U kunt weer toegang tot de bestanden en verwisselbare schijven krijgen door de onderdelen voor gegevensencryptie opnieuw te installeren.

[Programmaonderdelen toevoegen of verwijderen in de Beheerconsole \(MMC\)](#) 

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer Kaspersky Endpoint Security **voor Windows (11.9.0)** → **Programmaonderdelen wijzigen**.

## Stap 2: Taakinstellingen voor het wijzigen van programmaonderdelen

Selecteer de programmaonderdelen die beschikbaar zullen zijn op de computer van de gebruiker.

Selecteer het selectievakje **Incompatibele programma's van derden verwijderen**. De lijst met incompatibele programma's kan worden bekeken in het bestand `incompatible.txt`, dat deel uitmaakt van de [distributiekit](#). Als incompatibele programma's op de computer zijn geïnstalleerd, eindigt de installatie van Kaspersky Endpoint Security met een fout.

Schakel indien nodig de [wachtwoordbeveiliging](#) voor de taak in:

1. Klik op **Extra**.

2. Selecteer het selectievakje **Stel een wachtwoord in voor het wijzigen van de geïnstalleerde onderdelen**.

3. Voer de gegevens van het KAdmin-gebruikersaccount in.

## Stap 3: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 4. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of wanneer de computer niet actief is.

## Stap 5. Taaknaam definiëren



Voer een naam in voor de taak, bijvoorbeeld *Het onderdeel Programmacontrole toevoegen*.

## Stap 6. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Als gevolg hiervan wordt de set Kaspersky Endpoint Security-onderdelen op de computer van gebruikers gewijzigd in stille modus. De instellingen van beschikbare onderdelen worden in de lokale interface van het programma weergegeven. De onderdelen die werden meegeleverd bij het programma zijn uitgeschakeld en de instellingen van deze onderdelen zijn niet beschikbaar.

[Programmaonderdelen toevoegen of verwijderen in de Webconsole en Cloudconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Programmaonderdelen wijzigen**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Het onderdeel Programmacontrole toevoegen*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

## Stap 2: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. Selecteer bijvoorbeeld een aparte beheergroep of stel een selectie samen.

## Stap 3. Aanmaak van de taak voltooien

Schakel het selectievakje **Taakgegevens openen na aanmaak** in en voltooi de wizard. Selecteer in de taakeigenschappen het tabblad **Programma-instellingen** en selecteer de programmaonderdelen die beschikbaar zullen zijn.

Schakel indien nodig de [wachtwoordbeveiliging](#) voor de taak in:

1. Schakel in het blok **Advanced settings** het selectievakje **Use password for modifying the set of application components** in.

2. Voer de gegevens van het KLAdmin-gebruikersaccount in.

Sla de wijzigingen op en voer de taak uit.

Als gevolg hiervan wordt de set Kaspersky Endpoint Security-onderdelen op de computer van gebruikers gewijzigd in stille modus. De instellingen van beschikbare onderdelen worden in de lokale interface van het programma weergegeven. De onderdelen die werden meegeleverd bij het programma zijn uitgeschakeld en de instellingen van deze onderdelen zijn niet beschikbaar.

## Een upgrade voor een oude versie van het programma installeren

Wanneer u een oude versie van het programma wilt upgraden naar een nieuwe versie, moet u rekening houden met het volgende:

- We raden aan dat u alle actieve programma's afsluit voordat u met de installatie van de update begint.
- Als de computer harde schijven heeft die zijn geëncrypt met [Full Disk Encryption \(FDE\)](#), dan moet u alle geëncrypte harde schijven decrypten om Kaspersky Endpoint Security te upgraden van versie 10 naar versie 11.0.0 of hoger.

Kaspersky Endpoint Security blokkeert de Full Disk Encryption-functionaliteit voordat de update wordt gestart. Als Full Disk Encryption niet kan worden vergrendeld, zal de installatie van de upgrade niet starten. Na het updaten van het programma wordt de Full Disk Encryption-functionaliteit hersteld.

Kaspersky Endpoint Security ondersteunt updates voor de volgende versies van het programma:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 voor Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 voor Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 voor Windows (build 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 voor Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 voor Windows CF1 (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 voor Windows (build 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 voor Windows (build 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 voor Windows (build 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 voor Windows (build 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 voor Windows (build 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 voor Windows (build 11.8.0.384).

Wanneer u een upgrade uitvoert van Kaspersky Endpoint Security 10 Service Pack 2 voor Windows naar Kaspersky Endpoint Security 11.9.0 voor Windows, worden de bestanden die in Back-up of Quarantaine zijn geplaatst door de vorige versie van het programma overgezet naar Back-up in de nieuwe versie van het programma. Bij versies ouder dan Kaspersky Endpoint Security 10 Service Pack 2 voor Windows worden bestanden die in Back-up en Quarantaine zijn geplaatst in een oudere versie van het programma niet gemigreerd naar de nieuwere versie.

Kaspersky Endpoint Security kan op de volgende manieren worden geüpdatet op de computer:

- lokaal, met behulp van de [Installatiewizard](#).
- lokaal, via de [opdrachtregel](#).
- op afstand via [Kaspersky Security Center](#).
- op afstand via de Editor voor groepsbeleidsbeheer van Microsoft Windows (ga voor meer informatie naar de [website van de Technische ondersteuning van Microsoft](#)).

- op afstand, met behulp van de [System Center Configuration Manager](#).

Als het programma die in het bedrijfsnetwerk wordt ingezet een andere set componenten bevat dan de standaardset, is het updaten van het programma via de Administration Console (MMC) anders dan het updaten van het programma via de Web Console en Cloud Console. Houd rekening met het volgende wanneer u Kaspersky Endpoint Security bijwerkt:

- Webconsole van Kaspersky Security Center of Cloudconsole van Kaspersky Security Center.

Als u een installatiepakket hebt gemaakt voor de nieuwe versie van het programma met de standaardset componenten, dan wordt de set componenten op de computer van een gebruiker niet gewijzigd. Om Kaspersky Endpoint Security te gebruiken met de standaardset componenten, moet [u de eigenschappen van het installatiepakket openen](#), de set componenten wijzigen en vervolgens terugkeren naar de oorspronkelijke set componenten en de wijzigingen opslaan.

- Open de beheerconsole van Kaspersky Security Center.

De set applicatiecomponenten na de update komt overeen met de set componenten in het installatiepakket. Dat wil zeggen dat als de nieuwe versie van het programma de standaardset componenten heeft, dan wordt bijvoorbeeld BadUSB Attack Prevention van de computer verwijderd, aangezien deze component uitgesloten is van de standaardset. Om het programma te blijven gebruiken met dezelfde set componenten als vóór de update, selecteert u de vereiste componenten in de [installatiepakketinstellingen](#).

## Programma verwijderen

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

### Het programma op afstand verwijderen

U kunt het programma op afstand verwijderen met behulp van de taak *Programma op afstand verwijderen*. Tijdens de uitvoering van de taak zal Kaspersky Endpoint Security het hulpprogramma voor de verwijdering downloaden naar de computer van de gebruiker. Wanneer het programma volledig is verwijderd, wordt het hulpprogramma automatisch verwijderd.

[Het programma verwijderen via de Beheerconsole \(MMC\)](#) 

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Security Center Administration Server** → **Extra** → **Programma op afstand verwijderen**.

## Stap 2: Het programma selecteren dat moet worden verwijderd

Selecteer **Programma verwijderen dat wordt ondersteund door Kaspersky Security Center**.

## Stap 3: Taakinstellingen voor het verwijderen van programma's

Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)**.

## Stap 4. Verwijder hulpprogramma-instellingen

Configureer de volgende aanvullende programma-instellingen:

- **Download van hulpprogramma voor verwijdering forceren.** Selecteer de leveringsmethode voor het hulpprogramma:
  - **Met behulp van een netwerkagent.** Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens verwijderd met de tools van Netwerkagent.
  - **Met tools van het besturingssysteem via Administration Server.** Met behulp van de hulpprogramma's van het besturingssysteem zorgt Administration Server ervoor dat het hulpprogramma voor de verwijdering wordt geleverd aan clientcomputers. U kunt deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.
  - **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten.** Met behulp van de hulpprogramma's van het besturingssysteem wordt het hulpprogramma via distributiepunten geleverd aan clientcomputers geleverd. U kunt deze optie selecteren als het netwerk ten minste één distributiepunt heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).
- **Controleer het type besturingssysteem vóór de download.** Schakel indien nodig dit selectievakje uit. Zo voorkomt u dat het hulpprogramma voor de verwijdering wordt gedownload als het besturingssysteem van de computer niet voldoet aan de softwarevereisten. Als u zeker weet dat het besturingssysteem van de computer voldoet aan de softwarevereisten, kunt u deze controle overslaan.

Als het verwijderen van het programma met een [wachtwoord is beveiligd](#), doet u het volgende:

1. Schakel het selectievakje **Wachtwoord voor verwijdering gebruiken** in.

2. Klik op de knop **Bewerken**.

3. Voer het wachtwoord van het KAdmin-account in.

## Stap 5: De instelling voor herstart van het besturingssysteem selecteren

Na het verwijderen van het programma moet u de computer opnieuw opstarten. Selecteer de actie die wordt uitgevoerd om de computer opnieuw op te starten.

## Stap 6: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 7: Het account selecteren om de taak uit te voeren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security verwijdert met de hulpprogramma's van Netwerkagent, hoeft u geen account te selecteren.

## Stap 8. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of wanneer de computer niet actief is.

## Stap 9. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Kaspersky Endpoint Security 11.9.0 verwijderen*.

## Stap 10. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Het programma wordt in de stille modus verwijderd.

[Het programma verwijderen via de Webconsole en Cloudconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Programma** de optie **Kaspersky Security Center**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Programma op afstand verwijderen**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Kaspersky Endpoint Security verwijderen op computers van Technische Support*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

## Stap 2: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. Selecteer bijvoorbeeld een aparte beheergroep of stel een selectie samen.

## Stap 3. Instellingen voor de verwijdering van het programma configureren

Tijdens deze stap configureert u de instellingen voor de verwijdering van het programma:

1. Selecteer **Beheerd programma verwijderen**.

2. Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)**.

3. **Download van hulpprogramma voor verwijdering forceren**. Selecteer de leveringsmethode voor het hulpprogramma:

- **Met behulp van een netwerkagent**. Als geen netwerkagent is geïnstalleerd op de computer, wordt de eerste netwerkagent geïnstalleerd via de tools van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens verwijderd met de tools van Netwerkagent.
- **Met tools van het besturingssysteem via Administration Server**. Met behulp van de hulpprogramma's van het besturingssysteem zorgt Administration Server ervoor dat het hulpprogramma voor de verwijdering wordt geleverd aan clientcomputers. U kunt deze optie selecteren als geen netwerkagent is geïnstalleerd op de clientcomputer, maar de clientcomputer is verbonden met hetzelfde netwerk als Administration Server.
- **Met behulp van hulpprogramma's van het besturingssysteem via distributiepunten**. Met behulp van de hulpprogramma's van het besturingssysteem wordt het hulpprogramma via distributiepunten geleverd aan clientcomputers geleverd. U kunt deze optie selecteren als het netwerk ten minste één



distributiepoint heeft. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center](#).

4. Stel in het veld **Maximaal aantal gelijktijdige downloads** een limiet in voor het aantal verzoeken dat naar Administration Server wordt verstuurd om het hulpprogramma voor de verwijdering van het programma te downloaden. Een limiet voor het aantal verzoeken helpt te voorkomen dat het netwerk overbelast raakt.
5. Stel in het veld **Maximum aantal verwijderpogingen** een limiet in voor het aantal pogingen dat mag worden gedaan om het programma te verwijderen. Als de verwijdering van Kaspersky Endpoint Security eindigt met een fout, herstart de taak automatisch de verwijdering.
6. Schakel indien nodig het selectievakje **Controleer het type besturingssysteem vóór de download** uit. Zo voorkomt u dat het hulpprogramma voor de verwijdering wordt gedownload als het besturingssysteem van de computer niet voldoet aan de softwarevereisten. Als u zeker weet dat het besturingssysteem van de computer voldoet aan de softwarevereisten, kunt u deze controle overslaan.

#### Stap 4: Het account selecteren om de taak uit te voeren

Selecteer het account waarmee u de netwerkagent wilt installeren met behulp van de tools van het besturingssysteem. In dit geval zijn beheerdersrechten vereist voor toegang tot computers. U kunt meerdere accounts toevoegen. Als een account onvoldoende rechten heeft, gebruikt de installatiewizard het volgende account. Als u Kaspersky Endpoint Security verwijdert met de hulpprogramma's van Netwerkagent, hoeft u geen account te selecteren.

#### Stap 5. Aanmaak van de taak voltooien

Voltooi de wizard door op de knop **Finish** te klikken. U ziet een nieuwe taak in de lijst met taken.

Start een taak door het selectievakje naast de taak in te schakelen en op de knop **Starten** te klikken. Het programma wordt in de stille modus verwijderd. Wanneer de verwijdering is voltooid, toont Kaspersky Endpoint Security een bericht met de vraag om de computer opnieuw op te starten.

Als de verwijdering van het programma is [beveiligd met een wachtwoord](#), voert u het wachtwoord van het KLAdmin-account in de eigenschappen van de taak *Programma op afstand verwijderen* in. Zonder het wachtwoord wordt de taak niet uitgevoerd.

*Zo gebruikt u het wachtwoord van het KLAdmin-account met de taak 'Programma op afstand verwijderen':*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de Kaspersky Security Center-taak **Programma op afstand beheren**.

U ziet nu het venster met de taakeigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Schakel het selectievakje **Wachtwoord voor verwijdering gebruiken** in.

5. Voer het wachtwoord van het KLAdmin-account in.

6. Sla uw wijzigingen op.

U kunt het programma ook op afstand verwijderen via de Editor voor groepsbeleidsbeheer van Microsoft Windows (ga voor meer informatie naar de [website van de Technische ondersteuning van Microsoft](#) <sup>2</sup>).

## Het programma lokaal verwijderen

U kunt het programma lokaal verwijderen met de installatiewizard. Kaspersky Endpoint Security wordt verwijderd met de normale methode van een Windows-besturingssysteem: via het Configuratiescherm. De Installatiewizard wordt gestart. Volg de instructies op het scherm.

U kunt kiezen welke gegevens van het programma u wilt behouden voor later gebruik tijdens de volgende installatie van het programma (bijvoorbeeld wanneer u een upgrade naar een nieuwe versie van het programma uitvoert). Als u geen gegevens kiest, wordt het programma volledig verwijderd.

U kunt de volgende gegevens opslaan:

- **Activatiegegevens** waarmee u het programma niet opnieuw hoeft te activeren. Kaspersky Endpoint Security voegt automatisch een licentiebestand toe als de geldigheidsduur van de licentie nog niet ten einde is wanneer u het programma installeert.
- **Back-upbestanden** – bestanden die door het programma zijn gescand en in Back-up zijn geplaatst.

Bestanden van Back-up 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 te gebruiken, moet u die objecten terugzetten alvorens het programma te verwijderen. Kaspersky-experts raden wel aan dat u geen objecten uit Back-up terugzet omdat ze 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 toegang geven tot bestanden en schijven die vóór de verwijdering van het programma waren geëncrypt. Om de toegang tot geëncrypte bestanden en schijven te verzekeren, moet u ervoor zorgen dat u de functionaliteit voor gegevensencryptie selecteert wanneer u Kaspersky Endpoint Security opnieuw installeert. U hoeft verder niets te doen om toegang tot eerder geëncrypte bestanden en schijven te krijgen.

U kunt het programma ook lokaal verwijderen met de [opdrachtregel](#).

# Licentie van het programma activeren

In deze sectie vindt u algemene informatie over het licentiebeheer van Kaspersky Endpoint Security.

## 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 [softwarepakket van het programma](#) en vindt u ook in de installatiemap van het programma: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\\KES.

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.

De licentie geeft u het recht om het programma te gebruiken in overeenstemming met de voorwaarden van de Gebruiksrechtovereenkomst en om technische ondersteuning te ontvangen. De lijst met beschikbare functies en de gebruiksvoorwaarden van het programma zijn afhankelijk van het type licentie waaronder het geactiveerd is.

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.  
U kunt de toepassing onder een proeflicentie slechts één keer activeren.
- *Commerciële* – een betaalde licentie die u ontvangt wanneer u Kaspersky Endpoint Security aanschafft.  
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, worden de belangrijkste functies van het programma uitgeschakeld. Als u het programma wilt blijven gebruiken, moet u uw commerciële licentie verlengen. Als u niet van plan bent uw licentie te verlengen, moet u het programma van uw computer verwijderen.

## Over het licentiecertificaat

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

Het licentiecertificaat bevat de volgende licentie-informatie:

- Licentiecode of bestelnummer.
- Gegevens van de gebruiker aan wie de licentie is verleend.
- Gegevens van het programma dat met de licentie kan worden geactiveerd.
- Beperking van het aantal activeringen 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.
- Licentietype.

## Over het abonnement

Een *abonnement voor Kaspersky Endpoint Security* is een inkooporder voor het programma met specifieke parameters (zoals de verloopdatum van het abonnement en het 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 uw abonnement verlengen. Een abonnement met onbeperkte duur wordt automatisch verlengd als de diensten van de leverancier tijdig op voorhand zijn betaald.

Wanneer een abonnement met beperkte duur verloopt, krijgt u mogelijk een respijtperiode voor de verlenging van het abonnement. Tijdens die periode blijft het programma normaal werken. De beschikbaarheid en duur van zo'n respijtperiode wordt door de serviceprovider beslist.

Om Kaspersky Endpoint Security met een abonnement te gebruiken, moet u de [activatiecode](#) toepassen die u van de serviceprovider hebt gekregen. Nadat de activatiecode is toegepast, is de actieve licentie toegevoegd. De actieve licentie bepaalt de licentie voor het gebruik van het programma met een abonnement. U kunt het programma onder het abonnement niet activeren met een [licentiebestand](#). De serviceprovider kan alleen een activeringscode opgeven. Het is niet mogelijk om een reservelicentie toe te voegen als u een abonnement hebt.

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

## Over de licentiecode

Een *licentiesleutel* is een reeks bits die u kunt gebruiken om het programma te activeren en vervolgens te gebruiken in overeenstemming met de voorwaarden van de gebruiksrechtovereenkomst.

Bij een sleutel toegevoegd onder een abonnement wordt geen [Licentiecertificaat](#) geleverd.

U kunt een licentiesleutel aan het programma toevoegen door een sleutelbestand toe te passen of door een activeringscode in te voeren.

De code kan door Kaspersky worden geblokkeerd als de voorwaarden van de Gebruiksrechtovereenkomst worden geschonden. Als de sleutel geblokkeerd is, moet u een andere sleutel toevoegen om het programma verder te gebruiken.

Er zijn twee soorten licenties: actieve en reserve.

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

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

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

Als een sleutel wordt toegevoegd aan de lijst met verboden sleutels, blijft de toepassingsfunctionaliteit gedefinieerd door de [licentie gebruikt om het programma te activeren](#) acht dagen beschikbaar. Het programma stelt de gebruiker op de hoogte dat de sleutel is toegevoegd aan de lijst met verboden sleutels. Na acht dagen wordt de functionaliteit van het programma beperkt tot het functionaliteitsniveau dat beschikbaar is nadat de licentie is verlopen. U kunt beschermings- en controleonderdelen gebruiken en een scan 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.

## Over de activeringscode

Een *activeringscode* is een unieke reeks van 20 alfanumerieke tekens. U voert een activatiecode in om een licentiesleutel toe te voegen die Kaspersky Endpoint Security activeert. U ontvangt een activatiecode op het e-mailadres dat u heeft opgegeven na aankoop van Kaspersky Endpoint Security.

Als u het programma met een activeringscode wilt activeren, moet u verbonden zijn met internet om verbinding te maken met de activeringsservers van Kaspersky.

De actieve licentie wordt geïnstalleerd wanneer het programma met een activatiecode wordt geactiveerd. Een reservelicentie kan alleen worden toegevoegd met behulp van een activatiecode en kan niet worden toegevoegd met een licentiebestand.

Als een activeringscode na de activering van het programma verloren gaat, kunt u de activeringscode herstellen. Mogelijk hebt u een activeringscode nodig om bijvoorbeeld een [Kaspersky-bedrijfsaccount](#) te registreren. Als de activeringscode verloren is gegaan na de activering van het programma, neemt u contact op met de Kaspersky-partner bij wie u de licentie hebt gekocht.

## Over het licentiebestand

Een *licentiebestand* is een bestand met de extensie .key dat u krijgt van Kaspersky. Een licentiebestand dient om een licentie toe te voegen die het programma activeert.

U ontvangt een licentiebestand op het e-mailadres dat u heeft opgegeven toen u Kaspersky Endpoint Security kocht of de proefversie van Kaspersky Endpoint Security bestelde.

U hoeft geen verbinding te maken met de activeringsservers 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 verkoper van de licentie.
- Krijg op basis van uw bestaande activeringscode een licentiebestand op de [Kaspersky-website](#).

Een actieve sleutel wordt toegevoegd wanneer het programma met een licentiebestand wordt geactiveerd. Een reservelicentie kan alleen worden toegevoegd met behulp van een licentiebestand en kan niet worden toegevoegd met een activatiecode.

## Vergelijking van programmafunctionaliteit afhankelijk van licentietype voor werkstations

De functionaliteit van Kaspersky Endpoint Security op werkstations hangt af van het licentietype (zie onderstaande tabel).

[Bekijk ook de vergelijking van de programmafunctionaliteit voor servers](#)

Vergelijking van Kaspersky Endpoint Security-functies

| Functie                           | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Opt |
|-----------------------------------|---|---|--------------------------|---|---------------|
| <b>Advanced Threat Protection</b> |   |   |                          |   |               |
| Kaspersky Security Network        | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Gedragsdetectie                   | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Exploit-preventie                 | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Host Intrusion Prevention         | ✓   | ✓   | ✓                        | ✓   | ✓             |

|  |   |   |   |   |   |
|--|---|---|---|---|---|
| Remediation Engine   | ✓ | ✓ | ✓ | ✓ | ✓ |
| <b>Essential Threat Protection</b>   |   |   |   |   |   |
| File Threat Protection   | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web Threat Protection  | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mail Threat Protection   | ✓ | ✓ | ✓ | ✓ | ✓ |
| Firewall   | ✓ | ✓ | ✓ | ✓ | ✓ |
| Network Threat Protection  | ✓ | ✓ | ✓ | ✓ | ✓ |
| BadUSB Attack Prevention   | ✓ | ✓ | ✓ | ✓ | ✓ |
| AMSI-bescherming   | ✓ | ✓ | ✓ | ✓ | ✓ |
| <b>Security Controls</b>   |   |   |   |   |   |
| Programmacontrole  | ✓ | ✓ | ✓ | ✓ | ✓ |
| Apparaatcontrole   | ✓ | ✓ | ✓ | ✓ | ✓ |
| Webcontrole  | ✓ | ✓ | ✓ | ✓ | ✓ |
| Adaptieve controle op afwijkingen  | – | ✓ | ✓ | ✓ | ✓ |
| <b>Gegevensencryptie</b>   |   |   |   |   |   |
| Kaspersky Disk Encryption  | – | ✓ | ✓ | ✓ | ✓ |
| BitLocker-stationsversleuteling  | – | ✓ | ✓ | ✓ | ✓ |
| File Level Encryption  | – | ✓ | ✓ | ✓ | ✓ |
| Encryptie van verwisselbare schijven   | – | ✓ | ✓ | ✓ | ✓ |
| <b>Detection and Response</b>  |   |   |   |   |   |
| Endpoint Detection and Response Optimum  | – | – | – | ✓ | ✓ |
| Endpoint Detection and Response Expert   | – | – | – | – | – |
| Kaspersky Sandbox<br><i>(Kaspersky Sandbox-licentie moet afzonderlijk worden aangekocht)</i> | ✓ | ✓ | ✓ | ✓ | ✓ |

## Vergelijking van programmafunctionaliteit afhankelijk van licentietype voor servers

De functionaliteit van Kaspersky Endpoint Security op servers hangt af van het licentietype (zie onderstaande tabel).

[Bekijk ook de vergelijking van de programmafunctionaliteit voor werkstations](#)

| Functie                                 | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Opt |
|---|---|---|--------------------------|---|---------------|
| <b>Advanced Threat Protection</b>       |   |   |                          |   |               |
| Kaspersky Security Network              | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Gedragsdetectie                         | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Exploit-preventie                       | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Host Intrusion Prevention               | –   | –   | –                        | –   | –             |
| Remediation Engine                      | ✓   | ✓   | ✓                        | ✓   | ✓             |
| <b>Essential Threat Protection</b>      |   |   |                          |   |               |
| File Threat Protection                  | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Web Threat Protection                   | –   | ✓   | ✓                        | ✓   | ✓             |
| Mail Threat Protection                  | –   | ✓   | ✓                        | ✓   | ✓             |
| Firewall                                | ✓   | ✓   | ✓                        | ✓   | ✓             |
| Network Threat Protection               | ✓   | ✓   | ✓                        | ✓   | ✓             |
| BadUSB Attack Prevention                | ✓   | ✓   | ✓                        | ✓   | ✓             |
| AMSI-bescherming                        | ✓   | ✓   | ✓                        | ✓   | ✓             |
| <b>Security Controls</b>                |   |   |                          |   |               |
| Programmacontrole                       | –   | ✓   | ✓                        | ✓   | ✓             |
| Apparaatcontrole                        | –   | ✓   | ✓                        | ✓   | ✓             |
| Webcontrole                             | –   | ✓   | ✓                        | ✓   | ✓             |
| Adaptieve controle op afwijkingen       | –   | –   | –                        | –   | –             |
| <b>Gegevensencryptie</b>                |   |   |                          |   |               |
| Kaspersky Disk Encryption               | –   | –   | –                        | –   | –             |
| BitLocker-stationsversleuteling         | –   | ✓   | ✓                        | ✓   | ✓             |
| File Level Encryption                   | –   | –   | –                        | –   | –             |
| Encryptie van verwisselbare schijven    | –   | –   | –                        | –   | –             |
| <b>Detection and Response</b>           |   |   |                          |   |               |
| Endpoint Detection and Response Optimum | –   | –   | –                        | ✓   | ✓             |
| Endpoint Detection and Response Expert  | –   | –   | –                        | –   | –             |



|   |   |   |   |   |   |
|---|---|---|---|---|---|
| Kaspersky Sandbox<br>(Kaspersky Sandbox-licentie moet afzonderlijk worden aangekocht) | ✓ | ✓ | ✓ | ✓ | ✓ |
|---|---|---|---|---|---|

## Programma activeren

De *activering* is het proces waarbij een [licentie](#) wordt geactiveerd om een volledige functionele versie van het programma te gebruiken totdat de licentie verloopt. Voor de activering van het programma moet u een [licentiebestand](#) toevoegen.

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

- Lokaal vanuit de programma-interface door de [Activeringswizard](#) te gebruiken. U kunt zowel de actieve licentie als de reservelicentie op deze manier toevoegen.
- Op afstand met de [Kaspersky Security Center-software suite](#) door een taak voor het toevoegen van een licentiebestand aan te maken en vervolgens te starten. Op deze manier kunt u zowel de actieve licentie als de reservelicentie toevoegen.
- Op afstand door licentiebestanden en activeringscodes in de licentieopslag in Administration Server van Kaspersky Security Center te verdelen tussen clientcomputers. Voor meer informatie over het verdelen van licenties raadpleegt u de [Help van Kaspersky Security Center](#). Op deze manier kunt u zowel de actieve licentie als de reservelicentie toevoegen.

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

- Met de [opdrachtregel](#).

Het kan even duren om het programma met een activeringscode te activeren (tijdens de installatie op afstand of niet-interactieve installatie) wegens de verdeling van de belasting tussen de activeringsservers van Kaspersky. Als u het programma onmiddellijk wilt activeren, kunt u het actieve activeringsproces onderbreken en de activering met de Activeringswizard starten.

## Het programma activeren via Kaspersky Security Center

U kunt het programma op de volgende manieren op afstand activeren via Kaspersky Security Center:

- Met de taak *Licentie toevoegen*.  
Via deze methode kunt u een licentie toevoegen aan een specifieke computer of aan computers die tot een beheergroep behoren.
- Door een code die is opgeslagen op de Administration Server van Kaspersky Security Center te versturen naar de computers.  
Via deze methode kunt u een licentie automatisch toevoegen aan computers die al verbonden zijn met Kaspersky Security Center, alsook aan nieuwe computers. Hiervoor moet u de sleutel eerst toevoegen aan de Kaspersky Security Center Administration Server. Voor meer informatie over het toevoegen van codes aan de Administration Server van Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#).


- Door de code toe te voegen aan het Kaspersky Endpoint Security-installatiepakket.

Met deze methode kunt u de code toevoegen in [Eigenschappen installatiepakket](#) tijdens de implementatie van Kaspersky Endpoint Security. Het programma wordt automatisch geactiveerd na de installatie.

Er is een proefversie beschikbaar voor Kaspersky Security Center Cloud Console. De *proefversie* is een speciale versie van Kaspersky Security Center Cloud Console, ontworpen om een gebruiker vertrouwd te maken met de functies van het programma. In deze versie kunt u acties uitvoeren in een werkruimte gedurende een periode van 30 dagen. Alle beheerde applicaties worden automatisch uitgevoerd onder een proeflicentie voor Kaspersky Security Center Cloud Console, inclusief Kaspersky Endpoint Security. U kunt Kaspersky Endpoint Security echter niet activeren met zijn eigen proeflicentie wanneer de proeflicentie voor Kaspersky Security Center Cloud Console verloopt. Voor gedetailleerde informatie over licenties voor Kaspersky Security Center *Cloud Console* raadpleegt u de [Help van de Kaspersky Security Center Cloud Console](#)<sup>2</sup>.

Met de proefversie van Kaspersky Security Center Cloud Console kunt u later niet overschakelen naar een commerciële versie. Elke proefwerkruimte wordt automatisch verwijderd met al zijn inhoud nadat de periode van 30 dagen is verstreken.

Op de volgende manieren kunt u het gebruik van licenties monitoren:

- Bekijk het *rapport over het gebruik van codes* in de infrastructuur van het bedrijf (**Monitoring en rapportage** → **Rapporten**).
- Bekijk de status van computers op het tabblad **Devices** → **Managed devices**. Als het programma niet is geactiveerd, heeft de computer de status  *Programma is niet geactiveerd*.
- Bekijk licentie-informatie in de computereigenschappen.
- Bekijk de eigenschappen van de code (**Bewerkingen** → **Licentiebeheer**).

[Het programma activeren in de beheerconsole \(MMC\)](#)<sup>2</sup>

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)** → **Licentie toevoegen**.

## Stap 2. Een sleutel toevoegen

Voer een [activatiecode in](#) of selecteer een licentiebestand.

Voor meer informatie over het toevoegen van codes aan de Administration Server van Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#) <sup>2</sup>.

## Stap 3: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 4. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of wanneer de computer niet actief is.

## Stap 5. Taaknaam definiëren

Voer een naam in voor de taak, zoals *Kaspersky Endpoint Security voor Windows activeren*.

## Stap 6. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. Kaspersky Endpoint Security wordt nu op de computers van de gebruikers geactiveerd in stille modus.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Licentie toevoegen**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Activering van Kaspersky Endpoint Security voor Windows*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak. Ga naar de volgende stap.

## Stap 2: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 3. Een licentie selecteren

Selecteer de licentie waarmee u het programma wilt activeren. Ga naar de volgende stap.

U kunt codes toevoegen aan Webconsole (**Bewerkingen** → **Licentiebeheer**).

## Stap 4. Aanmaak van de taak voltooien

Voltooi de wizard door op de knop **Finish** te klikken. U ziet een nieuwe taak in de lijst met taken. Start een taak door het selectievakje naast de taak in te schakelen en op de knop **Starten** te klikken. Kaspersky Endpoint Security wordt nu op de computers van de gebruikers geactiveerd in stille modus.

In de eigenschappen van de taak *Licentie toevoegen* kunt u een reservelicentie aan de computer toevoegen. Een *reservelicentie* wordt actief wanneer de actieve licentie verloopt of wordt verwijderd. Als u een reservelicentie hebt, voorkomt u dat de functionaliteit van het programma wordt beperkt wanneer de licentie verloopt.

### [Automatisch een licentiesleutel toevoegen aan computers via de beheerconsole \(MMC\)](#)

1. Ga in de beheerconsole naar de map **Administration Server** → **Kaspersky-licenties** .  
Er wordt een lijst met licentiesleutels geopend.
2. Open de eigenschappen van de licentiesleutel.
3. Schakel in het gedeelte **Algemeen** het selectievakje **Automatisch gedistribueerde licentiesleutel** in.
4. Sla uw wijzigingen op.

Hierdoor wordt de licentie automatisch verspreid naar de juiste computers. Tijdens de automatische verspreiding van een licentie als actieve of reservelicentie wordt rekening gehouden met het maximale aantal computers waarvoor deze licentie kan worden gebruikt (ingesteld in de licentie-eigenschappen). Als het maximale aantal is bereikt, wordt de verspreiding van deze licentie automatisch gestopt. In het gedeelte **Apparaten** in de licentie-eigenschappen kunt u het aantal computers zien waaraan de licentie is toegevoegd, alsook andere gegevens.

### [Automatisch een licentiesleutel toevoegen aan computers via de webconsole en de cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole **Activiteiten** → **Licentiebeheer** → **Kaspersky-licenties**.  
Er wordt een lijst met licentiesleutels geopend.
2. Open de eigenschappen van de licentiesleutel.
3. Zet op het tabblad **Algemeen** de schakelaar **Licentie automatisch implementeren** aan.
4. Sla uw wijzigingen op.

Hierdoor wordt de licentie automatisch verspreid naar de juiste computers. Tijdens de automatische verspreiding van een licentie als actieve of reservelicentie wordt rekening gehouden met het maximale aantal computers waarvoor deze licentie kan worden gebruikt (ingesteld in de licentie-eigenschappen). Als het maximale aantal is bereikt, wordt de verspreiding van deze licentie automatisch gestopt. Op het tabblad **Apparaten** in de licentie-eigenschappen kunt u het aantal computers zien waaraan de licentie is toegevoegd, alsook andere gegevens.

## Activeringswizard gebruiken voor de activering van het programma

*Zo activeert u Kaspersky Endpoint Security met de Activeringswizard:*

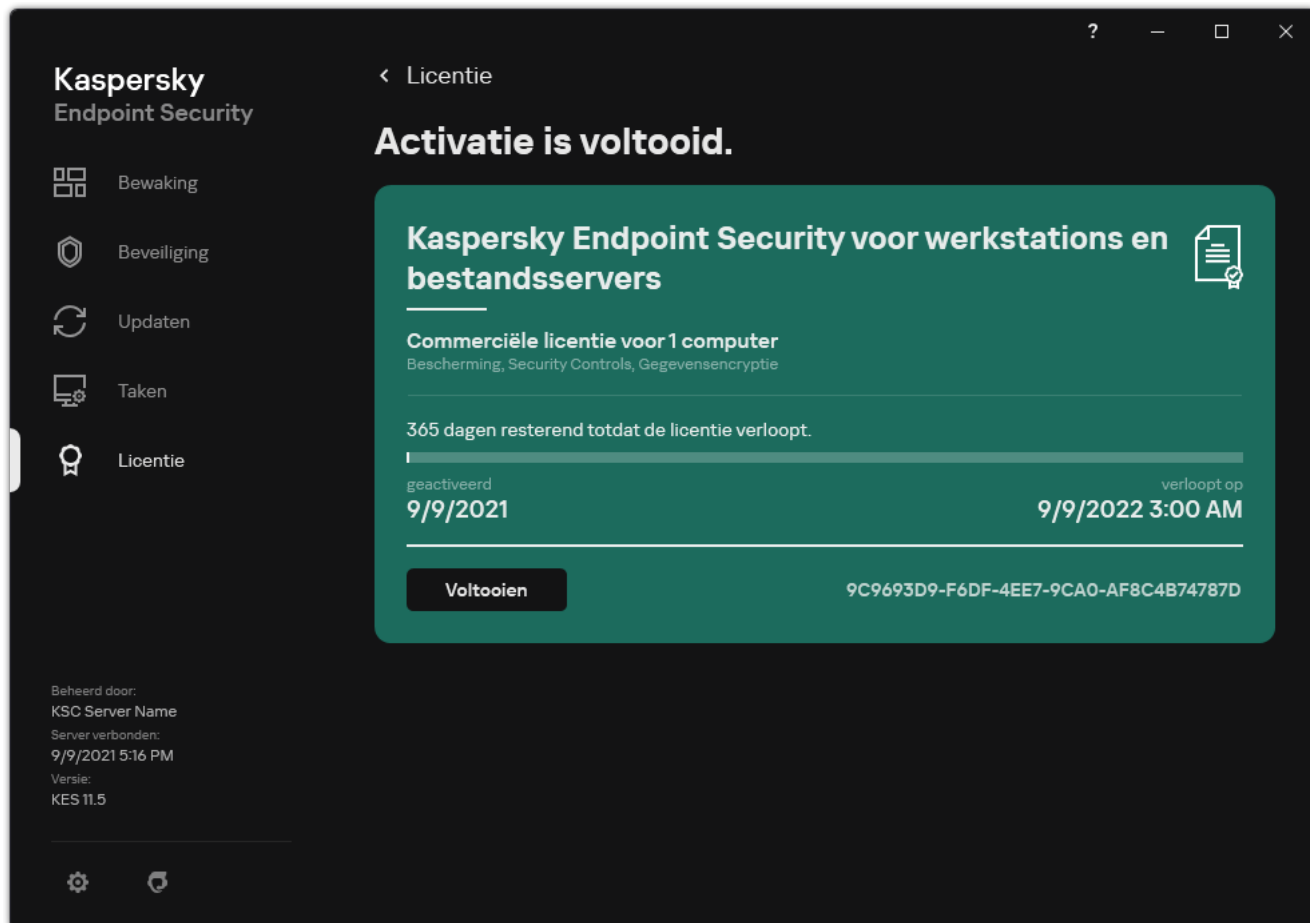
1. Ga in het hoofdvenster van het programma naar het gedeelte **Licentie**.
2. Klik op **Activeer het programma met een nieuwe licentie**.

De Activeringswizard van het programma wordt gestart. Volg de instructies van de Activeringswizard.

## Licentie-informatie bekijken

Zo bekijkt u informatie over een licentie:

Ga in het hoofdvenster van het programma naar het gedeelte **Licentie** (zie onderstaande afbeelding).



Het venster Licentiebeheer

In het gedeelte ziet u de volgende informatie:

- *Licentiestatus.* Op een computer kunnen verschillende [licenties](#) worden bewaard. Er zijn twee soorten licenties: actieve en reserve. Het programma kan maximaal één actieve licentie hebben. Een reservelicentie wordt pas actief nadat de actieve licentie is verlopen of nadat de actieve licentie is verwijderd door te klikken op de knop **Verwijderen**.
- *Programmanaam.* Volledige naam van het gekochte Kaspersky-programma.
- *Licentietype* De volgende [typen licenties](#) zijn verkrijgbaar: een evaluatielicentie en commerciële licentie.
- *Functionaliteit.* Functies van het programma die beschikbaar zijn met uw licentie. Deze functies zijn onder andere Bescherming, Security Controls, Gegevensencryptie en overige. De lijst met beschikbare functies staat ook in het [licentiecertificaat](#).
- *Aanvullende informatie over de licentie.* Begin- en einddatum van de geldigheidsduur van de licentie (alleen voor actieve licentie), resterende duur van de geldigheidsduur van de licentie.

Het tijdstip waarop de licentie verloopt wordt weergegeven volgens de tijdzone die op het besturingssysteem is ingesteld.

- *Licentie*. Een *sleutel* is een unieke alfanumerieke reeks die op basis van een activeringscode of een licentiebestand wordt gegenereerd.

U kunt in het venster Licentiebeheer ook het volgende doen:

- **Licentie kopen / Licentie verlengen**. Hiermee opent u de online shop op de Kaspersky-website waar u een licentie kunt kopen of verlengen. Hiertoe moet u gewoon de gegevens van uw bedrijf invoeren en de bestelling betalen.
- **Activeer het programma met een nieuwe licentie**. Hiermee start u de Activeringswizard van het programma. In deze wizard kunt u een licentie toevoegen met een activeringscode of licentiebestand. Via de activeringswizard van het programma kunt u een actieve licentie en slechts één reserveclicentie toevoegen.

## 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. Ga in het hoofdvenster van het programma naar het gedeelte **Licentie**.
2. Doe een van de volgende acties:
  - 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 kopen.

## Abonnement verlengen

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

Als u het programma met een onbeperkt abonnement gebruikt, controleert Kaspersky Endpoint Security de activeringsserver automatisch op verlengde licenties in de achtergrondmodus. Wanneer een licentie op de activeringsserver 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, meldt Kaspersky Endpoint Security u dit op de verloopdatum van het abonnement (of op de verloopdatum van de respijtperiode) en worden geen nieuwe pogingen ondernomen om 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.

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

1. Ga in het hoofdvenster van het programma naar het gedeelte **Licentie**.
2. Klik op **Contact opnemen met abonneerdersaanbieder**.

U kunt de abonnementsstatus handmatig updaten. Dit is mogelijk vereist als het abonnement na de respijtperiode is verlengd en de status van het programma niet automatisch is bijgewerkt.



# Gegevensverstrekking

## Gegevensverstrekking onder de licentieovereenkomst voor eindgebruikers

Als een [activeringscode](#) wordt toegepast om Kaspersky Endpoint Security te activeren, gaat u ermee akkoord om de volgende informatie periodiek en automatisch naar Kaspersky te versturen voor de controle van het correcte gebruik van het programma:

- type, versie en taalversie van Kaspersky Endpoint Security;
- versies van geïnstalleerde updates voor Kaspersky Endpoint Security;
- ID van de computer en ID van de specifieke Kaspersky Endpoint Security-installatie op de computer;
- serienummer en ID van actieve licentie;
- type, versie en bitrate van het besturingssysteem en naam van de virtuele omgeving (als Kaspersky Endpoint Security geïnstalleerd is in een virtuele omgeving);
- ID's van Kaspersky Endpoint Security-onderdelen die actief zijn wanneer de informatie wordt verstuurd.

Kaspersky kan deze informatie ook gebruiken om statistieken over de verspreiding en het gebruik van Kaspersky-software te genereren.

Door een activeringscode te gebruiken gaat u ermee akkoord om de eerder vermelde gegevens automatisch te versturen. Als u niet akkoord gaat met de verzending van deze informatie naar Kaspersky, moet u een [licentiebestand](#) gebruiken om Kaspersky Endpoint Security te activeren.

Door de voorwaarden van de Gebruiksrechtovereenkomst te accepteren, gaat u ermee akkoord om de volgende informatie automatisch te versturen:

- Wanneer u een upgrade van Kaspersky Endpoint Security uitvoert:
  - versie van Kaspersky Endpoint Security;
  - ID van Kaspersky Endpoint Security;
  - actieve sleutel;
  - unieke ID van de start van de upgradetaak;
  - unieke ID van de Kaspersky Endpoint Security-installatie.
- Wanneer u klikt op koppelingen in de Kaspersky Endpoint Security-interface:
  - versie van Kaspersky Endpoint Security;
  - versie van het besturingssysteem;
  - activeringsdatum van Kaspersky Endpoint Security;
  - verloopdatum van licentie;

- aanmaakdatum van de sleutel;
- installatiedatum van Kaspersky Endpoint Security;
- ID van Kaspersky Endpoint Security;
- ID van de gevonden kwetsbaarheid in het besturingssysteem;
- ID van de laatste geïnstalleerde update voor Kaspersky Endpoint Security;
- hash van het gedetecteerde bestand met een dreiging en de naam van deze dreiging volgens de Kaspersky-classificatie;
- categorie van de Kaspersky Endpoint Security-activeringsfout;
- code van de fout tijdens activering van Kaspersky Endpoint Security;
- aantal dagen tot de verloopdatum van de licentie;
- aantal dagen sinds het toevoegen van de sleutel;
- aantal dagen sinds het verlopen van de licentie;
- aantal computers waarop de actieve licentie wordt toegepast;
- actieve sleutel;
- periode van de Kaspersky Endpoint Security-licentie;
- huidige status van de licentie;
- type van de actieve licentie;
- programmatype;
- unieke ID van de start van de upgradetaak;
- unieke ID van de Kaspersky Endpoint Security-installatie op de computer;
- taal van de Kaspersky Endpoint Security-interface.

Ontvangen informatie wordt door Kaspersky beschermd overeenkomstig de wettelijke voorschriften en de vereisten en toepasselijke regelgevingen van Kaspersky. De gegevens worden via geëncrypte kanalen verstuurd.

Lees de Gebruiksrechtovereenkomst door en bezoek de [website van Kaspersky](#) voor meer informatie over de ontvangst, verwerking, opslag en vernietiging van informatie over het programmeergebruik nadat u akkoord bent gegaan met de Gebruiksrechtovereenkomst en de Kaspersky Security Network-verklaring. De bestanden 'license.txt' en 'ksn\_<taalcode>.txt' bevatten de tekst van de Gebruiksrechtovereenkomst en de Kaspersky Security Network-verklaring en worden bij het [distributiepakket](#) van het programma meegeleverd.

## Gegevensverstrekking tijdens het gebruik van Kaspersky Security Network

De set gegevens die Kaspersky Endpoint Security naar Kaspersky stuurt, is afhankelijk van het type licentie en de gebruiksinstellingen van Kaspersky Security Network.

## Gebruik van KSN onder licentie op niet meer dan 4 computers

Als u de Kaspersky Security Network-verklaring accepteert, gaat u ermee akkoord om de volgende informatie automatisch te verstrekken:

- informatie over KSN-configuratie-updates: ID van de actieve configuratie, ID van de ontvangen configuratie, foutcode van de configuratie-update;
- informatie over de te scannen bestanden en URL-adressen: de controlesommen van het gescande bestand (MD5, SHA2-256, SHA1) en bestandspatronen (MD5), de grootte van het patroon, de soort gedetecteerde dreiging en de naam ervan volgens de classificatie van de Rechthebbende, het ID voor de antivirusdatabases, het URL-adres waarvan de reputatie wordt gevraagd, alsook het verwijzende URL-adres, het ID van het protocol van de verbinding en het nummer van de gebruikte poort;
- ID van de scantaak die de bedreiging heeft gedetecteerd;
- informatie over gebruikte digitale certificaten om hun authenticiteit te verifiëren: de controlesommen (SHA256) van het gebruikte certificaat om het gescande object te ondertekenen en de openbare sleutel van het certificaat;
- het ID van het Software-onderdeel dat de scan uitvoert;
- de ID's van de antivirusdatabases en van de records in deze antivirusdatabases;
- Informatie over de activering van de Software op de Computer: de ondertekende header van het ticket van de activeringsservice (het ID van het regionale activeringscentrum, de controlesom van de activeringscode, de controlesom van het ticket, de aanmaakdatum van het ticket, de unieke ID van het ticket, de ticketversie, de licentiestatus, de begin-/einddatum en -tijd van de geldigheidsduur van het ticket, de unieke ID van de licentie, de licentieversie), de ID van het gebruikte certificaat voor de ondertekening van de ticket-header, de controlesom (MD5) van het licentiebestand.
- Informatie over de Software van de Rechthebbende: volledige versie, type, versie van het protocol dat wordt gebruikt om verbinding te maken met Kaspersky-services.

## Gebruik van KSN onder licentie op 5 of meer computers

Als u de Kaspersky Security Network-verklaring accepteert, gaat u ermee akkoord om de volgende informatie automatisch te verstrekken:

Als het selectievakje **Kaspersky Security Network** is ingeschakeld en het selectievakje **Uitgebreide KSN-modus inschakelen** is uitgeschakeld, wordt de volgende informatie verstuurd:

- informatie over KSN-configuratie-updates: ID van de actieve configuratie, ID van de ontvangen configuratie, foutcode van de configuratie-update;
- informatie over de te scannen bestanden en URL-adressen: de controlesommen van het gescande bestand (MD5, SHA2-256, SHA1) en bestandspatronen (MD5), de grootte van het patroon, de soort gedetecteerde dreiging en de naam ervan volgens de classificatie van de Rechthebbende, het ID voor de antivirusdatabases, het URL-adres waarvan de reputatie wordt gevraagd, alsook het verwijzende URL-adres, het ID van het protocol van de verbinding en het nummer van de gebruikte poort;
- ID van de scantaak die de bedreiging heeft gedetecteerd;
- informatie over gebruikte digitale certificaten om hun authenticiteit te verifiëren: de controlesommen (SHA256) van het gebruikte certificaat om het gescande object te ondertekenen en de openbare sleutel van het certificaat;

- het ID van het Software-onderdeel dat de scan uitvoert;
- de ID's van de antivirusdatabases en van de records in deze antivirusdatabases;
- Informatie over de activering van de Software op de Computer: de ondertekende header van het ticket van de activeringsservice (het ID van het regionale activeringscentrum, de controlesom van de activeringscode, de controlesom van het ticket, de aanmaakdatum van het ticket, de unieke ID van het ticket, de ticketversie, de licentiestatus, de begin-/einddatum en -tijd van de geldigheidsduur van het ticket, de unieke ID van de licentie, de licentieverie), de ID van het gebruikte certificaat voor de ondertekening van de ticket-header, de controlesom (MD5) van het licentiebestand.
- Informatie over de Software van de Rechthebbende: volledige versie, type, versie van het protocol dat wordt gebruikt om verbinding te maken met Kaspersky-services.

Als de selectievakjes **Uitgebreide KSN-modus inschakelen** en **Kaspersky Security Network** zijn ingeschakeld, verstuurt het programma naast de hierboven vermelde informatie ook deze informatie:

- informatie over de resultaten van de categorisering van de opgevraagde webbronnen, die het verwerkte URL- en IP-adres van de host bevat, de versie van het Software-onderdeel dat de categorisering heeft uitgevoerd, de methode van de categorisering, en de gedefinieerde categorieën voor de webbron;
- informatie over de software die op de Computer is geïnstalleerd: namen van de programma's en van de leveranciers ervan, registersleutels en hun waarden, informatie over bestanden van de geïnstalleerde software-onderdelen (controlesommen (MD5, SHA2-256, SHA1), de naam, het pad naar het bestand op de Computer, de grootte, de versie en de digitale handtekening);
- informatie over de staat van de antivirusbescherming van de computer: de versies en de release-tijdstempels van de antivirusdatabases die worden gebruikt, de ID van de taak en de ID van de software die scant;
- informatie over bestanden die de Eindgebruiker downloadt: de URL- en IP-adressen van de download en de downloadpagina's, het downloadprotocol-ID en het nummer van de verbindingspoort, de status van de URL als schadelijk of niet, de eigenschappen van het bestand, de bestandsgrootte en controlesommen (MD5, SHA2-256, SHA1), informatie over het proces dat het bestand heeft gedownload (controlesommen (MD5, SHA2-256, SHA1), de aanmaakdatum en -tijd, de status van automatisch afspelen, de eigenschappen, de namen van compressieprogramma's, informatie over handtekeningen, de markering van uitvoerbare bestanden, het ID van de bestandsindeling en entropie), de bestandsnaam en -pad op de Computer, de digitale handtekening van het bestand en de tijdstempel van het aanmaken, het URL-adres waar de detectie is gebeurd, het nummer van het script op de pagina dat als verdacht of schadelijk wordt gezien, informatie over HTTP-verzoeken die zijn aangemaakt en het antwoord daarop;
- informatie over de actieve programma's en hun modules: de gegevens over actieve processen op het systeem (proces-ID (PID)), de naam van het proces, informatie over het account waaruit het proces is gestart, het programma en de opdracht waarmee het proces is gestart, het volledige pad naar de bestanden van het proces en hun controlesommen (MD5, SHA2-256, SHA1), en de eerste opdrachtregel, het niveau van de integriteit van het proces, een beschrijving van het product waartoe het proces behoort (de naam van het product en informatie over de uitgever), evenals digitale certificaten die worden gebruikt en informatie die nodig is om de authenticiteit te verifiëren of informatie over het ontbreken van een digitale handtekening van een bestand), informatie over de modules die in de processen zijn geladen (hun naam, grootte, type, aanmaakdatums, kenmerken, controlesom (MD5, SHA2-256, SHA1) en de paden naar de modules op de Computer), informatie over PE-bestands-header, de namen van compressieprogramma's (als het bestand is verpakt);
- informatie over alle potentieel schadelijke objecten en activiteit: de naam van het gedetecteerde object en het volledige pad naar het object op de computer, de controlesommen van verwerkte bestanden (MD5, SHA2-256, SHA1), de datum en tijd van de detectie, de namen en grootten van geïnfecteerde bestanden en de paden ernaar, de code van de sjabloon van het pad, de vlag van het uitvoerbare bestand, de indicator die aangeeft of het object een container is, de naam van het compressieprogramma (als het bestand is gecomprimeerd), de code van het bestandstype, het ID van de bestandsindeling, de lijst met acties die door malware zijn uitgevoerd en de door de software en gebruiker genomen beslissing om er op te reageren, de ID's van de

antivirusdatabases en van de records in deze antivirusdatabases die zijn gebruikt om de beslissing te nemen, de indicator van een potentieel schadelijk object, de naam van de gedetecteerde dreiging volgens de classificatie van de Rechthebbende, het veiligheidsrisico, de detectiestatus en detectiemethode, de reden voor opname in de geanalyseerde context en volgnummer van het bestand in de context, de controlesom (MD5, SHA2-256, SHA1), de naam en kenmerken van het uitvoerbare bestand van het programma waarmee het geïnfecteerde bericht of de geïnfecteerde koppeling is verstuurd, de geanonimiseerde IP-adressen (IPv4 en IPv6) van de host van het geblokkeerde object, de bestandsentropie, de indicator voor automatisch starten van het bestand, het tijdstip van de eerste detectie in het systeem, het aantal keren dat het bestand is uitgevoerd sinds de laatste verzending van de statistieken, informatie over de naam, de controlesommen (MD5, SHA2-256, SHA1) en de grootte van het e-mailprogramma waarmee het schadelijke object is ontvangen, het ID van de softwaretaak die de scan heeft uitgevoerd, de indicator die aangeeft of de bestandsreputatie of handtekening is gecontroleerd, het resultaat van de bestandsverwerking, de controlesom (MD5) van het verzamelde patroon voor het object, de grootte van het patroon in bytes, en de technische specificaties van de toegepaste detectietechnologieën;

- informatie over gescande objecten: de toegewezen vertrouwensgroep waarin het bestand is geplaatst en/of waaruit het bestand is gehaald, de reden waarom het bestand in de categorie is geplaatst, het categorie-ID, informatie over de bron van de categorieën en de versie van de categoriedatabase, de markering van de vertrouwde certificering van het bestand, de naam van de leverancier van het bestand, de naam en versie van het softwareprogramma dat het bestand bevat;
- informatie over gedetecteerde kwetsbaarheden: het ID van de kwetsbaarheid in de database met kwetsbaarheden, de gevarenklasse van de kwetsbaarheid;
- informatie over emulatie van het uitvoerbare bestand: de bestandsgrootte en controlesommen (MD5, SHA2-256, SHA1), de versie van het emulatie-onderdeel, de emulatiediepte, een array van eigenschappen van logische blokken en functies binnen logische blokken die verkregen zijn tijdens de emulatie, de gegevens uit de PE-headers van het uitvoerbare bestand;
- de IP-adressen van de computer waarmee wordt aangevallen (IPv4 en IPv6), het nummer van de poort van de Computer die wordt aangevallen, het ID van het protocol van het IP-pakket met de aanval, het doelwit van de aanval (naam organisatie, website), de markering voor de reactie op de aanval, het gewicht van de aanval, het vertrouwensniveau;
- informatie over aanvallen waarbij netwerkbronnen worden vervalst, de DNS- en IP-adressen (IPv4 of IPv6) van bezochte websites;
- de DNS- en IP-adressen (IPv4 of IPv6) van de opgevraagde webbron, informatie over het bestand en webclient die de webbron opent, de naam, de grootte en controlesommen (MD5, SHA2-256, SHA1) van het bestand, het volledige pad naar het bestand en de code van de sjabloon van het pad, het resultaat van de controle van de digitale handtekening ervan, en de status ervan in KSN;
- informatie over het terugdraaien van malwareacties: gegevens over het bestand waarvan de activiteit is teruggedraaid (naam van het bestand, het volledige pad naar het bestand, de grootte en controlesommen (MD5, SHA2-256, SHA1) van het bestand), gegevens over geslaagde en mislukte acties om bestanden te verwijderen, hernoemen en kopiëren en om de waarden in het register te herstellen (namen van registersleutels en hun waarden), en informatie over systeembestanden die door malware zijn gewijzigd, vóór en na het terugdraaien;
- informatie over de reeks uitzonderingen voor het onderdeel Adaptieve controle op afwijkingen: het ID en de status van de regel die is geactiveerd, de actie die de Software heeft uitgevoerd wanneer de regel werd geactiveerd, het type gebruikersaccount waarmee het proces of de thread verdachte activiteit uitvoert, alsook het proces dat onderhevig was aan verdachte activiteit (het script-ID of de bestandsnaam van het proces, het volledige pad naar het procesbestand, de sjablooncode van het pad, de controlesommen (MD5, SHA2-256, SHA1) van het procesbestand); informatie over het object dat de verdachte acties heeft uitgevoerd alsook het object dat onderhevig was aan de verdachte acties (de naam van de registersleutel of de bestandsnaam, het volledige pad naar het bestand, de code van de padsjabloon, en de controlesommen (MD5, SHA2-256, SHA1) van het bestand);

- informatie over geladen softwaremodules: de naam, grootte en controlesommen (MD5, SHA2-256, SHA1) van het modulebestand, het volledige pad ernaar en de sjablooncode van het pad, de instellingen van de digitale handtekening van het modulebestand, de datum en tijd van de aanmaak van de handtekening, de naam van de houder en de organisatie die het modulebestand heeft ondertekend, het ID van het proces waarin de module is geladen, de naam van de leverancier van de module, en het volgnummer van de module in de laadwachtrij;
- informatie over de kwaliteit van de Software-interactie met de KSN-services: de begin- en einddatum en -tijd van de periode wanneer de statistieken zijn gegenereerd, informatie over de kwaliteit van verzoeken en de verbinding met alle gebruikte KSN-services (de ID van de KSN-service, het aantal geslaagde verzoeken, het aantal verzoeken met antwoorden vanuit de cache, het aantal mislukte verzoeken (netwerkproblemen, KSN dat is uitgeschakeld in de Software-instellingen, onjuiste routing), de tijdspanne van de geslaagde verzoeken, de tijdspanne van de geannuleerde verzoeken, de tijdspanne van de verzoeken met een overschreden tijdslimiet, het aantal verbindingen met KSN die uit de cache zijn gehaald, het aantal geslaagde verbindingen met KSN, het aantal mislukte verbindingen met KSN, het aantal geslaagde overdrachten, het aantal mislukte overdrachten, de tijdspanne van de geslaagde verbindingen met KSN, de tijdspanne van de mislukte verbindingen met KSN, de tijdspanne van de geslaagde overdrachten, de tijdspanne van de mislukte overdrachten);
- als een mogelijk schadelijk object wordt gedetecteerd, wordt informatie verstrekt over gegevens in het geheugen van de processen: elementen van de systeemobjecthiërarchie (ObjectManager), gegevens in UEFI BIOS-geheugen, namen van registersleutels en hun waarden;
- informatie over gebeurtenissen in de systeemlogboeken: de tijdstempel van de gebeurtenis, de naam van het logboek waarin de gebeurtenis is gevonden, het type en de categorie van de gebeurtenis, de naam van de bron en beschrijving van de gebeurtenis;
- informatie over netwerkverbindingen: de versie en controlesommen (MD5, SHA2-256, SHA1) van het bestand waaruit het proces is gestart dat de poort heeft geopend, het pad naar het procesbestand en de digitale handtekening, de lokale en externe IP-adressen, de nummers van poorten voor lokale en externe verbindingen, de verbindingstatus, het tijdstip wanneer de poort is geopend;
- informatie over de datum van software-installatie en activering op de computer: de ID van de partner die de licentie heeft verkocht, het serienummer van de licentie, de ondertekende kop van het ticket van de activeringsdienst (de ID van een regionaal activeringscentrum, de controlesom van de activeringscode, de controlesom van het ticket, de aanmaakdatum van het ticket, de unieke ID van het ticket, de ticketversie, de licentiestatus, de start-/ einddatum en tijd van het ticket, de unieke ID van de licentie, de licentieversie), de ID van het certificaat gebruikt om de ticketkop te ondertekenen, de controlesom (MD5) van het licentiebestand, de unieke ID van de software-installatie op de computer, het type en de ID van het programma dat wordt bijgewerkt, de ID van de updatetaak;
- informatie over de instellingen van alle geïnstalleerde updates en over recent geïnstalleerde/verwijderde updates, het type gebeurtenis dat de verzending van de updategegevens heeft veroorzaakt, de verstreken tijd sinds de installatie van de laatste update, informatie over de momenteel geïnstalleerde antivirusdatabases;
- informatie over de werking van de software op de computer: gegevens over het CPU-gebruik, gegevens over het geheugengebruik (Eigen bytes, Niet-wisselbare pool, Wisselbare pool), het aantal actieve threads in het softwareproces en openstaande threads, en de duur van de softwarewerking vóór de fout;
- aantal softwaredumps en systeemdumps (BSOD) sinds de installatie van de Software en sinds de laatste update: het ID en de versie van de Softwaremodule die is gecrasht, de geheugenopslag in het proces van de Software en informatie over de antivirusdatabases op het moment van de crash;
- gegevens over de systeemdump (BSOD): een vlag die aangeeft hoe vaak de BSOD voorkomt op de Computer, de naam van het stuurprogramma dat de BSOD heeft veroorzaakt, het adres en de geheugenopslag in het stuurprogramma, een vlag die aangeeft hoe lang de sessie van het besturingssysteem heeft geduurd voordat de BSOD optrad, de geheugenopslag van het stuurprogramma dat gecrasht is, het type opgeslagen geheugendump, de vlag voor de sessie van het besturingssysteem voordat de BSOD meer dan 10 minuten heeft geduurd, het unieke ID van de dump, de tijdstempel van de BSOD;

- informatie over fouten of prestatieproblemen tijdens de werking van de Software-onderdelen: het status-ID van de Software, het type fout, de code en oorzaak alsook het tijdstip van de fout, de ID's van het onderdeel, de module en het proces van het product waarin de fout is opgetreden, het ID van de taak of updatecategorie wanneer de fout is opgetreden, de logboeken van stuurprogramma's die door de Software zijn gebruikt (foutcode, naam van de module, naam van het bronbestand en de regel waar de fout is opgetreden);
- informatie over updates van antivirusdatabases en Software-onderdelen: de naam, de datum en tijd van indexbestanden die zijn download tijdens de laatste update en die tijdens de huidige update worden gedownload;
- informatie over een abnormale beëindiging van de Software: de tijdstempel van de aanmaak van de dump, het type ervan, het type gebeurtenis dat de abnormale beëindiging van de Software heeft veroorzaakt (onverwachte uitschakeling, crash van ander programma), de datum en tijd van de onverwachte uitschakeling;
- informatie over de compatibiliteit van de stuurprogramma's van de Software met hardware en software: informatie over besturingssysteemeigenschappen die de functionaliteit van Software-onderdelen beperken (Beveiligd opstarten, KPTI, WHQL Enforce, BitLocker, hoodlettergevoeligheid), het type van geïnstalleerde downloadsoftware (UEFI, BIOS), het ID van de Trusted Platform Module (TPM), de versie van de TPM, informatie over de geïnstalleerde CPU in de Computer, de uitvoermodus en parameters van Code-integriteit en Device Guard, de uitvoermodus van stuurprogramma's en de reden voor gebruik van de huidige modus, de versie van de stuurprogramma's van de Software, de status van de ondersteuning voor software- en hardwarevirtualisatie van de Computer;
- informatie over programma's van andere fabrikanten die de fout hebben veroorzaakt: hun naam, de versie en taalversie, de foutcode en informatie over de fout uit het systeemlogboek van programma's, het adres van de fout en de geheugenopslag van het programma van de andere leverancier, een vlag die aangeeft dat er een fout in het Software-onderdeel is opgetreden, de tijd dat het programma van een andere leverancier actief was voordat de fout optrad, de controlesommen (MD5, SHA2-256, SHA1) van de procesimage van het programma waarin de fout is opgetreden, het pad naar de procesimage van het programma en de sjablooncode van het pad, informatie van het systeemlogboek met een beschrijving van de fout met betrekking tot het programma, informatie over de programmamodule waarin een fout is opgetreden (informatie over de uitzondering, het geheugenadres van de crash als een afwijking in de programmamodule, de naam en de versie van de module, het ID van de programmacrash in de plug-in van de Rechthebbende en de geheugenopslag van de crash, de duur van de programmasessie voor de crash);
- de versie van het onderdeel Software-updater, het aantal crashes van het update-onderdeel tijdens het uitvoeren van updatetaken gedurende de complete gebruiksduur van het onderdeel, het ID van het type van de updatetaak, het aantal mislukte pogingen van het update-onderdeel om updatetaken te voltooien;
- informatie over de werking van de Software-onderdelen die het systeem bewaken: de volledige versies van de onderdelen, de datum en tijd van de start van de onderdelen, de code van de gebeurtenis die een overloop in de gebeurtenissenwachtrij veroorzaakte en het aantal dergelijke gebeurtenissen, het totale aantal gebeurtenissen die een overloop in de wachtrij veroorzaakten, informatie over het bestand van het proces van de initiator van de gebeurtenis (de naam van het bestand en het bijbehorende pad op de Computer, de sjablooncode van het bestandspad, de controlesommen (MD5, SHA2-256, SHA1) van het proces dat aan het bestand is gekoppeld, de bestandsversie), het ID van de onderschepping van de gebeurtenis, de volledige versie van het onderscheppingsfilter, het ID van het type onderschepte gebeurtenis, de grootte van de gebeurtenissenwachtrij en het aantal gebeurtenissen tussen de eerste gebeurtenis in de wachtrij en de huidige gebeurtenis, het aantal nog niet verwerkte gebeurtenissen in de wachtrij, informatie over het bestand van het proces van de initiator van de huidige gebeurtenis (de naam van het bestand en het bijbehorende pad op de Computer, de sjablooncode van het bestandspad, de controlesommen (MD5, SHA2-256, SHA1) van het proces dat aan het bestand is gekoppeld), de duur van de verwerking van de gebeurtenissen, de maximale duur van de verwerking van de gebeurtenissen, de waarschijnlijkheid van de verzending van statistieken, informatie over gebeurtenissen in het besturingssysteem waarvoor de maximale verwerkingsduur is overschreden (de datum en tijd van de gebeurtenis, het aantal herhaalde initialisaties van antivirusdatabases, de datum en tijd van de laatste herhaalde initialisatie van de antivirusdatabases na het updaten ervan, de vertraging in de verwerking van gebeurtenissen voor elk onderdeel dat het systeem bewaakt, het aantal gebeurtenissen in de wachtrij, het aantal verwerkte gebeurtenissen, het aantal gebeurtenissen van het huidige type dat vertraging heeft

opgelopen, de totale vertraging voor de gebeurtenissen van het huidige type, de totale vertraging voor alle gebeurtenissen);

- informatie uit de Windows-tool voor gebeurtenistracing (Event Tracing for Windows, ETW) bij eventuele prestatieproblemen van de Software, leveranciers van SysConfig / SysConfigEx / WinSATAssessment-gebeurtenissen van Microsoft: informatie over de Computer (het model, de fabrikant, de vormfactor van de behuizing, versie), informatie over de Windows-prestatie-metriek (WinSAT-beoordelingen, Windows-prestatie-index), de domeinnaam, informatie over fysieke en logische processors (het aantal fysieke en logische processors, de fabrikant, het model, het revisienummer, het aantal kernen, de klokfrequentie, het CPUID, de cachekenmerken, de kenmerken van de logische processors, de indicators voor ondersteunde modi en instructies), informatie over RAM-modules (het type, de vormfactor, de fabrikant, het model, de capaciteit, de granulariteit van geheugentoeewijzing), informatie over netwerkinterfaces (de IP- en MAC-adressen, de naam, de beschrijving, de configuratie van netwerkinterfaces, de uitsplitsing van het aantal en de grootte van de netwerkpakketten per type, de snelheid van de netwerkoverdrachten, de uitsplitsing van het aantal netwerkfouten per type), de configuratie van de IDE-controller, de IP-adressen van de DNS-servers, informatie over de videokaart (het model, de beschrijving, de fabrikant, de compatibiliteit, de grootte van het videogeheugen, de schermtoestemming, het aantal bits per pixel, de BIOS-versie), informatie over Plug en-Play-apparaten (de naam, de beschrijving, het apparaat-ID [PnP, ACPI], informatie over schijven en opslagapparaten (het aantal schijven of flashstations, de fabrikant, het model, de schijfgrootte, het aantal cilinders, het aantal tracks per cilinder, het aantal sectoren per track, de sectorgrootte, de cachekenmerken, het sequentiële nummer, het aantal partities, de configuratie van de SCSI-controller), informatie over logische schijven (het sequentiële nummer, de grootte van partities, de grootte van stations, de stationsletter, het partitietype, het type bestandssysteem, het aantal clusters, de clustergrootte, het aantal sectoren per cluster, het aantal lege en gebruikte clusters, de letter van het opstartbare station, het offset-adres van de partitie met betrekking tot de start van de schijf), informatie over de BIOS-systeemkaart (de fabrikant, de releasedatum, de versie), informatie over de systeemkaart (de fabrikant, het model, het type), informatie over het fysieke geheugen (de grootte van het gedeelde en beschikbare geheugen), informatie over services van het besturingssysteem (de naam, de beschrijving, de status, de tag, informatie over processen [naam en PID]), de parameters van het energieverbruik voor de Computer, de configuratie van de onderbrekingscontroller, het pad naar de Windows-systeem-mappen (Windows en System32), informatie over het besturingssysteem (de versie, de build, de releasedatum, de naam, het type, de installatiedatum), de grootte van het wisselbestand, informatie over beeldschermen (het aantal, de fabrikant, de schermtoestemming, de maximale resolutie, het type), informatie over het stuurprogramma van de videokaart (de fabrikant, de releasedatum, de versie);
- informatie uit ETW, leveranciers van EventTrace / EventMetadata-gebeurtenissen van Microsoft: informatie over de opeenvolging van systeemgebeurtenissen (het type, de tijd, de datum, de tijdzone), metagegevens over het bestand met de tracingresultaten (de naam, de structuur, de tracingparameters, de uitsplitsing van het aantal traces per type), informatie over het besturingssysteem (de naam, het type, de versie, de build, de releasedatum, de begintijd);
- informatie uit ETW, leveranciers van Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power-gebeurtenissen van Microsoft: informatie over gestarte en voltooide processen (de naam, het PID, de startparameters, de opdrachtregel, de retourcode, de parameters van het energiebeheer, het tijdstip van de start en voltooiing, het type toegangstoken, het SID, het SessionID, het aantal geïnstalleerde descriptors), informatie over wijzigingen in threadprioriteiten (het TID, de prioriteit, de tijd), informatie over schijfbewerkingen van het proces (het type, de tijd, de grootte, het aantal), de geschiedenis van wijzigingen in de structuur en de capaciteit van bruikbare geheugenprocessen;
- informatie uit ETW, leveranciers van StackWalk / Perfinfo-gebeurtenissen van Microsoft: informatie over prestatietellers (de prestaties van individuele stukken code, de opeenvolging van functie-aanroepen, het PID, het TID, de adressen en kenmerken van ISRs en DPCs);
- informatie uit ETW, leverancier van KernelTraceControl-ImageID-gebeurtenissen van Microsoft: informatie over uitvoerbare bestanden en DLL's (de naam, de imagegrootte, het volledige pad), informatie over PDB-bestanden (de naam, het ID), VERSIONINFO-resourcegegevens voor uitvoerbare bestanden (de naam, de beschrijving, de maker, de lokalisatie, de programmaversie en het ID, de bestandsversie en het ID);
- informatie uit ETW, leveranciers van FileIo / DiskIo / Image / Windows Kernel Disk-gebeurtenissen van Microsoft: informatie over bestands- en schijfbewerkingen (het type, de capaciteit, de begintijd, de voltooiingstijd, de duur,



de voltooiingsstatus, het PID, het TID, de adressen van de functie-aanroep van het stuurprogramma, I/O Request Packet (IRP), Windows-bestandskenmerken), informatie over bestanden die betrokken zijn bij bestands- en schijfbewerkingen (de naam, de versie, de grootte, het volledige pad, de kenmerken, de offset, de imagecontrolesom, open en toegangsopties);

- informatie uit ETW, leverancier van PageFault-gebeurtenissen van Microsoft: informatie over toegangsfouten bij de geheugenpagina (het adres, de tijd, de grootte, het PID, het TID, de kenmerken van het Windows-bestand, de parameters van de geheugentoewijzing);
- informatie uit ETW, leverancier van Thread-gebeurtenissen van Microsoft: informatie over de aanmaak/voltooiing van threads, informatie over gestarte threads (het PID, het TID, de grootte van de stack, de prioriteiten en toewijzing van CPU-bronnen, I/O-bronnen, geheugenpagina's tussen threads, het stack-adres, het adres van de init-functie, het adres van Thread Environment Block (TEB), de Windows-servicetag);
- informatie uit ETW, leverancier van Microsoft Windows Kernel Memory-gebeurtenissen van Microsoft: informatie over bewerkingen voor geheugenbeheer (de voltooiingsstatus, de tijd, de hoeveelheid, het PID), de structuur van de geheugentoewijzing (het type, de capaciteit, het SessionID, het PID);
- informatie over de werking van de Software bij eventuele prestatieproblemen: het ID van de Software-installatie, het type en de waarde van drop in-prestaties, informatie over de opeenvolging van gebeurtenissen in de Software (de tijd, de tijdzone, het type, de voltooiingsstatus, het ID van het Software-onderdeel, het ID van het Software-scenario, het TID, het PID, de adressen van de aanroep van de functie), informatie over te controleren netwerkverbindingen (de URL, de richting van de verbinding, de grootte van het netwerkpakket), informatie over PDB-bestanden (de naam, het ID, de imagegrootte van het uitvoerbare bestand), informatie over te controleren bestanden (de naam, het volledige pad, de controlesom), de parameters voor de bewaking van de prestaties van de Software;
- informatie over een de laatste mislukte laatste herstart van het besturingssysteem: het aantal mislukte heropstarten sinds de installatie van het besturingssysteem, gegevens over de systeemdump (de code en parameters van een fout, de naam, de versie en de controlesom (CRC32) van de module die een fout in de werking van het besturingssysteem heeft veroorzaakt, het foutadres als een offset in de module, controlesommen (MD5, SHA2-256, SHA1) van de systeemdump);
- informatie voor de controle van de authenticiteit van digitale certificaten die voor de ondertekening van bestanden worden gebruikt: de vingerafdruk van het certificaat, het algoritme van de controlesom, de openbare sleutel en het serienummer van het certificaat, de naam van de verlener van het certificaat, het resultaat van de validatie van het certificaat en het database-ID van het certificaat;
- informatie over het proces dat de aanval op de zelfbescherming van de Software uitvoert: de naam en de grootte van het procesbestand, de controlesommen (MD5, SHA2-256, SHA1), het volledige pad naar het procesbestand en de sjablooncode van het bestandspad, de tijdstempels van de aanmaak/build, de vlag van het uitvoerbare bestand, de kenmerken van het procesbestand, informatie over het gebruikte certificaat om het procesbestand te ondertekenen, de code van het gebruikte account om het proces te starten, het ID van uitgevoerde bewerkingen om toegang tot het proces te krijgen, het type van de bron waarmee de bewerking is uitgevoerd (het proces, het bestand, het registerobject, de FindWindow-zoekfunctie), de naam van de bron waarmee de bewerking is uitgevoerd, de vlag voor het resultaat van de bewerking, de status van het bestand van het proces en de handtekening ervan volgens het KSN;
- Informatie over de software van de Rechthebbende: volledige versie, type, taalversie en status van de gebruikte software, versies van de geïnstalleerde softwareonderdelen en de status van hun werking, gegevens over geïnstalleerde software-updates, de waarde van het TARGET-filter en de versie van het gebruikte protocol om verbinding te maken met de services van de Rechthebbende.
- informatie over geïnstalleerde hardware in de Computer: het type, de naam, de naam van het model, de firmwareversie, de parameters van ingebouwde en aangesloten apparaten, het unieke ID van de Computer met de geïnstalleerde software;

- informatie over de versies van het besturingssysteem en geïnstalleerde updates, de woordgrootte, de editie en de parameters van het uitvoermodus van het besturingssysteem, de versie en de controlesommen (MD5, SHA2-256, SHA1) van het kernelbestand van het besturingssysteem, en de datum en tijd van de opstart van het besturingssysteem;
- uitvoerbare en niet-uitvoerbare bestanden, geheel of gedeeltelijk;
- delen van het RAM-geheugen van de computer;
- sectoren die betrokken zijn bij het opstarten van het besturingssysteem;
- pakketten met gegevens over netwerkverkeer;
- webpagina's en e-mails met verdachte en kwaadaardige objecten.
- beschrijving van de klassen en instanties van klassen van de WMI-opslagplaats;
- rapporten over toepassingsactiviteiten:
  - de naam, grootte en versie van het bestand dat wordt verzonden, de beschrijving en controlesommen (MD5, SHA2-256, SHA1), bestandsformaat-ID, de naam van de leverancier van het bestand, de naam van het product waartoe het bestand behoort, volledig pad naar het bestand op de computer, sjablooncode van het pad, de tijdstempels van het maken en wijzigen van het bestand;
  - begin- en einddatum/-tijd van de geldigheidsperiode van het certificaat (als het bestand een digitale handtekening heeft), de datum en het tijdstip van de handtekening, de naam van de uitgever van het certificaat, informatie over de certificaathouder, de vingerafdruk, de openbare sleutel van het certificaat en geschikte algoritmen en het serienummer van het certificaat;
  - de naam van het account van waaruit het proces wordt uitgevoerd;
  - controlesommen (MD5, SHA2-256, SHA1) van de naam van de computer waarop het proces wordt uitgevoerd;
  - titels van de procesvensters;
  - ID voor de antivirusdatabases, naam van de gedetecteerde dreiging volgens de classificatie van de Rechthebbende;
  - gegevens over de geïnstalleerde licentie, de ID, het type en de vervaldatum;
  - lokale tijd van de computer op het moment van informatieverstrekking;
  - namen van en paden naar bestanden die door het proces zijn geopend;
  - namen van registersleutels en hun waarden die door het proces zijn aangeroepen;
  - URL- en IP-adressen die het proces heeft gebruikt;
  - URL- en IP-adressen waarvan het actieve bestand werd gedownload.

## Gegevensverstrekking bij het gebruik van oplossingen voor Detection and Response

Op computers waarop Kaspersky Endpoint Security is geïnstalleerd, worden gegevens voorbereid voor automatische verzending naar [Detectie en respons van Kaspersky Endpoint](#) en [Kaspersky-sandbox](#) server is opgeslagen. Bestanden worden in eenvoudige, niet-versleutelde vorm op computers opgeslagen.

De specifieke gegevensset is afhankelijk van de oplossing waarin Kaspersky Endpoint Security wordt gebruikt.

## Kaspersky Endpoint Detection and Response

Alle gegevens die het programma lokaal op de computer opslaat, worden van de computer verwijderd wanneer Kaspersky Endpoint Security wordt verwijderd.

### Gegevens ontvangen als gevolg van IOC-scan taakuitvoering (standaardtaak)

Kaspersky Endpoint Security verzendt automatisch gegevens op de *IOC-scan* taakuitvoeringsresultaten naar Kaspersky Security Center.

De gegevens in de uitvoeringsresultaten van de *IOC-scan*-taak kunnen de volgende informatie bevatten:

- IP-adres uit de ARP-tabel
- Fysiek adres uit de ARP-tabel
- DNS-recordtype en -naam
- IP-adres van de beveiligde computer
- Fysiek adres (MAC-adres) van de beveiligde computer
- Identificatie in het gebeurtenislogboek
- Naam gegevensbron in het logboek
- Lognaam
- Het tijdstip van de gebeurtenis
- MD5- en SHA256-hashes van het bestand
- Volledige naam van het bestand (inclusief pad)
- Bestandsgrootte
- Extern IP-adres en poort waarmee tijdens het scannen verbinding is gemaakt
- IP-adres lokale adapter
- Poort open op de lokale adapter
- Protocol als nummer (volgens de IANA-standaard)
- De naam van het proces

- Argumenten verwerken
- Pad naar het procesbestand
- Windows-identificatie (PID) van het proces
- Windows-identificatie (PID) van het bovenliggende proces
- Gebruikersaccount waarmee het proces is gestart
- Datum en tijd waarop het proces is gestart
- Service naam
- Dienstbeschrijving
- Pad en naam van de DLL-service (voor svchost)
- Pad en naam van het uitvoerbare servicebestand
- Windows-ID (PID) van de service
- Servicetype (bijvoorbeeld een kernelstuurprogramma of adapter)
- Service status
- Servicestartmodus
- Gegevens van gebruikersaccount
- Volumenaam
- Volume brief
- Volumetype
- Windows-registerbestanden
- Registercomponentwaarde
- Pad naar registersleutel (zonder component en waardenam)
- Register instelling
- Systeem (omgeving)
- Naam en versie van het besturingssysteem dat op de computer is geïnstalleerd
- Netwerknnaam van de beveiligde computer
- Domein of groep waartoe de beveiligde computer behoort
- Browsernaam
- Versie van de browser

- Tijdstip waarop de webresource voor het laatst is geopend
- URL van het HTTP-verzoek
- Naam van het account dat wordt gebruikt voor het HTTP-verzoek
- Bestandsnaam van het proces dat het HTTP-verzoek heeft gedaan
- Volledig pad naar het bestand van het proces dat het HTTP-verzoek heeft gedaan
- Windows-identificatie (PID) van het proces dat het HTTP-verzoek heeft gedaan
- HTTP-verwijzer (HTTP-verzoek bron-URL)
- URI van de resource aangevraagd via HTTP
- Informatie over de HTTP-user-agent (de applicatie die het HTTP-verzoek heeft gedaan)
- Uitvoeringstijd van HTTP-verzoek
- Unieke identificatie van het proces dat het HTTP-verzoek heeft gedaan

## Gegevens voor het maken van een ontwikkelingsketen voor bedreigingen

Gegevens voor het maken van een ontwikkelingsketen voor bedreigingen worden standaard zeven dagen bewaard. De gegevens worden automatisch naar Kaspersky Security Center verzonden.

Gegevens voor het maken van een ontwikkelingsketen voor bedreigingen kunnen de volgende informatie bevatten:

- Datum en tijd van het incident
- Detectie naam
- Scan-modus
- Status van de laatste actie met betrekking tot de detectie
- Reden waarom de detectieverwerking is mislukt
- Gedetecteerd objecttype
- Naam gedetecteerd object
- Bedreigingsstatus nadat het object is verwerkt
- Reden waarom uitvoering van acties op het object is mislukt
- Acties die zijn uitgevoerd om kwaadaardige acties ongedaan te maken
- Informatie over het verwerkte object:
  - Unieke identificatie van het proces
  - Unieke identificatie van het bovenliggende proces

- Unieke identificatie van het procesbestand
- Windows-proces-ID (PID)
- Verwerk de opdrachtregel
- Gebruikersaccount waarmee het proces is gestart
- Code van de aanmeldingssessie waarin het proces wordt uitgevoerd
- Type van de sessie waarin het proces wordt uitgevoerd
- Integriteitsniveau van het verwerkte proces
- Lidmaatschap van het gebruikersaccount waarmee het proces is gestart in de geprivilegieerde lokale en domeingroepen
- Identificatie van het verwerkte object
- Volledige naam van het verwerkte object
- Identificatie van het beveiligde apparaat
- Volledige naam van het object (lokale bestandsnaam of gedownload bestand webadres)
- MD5- of SHA256-hash van het verwerkte object
- Type van het verwerkte object
- Aanmaakdatum van het verwerkte object
- Datum waarop het verwerkte object voor het laatst is gewijzigd
- Grootte van het verwerkte object
- Attributen van het verwerkte object
- Organisatie die het verwerkte object heeft ondertekend
- Resultaat van de verificatie van het digitale certificaat van het verwerkte object
- Beveiligings-ID (SID) van het verwerkte object
- Tijdzone-ID van het verwerkte object
- Webadres van de verwerkte objectdownload (alleen voor bestanden op schijf)
- Naam van de toepassing die het bestand heeft gedownload
- MD5 en SHA256-hashes van de toepassing die het bestand heeft gedownload
- Naam van de toepassing die het bestand het laatst heeft gewijzigd
- MD5 en SHA256-hashes van de toepassing die het bestand het laatst heeft gewijzigd
- Aantal verwerkte objectstarts

- Datum en tijd waarop het verwerkte object voor het eerst is gestart
- Unieke ID's van het bestand
- Volledige naam van het bestand (lokale bestandsnaam of gedownload bestand webadres)
- Pad naar de verwerkte Windows-registervariabele
- Naam van de verwerkte Windows-registervariabele
- Waarde van de verwerkte Windows-registervariabele
- Type van de verwerkte Windows-registervariabele
- Indicator van het verwerkte lidmaatschap van de registersleutel in het punt voor automatisch starten
- Webadres van het verwerkte webverzoek
- Linkbron van het verwerkte webverzoek
- User-agent van het verwerkte webverzoek
- Type van het verwerkte webverzoek (GET or POST).
- Lokale IP-poort van het verwerkte webverzoek
- Externe IP-poort van het verwerkte webverzoek
- Verbindingsrichting (inkomend of uitgaand) van het verwerkte webverzoek
- Identificatie van het proces waarin de schadelijke code is ingebed

## Kaspersky Sandbox

Alle gegevens die het programma lokaal op de computer opslaat, worden van de computer verwijderd wanneer Kaspersky Endpoint Security wordt verwijderd.

### Service gegevens

Kaspersky Endpoint Security slaat de volgende gegevens op die worden verwerkt tijdens de automatische reactie:

- Verwerkte bestanden en gegevens die door de gebruiker zijn ingevoerd tijdens de configuratie van de ingebouwde agent van Kaspersky Endpoint Security:
  - In quarantaine geplaatste bestanden
  - Openbare sleutel van het certificaat dat wordt gebruikt voor integratie met Kaspersky Sandbox
- Cache van de ingebouwde agent van Kaspersky Endpoint Security:

- Tijdstip waarop de scanresultaten naar de cache zijn geschreven
- MD5-hash van de scantaak
- Scantaak-ID
- Scanresultaat voor het object
- Wachtrij van objectscanverzoeken:
  - ID van het object in de wachtrij
  - Tijdstip waarop het object in de wachtrij is geplaatst
  - Verwerkingsstatus van het object in de wachtrij
  - ID van de gebruikerssessie in het besturingssysteem waarin de objectscantaak is gemaakt
  - Systeem-ID (SID) van de gebruiker van het besturingssysteem wiens account is gebruikt om de taak te maken
  - MD5-hash van de objectscantaak
- Informatie over de taken waarvoor de ingebouwde agent van Kaspersky Endpoint Security wacht op scanresultaten van Kaspersky Sandbox:
  - Tijdstip waarop de objectscantaak is ontvangen
  - Objectverwerkings status
  - ID van de gebruikerssessie in het besturingssysteem waarin de objectscantaak is gemaakt
  - Identificatie van de objectscantaak
  - MD5-hash van de objectscantaak
  - Systeem-ID (SID) van de gebruiker van het besturingssysteem wiens account is gebruikt om de taak te maken
  - XML-schema van het automatisch aangemaakte IOC
  - MD5- of SHA256-hash van het gescande object
  - Verwerkingsfouten
  - Namen van de objecten waarvoor de taak is aangemaakt
  - Scanresultaat voor het object

## Gegevens in verzoeken aan Kaspersky Sandbox

De volgende gegevens van verzoeken van de ingebouwde agent van Kaspersky Endpoint Security aan Kaspersky Sandbox worden lokaal op de computer opgeslagen:

- MD5-hash van de scantaak



- Scantaak-ID
- Gescand object en alle gerelateerde bestanden

## Gegevens ontvangen als gevolg van IOC-scan taakuitvoering (op zichzelf staande taak)

Kaspersky Endpoint Security verzendt automatisch gegevens op de *IOC-scan* taakuitvoeringsresultaten naar Kaspersky Security Center.

De gegevens in de uitvoeringsresultaten van de *IOC-scan*-taak kunnen de volgende informatie bevatten:

- IP-adres uit de ARP-tabel
- Fysiek adres uit de ARP-tabel
- DNS-recordtype en -naam
- IP-adres van de beveiligde computer
- Fysiek adres (MAC-adres) van de beveiligde computer
- Identificatie in het gebeurtenislogboek
- Naam gegevensbron in het logboek
- Lognaam
- Het tijdstip van de gebeurtenis
- MD5- en SHA256-hashcodes van het bestand
- Volledige naam van het bestand (inclusief pad)
- Bestandsgrootte
- Extern IP-adres en poort waarmee tijdens het scannen verbinding is gemaakt
- IP-adres lokale adapter
- Poort open op de lokale adapter
- Protocol als nummer (volgens de IANA-standaard)
- De naam van het proces
- Argumenten verwerken
- Pad naar het procesbestand
- Windows-identificatie (PID) van het proces
- Windows-identificatie (PID) van het bovenliggende proces
- Gebruikersaccount waarmee het proces is gestart

- Datum en tijd waarop het proces is gestart
- Service naam
- Dienstbeschrijving
- Pad en naam van de DLL-service (voor svchost)
- Pad en naam van het uitvoerbare servicebestand
- Windows-ID (PID) van de service
- Servicetype (bijvoorbeeld een kernelstuurprogramma of adapter)
- Service status
- Servicestartmodus
- Gegevens van gebruikersaccount
- Volumenaam
- Volume brief
- Volumetype
- Windows-registerbestanden
- Registercomponentwaarde
- Pad naar registersleutel (zonder component en waardenam)
- Register instelling
- Systeem (omgeving)
- Naam en versie van het besturingssysteem dat op de computer is geïnstalleerd
- Netwerknnaam van de beveiligde computer
- Domein of groep waartoe de beveiligde computer behoort
- Browsernaam
- Versie van de browser
- Tijdstip waarop de webresource voor het laatst is geopend
- URL van het HTTP-verzoek
- Naam van het account dat wordt gebruikt voor het HTTP-verzoek
- Bestandsnaam van het proces dat het HTTP-verzoek heeft gedaan
- Volledig pad naar het bestand van het proces dat het HTTP-verzoek heeft gedaan

- Windows-identificatie (PID) van het proces dat het HTTP-verzoek heeft gedaan
- HTTP-verwijzer (HTTP-verzoek bron-URL)
- URI van de resource aangevraagd via HTTP
- Informatie over de HTTP-user-agent (de applicatie die het HTTP-verzoek heeft gedaan)
- Uitvoeringstijd van HTTP-verzoek
- Unieke identificatie van het proces dat het HTTP-verzoek heeft gedaan

## Naleving van de wetgeving van de Europese Unie (AVG)

Kaspersky Endpoint Security kan gegevens naar Kaspersky verzenden in de volgende scenario's:

- Bij het gebruik van Kaspersky Security Network.
- Bij de activatie van het programma met een activatiecode.
- Tijdens het updaten van programmamodules en antivirusdatabases.
- Tijdens het volgen van koppelingen in de programma-interface.
- Bij het schrijven naar dumps.

Ongeacht de gegevensclassificatie en het gebied van waaruit de gegevens worden ontvangen, houdt Kaspersky zich aan hoge normen voor gegevensbeveiliging en past het verschillende wettelijke, organisatorische en technische maatregelen toe om de gegevens van gebruikers te beschermen, om gegevensbeveiliging en vertrouwelijkheid te garanderen, en ook om de naleving van gebruikersrechten te waarborgen zoals bepaald door de toepasselijke wetgeving. De tekst van het Privacybeleid is opgenomen in de [distributiekit van het programma](#) en is beschikbaar op de [Kaspersky-website](#).

Lees voordat u Kaspersky Endpoint Security gebruikt zorgvuldig de beschrijving van de verzonden gegevens in de [Gebruiksrechtovereenkomst](#) en de [Kaspersky Security Network-verklaring](#). Als specifieke gegevens die in een van de beschreven scenario's door Kaspersky Endpoint Security worden verzonden, kunnen worden geclassificeerd als persoonsgegevens volgens uw lokale wetgeving of norm, moet u ervoor zorgen dat dergelijke gegevens legaal worden verwerkt en de toestemming van eindgebruikers verkrijgen voor het verzamelen en verzenden van dergelijke gegevens.

Lees de Gebruiksrechtovereenkomst door en bezoek de [website van Kaspersky](#) voor meer informatie over de ontvangst, verwerking, opslag en vernietiging van informatie over het programmeergebruik nadat u akkoord bent gegaan met de Gebruiksrechtovereenkomst en de Kaspersky Security Network-verklaring. De bestanden 'license.txt' en 'ksn\_<taalcode>.txt' bevatten de tekst van de Gebruiksrechtovereenkomst en de Kaspersky Security Network-verklaring en worden bij het [distributiepakket](#) van het programma meegeleverd.

Als u geen gegevens naar Kaspersky wilt verzenden, kunt u de verstrekking van gegevens uitschakelen.

## Over Kaspersky Security Network

Door Kaspersky Security Network te gebruiken, gaat u ermee akkoord automatisch de gegevens te verstrekken die worden vermeld in de [Kaspersky Security Network-verklaring](#). Als u niet akkoord gaat met het verstrekken van deze gegevens aan Kaspersky, gebruik dan Privaat KSN of [schakel het gebruik van KSN uit](#). Voor meer informatie over Privaat KSN raadpleegt u de *documentatie van Kaspersky Private Security Network*.

## Het programma activeren met een activeringscode

Door een activeringscode te gebruiken, gaat u ermee akkoord automatisch de gegevens te verstrekken die worden vermeld in de [Gebruiksrechtovereenkomst](#). Als u niet akkoord gaat met de verzending van deze informatie naar Kaspersky, moet u een [licentiebestand gebruiken om Kaspersky Endpoint Security te activeren](#).

## Het bijwerken van programmamodules en antivirusdatabases

Door Kaspersky-servers te gebruiken, gaat u ermee akkoord automatisch de gegevens te verstrekken die worden vermeld in de [Gebruiksrechtovereenkomst](#). Kaspersky heeft deze informatie nodig om te verifiëren dat Kaspersky Endpoint Security rechtmatig wordt gebruikt. Als u niet akkoord gaat met het verstrekken van deze informatie aan Kaspersky, gebruik dan [Kaspersky Security Center voor database-updates](#) of [Kaspersky Update Utility](#).

## Het volgen van links in de programma-interface

Door links in de programma-interface te gebruiken, gaat u ermee akkoord automatisch de gegevens te verstrekken die worden vermeld in de [Gebruiksrechtovereenkomst](#). De precieze lijst met gegevens die in elke specifieke link worden verzonden, hangt af van waar de link zich in de programma-interface bevindt en welk probleem ermee moet worden opgelost. Als u niet akkoord gaat met het verstrekken van deze gegevens aan Kaspersky, gebruik dan de [vereenvoudigde programma-interface](#) of [verberg de programma-interface](#).

## Dump schrijven

Als u het [schrijven van dumpbestanden](#) hebt ingeschakeld, maakt Kaspersky Endpoint Security een dumpbestand dat alle geheugendata van programmaprocessen bevat op het moment dat dit dumpbestand werd gemaakt.

## Aan de slag

Nadat u Kaspersky Endpoint Security hebt geïnstalleerd, kunt u het programma beheren met behulp van de volgende interfaces:

- [Lokale programma-interface](#).
- Open de beheerconsole van Kaspersky Security Center.
- Webconsole van Kaspersky Security Center.
- Kaspersky Security Center-cloudconsole.

### Beheerconsole van 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 en stoppen.

Het programma kan via Kaspersky Security Center worden beheerd met behulp van de beheerplug-in van Kaspersky Endpoint Security.

Voor gedetailleerde informatie over het beheer van het programma via Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#).

### Kaspersky Security Center-webconsole en Kaspersky Security Center-cloudconsole

Webconsole van Kaspersky Security Center (hierna ook de *Webconsole* genoemd) is een web-app voor het centrale beheer en onderhoud van het beveiligingssysteem van een bedrijfsnetwerk. Webconsole is een Kaspersky Security Center-onderdeel met een gebruikersinterface. Voor gedetailleerde informatie over de webconsole van Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#).

Kaspersky Security Center Cloud Console (hierna ook de *Cloudconsole* genoemd) is een cloudoplossing voor de bescherming en het beheer van bedrijfsnetwerken. Voor gedetailleerde informatie over de Cloudconsole van Kaspersky Security Center raadpleegt u de [Help van de Cloudconsole van Kaspersky Security Center](#).

Met Webconsole en Cloudconsole kunt u het volgende doen:

- Bewaak de status van het beveiligingssysteem van uw bedrijf.
- Installeer Kaspersky-programma's op apparaten in uw netwerk.
- Beheer geïnstalleerde programma's.
- Bekijk rapporten over de status van het beveiligingssysteem.

Het beheer van Kaspersky Endpoint Security via de Webconsole, Cloudconsole en Beheerconsole van Kaspersky Security Center biedt verschillende opties. De [beschikbare onderdelen en taken](#) verschillen ook naargelang de console die u gebruikt.

# Informatie over de beheerplug-in Kaspersky Endpoint Security voor Windows

De beheerplug-in voor Kaspersky Endpoint Security voor Windows maakt interactie mogelijk tussen Kaspersky Endpoint Security en Kaspersky Security Center. Met de beheerplug-in kunt u Kaspersky Endpoint Security beheeren met: [beleid](#), [taken](#) en [lokale programma-instellingen](#). Interactie met Kaspersky Security Center webconsole wordt verzorgd door de webplug-in.

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.

De webplug-in is niet standaard geïnstalleerd in de Webconsole van Kaspersky Security Center. In tegenstelling tot de Beheerplug-in voor de Beheerconsole van Kaspersky Security Center, die op het werkstation van de beheerder wordt geïnstalleerd, moet de webplug-in worden geïnstalleerd op een computer waarop de Webconsole van Kaspersky Security Center is geïnstalleerd. De functionaliteit van de webplug-in is beschikbaar voor alle beheerders die toegang hebben tot Webconsole in een browser. In de interface van webconsole kunt u de lijst met geïnstalleerde webplug-ins bekijken: **Console settings** → **Web Plug-ins**. Voor meer informatie over de compatibiliteit van de versies van de webplug-in en Webconsole raadpleegt u de [Help van Kaspersky Security Center](#).

## Webplug-in installeren

U kunt de webplug-in als volgt installeren:

- Installeer de webplug-in met de wizard Snelle start van de Webconsole van Kaspersky Security Center.  
U wordt door Webconsole automatisch gevraagd om de wizard 'Snelle start' te starten wanneer u Webconsole voor het eerst verbindt met Administration Server. U kunt de wizard Snelle start ook starten via de interface van Webconsole (**Discovery & Deployment** → **Deployment & Assignment** → **Quick Start Wizard**). De wizard Snelle start kan ook controleren of de geïnstalleerde webplug-ins up-to-date zijn en kan de noodzakelijke updates downloaden. Voor meer informatie over de wizard Snelle start voor Webconsole van Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#).
- Installeer de webplug-in via de lijst met beschikbare distributiepakketten in Webconsole.  
Voor de installatie van de webplug-in selecteert u het distributiepakket van de Kaspersky Endpoint Security-webplug-in in de interface van Webconsole (**Console settings** → **Web plug-ins**). De lijst met beschikbare distributiepakketten wordt automatisch geüpdatet wanneer nieuwe versies van Kaspersky-programma's worden gereleased.
- Download het distributiepakket naar de Webconsole vanaf een externe bron.  
Voeg het ZIP-bestand van het distributiepakket voor de Kaspersky Endpoint Security-webplug-in toe aan de interface van Webconsole om de webplug-in te installeren: **Console settings** → **Web plug-ins**. Het distributiepakket van de webplug-in kan bijvoorbeeld vanaf de Kaspersky-website worden gedownload.

## Beheerplug-in updaten

Om de Beheerplug-in Kaspersky Endpoint Security voor Windows bij te werken, downloadt u de nieuwste versie van de plug-in (inbegrepen in de [distributiekit](#)) en voert u de installatiewizard van de plug-in uit.

Als een nieuwe versie van de webplug-in beschikbaar is, toont Webconsole de melding *Er zijn updates beschikbaar voor de gebruikte plug-ins*. U kunt de versie van de webplug-in updaten via deze melding van Webconsole. U kunt ook handmatig zoeken naar nieuwe versies van de webplug-in in de interface van Webconsole (**Console settings** → **Web plug-ins**). De vorige versie van de webplug-in wordt tijdens de update automatisch verwijderd.

Wanneer de webplug-in wordt geüpdatet, worden de bestaande items (bijvoorbeeld beleidsregels of taken) opgeslagen. De nieuwe instellingen van items die nieuwe functies van Kaspersky Endpoint Security implementeren, verschijnen in de bestaande onderdelen en hebben de standaardwaarden.

Zo kunt u de webplug-in updaten:

- Update de webplug-in via de lijst met webplug-ins in de online modus.

Hiervoor moet u het distributiepakket van de Kaspersky Endpoint Security-webplug-in in de interface van Webconsole selecteren (**Console settings** → **Web plug-ins**). Webconsole zoekt naar beschikbare updates op Kaspersky-servers en downloadt de relevante updates.

- Update de webplug-in met een bestand.

Hiervoor moet u het ZIP-bestand van het distributiepakket voor de Kaspersky Endpoint Security-webplug-in in de interface van Webconsole selecteren: **Console settings** → **Web plug-ins**. Het distributiepakket van de webplug-in kan bijvoorbeeld vanaf de Kaspersky-website worden gedownload. U kunt de Kaspersky Endpoint Security-webplug-in alleen naar een nieuwere versie updaten. De webplug-in kan niet naar een oudere versie worden geüpdatet.

Als een item wordt geopend (zoals een beleid of een taak), controleert de webplug-in de informatie over de compatibiliteit ervan. Als de versie van de webplug-in gelijk is aan of nieuwer is dan de vermelde versie in de informatie over de compatibiliteit, kunt u de instellingen van dit item wijzigen. Anders kunt u de webplug-in niet gebruiken om de instellingen van het geselecteerde item te wijzigen. U wordt aanbevolen om de webplug-in te updaten.

## Speciale aandachtspunten bij het werken met verschillende versies van beheerplug-ins

U kunt Kaspersky Endpoint Security alleen via Kaspersky Security Center beheren als u een beheerplug-in hebt waarvan de versie gelijk is aan of hoger is dan de versie die is gespecificeerd in de informatie over de compatibiliteit van Kaspersky Endpoint Security met de beheerplug-in. U kunt de minimaal vereiste versie van de beheerplug-in bekijken in het bestand `installer.ini` dat is opgenomen in de [distributiekit](#).

Als een item wordt geopend (zoals een beleid of een taak), 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 item wijzigen. Anders kunt u de beheerplug-in niet gebruiken om de instellingen van het geselecteerde item te wijzigen. U wordt aanbevolen om de beheerplug-in bij te werken.

## Beheerplug-in voor Kaspersky Endpoint Security 10 voor Windows upgraden

Als de Beheerplug-in voor Kaspersky Endpoint Security 10 voor Windows is geïnstalleerd in de Beheerconsole, moet u bij de installatie van de Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows rekening houden met het volgende:


- De Beheerplug-in voor Kaspersky Endpoint Security 10 voor Windows wordt niet verwijderd en kan nog steeds worden gebruikt. Daarom heeft u toegang tot twee beheerplug-ins om met programmaversies 10 en 11 te werken.
- De Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows biedt geen ondersteuning voor het beheer van Kaspersky Endpoint Security 10 voor Windows op computers van gebruikers.
- De Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows biedt geen ondersteuning voor items (bijvoorbeeld een beleid of een taak) die zijn gemaakt met de Beheerplug-in voor Kaspersky Endpoint Security 10 voor Windows.

U kunt de wizard voor batchconversie gebruiken om beleid en taken om te zetten van versie 10 naar versie 11. Voor meer informatie over het omzetten van beleidsregels en taken raadpleegt u de [Help van Kaspersky Security Center](#).

## Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows upgraden

Als de Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows is geïnstalleerd in de Beheerconsole, moet u bij de installatie van een nieuwe versie van de Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows rekening houden met het volgende:

- De vorige versie van de Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows wordt verwijderd.
- De nieuwe versie van de Beheerplug-in voor Kaspersky Endpoint Security 11 voor Windows biedt ondersteuning voor het beheer van de vorige versie van Kaspersky Endpoint Security 11 voor Windows op computers van gebruikers.
- U kunt de nieuwe versie van de Beheerplug-in gebruiken om de instellingen te wijzigen in een beleid, taak of ander item die door de vorige versie van de Beheerplug-in zijn gemaakt.
- De nieuwe versie van de Beheerplug-in wijst standaardwaarden aan de nieuwe instellingen toe wanneer een beleid, beleidsprofiel of taak voor het eerst wordt opgeslagen.

Na de upgrade van de Beheerplug-in is het aanbevolen om de waarden van de nieuwe instellingen in beleid en profielen te controleren en op te slaan. Als u dit niet doet, worden standaardwaarden toegewezen aan de nieuwe groepen van Kaspersky Endpoint Security-instellingen op de computer van de gebruiker en kunnen deze groepen worden bewerkt (het kenmerk ) . Het is aanbevolen om eerst de instellingen van beleid en beleidsprofielen op het hoogste niveau in de hiërarchie te controleren. U wordt ook aanbevolen om het gebruikersaccount te gebruiken dat toegangsrechten voor alle functionele onderdelen van Kaspersky Security Center heeft.

Voor meer informatie over de nieuwe mogelijkheden van het programma raadpleegt u de Releaseopmerkingen of de [Help van het programma](#).

- Als een nieuwe parameter is toegevoegd aan een groep instellingen in de nieuwe versie van de Beheerplug-in, is de eerder gedefinieerde status van het kenmerk  /  voor deze groep instellingen niet gewijzigd.
- Bij het upgraden van de beheerplug-in naar versie 11.2.0, moet u een beleid openen om het automatisch te converteren. Wanneer u dit doet, vraagt Kaspersky Endpoint Security u om bevestiging om deel te nemen aan KSN. Als u het programma al hebt bijgewerkt naar versie 11.20 op de computers van uw organisatie, wordt deelname aan KSN uitgeschakeld totdat u de voorwaarden voor deelname aan KSN accepteert.



## Bijzondere aandachtspunten bij het gebruik van geëncrypte protocollen voor interactie met externe services

Kaspersky Endpoint Security en Kaspersky Security Center gebruiken een versleuteld communicatiekanaal met TLS (Transport Layer Security) om met externe services van Kaspersky te werken. Kaspersky Endpoint Security gebruikt externe services voor de volgende functies:

- databases en softwaremodules van het programma updaten;
- activatie van het programma met een activatiecode (activatie 2.0);
- het gebruik van Kaspersky Security Network.

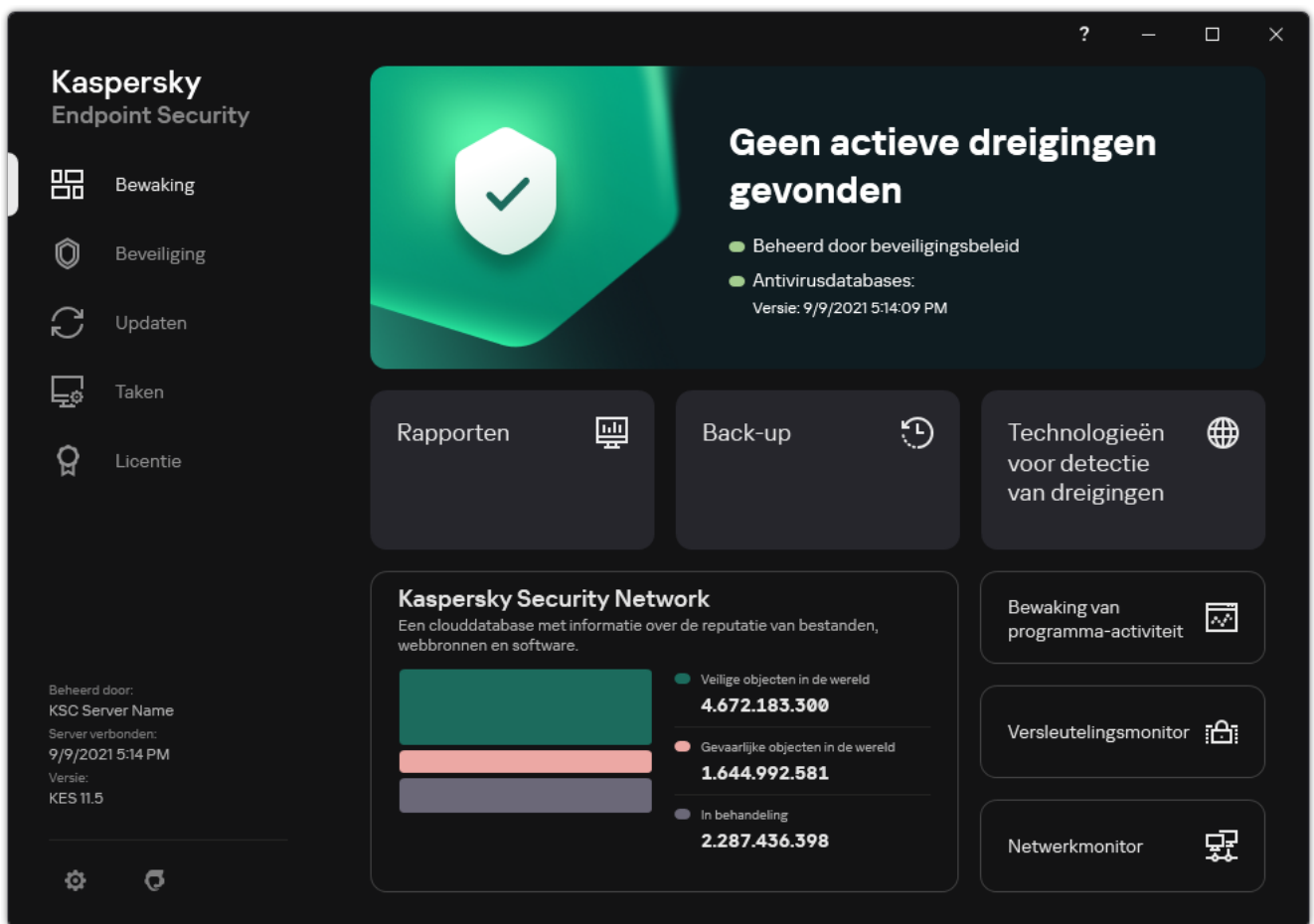
Gebruik van TLS beveiligt het programma door de volgende functies te bieden:

- Encryptie. De inhoud van berichten is vertrouwelijk en wordt niet bekendgemaakt aan externe gebruikers.
- Integriteit. De ontvanger van het bericht heeft de zekerheid dat de inhoud van het bericht niet is gewijzigd sinds het bericht is doorgestuurd door de afzender.
- Authenticatie. De ontvanger heeft de zekerheid dat communicatie alleen tot stand komt met een vertrouwde Kaspersky-server.

Kaspersky Endpoint Security gebruikt openbare-sleutelcertificaten voor serververificatie. Voor het werken met certificaten is een openbare sleutelinfrastructuur (Public Key Infrastructure (PKI)) vereist. Een certificaatautoriteit maakt deel uit van een PKI. Kaspersky gebruikt zijn eigen certificaatautoriteit omdat Kaspersky-services zeer technisch en niet openbaar zijn. In dit geval, wanneer rootcertificaten van Thawte, VeriSign, GlobalTrust en andere worden ingetrokken, blijft de Kaspersky PKI zonder onderbrekingen operationeel.

Omgevingen met MITM (software- en hardwaretools die het parseren van het HTTPS-protocol ondersteunen) worden door Kaspersky Endpoint Security als onveilig beschouwd. Er kunnen fouten optreden bij het werken met Kaspersky-services. Er kunnen bijvoorbeeld fouten optreden bij het gebruik van zelfondertekende certificaten. Deze fouten kunnen optreden omdat een HTTPS-inspectietool uit uw omgeving de Kaspersky PKI niet herkent. U kunt dit verhelpen door [uitsluitingen voor interactie met externe services te configureren](#).

## Programma-interface



Het hoofdvenster van het programma

## Bewaking

- **Rapporten.** Bekijk gebeurtenissen die zich hebben voorgedaan tijdens het gebruik van de applicatie, individuele componenten en taken.
- **Back-up.** Bekijk een lijst van opgeslagen kopieën van geïnfecteerde bestanden die het programma heeft verwijderd.
- **Technologieën voor detectie van dreigingen.** Bekijk informatie over technologieën voor detectie van dreigingen en het aantal bedreigingen dat door deze technologieën is gedetecteerd.
- **Kaspersky Security Network.** Status van de verbinding tussen Kaspersky Endpoint Security en Kaspersky Security Network, en globale KSN-statistieken. *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 dreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. Als u deelneemt aan Kaspersky Security Network, ontvangt Kaspersky Endpoint Security van de KSN-services informatie over de categorie en reputatie van gescande bestanden, alsook informatie over de reputatie van gescande webadressen.
- **Bewaking van programma-activiteit.** Bekijk informatie over de werking van geïnstalleerde applicaties. Systeembewaking houdt de bestands-, register- en besturingssysteemgebeurtenissen voor een programma.
- **Netwerkmonitor.** [Bekijk informatie over de netwerkactiviteit van de computer](#) in realtime.

|   |   |
|---|---|
|   | <ul style="list-style-type: none"> <li>• <b>Versleutelingsmonitor.</b> Bewaakt het encryptie- of decryptieproces van de schijf in realtime. Versleutelingsmonitor is beschikbaar als het onderdeel Kaspersky Disk Encryption of BitLocker-stationsversleuteling is geïnstalleerd.</li> </ul>  |
| <b>Beveiliging</b>  | Bedrijfsstatus van geïnstalleerde componenten. U kunt ook onderdelen configureren of rapporten bekijken.  |
| <b>Updaten</b>  | Updatetaken van Kaspersky Endpoint Security beheren. U kunt <a href="#">antivirusdatabases en programmamodules bijwerken en de laatste update terugdraaien</a> . Een beheerder kan <a href="#">het gedeelte verbergen voor de gebruiker</a> of <a href="#">het taakbeheer beperken</a> .  |
| <b>Taken</b>  | Scantaken van Kaspersky Endpoint Security beheren. U kunt een <a href="#">virusscan</a> en een <a href="#">applicatie-integriteitscontrole uitvoeren</a> . Een beheerder kan <a href="#">taken verbergen voor een gebruiker</a> of <a href="#">het beheer van taken beperken</a> .  |
| <b>Licentie</b>   | Licentiebeheer van het programma. U kunt <a href="#">een licentie kopen</a> , <a href="#">het programma activeren</a> of <a href="#">een abonnement verlengen</a> . U kunt ook <a href="#">informatie over de huidige licentie bekijken</a> .   |
|  | Programma-instellingen configureren Een beheerder kan <a href="#">wijzigingen in instellingen in Kaspersky Security Center verbieden</a> .  |
|  | Informatie over het programma: huidige versie van Kaspersky Endpoint Security, releasedatum van de database, sleutel en andere informatie. U kunt ook naar de informatiebronnen van Kaspersky gaan voor nuttige informatie, aanbevelingen en antwoorden op veelgestelde vragen over de aankoop, installatie en het gebruik van het programma. |
|  | Berichten met informatie over beschikbare updates en aanvraag voor toegang tot geëncrypte bestanden en apparaten.   |





## 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.

Het pictogram van het programma kan de volgende status hebben om informatie over de werking te geven:

- Het pictogram  betekent dat alle kritieke beschermingsonderdelen van het programma zijn ingeschakeld. Kaspersky Endpoint Security geeft een waarschuwing  weer als de gebruiker bijvoorbeeld een actie moet uitvoeren, zoals de computer opnieuw opstarten na het updaten van het programma.
- Het pictogram  geeft aan dat kritisch belangrijke beschermingsonderdelen van het programma uitgeschakeld of defect zijn. Beschermingsonderdelen kunnen bijvoorbeeld een storing ondervinden als de licentie is verlopen of als gevolg van een programmafout. Kaspersky Endpoint Security geeft een waarschuwing  met een beschrijving van het probleem met computerbeveiliging.

Het contextmenu van het programmapictogram bevat de volgende opties:

- **Kaspersky Endpoint Security voor Windows.** Deze optie opent het hoofdvenster van het programma. In dit venster kunt u de werking van programmaonderdelen en -taken aanpassen en kunt u de statistieken over verwerkte bestanden en gedetecteerde dreigingen bekijken.

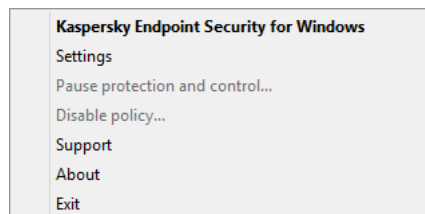
- **Bescherming pauzeren / Bescherming hervatten.** Pauzeer de werking van alle beschermings- en controleonderdelen die niet zijn gemarkeerd met een hangslot (🔒) in het beleid. U wordt aanbevolen het Kaspersky Security Center-beleid uit te schakelen alvorens deze bewerking uit te voeren.

Voordat het programma de werking van beschermings- en controleonderdelen pauzeert, wordt [wachtwoord voor de toegang tot Kaspersky Endpoint Security](#) gevraagd (wachtwoord van account of tijdelijk wachtwoord). U kunt dan selecteren hoelang de pauze moet duren: een specifieke periode, tot de herstart of op verzoek van de gebruiker.

Dit contextmenu is beschikbaar als [Wachtwoordbeveiliging is ingeschakeld](#). Als u de werking van beschermings- en controleonderdelen wilt hervatten, klikt u op **Bescherming hervatten** in het contextmenu van het programma.

Het pauzeren van de werking van beschermings- en controleonderdelen is niet van invloed op de prestaties van update- en scantaken. Het programma blijft ook Kaspersky Security Network gebruiken.

- **Beleid uitschakelen / Beleid inschakelen.** Hiermee schakelt u een Kaspersky Security Center-beleid op de computer uit. Alle Kaspersky Endpoint Security-instellingen kunnen worden geconfigureerd, inclusief instellingen met een gesloten hangslot in het beleid (🔒). Als het beleid is uitgeschakeld, dan vraagt het programma het [wachtwoord voor toegang tot Kaspersky Endpoint Security](#) (accountwachtwoord of tijdelijk wachtwoord). Dit contextmenu is beschikbaar als [Wachtwoordbeveiliging is ingeschakeld](#). Als u het beleid wilt inschakelen, selecteert u **Beleid inschakelen** in het contextmenu van het programma.
- **Instellingen.** Opent het venster met de programma-instellingen.
- **Support.** Hiermee opent u een venster met noodzakelijke informatie om contact op te nemen met de Technische Support van Kaspersky.
- **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.



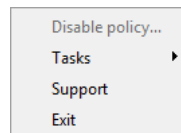
Contextmenu van het programmapictogram

## Vereenvoudigde programma-interface

Als een Kaspersky Security Center-beleid dat is geconfigureerd om [de vereenvoudigde programma-interface weer te geven](#) wordt toegepast op een clientcomputer waarop Kaspersky Endpoint Security is geïnstalleerd, is het hoofdvenster van het programma niet beschikbaar op deze clientcomputer. Klik rechts om het contextmenu van het Kaspersky Endpoint Security-pictogram te openen (zie afbeelding hieronder). U ziet de volgende opties:

- **Beleid uitschakelen / Beleid inschakelen.** Hiermee schakelt u een Kaspersky Security Center-beleid op de computer uit. Alle Kaspersky Endpoint Security-instellingen kunnen worden geconfigureerd, inclusief instellingen met een gesloten hangslot in het beleid (🔒). Als het beleid is uitgeschakeld, dan vraagt het programma het [wachtwoord voor toegang tot Kaspersky Endpoint Security](#) (accountwachtwoord of tijdelijk wachtwoord). Dit contextmenu is beschikbaar als [Wachtwoordbeveiliging is ingeschakeld](#). Als u het beleid wilt inschakelen, selecteert u **Beleid inschakelen** in het contextmenu van het programma.

- **Taken.** Vervolgkeuzelijst met de volgende opties:
  - Integriteitscontrole.
  - Vorige versie van databases terugdraaien.
  - Volledige Scan.
  - Selectieve Scan.
  - Kritieke Gebiedenscan.
  - Database updaten.
- **Support.** Hiermee opent u een venster met noodzakelijke informatie om contact op te nemen met de Technische Support van Kaspersky.
- **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 wanneer de vereenvoudigde interface wordt gebruikt

## De weergave van de programma-interface configureren

U kunt de weergavemodus van de programma-interface voor een gebruiker configureren. De gebruiker kan op de volgende manieren met het programma communiceren:

- **With simplified interface.** Op een clientcomputer is het hoofdvenster van het programma niet toegankelijk en is alleen het [pictogram in het Windows-systeemvak](#) beschikbaar. Via het contextmenu van het pictogram kan de gebruiker [een beperkt aantal bewerkingen met Kaspersky Endpoint Security uitvoeren](#). Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.
- **With full interface.** Op een clientcomputer zijn het hoofdvenster van Kaspersky Endpoint Security en het [pictogram in het Windows-systeemvak](#) beschikbaar. Via het contextmenu van het pictogram kan de gebruiker bewerkingen met Kaspersky Endpoint Security uitvoeren. Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.
- **No interface.** Op een clientcomputer wordt de werking van Kaspersky Endpoint Security niet aangegeven. Het [pictogram in het Windows-systeemvak](#) en de meldingen zijn niet beschikbaar.

[De weergavemodus van de programma-interface configureren in de beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Polities**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
6. Doe in het blok **Interactie met gebruiker** een van het volgende:
  - Schakel het selectievakje **Gebruikersinterface weergeven** in als u de volgende interface-elementen wilt weergeven op de clientcomputer:
    - Map met de programmaam in het menu **Start**
    - [Kaspersky Endpoint Security-pictogram](#) in het systeemvak van de taakbalk in Microsoft Windows
    - Pop-upmeldingen
  - Als dit selectievakje is ingeschakeld, kan de geselecteerde gebruiker programma-instellingen in de programma-interface zien en, afhankelijk van diens rechten, wijzigen.
  - Schakel het selectievakje **Gebruikersinterface weergeven** uit als u alle tekenen van Kaspersky Endpoint Security op de clientcomputer wilt verbergen.
7. Schakel in het blok **Interactie met gebruiker** het selectievakje **Vereenvoudigde interface weergeven** in als u de [vereenvoudigde programma-interface](#) wilt weergeven op een clientcomputer waarop Kaspersky Endpoint Security is geïnstalleerd.

[De weergavemodus van de applicatie-interface configureren in de webconsole en cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Interface**.
5. Configureer in het blok **Interaction with user** hoe de programma-interface wordt weergegeven:
  - **With simplified interface.** Op een clientcomputer is het hoofdvenster van het programma niet toegankelijk en is alleen het [pictogram in het Windows-systeemvak](#) beschikbaar. Via het contextmenu van het pictogram kan de gebruiker [een beperkt aantal bewerkingen met Kaspersky Endpoint Security uitvoeren](#). Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.
  - **With full interface.** Op een clientcomputer zijn het hoofdvenster van Kaspersky Endpoint Security en het [pictogram in het Windows-systeemvak](#) beschikbaar. Via het contextmenu van het pictogram kan de gebruiker bewerkingen met Kaspersky Endpoint Security uitvoeren. Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.
  - **No interface.** Op een clientcomputer wordt de werking van Kaspersky Endpoint Security niet aangegeven. Het [pictogram in het Windows-systeemvak](#) en de meldingen zijn niet beschikbaar.
6. Sla uw wijzigingen op.

## Aan de slag

Na de implementatie van het programma op clientcomputers moet u de volgende acties uitvoeren als u met Kaspersky Endpoint Security wilt werken via Webconsole van Kaspersky Security Center:

- Maak en configureer een beleid.  
U kunt een beleid gebruiken om identieke instellingen van Kaspersky Endpoint Security toe te passen op alle clientcomputers in een beheergroep. De wizard Snelle start van Kaspersky Security Center maakt automatisch een beleid voor Kaspersky Endpoint Security.
- Maak de taken *Updaten* en *Virusscan*.  
De taak *Updaten* is vereist om de beveiliging van de computer up-tot-date te houden. Wanneer de taak wordt uitgevoerd, [worden de antivirusdatabases en programmamodules geüpdatet](#) door Kaspersky Endpoint Security. De taak *Updaten* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center. Voor het maken van de taak *Updaten* installeert u de webplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.  
De taak *Virusscan* is vereist voor de tijdige detectie van virussen en andere malware. U moet de taak *Virusscan* handmatig aanmaken.

[Een virusscantaak maken in de Beheerconsole \(MMC\)](#) 

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security for Windows (11.9.0) Virusscan**.

## Stap 2. Scanbereik

De lijst maken met objecten die Kaspersky Endpoint Security scant wanneer het een scantaak uitvoert.

## Stap 3: Actie van Kaspersky Endpoint Security

Kies de actie bij de detectie van een dreiging:

- **Desinfecteren of verwijderen als desinfectie mislukt.** Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.
- **Desinfecteren of melden als desinfectie mislukt.** Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.
- **Melden.** Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security de informatie over geïnfecteerde bestanden toe aan de lijst met actieve dreigingen wanneer deze bestanden worden gedetecteerd.
- **Geavanceerde desinfectie direct uitvoeren.** Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security de geavanceerde desinfectietechnologie om actieve dreigingen tijdens de scan te behandelen.

De *geavanceerde desinfectietechnologie* dient om schadelijke 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 dreiging 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. Na het uitvoeren van de geavanceerde desinfectie start Kaspersky Endpoint Security de computer opnieuw op zonder de gebruiker om bevestiging te vragen.

Configureer de taakuitmodus met behulp van **Run only when the computer is idle**. Dit selectievakje schakelt de functie in of uit waarmee u de *virusscantaak* uitstelt als de computerbronnen beperkt zijn. Kaspersky Endpoint Security pauzeert de *virusscantaak* als de schermbeveiliging uitgeschakeld is en de computer ontgrendeld is.

## Stap 4: De apparaten selecteren waaraan de taak zal worden toegewezen



Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

### Stap 5: Het account selecteren om de taak uit te voeren

Selecteer een account om de *virusscantaak* uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount. Als het scanbereik netwerkstations of andere objecten met beperkte toegang omvat, selecteert u een gebruikersaccount met voldoende toegangsrechten.

### Stap 6. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of nadat antivirusdatabases zijn gedownload naar de opslagplaats.

### Stap 7. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Dagelijkse volledige scan*.

### Stap 8. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. De taak Virusscan wordt volgens het opgegeven schema uitgevoerd op de computers van de gebruikers.

[Een virusscantaak maken in de webconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Virusscan**.

c. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Wekelijkse scan*.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Ga naar de volgende stap.

5. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de lijst met taken.

6. Ga naar de taakeigenschappen om het schema van de taak te configureren.

U wordt aanbevolen een schema voor de taak in te stellen zodat deze ten minste één keer per week wordt uitgevoerd.

7. Schakel het selectievakje naast de taak in.

8. Klik op de knop **Run**.

U kunt de status van de taak monitoren en kunt het aantal apparaten zien waarop de taak met succes of met een fout is voltooid.

De taak Virusscan wordt volgens het opgegeven schema uitgevoerd op de computers van de gebruikers.

## Beleid beheren

Een *beleid* is een verzameling van programma-instellingen die voor een beheergroep zijn gedefinieerd. U kunt meer dan één beleid configureren met verschillende waarden voor een programma. Een programma kan met verschillende instellingen voor verschillende beheergroepen worden uitgevoerd. Elke beheergroep kan een eigen beleid voor een programma hebben.

De netwerkagent verstuurt tijdens de *synchronisatie* de beleidsinstellingen naar de clientcomputers. Standaard voert Administration Server de synchronisatie meteen na de wijziging van de beleidsinstellingen uit. Voor de synchronisatie wordt UDP-poort 15000 op de clientcomputer gebruikt. De Administration Server voert standaard elke 15 minuten een synchronisatie uit. Als de gewijzigde beleidsinstellingen niet kunnen worden gesynchroniseerd, wordt een nieuwe synchronisatiepoging ondernomen volgens het geconfigureerde schema.

### Actief en inactief beleid

Een beleid is bedoeld voor een groep beheerde computers en kan actief of inactief zijn. De instellingen van een actief beleid worden tijdens de synchronisatie opgeslagen op de clientcomputers. U kunt maximaal één beleid tegelijk toepassen op een computer. Daarom kan slechts één beleid in elke groep actief zijn.

U kunt meer dan één inactief beleid maken. Een inactief beleid is niet van invloed op programma-instellingen op computers in het netwerk. Een inactief beleid is bedoeld als voorbereiding op noodsituaties, zoals een virusaanval. Als er bijvoorbeeld een aanval via een flashstation wordt uitgevoerd, kunt u een beleid activeren dat de toegang tot flashstations blokkeert. In dit geval wordt het actieve beleid automatisch inactief.

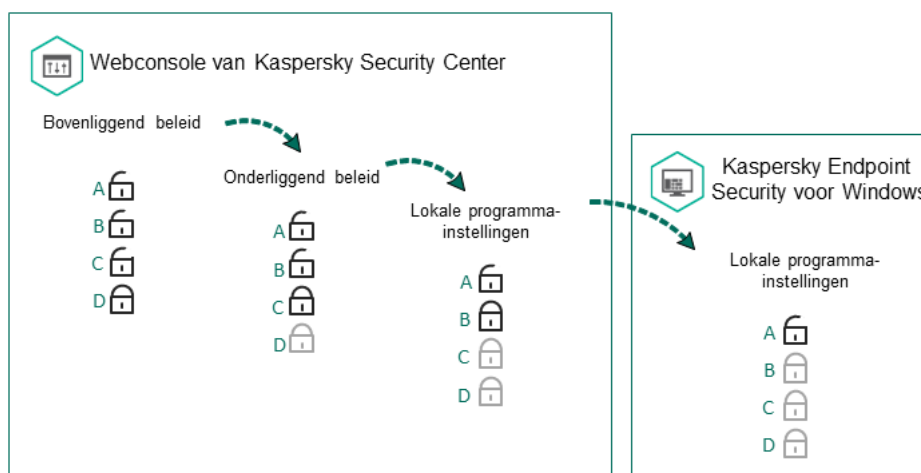
## Afwezigheidsbeleid

Een afwezigheidsbeleid wordt geactiveerd wanneer de computer niet meer verbonden is met het bedrijfsnetwerk.

## Overname van instellingen

Beleid is, net als beheergroepen, in een hiërarchie gerangschikt. Standaard neemt een onderliggend beleid instellingen over van het bovenliggende beleid. Een *onderliggend beleid* is een beleid voor geneste hiërarchieniveaus, dat een beleid is voor geneste beheergroepen en secundaire Administration Servers. U kunt het overnemen van instellingen van het bovenliggende beleid uitschakelen.

Elke beleidsinstelling heeft het kenmerk  dat aangeeft of deze instelling kan worden gewijzigd in het onderliggende beleid of in de [lokale programma-instellingen](#). Het kenmerk  is alleen van toepassing als de overname van de bovenliggende beleidsinstellingen is ingeschakeld voor het onderliggende beleid. Een afwezigheidsbeleid is niet van invloed op een ander beleid in de hiërarchie van beheergroepen.



Overname van instellingen




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.


## Een beleid aanmaken

[Een beleid maken in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de map **Managed devices** 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 **Polities**.
4. Klik op de knop **Nieuw beleid**.  
De wizard Beleid wordt gestart.
5. Volg de instructies van de wizard Beleid.

[Een beleid maken in de Webconsole en de Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de knop **Add**.  
De wizard Beleid wordt gestart.
3. Selecteer Kaspersky Endpoint Security en klik op **Volgende**.
4. Lees en accepteer de voorwaarden van de Kaspersky Security Network-verklaring (KSN) en klik op **Volgende**.
5. Op het tabblad **Algemeen** kunt u de volgende acties uitvoeren:
  - Wijzig de naam van het beleid.
  - Selecteer de status van het beleid:
    - **Actief**. Na de volgende synchronisatie wordt het beleid gebruikt als het actieve beleid op de computer.
    - **Inactief**. Back-upbeleid. Een inactief beleid kan indien nodig worden geactiveerd.
    - **Afwezig**. Het beleid wordt geactiveerd wanneer de computer niet meer verbonden is met het bedrijfsnetwerk.
  - Configureer de overname van instellingen:
    - **Instellingen van bovenliggend beleid overnemen**. Als deze schakelaar is ingeschakeld, worden de waarden voor de beleidsinstellingen van het hoogste beleid in hiërarchie overgenomen. De beleidsinstellingen kunnen niet worden bewerkt als  is ingesteld voor het bovenliggende beleid.
    - **Overname van instellingen in onderliggend beleid verplichten**. Als de schakelaar is ingeschakeld, worden de waarden van de beleidsinstellingen doorgegeven aan een onderliggend beleid. In de eigenschappen van het onderliggende beleid wordt de schakelaar **Instellingen van bovenliggend beleid overnemen** automatisch aangezet en kan deze niet worden uitgezet. Instellingen van een onderliggend beleid worden overgenomen van het bovenliggende beleid, behalve voor de instellingen met de markering . Instellingen van een onderliggend beleid kunnen niet worden bewerkt als  is ingesteld voor het bovenliggende beleid.
6. U kunt op het tabblad **Programma-instellingen** de [beleidsinstellingen voor Kaspersky Endpoint Security](#) configureren.
7. Sla uw wijzigingen op.

De instellingen van Kaspersky Endpoint Security zullen tijdens de volgende synchronisatie worden geconfigureerd op clientcomputers. U kunt informatie bekijken over het beleid dat op de computer wordt toegepast in de interface van Kaspersky Endpoint Security door op de knop  op het hoofdscherm te klikken (bijvoorbeeld de beleidsnaam). Hiervoor moet u in de instellingen van het Network Agent-beleid de ontvangst van uitgebreide beleidsgegevens inschakelen. Voor meer informatie over een Network Agent-beleid raadpleegt u de [Help van Kaspersky Security Center](#) .

Indicator voor beschermingsniveau

De indicator voor het beschermingsniveau wordt boven in het venster **Eigenschappen: <naam van beleid>** weergegeven. De indicator kan een van de volgende waarden hebben:

- **Hoog beschermingsniveau.** De indicator heeft deze waarde en wordt groen als alle onderdelen uit de volgende categorieën zijn ingeschakeld:
  - **Kritiek.** Deze categorie bevat de volgende onderdelen:
    - File Threat Protection.
    - Gedragsdetectie.
    - Exploit-preventie.
    - Remediation Engine.
  - **Belangrijk.** Deze categorie bevat de volgende onderdelen:
    - Kaspersky Security Network.
    - Web Threat Protection.
    - Mail Threat Protection.
    - Host Intrusion Prevention.
- **Gemiddeld beschermingsniveau.** De indicator heeft deze waarde en wordt geel als een van de belangrijke onderdelen is uitgeschakeld.
- **Laag beschermingsniveau.** De indicator heeft deze waarde en wordt rood in een van de volgende gevallen:
  - Een of meer essentiële onderdelen zijn uitgeschakeld.
  - Twee of meer belangrijke onderdelen zijn uitgeschakeld.

Als de indicator voor **Gemiddeld beschermingsniveau** of **Laag beschermingsniveau** wordt weergegeven, ziet u rechts van de indicator een link die het venster **Aanbevolen beschermingsonderdelen**. In dit venster kunt u de aanbevolen beschermingsonderdelen inschakelen.

## Taakbeheer

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 selectie van computers.

U kunt een willekeurig aantal groepstaken, taken voor een selectie van computers of lokale taken maken. Voor meer informatie over het werken met beheergroepen en selecties van computers raadpleegt u de [Help van Kaspersky Security Center](#).

Kaspersky Endpoint Security ondersteunt de volgende taken:

- **Virusscan**. Kaspersky Endpoint Security scant de in de taakinstellingen opgegeven computergebieden op virussen en andere dreigingen. De taak *Virusscan* is vereist voor de werking van Kaspersky Endpoint Security en wordt tijdens de wizard Snelle start gemaakt. U wordt aanbevolen [een schema voor de taak in te stellen](#) zodat deze ten minste één keer per week wordt uitgevoerd.
- **Licentie toevoegen**. Kaspersky Endpoint Security voegt een licentie voor de activering van programma's toe, waaronder een extra licentie. Voordat u de taak uitvoert, moet u ervoor zorgen dat het aantal computers waarop u de taak wilt uitvoeren niet hoger is dan het aantal computers dat door de licentie is toegestaan.
- **Programmaonderdelen wijzigen**. Kaspersky Endpoint Security installeert of verwijdert onderdelen op clientcomputers volgens de lijst met onderdelen die in de taakinstellingen is opgegeven. Het onderdeel File Threat Protection kan niet worden verwijderd. De optimale reeks Kaspersky Endpoint Security-onderdelen zorgt ervoor dat voldoende computerbronnen worden behouden.
- **Inventarisatie**. Kaspersky Endpoint Security ontvangt informatie over alle uitvoerbare bestanden van programma's die op computers zijn opgeslagen. De taak *Inventarisatie* wordt door het onderdeel Programmacontrole uitgevoerd. Als het onderdeel Programmacontrole is niet geïnstalleerd, eindigt de taak met een fout.
- **Updaten**. Kaspersky Endpoint Security updatet databases en programmamodules. De taak *Updaten* is vereist voor de werking van Kaspersky Endpoint Security en wordt tijdens de wizard Snelle start gemaakt. U wordt aanbevolen een schema te configureren dat de taak ten minste één keer per dag uitvoert.
- **Gegevens wissen**. Kaspersky Endpoint Security verwijdert bestanden en mappen van de computers van gebruikers onmiddellijk of als er al lange tijd geen verbinding met Kaspersky Security Center is gemaakt.
- **Update terugdraaien**. Kaspersky Endpoint Security draait de laatste update van de databases en programmamodules terug. Dit kan noodzakelijk zijn als de nieuwe databases bijvoorbeeld onjuiste gegevens bevatten die ervoor kunnen zorgen dat Kaspersky Endpoint Security een veilig programma blokkeert.
- **Integriteitscontrole**. Kaspersky Endpoint Security analyseert programmabestanden, controleert bestanden op beschadiging of wijzigingen en verifieert de digitale handtekeningen van programmabestanden.
- **Accounts voor Authenticatie-agent beheren**. Kaspersky Endpoint Security configureert de accountinstellingen van de Authenticatie-agent. Er is een Authenticatie-agent nodig om met geëncrypte schijven te werken. Voordat het besturingssysteem wordt geladen, moet de gebruiker de authenticatie bij de agent voltooien.

Taken worden pas op een computer uitgevoerd als [Kaspersky Endpoint Security actief is](#).

## Een nieuwe taak toevoegen

### [Een taak maken in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer de map **Taken** in de structuur van de Beheerconsole.
3. Klik op de knop **Nieuwe taak**.  
De wizard Taak wordt gestart.
4. Volg de instructies van de wizard Taak.


## Een taak maken in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de knop **Add**.  
De wizard Taak wordt gestart.
3. Configureer de taakinstellingen:
  - a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.
  - b. Selecteer in de vervolgkeuzelijst **Taaktype** de taak die u wilt uitvoeren op computers van gebruikers.
  - c. Typ in het veld **Task name** een korte omschrijving.
  - d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.
4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Ga naar de volgende stap.
5. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de lijst met taken. De taak heeft de standaardinstellingen. Ga naar de taakeigenschappen om de taakinstellingen te configureren. Als u een taak wilt starten, moet u het selectievakje naast de taak inschakelen en op de knop **Starten** klikken. Nadat de taak is gestart, kunt u de taak onderbreken en later hervatten.

In de lijst met taken kunt u de resultaten van de taak monitoren. Deze resultaten bevatten de status van de taak en de statistieken over de uitvoering van de taak op computers. U kunt ook een selectie van gebeurtenissen maken om de voltooiing van taken te monitoren (**Monitoring en rapportage** → **Selecties van gebeurtenissen**). Voor meer informatie over selecties van gebeurtenissen raadpleegt u de [Help van Kaspersky Security Center](#) . De resultaten van de taak worden ook lokaal opgeslagen in het Windows-gebeurtenislogboek en in [rapporten van Kaspersky Endpoint Security](#).

## Toegangsbeheer voor taken

De rechten voor de toegang 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 Kaspersky Security Center Administration Server. Voor meer informatie over taakbeheer via Kaspersky Security Center raadpleegt u de [Help van Kaspersky Security Center](#) .

U kunt gebruikersrechten voor toegang tot taken configureren met behulp van beleid (*taakbeheermodus*). U kunt bijvoorbeeld groepstaken verbergen in de Kaspersky Endpoint Security-interface.

## [De taakbeheermodus configureren in de Kaspersky Endpoint Security-interface via de Beheerconsole \(MMC\)](#)



1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het beleidsvenster **Lokale taken** → **Taakbeheer**.
6. Configureer de taakbeheermodus (zie onderstaande tabel).
7. Sla uw wijzigingen op.

### [De taakbeheermodus configureren in de Kaspersky Endpoint Security-interface via de webconsole](#)


1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Lokale taken** → **Taakbeheer**.
5. Configureer de taakbeheermodus (zie onderstaande tabel).
6. Sla uw wijzigingen op.

#### Instellingen van Taakbeheer

| Parameter                                | Beschrijving   |
|--|--|
| <b>Gebruik van lokale taken toestaan</b> | <p>Als het selectievakje is ingeschakeld, worden lokale taken in de lokale interface van Kaspersky Endpoint Security weergegeven. Wanneer er geen aanvullende beleidsbeperkingen zijn, kan de gebruiker taken configureren en starten. Het configureren van het taakuitvoerschema blijft echter onbeschikbaar voor de gebruiker. De gebruiker kan taken alleen handmatig uitvoeren.</p> <p>Als het selectievakje is uitgeschakeld, wordt het gebruik van lokale taken gestopt. In deze modus worden de lokale taken niet volgens het schema uitgevoerd. Taken kunnen niet in de lokale interface van Kaspersky Endpoint Security of via de opdrachtregel worden gestart of geconfigureerd.</p> <p>Een gebruiker kan wel een virusscan van een bestand of een map starten door de optie <b>Scannen op virussen</b> in het contextmenu van het bestand of de map te selecteren. De scantaak wordt met de standaardwaarden van de instellingen voor de aangepaste scantaak gestart.</p> |
| <b>Weergave van groepstaken toestaan</b> | <p>Als het selectievakje is ingeschakeld, worden groepstaken in de lokale interface van Kaspersky Endpoint Security weergegeven. De gebruiker kan de lijst met alle taken in de programma-interface bekijken.</p>  |

|  |   |
|--|---|
|  | Als het selectievakje is uitgeschakeld, geeft Kaspersky Endpoint Security een lege takenlijst weer.   |
| <b>Beheer van groepstaken toestaan</b> | <p>Als het selectievakje is ingeschakeld, kunnen gebruikers groepstaken starten en stoppen die zijn opgegeven in Kaspersky Security Center. Gebruikers kunnen taken starten en stoppen in de programma-interface of in de vereenvoudigde programma-interface.</p> <p>Als het selectievakje is uitgeschakeld, start Kaspersky Endpoint Security automatisch geplande taken of start de beheerder taken handmatig in Kaspersky Security Center.</p> |

## Lokale programma-instellingen configureren

In Kaspersky Security Center kunt u de instellingen van Kaspersky Endpoint Security voor een bepaalde computer configureren. Deze zijn de *lokale programma-instellingen*. Sommige instellingen zijn mogelijk niet beschikbaar voor bewerking. Deze instellingen zijn vergrendeld met het kenmerk  in de [beleidseigenschappen](#).

### [De lokale programma-instellingen configureren in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
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 Kaspersky Endpoint Security.
8. Klik op de knop **Eigenschappen** onder de lijst met Kaspersky-programma's.  
U ziet nu het venster **Instellingen van Kaspersky Endpoint Security voor Windows**.
9. Configureer in het gedeelte **Algemene instellingen** Kaspersky Endpoint Security en Rapporten en Opslag.  
De andere gedeeltes van het venster **Instellingen van Kaspersky Endpoint Security voor Windows** zijn standaard voor Kaspersky Security Center. Een beschrijving van deze gedeeltes vindt u in de Help 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 **Algemene instellingen** configureert.

10. Sla uw wijzigingen op.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Programma's**.
4. Klik op **Kaspersky Endpoint Security voor Windows**.  
U ziet nu de lokale programma-instellingen.
5. Selecteer het tabblad **Application settings**.
6. Configureer de lokale programma-instellingen.
7. Sla uw wijzigingen op.

Lokale programma-instellingen zijn identiek aan [beleidsinstellingen](#), behalve voor encryptie-instellingen.

## Kaspersky Endpoint Security starten en stoppen

Kaspersky Endpoint Security wordt na de installatie op de computer van een gebruiker automatisch gestart. Standaard wordt Kaspersky Endpoint Security na de opstart van het besturingssysteem gestart. Het is niet mogelijk om het automatisch opstarten van het programma in de instellingen van het besturingssysteem te configureren.


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. In het geval dat de antivirusdatabases worden gedownload wanneer Kaspersky Endpoint Security wordt gestart in een al opgestart besturingssysteem, is de computer niet minder beschermd.

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
6. Gebruik het selectievakje **Kaspersky Endpoint Security voor Windows starten bij opstart van computer** om de opstart van het programma te configureren.
7. Sla uw wijzigingen op.

### [Opstarten van Kaspersky Endpoint Security configureren in de webconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Programma-instellingen**.
5. Gebruik het selectievakje **Start Kaspersky Endpoint Security on computer startup (recommended)** om de opstart van het programma te configureren.
6. Sla uw wijzigingen op.

### [Opstarten van Kaspersky Endpoint Security configureren in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik het selectievakje **Kaspersky Endpoint Security voor Windows starten bij opstart van computer** om de opstart van het programma te configureren.
4. Sla uw wijzigingen op.

Kaspersky-experts raden aan dat u Kaspersky Endpoint Security niet handmatig stopt omdat u hierdoor de computer en uw persoonlijke gegevens blootstelt aan dreigingen. U kunt indien nodig de [computerbescherming pauzeren](#) zolang u dat wilt zonder het programma te stoppen.

U kunt de programmastatus volgen met de widget **Beveiligingsstatus**.

### [Kaspersky Endpoint Security starten of stoppen in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
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**.
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.
8. Doe het volgende:
  - Als u het programma wilt starten, klikt u op de knop  rechts van de lijst met Kaspersky-programma's:
  - Als u het programma wilt stoppen, klikt u op de knop  rechts van de lijst met Kaspersky-programma's:

### [Kaspersky Endpoint Security starten of stoppen in de webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Klik op de naam van de computer waarop u Kaspersky Endpoint Security wilt starten of stoppen.  
U ziet nu het venster met computereigenschappen.
3. Selecteer het tabblad **Programma's**.
4. Schakel het selectievakje naast **Kaspersky Endpoint Security voor Windows** in.
5. Klik op de knop **Starten** of **Stoppen**.

### [Kaspersky Endpoint Security starten of stoppen vanaf de opdrachtregel](#)

Om het programma via de opdrachtregel te stoppen, moet u [extern beheer van systeemservices inschakelen](#).



Het bestand 'klpsm.exe', dat bij het distributiepakket van Kaspersky Endpoint Security wordt meegeleverd, wordt gebruikt om het programma vanaf de opdrachtregel te starten of te stoppen.

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.
2. Ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.
3. Typ `klpsm.exe start_avp_service` om het programma vanaf de opdrachtregel te starten.
4. Om het programma vanaf de opdrachtregel te stoppen, typt u `klpsm.exe stop_avp_service`.

## 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 controleonderdelen 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 ingeschakeld.

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 **Bescherming pauzeren** (zie onderstaande afbeelding).

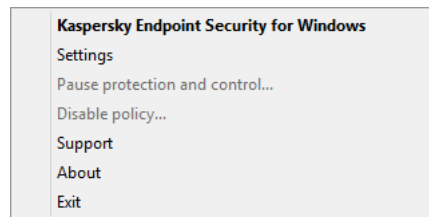
Dit contextmenu is beschikbaar als [Wachtwoordbeveiliging is ingeschakeld](#).

3. Selecteer één van de volgende opties:

- **Pauzeren gedurende <tijdsperiode>** - de bescherming en de controle van de computer worden na de gekozen tijd in de onderstaande vervolgkeuzelijst hervat.
- **Pauzeren tot de herstart van het programma**- de bescherming en de controle van de computer worden hervat nadat u het programma opnieuw hebt opgestart 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. Klik op **Bescherming pauzeren**.

Kaspersky Endpoint Security pauzeert de werking van alle beschermings- en controleonderdelen die niet zijn gemarkeerd met een hangslot (🔒) in het beleid. U wordt aanbevolen het Kaspersky Security Center-beleid uit te schakelen alvorens deze bewerking uit te voeren.



Contextmenu van het programmapictogram

*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 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.

## 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.  
Hiervoor 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Instellingen beheren** in het venster met de programma-instellingen.
3. Klik op **Exporteren**.
4. Geef in het geopende venster 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. Sla het bestand op.

*Zo importeert u de instellingen van Kaspersky Endpoint Security vanuit een configuratiebestand:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Instellingen beheren** in het venster met de programma-instellingen.
3. Klik op **Importeren**.
4. Geef in het venster dat wordt geopend het pad in naar het configuratiebestand.
5. Open het bestand.

Alle waarden van de instellingen van Kaspersky Endpoint Security worden overeenkomstig het geselecteerde configuratiebestand ingesteld.

## Standaardinstellingen van het programma herstellen

U kunt de instellingen die zijn aanbevolen door Kaspersky lab voor Endpoint Security op elk moment herstellen. Wanneer de instellingen zijn hersteld, wordt het **Aanbevolen** beveiligingsniveau ingesteld voor alle beschermingsonderdelen.

*De standaardinstellingen van het programma herstellen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Instellingen beheren** in het venster met de programma-instellingen.
3. Klik op **Terugzetten**.
4. Sla uw wijzigingen op.



# Virusscan van de computer

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.

Kaspersky Endpoint Security scant geen bestanden waarvan de inhoud zich in de OneDrive-cloudopslag bevindt en maakt logboekvermeldingen aan waarin staat dat deze bestanden niet zijn gescand.

## Volledige Scan

Een grondige scan van de hele computer. Kaspersky Endpoint Security scant 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

Kaspersky-experts raden u aan om het scanbereik van de taak *Volledige scan* niet te wijzigen.

Om het gebruik van computerbronnen te beperken, is het raadzaam om in plaats van een volledige scan een [achtergrondscanscan](#) uit te voeren. Dit is niet van invloed op het beveiligingsniveau van de computer.

## Kritieke Gebiedenscan

Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.

Kaspersky-experts raden u aan het scanbereik van de taak *Kritieke Gebiedenscan* niet te wijzigen.

## Aangepaste Scan

Kaspersky Endpoint Security scant de objecten die door de gebruiker worden geselecteerd. U kunt een willekeurig object uit de volgende lijst scannen:

- Systeemgeheugen
- Objecten die bij de opstart van het besturingssysteem worden geladen
- Back-up van het besturingssysteem

- Microsoft Outlook-mailbox
- Harde, verwisselbare en netwerkschijven
- Een geselecteerd bestand

## Achtergrondscan

Een *achtergrondscan* is een scanmodus van Kaspersky Endpoint Security waarin geen meldingen aan de gebruiker worden weergegeven. De achtergrondscan vereist minder computerbronnen dan andere scans (zoals een volledige scan). In deze modus scant Kaspersky Endpoint Security opstartobjecten, opstartsectoren, het systeemgeheugen en de systeempartitie.

## Integriteitscontrole

Kaspersky Endpoint Security controleert de programmamodules op beschadiging of wijzigingen.

## 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. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Kaspersky Endpoint Security heeft de vooraf gedefinieerde standaardtaken *Volledige Scan*, *Kritieke Gebiedenscan* en *Aangepaste Scan*. Als het Kaspersky Security Center-beheersysteem is geïmplementeerd in uw bedrijf, kunt u [een virusscantaak maken](#) en de scan configureren. De [taak \*Achtergrondscan\*](#) is ook beschikbaar in Kaspersky Security Center. De achtergrondscan kan niet worden geconfigureerd.

[Een virusscan starten via Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Taken**.
4. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.  
[Maak indien nodig een virusscantaak.](#)
5. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
6. Configureer de scantaak (zie onderstaande tabel).  
[Configureer indien nodig het schema voor de scantaak.](#)
7. Sla uw wijzigingen op.
8. Start de scantaak.

Kaspersky Endpoint Security begint met het scannen van de computer. Als de gebruiker de uitvoering van de taak heeft onderbroken (bijvoorbeeld door de computer uit te zetten), zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar de scan werd onderbroken.

### [Een virusscan starten via de Webconsole en Cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de scantaak.  
U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Configureer de scantaak (zie onderstaande tabel).  
[Configureer indien nodig het schema voor de scantaak.](#)
5. Sla uw wijzigingen op.
6. Start de scantaak.

Kaspersky Endpoint Security begint met het scannen van de computer. Als de gebruiker de uitvoering van de taak heeft onderbroken (bijvoorbeeld door de computer uit te zetten), zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar de scan werd onderbroken.

### [Een virusscan starten via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.

2. Selecteer de scantaak in de lijst met taken en klik op .

3. Configureer de scantaak (zie onderstaande tabel).

[Configureer indien nodig het schema voor de scantaak.](#)

4. Sla uw wijzigingen op.

5. Start de scantaak.

Kaspersky Endpoint Security begint met het scannen van de computer. De toepassing toont de voortgang van de scan, het aantal gescande bestanden en de resterende scantijd. U kunt de taak op elk moment stoppen door op de knop **Stoppen** te klikken. Als u de scantaak niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

#### Scaninstellingen

| Parameter                                  | Beschrijving  |
|--|---|
| <b>Beveiligingsniveau</b>                  | <p>Kaspersky Endpoint Security kan verschillende groepen van instellingen gebruiken om een scan uit te voeren. Deze groepen van instellingen die in het programma zijn opgeslagen, worden <i>beveiligingsniveaus</i> genoemd:</p> <ul style="list-style-type: none"><li>• <b>Hoog.</b> Kaspersky Endpoint Security scant alle soorten bestanden. Wanneer samengestelde bestanden worden gescand, scant Kaspersky Endpoint Security ook bestanden met een e-mailindeling.</li><li>• <b>Aanbevolen.</b> Kaspersky Endpoint Security scant alleen de opgegeven bestandsindelingen op alle harde schijven, netwerkschijven en verwisselbare schijven van de computer, evenals ingesloten OLE-objecten. Kaspersky Endpoint Security scant geen archieven of installatiepakketten.</li><li>• <b>Laag.</b> Kaspersky Endpoint Security scant alleen nieuwe of gewijzigde bestanden met de opgegeven extensies op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Kaspersky Endpoint Security scant geen samengestelde bestanden.</li></ul> <p>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.</p> |
| <b>Actie bij detectie van een dreiging</b> | <p><b>Desinfecteren of verwijderen als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.</p> <p><b>Desinfecteren of blokkeren als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.</p> <p><b>Melden.</b> Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security de informatie over geïnfecteerde bestanden toe aan de lijst met actieve dreigingen wanneer deze bestanden worden gedetecteerd.</p>   |

|  |  |
|--|--|
|  | <p>Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt Kaspersky Endpoint Security een reservekopie van het bestand voor het geval u <a href="#">het bestand moet herstellen of als het in de toekomst kan worden gedesinfecteerd</a>.</p> <p>Bij het vinden van geïnfecteerde bestanden die onderdeel zijn van het Windows Store-programma probeert Kaspersky Endpoint Security het bestand te wissen.</p>  |
| <p><b>Run Advanced Disinfection immediately</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p>Een geavanceerde desinfectie tijdens een virusscantaak op een computer wordt alleen uitgevoerd als de functie <a href="#">Geavanceerde desinfectie is ingeschakeld</a> in de eigenschappen van het beleid dat op deze computer is toegepast.</p> <p>Als het selectievakje is ingeschakeld, desinfecteert Kaspersky Endpoint Security de actieve infectie meteen na de detectie tijdens de uitvoering van de virusscantaak. Nadat de actieve infectie is gedesinfecteerd, start Kaspersky Endpoint Security de computer opnieuw op zonder dit aan de gebruiker te vragen.</p> <p>Als het selectievakje is uitgeschakeld, desinfecteert Kaspersky Endpoint Security de actieve infectie niet meteen na de detectie tijdens de uitvoering van de virusscantaak. Kaspersky Endpoint Security genereert gebeurtenissen over actieve infecties in de lokale programmarapporten en in Kaspersky Security Center. De actieve infectie kan worden gedesinfecteerd als de virusscantaak opnieuw wordt gestart wanneer de functie Geavanceerde desinfectie is ingeschakeld. Op deze manier kan de systeembeheerder het gepaste tijdstip voor de geavanceerde desinfectie kiezen en kan deze de computers daarna automatisch opnieuw opstarten.</p> |
| <p><b>Scanbereik</b></p>   | <p>Lijst met objecten die Kaspersky Endpoint Security scant wanneer het een scantaak uitvoert. Mogelijke objecten in het scanbereik zijn onder andere het kernelgeheugen, actieve processen, opstartsectoren, back-upopslag van het systeem, e-maildatabases, harde schijf, verwisselbare schijf, netwerkschijf, map of bestand.</p>   |
| <p><b>Planning van scan</b></p>  | <p><b>Handmatig.</b> Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt.</p> <p><b>Volgens schema.</b> In deze uitvoermodus voor scantaken wordt de scantaak door Kaspersky Endpoint Security gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten.</p>  |
| <p><b>Stel start na programmastart uit met N minuten</b></p>   | <p>Uitgestelde start van de scantaak na het starten van het programma. Bij de opstart van het besturingssysteem worden veel processen uitgevoerd. Daarom is het beter om de scantaak uit te stellen in plaats van deze meteen na het starten van Kaspersky Endpoint Security uit te voeren.</p>  |
| <p><b>Overgeslagen taken starten</b></p>   | <p>Als het selectievakje is ingeschakeld, wordt de overgeslagen scantaak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De scantaak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de scantaak. Als het selectievakje is uitgeschakeld, worden overgeslagen scantaken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende scantaak uit volgens het huidige schema.</p>   |

|   |  |
|---|--|
| <p><b>Alleen starten als de computer inactief is</b></p>                    | <p>Uitgestelde start van de scantaak wanneer computerbronnen bezet zijn. Kaspersky Endpoint Security start de scantaak als de computer vergrendeld wordt of als de schermbeveiliging is ingeschakeld. Als u de uitvoering van de taak hebt onderbroken door de computer bijvoorbeeld te ontgrendelen, zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar deze werd onderbroken.</p>  |
| <p><b>Scan starten namens</b></p>   | <p>Standaard wordt de scantaak uitgevoerd in naam van de gebruiker met wiens rechten u bent geregistreerd in het besturingssysteem. Het beschermingsbereik kan netwerkstations of andere objecten omvatten waarvoor speciale toegangsrechten vereist zijn. U kunt een gebruiker met de vereiste rechten opgeven in de instellingen van Kaspersky Endpoint Security en de scantaak onder dit gebruikersaccount uitvoeren.</p>   |
| <p><b>Bestandstypen</b></p>   | <div data-bbox="486 577 1493 734" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security beschouwt bestanden zonder extensie als uitvoerbare bestanden. Kaspersky Endpoint Security scant altijd uitvoerbare bestanden ongeacht de bestandstypen die u wilt laten scannen.</p> </div> <p><b>Alle bestanden.</b> Als deze instelling is ingeschakeld, worden alle bestanden gecontroleerd door Kaspersky Endpoint Security, zonder uitzondering (alle indelingen en extensies).</p> <p><b>Bestanden gescand op indeling.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.</p> <p><b>Bestanden gescand op extensie.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.</p> <p>Standaard scant Kaspersky Endpoint Security bestanden volgens indeling. Het scannen van bestanden volgens extensie is minder veilig omdat een schadelijk bestand een extensie kan hebben die niet voorkomt op de lijst met potentieel infecteerbare bestanden (bijvoorbeeld .123).</p> |
| <p><b>Scan alleen nieuwe en gewijzigde bestanden</b></p>                    | <p>Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.</p>   |
| <p><b>Sla objecten over waarvan de scan langer duurt dan N seconden</b></p> | <p>Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.</p>   |
| <p><b>Scan archieven</b></p>  | <p>ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling. Bij het controleren van archieven voert het programma een recursief uitpakken uit. Zo kunnen bedreigingen worden gedetecteerd in archieven op meerdere niveaus (archieff in een archief).</p>  |
| <p><b>Scan distributiepakketten</b></p>                                     | <p>Dit selectievakje schakelt het scannen van distributiepakketten van andere fabrikanten in of uit.</p>   |
| <p><b>Scan Microsoft Office-bestanden</b></p>                               | <p>Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.</p>   |
|   |  |

|   |  |
|---|--|
| <p><b>Scan e-mailindelingen</b></p>   | <p>Het scannen van e-mailindelingen en de e-maildatabase. Het programma scant PST- en OST-bestanden gebruikt door MS Outlook en Windows Mail/Outlook Express e-mailclients, evenals EML-bestanden.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security ondersteunt de 64-bits versie van MS Outlook e-mailclient niet. Dit betekent dat Kaspersky Endpoint Security geen MS Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van MS Outlook op de computer is geïnstalleerd, zelfs als <a href="#">e-mail is opgenomen in het scanbereik</a>.</p> </div> <p>Als het selectievakje is ingeschakeld, splitst Kaspersky Endpoint Security het bestand met de e-mailindeling op in onderdelen (header, tekst, bijlagen) en scant het ze op dreigingen.</p> <p>Als dit selectievakje is uitgeschakeld, scant Kaspersky Endpoint Security het bestand met de e-mailindeling als een enkel bestand.</p> |
| <p><b>Scan wachtwoordbeveiligde archieven</b></p>   | <p>Als het selectievakje is ingeschakeld, worden archieven met wachtwoordbeveiliging gescand door Kaspersky Endpoint Security. Alvorens bestanden in een archief kunnen worden gescand, wordt u gevraagd het wachtwoord in te voeren.</p> <p>Als het selectievakje is uitgeschakeld, worden archieven met wachtwoordbeveiliging niet gescand door Kaspersky Endpoint Security.</p>   |
| <p><b>Pak grote samengestelde bestanden niet uit</b></p>  | <p>Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde.</p> <p>Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door Kaspersky Endpoint Security.</p> <p>Kaspersky Endpoint Security scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.</p>   |
| <p><b>Machine learning en analyse op basis van definities</b></p>   | <p>De methode 'Machine learning en analyse op basis van definities' gebruikt de Kaspersky Endpoint Security-databases die beschrijvingen van bekende dreigingen en neutralisatiemethoden bevatten. Een bescherming die gebruikmaakt van deze methode zorgt voor een minimale beveiliging.</p> <p>Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.</p>  |
| <p><b>Heuristische analyse</b></p>  | <p>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.</p> <p>Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.</p>  |
| <p><b>iSwift-technologie</b></p> <p><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i></p> | <p>Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.</p>  |



|   |   |
|---|---|
| <p><b>iChecker-technologie</b></p> <p><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i></p> | <p>Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).</p> |
|---|---|

## Verwisselbare schijven scannen wanneer ze op de computer zijn aangesloten

Kaspersky Endpoint Security scant alle bestanden die u start of kopieert, zelfs als deze bestanden op een verwisselbare schijf staan (File Threat Protection-onderdeel). Als u de verspreiding van virussen en andere malware wilt voorkomen, kunt u configureren dat verwisselbare schijven automatisch worden gescand wanneer ze op de computer worden aangesloten. Kaspersky Endpoint Security probeert automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd. Het onderdeel houdt een computer veilig door scans uit te voeren die technologie zoals machine learning, heuristische analyse (hoog niveau) en analyse op basis van definities implementeren. Kaspersky Endpoint Security maakt ook gebruik van iSwift- en iChecker-scanoptimalisatietechnologieën. De technologieën staan altijd aan en kunnen niet worden uitgeschakeld.

### [Start van Scan van verwisselbare schijven configureren via de Beheerconsole \(MMC\)](#)


1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruijnte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Lokale taken** → **Removable drives scan** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Actie bij aansluiting van verwisselbare schijf** de optie **Gedetailleerde Scan** of **Snelle Scan**.
7. Configureer geavanceerde opties voor Scan van verwisselbare schijven (zie onderstaande tabel).
8. Sla uw wijzigingen op.

### [Start van Scan van verwisselbare schijven configureren via de Webconsole en Cloudconsole](#)



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Lokale taken** → **Removable drives scan**.
5. Selecteer in de vervolgkeuzelijst **Action when a removable drive is connected** de optie **Detailed Scan** of **Quick Scan**.
6. Configureer geavanceerde opties voor Scan van verwisselbare schijven (zie onderstaande tabel).
7. Sla uw wijzigingen op.

### Start van Scan van verwisselbare schijven configureren via de programma-interface

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
3. Gebruik de schakelaar **Scan van verwisselbare schijven** om scans van verwisselbare schijven in of uit te schakelen bij het verbinden met de computer.
4. Configureer geavanceerde opties voor Scan van verwisselbare schijven (zie onderstaande tabel).
5. Sla uw wijzigingen op.

Kaspersky Endpoint Security voert de Scan van verwisselbare schijven uit voor verwisselbare schijven die kleiner zijn dan de opgegeven maximale grootte. Als u de taak *Scan van verwisselbare schijven* niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

Instellingen van de taak Scan van verwisselbare schijven

| Parameter   | Beschrijving  |
|---|---|
| <b>Actie bij aansluiting van verwisselbare schijf</b> | <p><b>Gedetailleerde Scan.</b> Als een verwisselbare schijf wordt aangesloten wanneer deze optie is geselecteerd, scant Kaspersky Endpoint Security alle bestanden op de verwisselbare schijf, inclusief geneste bestanden in samengestelde bestanden, archieven, distributiekpakketten en bestanden met Office-indelingen. Kaspersky Endpoint Security scant geen bestanden met een e-mailindeling of archieven met wachtwoordbeveiliging.</p> <p><b>Snelle Scan.</b> Als deze optie is geselecteerd en een verwisselbare schijf wordt aangesloten, scant Kaspersky Endpoint Security alleen <a href="#">bestanden met specifieke indelingen</a> die heel kwetsbaar zijn voor infecties en pakt het geen samengestelde objecten uit.</p> |
| <b>Maximale grootte van verwisselbare schijven</b>    | <p>Als dit selectievakje is ingeschakeld, wordt de gekozen actie in de vervolgkeuzelijst <b>Actie bij aansluiting van verwisselbare schijf</b> door Kaspersky Endpoint Security uitgevoerd op verwisselbare schijven die kleiner dan de opgegeven waarde zijn.</p> <p>Als het selectievakje is uitgeschakeld, wordt de gekozen actie in de vervolgkeuzelijst <b>Actie bij aansluiting van verwisselbare schijf</b> door Kaspersky Endpoint Security uitgevoerd op verwisselbare schijven van elke grootte.</p>  |

|  |  |
|--|--|
| <b>Toon voortgang van scan</b>             | <p>Als het selectievakje is ingeschakeld, geeft Kaspersky Endpoint Security de voortgang van de scan van verwisselbare schijven weer in een afzonderlijk venster en in het gedeelte <b>Taken</b>.</p> <p>Als het selectievakje is uitgeschakeld, voert Kaspersky Endpoint Security de scan van verwisselbare schijven op de achtergrond uit.</p> |
| <b>Voorkom het stoppen van de scantaak</b> | <p>Als dit selectievakje is ingeschakeld, zijn voor de scantaak voor verwisselbare schijven in de lokale interface van Kaspersky Endpoint Security de knop <b>Stoppen</b> in het gedeelte <b>Taken</b> en de knop <b>Stoppen</b> in het venster scan van verwisselbare schijven niet beschikbaar.</p>  |

## Achtergrondscan

Een *achtergrondscan* is een scanmodus van Kaspersky Endpoint Security waarin geen meldingen aan de gebruiker worden weergegeven. De achtergrondscan vereist minder computerbronnen dan andere scans (zoals een volledige scan). In deze modus scant Kaspersky Endpoint Security opstartobjecten, opstartsectoren, het systeemgeheugen en de systeempartitie. In de volgende gevallen wordt een achtergrondscan gestart:

- Na het updaten van de antivirusdatabases.
- 30 minuten na het starten van Kaspersky Endpoint Security.
- Elke zes uur.
- Als de computer vijf minuten of langer inactief is (de computer is vergrendeld of de schermbeveiliging is ingeschakeld).

Bij een inactieve computer wordt de achtergrondscan onderbroken als aan een van de volgende voorwaarden wordt voldaan:

- De computer wordt opnieuw actief gebruikt.

Als de achtergrondscan al meer dan tien dagen niet is uitgevoerd, wordt de scan niet onderbroken.

- De computer (laptop) is overgegaan op de accumulomodus.

Wanneer Kaspersky Endpoint Security een achtergrondscan uitvoert, worden geen bestanden gescand waarvan de inhoud zich in de OneDrive-cloudopslag bevindt.

### [Achtergrondscans inschakelen via de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Lokale taken** → **Background scan** in het beleidsvenster.
6. Gebruik het selectievakje **Schakel achtergrondscan in** om achtergrondscans in of uit te schakelen.
7. Sla uw wijzigingen op.

### [Achtergrondscans inschakelen via de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Lokale taken** → **Background scan**.
5. Gebruik het selectievakje **Enable background scan** om achtergrondscans in of uit te schakelen.
6. Sla uw wijzigingen op.

### [Achtergrondscans inschakelen via de programma-interface](#)

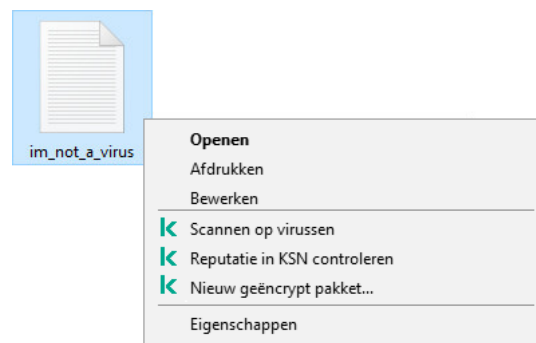
1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
3. Gebruik de schakelaar **Achtergrondscan** om achtergrondscans in of uit te schakelen.
4. Sla uw wijzigingen op.

Als u *Achtergrondscan* niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

## Scannen vanuit contextmenu

Met Kaspersky Endpoint Security kunt u via het contextmenu individuele bestanden scannen op virussen en andere malware (zie onderstaande afbeelding).

Wanneer u een scan vanuit het contextmenu start, scant Kaspersky Endpoint Security geen bestanden waarvan de inhoud zich in de OneDrive-cloudopslag bevindt.



Scannen vanuit contextmenu


### [Scannen vanuit contextmenu configureren via Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Lokale taken** → **Scan from Context Menu** in het beleidsvenster.
6. Configureer Scannen vanuit contextmenu (zie onderstaande tabel).
7. Sla uw wijzigingen op.

### [Scannen vanuit contextmenu configureren via de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Lokale taken** → **Scan from Context Menu**.
5. Configureer Scannen vanuit contextmenu (zie onderstaande tabel).
6. Sla uw wijzigingen op.

### [Scannen vanuit contextmenu configureren via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
3. Configureer Scannen vanuit contextmenu (zie onderstaande tabel).
4. Sla uw wijzigingen op.

Als u de taak *Scannen vanuit contextmenu* niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

Instellingen van de taak Scannen vanuit contextmenu

| Parameter                                  | Beschrijving  |
|--|---|
| <b>Beveiligingsniveau</b>                  | <p>Kaspersky Endpoint Security kan verschillende groepen van instellingen gebruiken om een scan uit te voeren. Deze groepen van instellingen die in het programma zijn opgeslagen, worden <i>beveiligingsniveaus</i> genoemd:</p> <ul style="list-style-type: none"> <li>• <b>Hoog.</b> Kaspersky Endpoint Security scant alle soorten bestanden. Wanneer samengestelde bestanden worden gescand, scant Kaspersky Endpoint Security ook bestanden met een e-mailindeling.</li> <li>• <b>Aanbevolen.</b> Kaspersky Endpoint Security scant alleen de opgegeven bestandsindelingen op alle harde schijven, netwerkschijven en verwisselbare schijven van de computer, evenals ingesloten OLE-objecten. Kaspersky Endpoint Security scant geen archieven of installatiepakketten.</li> <li>• <b>Laag.</b> Kaspersky Endpoint Security scant alleen nieuwe of gewijzigde bestanden met de opgegeven extensies op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Kaspersky Endpoint Security scant geen samengestelde bestanden.</li> </ul> |
| <b>Actie bij detectie van een dreiging</b> | <p><b>Desinfecteren of verwijderen als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.</p> <p><b>Desinfecteren of blokkeren als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.</p> <p><b>Melden.</b> Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security de informatie over geïnfecteerde bestanden toe aan de lijst met actieve dreigingen wanneer deze bestanden worden gedetecteerd.</p>   |
| <b>Bestandstypen</b>                       | <div style="border: 1px solid gray; padding: 10px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security beschouwt bestanden zonder extensie als uitvoerbare bestanden. Kaspersky Endpoint Security scant altijd uitvoerbare bestanden ongeacht de bestandstypen die u wilt laten scannen.</p> </div> <p><b>Alle bestanden.</b> Als deze instelling is ingeschakeld, worden alle bestanden gecontroleerd door Kaspersky Endpoint Security, zonder uitzondering (alle indelingen en extensies).</p>  |

|  |  |
|--|--|
|  | <p><b>Bestanden gescand op indeling.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.</p> <p><b>Bestanden gescand op extensie.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.</p> <p>Standaard scant Kaspersky Endpoint Security bestanden volgens indeling. Het scannen van bestanden volgens extensie is minder veilig omdat een schadelijk bestand een extensie kan hebben die niet voorkomt op de lijst met potentieel infecteerbare bestanden (bijvoorbeeld .123).</p> |
| <b>Scan alleen nieuwe en gewijzigde bestanden</b>                    | Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.  |
| <b>Sla objecten over waarvan de scan langer duurt dan N seconden</b> | Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.  |
| <b>Scan archieven</b>  | ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling. Bij het controleren van archieven voert het programma een recursief uitpakken uit. Zo kunnen bedreigingen worden gedetecteerd in archieven op meerdere niveaus (archief in een archief).  |
| <b>Scan distributiepakketten</b>                                     | Het selectievakje schakelt het scannen van distributiepakketten in of uit.   |
| <b>Scan Microsoft Office-bestanden</b>                               | Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.  |
| <b>Scan e-mailindelingen</b>   | <p>Het scannen van e-mailindelingen en de e-maildatabase. Het programma scant PST- en OST-bestanden gebruikt door MS Outlook en Windows Mail/Outlook Express e-mailclients, evenals EML-bestanden.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security ondersteunt de 64-bits versie van MS Outlook e-mailclient niet. Dit betekent dat Kaspersky Endpoint Security geen MS Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van MS Outlook op de computer is geïnstalleerd, zelfs als <a href="#">e-mail is opgenomen in het scanbereik</a>.</p> </div> <p>Als het selectievakje is ingeschakeld, splitst Kaspersky Endpoint Security het bestand met de e-mailindeling op in onderdelen (header, tekst, bijlagen) en scant het ze op dreigingen.</p> <p>Als dit selectievakje is uitgeschakeld, scant Kaspersky Endpoint Security het bestand met de e-mailindeling als een enkel bestand.</p>                      |
| <b>Scan wachtwoordbeveiligde archieven</b>                           | Als het selectievakje is ingeschakeld, worden archieven met wachtwoordbeveiliging gescand door Kaspersky Endpoint Security. Alvorens bestanden in een archief kunnen worden gescand, wordt u gevraagd het wachtwoord in te voeren.   |

|  |   |
|--|---|
|  | Als het selectievakje is uitgeschakeld, worden archieven met wachtwoordbeveiliging niet gescand door Kaspersky Endpoint Security.   |
| <b>Pak grote samengestelde bestanden niet uit</b>          | <p>Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde.</p> <p>Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door Kaspersky Endpoint Security.</p> <p>Kaspersky Endpoint Security scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.</p>  |
| <b>Machine learning en analyse op basis van definities</b> | <p>De methode 'Machine learning en analyse op basis van definities' gebruikt de Kaspersky Endpoint Security-databases die beschrijvingen van bekende dreigingen en neutralisatiemethoden bevatten. Een bescherming die gebruikmaakt van deze methode zorgt voor een minimale beveiliging.</p> <p>Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.</p>   |
| <b>Heuristische analyse</b>                                | <p>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.</p> <p>Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.</p> |
| <b>iSwift-technologie</b>                                  | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.  |
| <b>iChecker-technologie</b>                                | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).  |

## Controle van programma-integriteit

Kaspersky Endpoint Security controleert de programmamodules op beschadiging of wijzigingen. Als een programmabibliotheek bijvoorbeeld een onjuiste digitale handtekening heeft, wordt de bibliotheek als beschadigd beschouwd. De taak *Integriteitscontrole* is bedoeld voor het scannen van programmabestanden. Start de taak *Integriteitscontrole* als Kaspersky Endpoint Security een schadelijk object heeft gevonden maar het niet heeft geneutraliseerd.

U kunt de taak *Integriteitscontrole* zowel in de Webconsole van Kaspersky Security Center als in de Beheerconsole maken. Het is niet mogelijk om een taak in Kaspersky Security Center Cloud Console te maken.

De programma-integriteit kan in de volgende gevallen worden geschonden:

- Een schadelijk object heeft bestanden van Kaspersky Endpoint Security gewijzigd. In dit geval moet u de procedure uitvoeren voor het herstellen van Kaspersky Endpoint Security met behulp van de hulpprogramma's van het besturingssysteem. Na het herstel start u een volledige scan van de computer en herhaalt u de integriteitscontrole.
- De digitale handtekening is verlopen. In dit geval moet u Kaspersky Endpoint Security updaten.

[Een programma-integriteitscontrole uitvoeren via de Beheerconsole \(MMC\)](#) 



1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

### Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)** → **Integriteitscontrole**.

### Stap 2: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

### Stap 3. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of wanneer een virusuitbraak wordt gedetecteerd.

### Stap 4. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Integriteitscontrole nadat de computer was geïnfecteerd*.

### Stap 5. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. Kaspersky Endpoint Security controleert nu de integriteit van het programma. U kunt ook een schema voor de controle van de programma-integriteit configureren in de taakeigenschappen (zie onderstaande tabel).

[Een programma-integriteitscontrole uitvoeren via de Webconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Integriteitscontrole**.

c. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Integriteit van het programma controleren na een infectie*.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Ga naar de volgende stap.

5. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de lijst met taken.

6. Schakel het selectievakje naast de taak in.

Kaspersky Endpoint Security controleert nu de integriteit van het programma. U kunt ook een schema voor de controle van de programma-integriteit configureren in de taakeigenschappen (zie onderstaande tabel).

### [Een integriteitscontrole starten via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.

2. U ziet nu de lijst met taken: selecteer de taak *Integriteitscontrole* en klik op **Scan starten**.

Kaspersky Endpoint Security controleert nu de integriteit van het programma. U kunt ook een schema voor de controle van de programma-integriteit configureren in de taakeigenschappen (zie onderstaande tabel).

Als u *Integriteitscontrole* niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

Instellingen voor de taak Integriteitscontrole

| Parameter                         | Beschrijving   |
|-----------------------------------|--|
| <b>Planning van scan</b>          | <b>Handmatig.</b> Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt.<br><b>Volgens schema.</b> In deze uitvoermodus voor scantaken wordt de scantaak door Kaspersky Endpoint Security gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten. |
| <b>Overgeslagen taken starten</b> | Als het selectievakje is ingeschakeld, wordt de overgeslagen scantaak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De scantaak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de scantaak.  |

|   |  |
|---|--|
|   | Als het selectievakje is uitgeschakeld, worden overgeslagen scantaken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende scantaak uit volgens het huidige schema.  |
| <b>Alleen starten als de computer inactief is</b> | Uitgestelde start van de scantaak wanneer computerbronnen bezet zijn. Kaspersky Endpoint Security start de scantaak als de computer vergrendeld wordt of als de schermbeveiliging is ingeschakeld. Als u de uitvoering van de taak hebt onderbroken door de computer bijvoorbeeld te ontgrendelen, zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar deze werd onderbroken. |

## Scanbereik bewerken

Het *Scanbereik* is een lijst met paden naar mappen en paden die Kaspersky Endpoint Security scant wanneer de taak wordt uitgevoerd. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.

Als u het scanbereik wilt bewerken, raden we aan dat u de taak *Aangepaste Scan* gebruikt. Kaspersky-experts raden u aan het scanbereik van de taak *Volledige Scan* en *Kritieke Gebiedenscan* niet te wijzigen.

Kaspersky Endpoint Security heeft de volgende vooraf gedefinieerde objecten als onderdeel van het scanbereik:

- **Mijn e-mail.**  
Bestanden van het e-mailprogramma Outlook: gegevensbestanden (PST), offline gegevensbestanden (OST).
- **Systeemgeheugen.**
- **Opstartobjecten.**  
Geheugen dat worden gebruikt door processen en uitvoerbare bestanden van programma's die bij de opstart van het systeem worden gestart.
- **Schijfopstartsectoren.**  
Opstartsectoren van harde schijven en verwisselbare schijven.
- **Systeemback-up.**  
Inhoud van de map System Volume Information.
- **Alle externe apparaten.**
- **All hard drives.**
- **All network drives.**

Als u mappen of bestanden wilt uitsluiten van het scanbereik, [voegt u de map of het bestand toe aan de vertrouwde zone](#).

[Een scanuitzondering bewerken via de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Taken**.
4. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.  
[Maak indien nodig een virusscantaak.](#)
5. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
6. Klik in het gedeelte **Scanbereik** op **Instellingen**.
7. Selecteer in het venster dat opent de objecten die u aan het scanbereik wilt toevoegen of daarvan wilt uitsluiten.
8. Als u een nieuw object aan het scanbereik wilt toevoegen:

- a. Klik op **Toevoegen**.

- b. Voer in het veld **Object** het pad naar de map of het bestand in.

Gebruik maskers:

- Het teken **\*** (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens **\** en **/** (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker **C:\\*\\*.txt** omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes **\*\*** stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens **\** en **/** (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker **C:\Voorbeeld\\*\*\\*.txt** omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in de map **Voorbeeld** en de submappen ervan bevinden. Het masker moet ten minste één genest niveau bevatten. Het masker **C:\\*\*\\*.txt** is geen geldig masker.
- Het teken **?** (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens **\** en **/** (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker **C:\Voorbeeld\???.txt** omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam **Voorbeeld** bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt een object van scans uitsluiten zonder het uit de lijst met objecten in het scanbereik te verwijderen. Schakel hiervoor het selectievakje naast het object uit.

9. Sla uw wijzigingen op.

[Een scanuitzondering bewerken via de Webconsole en Cloudconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de scantask.

U ziet nu het venster met de taakeigenschappen. [Maak indien nodig een virusscantaak](#).

3. Selecteer het tabblad **Application settings**.

4. Selecteer in het gedeelte **Scan scope** de objecten die u aan het scanbereik wilt toevoegen of daarvan wilt uitsluiten.

5. Als u een nieuw object aan het scanbereik wilt toevoegen:

a. Klik op de knop **Add**.

b. Voer in het veld **Path** het pad naar de map of het bestand in.

Gebruik maskers:

- Het teken `*` (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\*\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes `**` stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in de map `Voorbeeld` en de submappen ervan bevinden. Het masker moet ten minste één genest niveau bevatten. Het masker `C:\**\*.txt` is geen geldig masker.
- Het teken `?` (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Voorbeeld` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt een object van scans uitsluiten zonder het uit de lijst met objecten in het scanbereik te verwijderen. Dat doet u door de schakelaar ernaast uit te zetten.

6. Sla uw wijzigingen op.

## [Een scanbereik bewerken via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.

2. Selecteer in de takenlijst *Aangepaste Scan* in de lijst met taken en klik op **Selecteren**.

U kunt ook het scanbereik voor andere taken bewerken. Kaspersky-experts raden u aan het scanbereik van de taak *Volledige Scan* en *Kritieke Gebiedenscan* niet te wijzigen.

3. Selecteer in het venster dat opent de objecten die u aan het scanbereik wilt toevoegen.

4. Sla uw wijzigingen op.

Als u de scantaak niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

## Een geplande scan uitvoeren

Een volledige scan van de computer duurt wel even en vereist ook heel wat computerbronnen. Daarom doet u er goed aan een gepast tijdstip voor de scan te kiezen, zodat de prestaties van andere software op uw computer niet negatief worden beïnvloed. Met Kaspersky Endpoint Security kunt u een normaal schema voor computerscans configureren. Dit kan handig zijn als uw bedrijf een werkschema hanteert. U kunt bijvoorbeeld instellen dat een computerscan 's nachts of in het weekend wordt uitgevoerd. 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.

Als het niet mogelijk is om een optimaal schema voor scans te configureren, kunt u Kaspersky Endpoint Security een computerscan laten uitvoeren wanneer aan de volgende speciale voorwaarden wordt voldaan:

- Na een database-update.

Kaspersky Endpoint Security voert de computerscan uit met de geüpdatete databases.

- Na het starten van het programma.

Kaspersky Endpoint Security voert een computerscan uit wanneer een bepaalde tijd na het starten van het programma is verstreken. Bij de opstart van het besturingssysteem worden veel processen uitgevoerd. Daarom is het beter om de scantaak uit te stellen in plaats van deze meteen na het starten van Kaspersky Endpoint Security uit te voeren.

- Wake on LAN.

Kaspersky Endpoint Security voert een geplande computerscan uit zelfs als de computer uit staat. Hiervoor gebruikt het programma de Wake on LAN-functie van het besturingssysteem. Met de Wake on LAN-functie kan de computer op afstand worden aangezet door een speciaal signaal via het lokale netwerk te sturen. Als u deze functie wilt gebruiken, moet u de Wake on LAN-instellingen in de BIOS-instellingen inschakelen.

U kunt de uitvoering van een *virusscantaak* met Wake on LAN alleen in Kaspersky Security Center configureren. Het gebruik van Wake on LAN voor computerscans kunt u dus niet inschakelen in de programma-interface.

- Als de computer inactief is.

Kaspersky Endpoint Security voert een geplande computerscan uit als de schermbeveiliging of -vergrendeling actief is. Als de gebruiker de computer ontgrendelt, pauzeert Kaspersky Endpoint Security de scan. Hierdoor kan het enkele dagen duren voordat het programma een volledige computerscan heeft uitgevoerd.

[Een schema voor scans configureren via de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Taken**.
4. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.  
[Maak indien nodig een virusscantaak.](#)
5. Selecteer het gedeelte **Schema** in het venster met taakeigenschappen.
6. Configureer het schema voor scantaken.
7. Afhankelijk van de geselecteerde frequentie configureert u geavanceerde instellingen die het schema voor de uitvoering van de taken definiëren (zie onderstaande tabel).
8. Sla uw wijzigingen op.

### [Het schema voor scans configureren via de Webconsole en Cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de scantaak.  
U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Schema**.
4. Configureer het schema voor scantaken.
5. Afhankelijk van de geselecteerde frequentie configureert u geavanceerde instellingen die het schema voor de uitvoering van de taken definiëren (zie onderstaande tabel).
6. Sla uw wijzigingen op.

### [Het schema voor scans configureren via de programma-interface](#)

U kunt een schema voor scans alleen configureren als er geen beleid is toegepast op de computer. Als u een schema voor *virusscans* wilt configureren voor computers waarop een beleid is toegepast, dan kunt u dat doen in Kaspersky Security Center.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
 

U kunt een schema voor de uitvoering van een Volledige Scan, Kritieke Gebiedenscan of Integriteitscontrole configureren. U kunt een Aangepaste Scan alleen handmatig uitvoeren.
3. Klik op **Planning van scan**.
4. Configureer in het venster dat opent de planning van de scantaak.
5. Afhankelijk van de geselecteerde frequentie configureert u geavanceerde instellingen die het schema voor de uitvoering van de taken definiëren (zie onderstaande tabel).
6. Sla uw wijzigingen op.

Instellingen van schema voor scans

| Parameter   | Beschrijving  |
|---|---|
| <b>Planning van scan</b>  | <p><b>Handmatig.</b> Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt.</p> <p><b>Volgens schema.</b> In deze uitvoermodus voor scantaken wordt de scantaak door Kaspersky Endpoint Security gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten.</p>   |
| <b>Stel start na programmastart uit met N minuten</b>                       | Uitgestelde start van de scantaak na het starten van het programma. Bij de opstart van het besturingssysteem worden veel processen uitgevoerd. Daarom is het beter om de scantaak uit te stellen in plaats van deze meteen na het starten van Kaspersky Endpoint Security uit te voeren.  |
| <b>Overgeslagen taken starten</b>   | Als het selectievakje is ingeschakeld, wordt de overgeslagen scantaak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De scantaak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de scantaak. Als het selectievakje is uitgeschakeld, worden overgeslagen scantaken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende scantaak uit volgens het huidige schema. |
| <b>Alleen starten als de computer inactief is</b>                           | Uitgestelde start van de scantaak wanneer computerbronnen bezet zijn. Kaspersky Endpoint Security start de scantaak als de computer vergrendeld wordt of als de schermbeveiliging is ingeschakeld. Als u de uitvoering van de taak hebt onderbroken door de computer bijvoorbeeld te ontgrendelen, zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar deze werd onderbroken.  |
| <b>Automatische willekeurige vertraging gebruiken voor starten van taak</b> | Als het selectievakje is ingeschakeld, wordt de taak niet strikt volgens het schema uitgevoerd maar willekeurig binnen een bepaald interval. Hierdoor zullen de starttijden van de taak verschillen. Dankzij de willekeurige starttijden wordt voorkomen dat een groot aantal computers tegelijk verbinding maakt met de Administration Server wanneer de taak volgens een schema wordt uitgevoerd.   |



|  |   |
|--|---|
| <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p>   | <p>Het bereik van de willekeurige starttijden wordt automatisch berekend wanneer de taak wordt gemaakt en is afhankelijk van het aantal computers waaraan de taak is toegewezen. Bijgevolg wordt de taak altijd uitgevoerd op de berekende starttijd. Als de taakinstellingen echter worden gewijzigd of als de taak handmatig wordt gestart, verandert de berekende starttijd.</p> <p>Als het selectievakje is uitgeschakeld, wordt de taak precies op het geplande tijdstip uitgevoerd.</p> |
| <p><b>Taak stoppen als deze langer dan N (min) heeft gelopen</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p>              | <p>De uitvoeringstijd van de taak beperken Na de opgegeven tijd stopt Kaspersky Endpoint Security de taak. De taak is niet gemarkeerd als voltooid. De volgende keer dat Kaspersky Endpoint Security de taak uitvoert, wordt deze vanaf het begin en op schema uitgevoerd.</p> <p>Om de uitvoeringstijd van de taak te verkorten, kunt u bijvoorbeeld <a href="#">het scanbereik configureren</a> of <a href="#">de scan optimaliseren</a>.</p>   |
| <p><b>Apparaat activeren voordat taak wordt gestart via Wake on LAN (min)</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p>Als het selectievakje is ingeschakeld, wordt het besturingssysteem van de computer een bepaalde tijd op voorhand opgestart voordat de taak wordt uitgevoerd. De standaardvertraging is 5 minuten.</p> <p>Schakel het selectievakje in als u de taak wilt uitvoeren op alle computers, inclusief computers die uit staan.</p>   |

## Een scan uitvoeren namens een andere gebruiker

Standaard wordt de scantaak uitgevoerd in naam van de gebruiker met wiens rechten u bent geregistreerd in het besturingssysteem. Het beschermingsbereik kan netwerkstations of andere objecten omvatten waarvoor speciale toegangsrechten vereist zijn. U kunt een gebruiker met de vereiste rechten opgeven in de instellingen van Kaspersky Endpoint Security en de scantaak onder dit gebruikersaccount uitvoeren.

U kunt de volgende scans uitvoeren namens een andere gebruiker:

- Kritieke Gebiedenscan.
- Volledige Scan.
- Aangepaste Scan.
- [Scannen vanuit contextmenu](#).

U kunt geen gebruikersrechten configureren om een [Scan van verwisselbare schijven](#), een [Achtergrondscan](#) of een [Integriteitscontrole](#) uit te voeren.


[Een scan namens een andere gebruiker uitvoeren via de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Taken**.
4. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.
5. Selecteer het gedeelte **Account** in het venster met taakeigenschappen.
6. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om een scantaak uit te voeren.
7. Sla uw wijzigingen op.

### [Een scan namens een andere gebruiker uitvoeren via de Webconsole of Cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de scantaak.  
U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Instellingen**.
4. Klik in het gedeelte **Account** op **Instellingen**.
5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om een scantaak uit te voeren.
6. Sla uw wijzigingen op.

### [Een scan namens een andere gebruiker uitvoeren via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
3. Selecteer in de taakeigenschappen **Geavanceerde instellingen** → **Scan starten namens**.
4. Voer in het venster dat opent de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om een scantaak uit te voeren.
5. Sla uw wijzigingen op.

Als u de scantaak niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

## Scanoptimalisatie

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).

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.

U kunt ook de iChecker- en iSwift-technologieën inschakelen. The iChecker- en iSwift-technologieën optimaliseren de snelheid waarmee bestanden worden gescand door de bestanden die sinds de laatste scan niet zijn gewijzigd uit te sluiten.

[Scans optimaliseren via de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Taken**.
4. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.  
[Maak indien nodig een virusscantaak.](#)
5. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
6. In het blok **Beschermingsniveau**, klikt u op de knop **Instellingen**.  
U ziet nu het venster met de instellingen van de scantaak.
7. Configureer de scaninstellingen in het blok **Scanoptimalisatie**:
  - **Scan alleen nieuwe en gewijzigde bestanden.** Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.  
U kunt ook configureren dat nieuwe bestanden volgens type worden gescand. Zo kunt u bijvoorbeeld alle distributiepakketten scannen en alleen nieuwe en Office-bestanden scannen.
  - **Sla bestanden over waarvan scan langer duurt dan N s.** Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.
8. Klik op **Extra**.  
U ziet nu het venster met instellingen voor het scannen van samengestelde bestanden.
9. Schakel in het blok **Maximale grootte** het selectievakje **Grote samengestelde bestanden niet uitpakken** in. Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.

Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Grote samengestelde bestanden niet uitpakken** is ingeschakeld.
10. Klik op **OK**.
11. Selecteer het tabblad **Extra**.
12. Schakel in het blok **Scantechnologieën** de selectievakjes in naast de namen van de technologieën die u tijdens een scan wilt gebruiken.
  - **iSwift-technologie.** Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.

- **iChecker-technologie.** Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).

13. Sla uw wijzigingen op.

### [Scans optimaliseren via de Webconsole en Cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de scantaak.

U ziet nu het venster met de taakeigenschappen. [Maak indien nodig een virusscantaak](#).

3. Selecteer het tabblad **Application settings**.

4. Schakel in het blok **Action on threat detection** het selectievakje **Scan only new and changed files** in.

Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.

U kunt ook configureren dat nieuwe bestanden volgens type worden gescand. Zo kunt u bijvoorbeeld alle distributiepakketten scannen en alleen nieuwe en Office-bestanden scannen.

5. Schakel het selectievakje **Do not unpack large compound files** in. Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.

Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Do not unpack large compound files** is ingeschakeld.

6. Schakel in het blok **Advanced settings** het selectievakje **Skip files that are scanned for longer than N sec** in. Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.

7. Sla uw wijzigingen op.

### [Scans optimaliseren via de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar het gedeelte **Taken**.
2. Selecteer de scantaak in de lijst met taken en klik op .
3. Klik op **Geavanceerde instellingen**.
4. Configureer in het blok **Scanoptimalisatie** de scaninstellingen:
  - **Scan alleen nieuwe en gewijzigde bestanden.** Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.  
U kunt ook configureren dat nieuwe bestanden volgens type worden gescand. Zo kunt u bijvoorbeeld alle distributiepakketten scannen en alleen nieuwe en Office-bestanden scannen.
  - **Sla objecten over waarvan de scan langer duurt dan N seconden.** Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.
5. Schakel in het blok **Beperking van grootte** het selectievakje **Pak grote samengestelde bestanden niet uit** in. Hiermee stelt u een tijdslimiet in voor het scannen van een enkel object. Na de opgegeven tijd stopt Kaspersky Endpoint Security met het scannen van een bestand. Op deze manier wordt de duur van een scan ingekort.

Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Pak grote samengestelde bestanden niet uit** is ingeschakeld.

6. Schakel in het blok **Scantechnologieën** de selectievakjes in naast de namen van de technologieën die u tijdens een scan wilt gebruiken.
  - **iSwift-technologie.** Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.
  - **iChecker-technologie.** Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).
7. Sla uw wijzigingen op.

Als u de scantaak niet ziet, heeft de beheerder [het gebruik van lokale taken verboden in het beleid](#).

## Databases en softwaremodules van het programma bijwerken

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 dreigingen en methoden om ze onschadelijk te maken. Voor een snelle detectie van dreigingen wordt u aanbevolen de databases en programmamodules regelmatig te updaten.

Voor periodieke updates hebt u een actieve licentie nodig. Zonder actieve licentie kunt u maar één keer een update uitvoeren.

De updateservers van Kaspersky zijn de voornaamste updatebron voor Kaspersky Endpoint Security.

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 proxyserver aanpassen.

Updates worden gedownload via het HTTPS-protocol. Ze kunnen ook via het HTTP-protocol worden gedownload als ze niet via het HTTPS-protocol kunnen worden gedownload.

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 dreigingen 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 geüpdatet met records van nieuwe dreigingen 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).

Informatie over de huidige staat van de Kaspersky Endpoint Security-databases is zichtbaar in het hoofdvenster van het programma of de knopinfo die u ziet als u de muisaanwijzer over het pictogram van het programma in het systeemvak beweegt.

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.

## Updatescenario's voor database en programmamodule

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 dreigingen en methoden om ze onschadelijk te maken. Voor een snelle detectie van dreigingen wordt u aanbevolen de databases en programmamodules regelmatig te updaten.

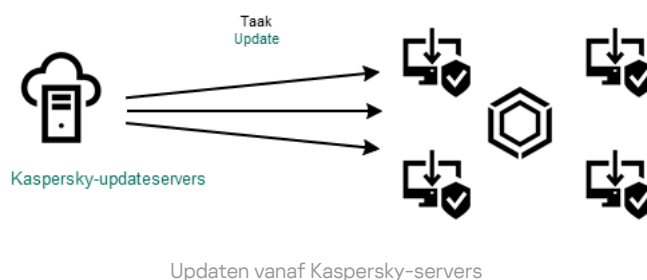
De volgende objecten worden op computers van gebruikers geüpdatet:

- Antivirusdatabases. De antivirusdatabases bevatten databases met definities van malware, beschrijvingen van netwerkaanvallen, databases met schadelijke webadressen en phishingadressen, databases met banners, databases met spam en andere gegevens.
- Programmamodules. Module-updates zijn bedoeld voor het elimineren van kwetsbaarheden in het programma en voor het verbeteren van de computerbescherming. Module-updates kunnen het gedrag van programmaonderdelen wijzigen en nieuwe functies toevoegen.

Kaspersky Endpoint Security ondersteunt de volgende scenario's voor het updaten van databases en programmamodules:

- Updaten vanaf Kaspersky-servers.

De Kaspersky-updateservers bevinden zich in meerdere landen wereldwijd. Dit zorgt voor een hoge betrouwbaarheid van de updates. Als een update niet kan worden uitgevoerd vanaf een server, schakelt Kaspersky Endpoint Security over naar de volgende server.



- Gecentraliseerde updates.

Met gecentraliseerde updates wordt minder internetverkeer verbruikt en zijn handig op te volgen.

Bij gecentraliseerde updates moet u de volgende stappen uitvoeren:

1. Download het updatepakket naar een opslagplaats in het bedrijfsnetwerk.

Het updatepakket wordt vanaf de opslagplaats gedownload door de Administration Server-taak *Updates downloaden naar Administration Server-opslagplaats*.

2. Download het updatepakket naar een gedeelde map (optioneel).

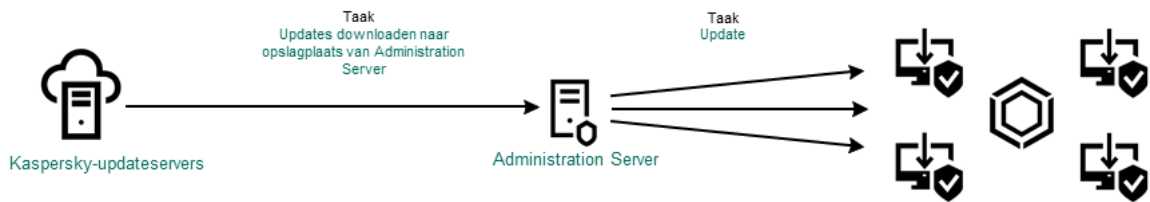
Op de volgende manieren kunt u het updatepakket naar een gedeelde map downloaden:

- Met de taak *Updaten* van Kaspersky Endpoint Security. De taak is bedoeld voor een van de computers in het lokale bedrijfsnetwerk.
- Met Kaspersky Update Utility. Voor gedetailleerde informatie over het gebruik van Kaspersky Update Utility raadpleegt u de [Knowledge Base van Kaspersky](#).

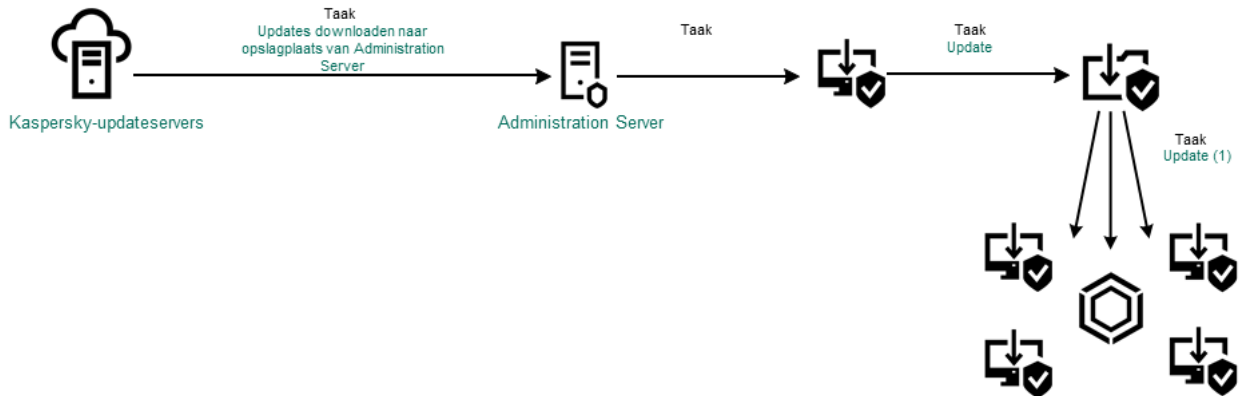
3. Verstuur het updatepakket naar clientcomputers.



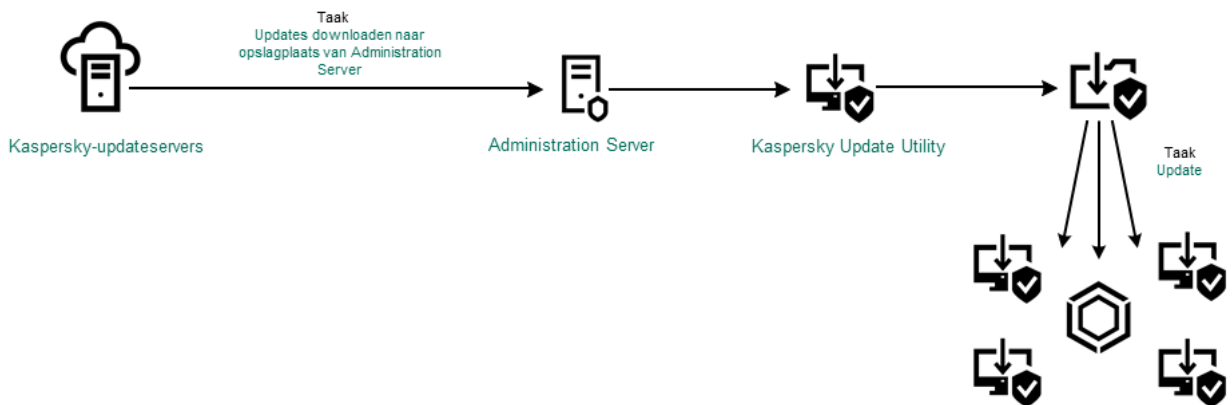
Het updatepakket wordt naar clientcomputers verspreid met de taak *Updaten* van Kaspersky Endpoint Security. U kunt een onbeperkt aantal updatetaken voor elke beheergroep maken.



Updaten vanaf een opslagplaats op een server



Updaten vanaf een gedeelde map



Updaten met Kaspersky Update Utility

Voor Webconsole bevat de standaardlijst met updatebronnen de Administration Server van Kaspersky Security Center en Kaspersky-updateservers. Voor Kaspersky Security Center Cloud Console bevat de standaardlijst met updatebronnen distributiepunten en Kaspersky-updateservers. Voor meer informatie over distributiepunten raadpleegt u de [Help van Kaspersky Security Center Cloud Console](#). U kunt andere updatebronnen aan de lijst toevoegen. U kunt HTTP-/FTP-servers en gedeelde mappen als updatebronnen opgeven. Als een update niet kan worden uitgevoerd vanaf een updatebron, schakelt Kaspersky Endpoint Security over naar de volgende bron.

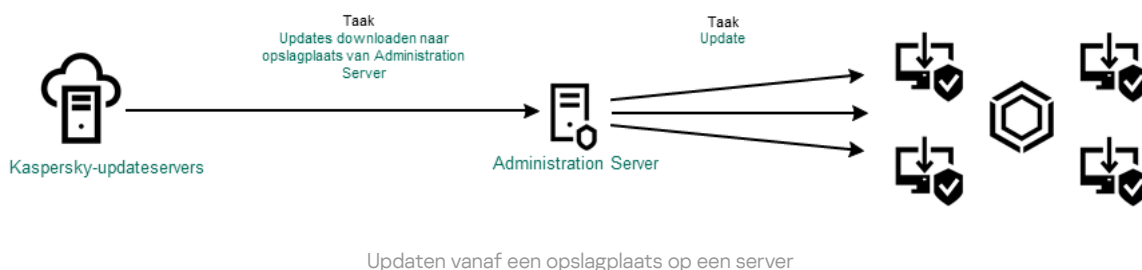
Updates worden gedownload vanaf Kaspersky-updateservers of vanaf andere FTP- of HTTP-servers via de standaard netwerkprotocollen. Als u voor de toegang tot de updatebron verbonden moet zijn met een proxyserver, [geeft u de proxyserverinstellingen in de beleidsinstellingen van Kaspersky Endpoint Security op](#).

## Updaten vanaf een opslagplaats op een server

Als u minder internetverkeer wilt verbruiken, kunt u het updaten van databases en programmamodules op computers binnen het bedrijfsnetwerk met behulp van een opslagplaats op een server configureren. In dit geval moet Kaspersky Security Center een updatepakket downloaden naar de opslagplaats (FTP- of HTTP-server, netwerkmap of lokale map) vanaf de Kaspersky-updateservers. Andere computers in het bedrijfsnetwerk kunnen dan het updatepakket in de opslagplaats op de server ophalen.

Zo configureert u het updaten van databases en programmamodules vanaf een opslagplaats op een server:

1. Configureer de download van een updatepakket naar de Administration Server-opslagplaats (de taak *Updates downloaden naar Administration Server-archief*).
2. Configureer het ophalen van updates voor databases en programmamodules in de opslagplaats op de server voor de resterende computers in het bedrijfsnetwerk (de taak *Updaten*).



Zo configureert u het downloaden van een updatepakket naar de opslagplaats op de server:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Selecteer de Administration Server-taak **Download updates to the Administration Server repository**.

U ziet nu het venster met de taakeigenschappen.

De taak *Updates downloaden naar Administration Server-archief* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center en komt mogelijk slechts één keer voor.

3. Selecteer het tabblad **Application settings**.

4. Klik in het blok **Andere instellingen** op **Configureren**.

5. Geef in het veld **Folder for storing updates** het adres van de FTP- of HTTP-server op, of de netwerkmap of lokale map waarnaar Kaspersky Security Center het updatepakket moet kopiëren dat het van de Kaspersky-updateservers heeft ontvangen.

De volgende structuur voor het pad wordt gebruikt voor updatebronnen:

- Voor een FTP- of HTTP-server voert u het webadres of IP-adres in.

Bijvoorbeeld `http://dn1-01.geo.kaspersky.com/` of `93.191.13.103`.

Voor een FTP-server kunt u de authenticatie-instellingen in het adres opgeven in de volgende structuur:  
`ftp://<gebruikersnaam>:<wachtwoord>@<node>:<poort>`.

- Voer voor een netwerkmap het UNC-pad in.

Bijvoorbeeld `\\Server\Share\Update distribution`.

- Voor een lokale map voert u het volledige pad naar de map in.

Bijvoorbeeld `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Sla uw wijzigingen op.

Zo configureert u het updaten van Kaspersky Endpoint Security vanaf de opgegeven opslagplaats op de server:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de taak **Update** voor Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

De taak *Updaten* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center. Voor het maken van de taak *Updaten* installeert u de webplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Local mode**.

4. Klik in de lijst met updatebronnen op de knop **Add**.

5. Geef in het veld **Source** het adres van de FTP- of HTTP-server op, of de netwerkmap of lokale map waar Kaspersky Security Center het updatepakket moet ophalen dat het van de Kaspersky-servers heeft ontvangen.

Het adres van de updatebron moet overeenkomen met het adres dat u hebt opgegeven in het veld **Folder for storing updates** wanneer u het downloaden van de updates naar de opslagplaats op de server hebt geconfigureerd (zie *eerder vermelde instructies*).

6. Selecteer in het blok **Status Enabled**.

7. Klik op **OK**.

8. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

9. Sla uw wijzigingen op.

Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

## Updaten vanaf een gedeelde map

Als u minder internetverkeer wilt verbruiken, kunt u het updaten van databases en programmamodules op computers binnen het bedrijfsnetwerk met behulp van een gedeelde map configureren. In dit geval ontvangt een van de computers in het bedrijfsnetwerk de updatepakketten vanaf Administration Server van Kaspersky Security Center of vanaf de Kaspersky-updateservers en worden de ontvangen updatepakketten naar de gedeelde map gekopieerd. Andere computers in het bedrijfsnetwerk kunnen dan het updatepakket in deze gedeelde map ophalen.

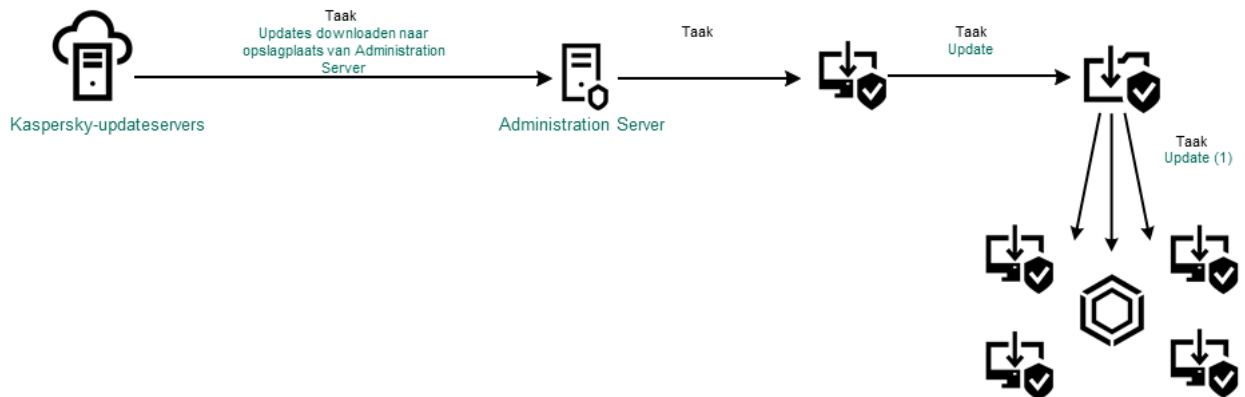
Zo configureert u het updaten van databases en programmamodules vanuit een gedeelde map:

1. [Configureren van updates van database en programmamodules vanuit een serveropslagplaats](#).

2. Schakel het kopiëren van een updatepakket naar een gedeelde map in op een van de computers in het bedrijfsnetwerk (zie onderstaande instructies).

3. Configureer het ophalen van updates voor databases en programmamodules in de gedeelde map voor de resterende computers in het bedrijfsnetwerk (zie onderstaande instructies).

De versie en lokalisering van de Kaspersky Endpoint Security-toepassing die het updatepakket naar een gedeelde map kopieert, moet overeenkomen met de versie en lokalisering van het programma dat databases uit de gedeelde map bijwerkt. Als versies of lokaliseringen van de programma's niet overeenkomen, kan de database-update eindigen met een fout.



Updaten vanaf een gedeelde map

Zo schakelt u het kopiëren van het updatepakket naar de gedeelde map in:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.

De taak *Updaten* moet toegewezen zijn aan een computer die als updatebron zal optreden.

2. Klik op de taak **Update** voor Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

De taak *Updaten* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center. Voor het maken van de taak *Updaten* installeert u de webplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Local mode**.

4. Configureer de updatebronnen.

De updatebronnen kunnen Kaspersky-updateservers, Administration Server van Kaspersky Security Center, andere FTP- of HTTP-servers, lokale mappen of netwerkmappen zijn.

5. Schakel het selectievakje **Copy updates to folder** in.

6. Voer in het veld **Path** het UNC-pad naar de gedeelde map in (bijvoorbeeld \\Server\Share\Update distribution).

Als het veld leeg wordt gelaten, kopieert Kaspersky Endpoint Security het updatepakket naar de map C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

7. Sla uw wijzigingen op.

Zo configureert u het updaten vanuit een gedeelde map:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Update**.

c. Typ in het veld **Task name** een korte omschrijving, zoals *Updaten vanuit een gedeelde map*.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

De taak *Update* moet toegewezen zijn aan de computers van het bedrijfsnetwerk, behalve de computer die als updatebron optreedt.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak en ga naar de volgende stap.

5. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de tabel met taken.

6. Klik op de nieuwe taak *Update*.

U ziet nu het venster met de taakeigenschappen.

7. Ga naar het gedeelte **Application settings**.

8. Selecteer het tabblad **Local mode**.

9. Klik in het blok **Update source** op **Toevoegen**.

10. Geef in het veld **Source** het pad naar de gedeelde map op.

Het bronadres moet overeenkomen met het adres dat u eerder hebt opgegeven in het veld **Path** wanneer u het kopiëren van het updatepakket naar de gedeelde map hebt geconfigureerd (zie *eerder vermelde instructies*).

11. Klik op **OK**.

12. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

13. Sla uw wijzigingen op.

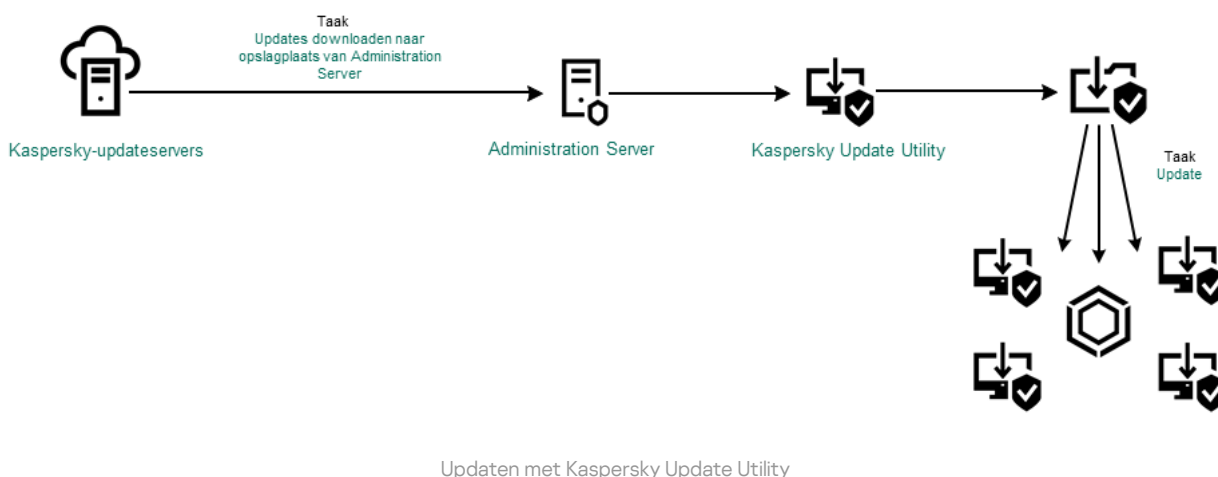
## Updaten met Kaspersky Update Utility

Wilt u minder internetverkeer verbruiken, dan kunt u databases en programmamodules op computers binnen het bedrijfsnetwerk updaten via een gedeelde map met behulp van de Kaspersky Update Utility. In dit geval ontvangt een van de computers in het bedrijfsnetwerk de updatepakketten vanaf de Administration Server van Kaspersky Security Center of vanaf de Kaspersky-updateservers en worden de ontvangen updatepakketten naar de gedeelde map gekopieerd met behulp van het hulpprogramma. Andere computers in het bedrijfsnetwerk kunnen dan het updatepakket in deze gedeelde map ophalen.

Zo configureert u het updaten van databases en programmamodules vanuit een gedeelde map:

1. [Configureren van updates van database en programmamodules vanuit een serveropslagplaats.](#)
2. Installeer Kaspersky Update Utility op een van de computers van het bedrijfsnetwerk.
3. Configureer het kopiëren van het updatepakket naar de gedeelde map in de instellingen van Kaspersky Update Utility.
4. Configureer het ophalen van updates voor databases en programmamodules in de gedeelde map voor de resterende computers in het bedrijfsnetwerk.

De versie en lokalisering van de Kaspersky Endpoint Security-toepassing die het updatepakket naar een gedeelde map kopieert, moet overeenkomen met de versie en lokalisering van het programma dat databases uit de gedeelde map bijwerkt. Als versies of lokaliseringen van de programma's niet overeenkomen, kan de database-update eindigen met een fout.



U kunt het distributiepakket van Kaspersky Update Utility downloaden vanaf de [website van de Technische Support van Kaspersky](#). Na de installatie van het hulpprogramma selecteert u de updatebron (bijvoorbeeld de Administration Server-opslagplaats) en de gedeelde map waarnaar Kaspersky Update Utility de updatepakketten zal kopiëren. Voor gedetailleerde informatie over het gebruik van Kaspersky Update Utility [raadpleegt u de Knowledge Base van Kaspersky](#).

Zo configureert u het updaten vanuit een gedeelde map:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.

2. Klik op de taak **Update** voor Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

De taak *Updaten* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center. Voor het maken van de taak *Updaten* installeert u de webplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Local mode**.
4. Klik in de lijst met updatebronnen op de knop **Toevoegen**.
5. Voer in het veld **Source** het UNC-pad naar de gedeelde map in (bijvoorbeeld \\Server\Share\Update distribution).

Het bronadres moet overeenkomen met het adres in de instellingen van Kaspersky Update Utility.

6. Klik op **OK**.
7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.
8. Sla uw wijzigingen op.

## Updaten in mobiele modus

De *mobiele modus* is de modus waarin Kaspersky Endpoint Security werkt wanneer een computer niet langer verbonden is met het bedrijfsnetwerk (*offline computer*). Voor meer informatie over het werken met offline computers en gebruikers die niet op kantoor zijn, raadpleegt u de [Help van Kaspersky Security Center](#).

Een offline computer buiten het bedrijfsnetwerk kan geen verbinding maken met Administration Server om databases en programmamodules te updaten. Standaard worden in de mobiele modus alleen Kaspersky-updateservers gebruikt als updatebron om databases en programmamodules te updaten. Het gebruik van een proxyserver om verbinding te maken met het internet wordt bepaald via een speciaal [afwezigheidsbeleid](#). Het afwezigheidsbeleid moet apart worden gemaakt. Wanneer Kaspersky Endpoint Security naar de mobiele modus is overgeschakeld, wordt de updatetaak elke twee uur gestart.

*Zo configureert u de update-instellingen voor de mobiele modus:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de taak **Update** voor Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

De taak *Updaten* wordt automatisch gemaakt door de wizard Snelle start van de Webconsole van Kaspersky Security Center. Voor het maken van de taak *Updaten* installeert u de webplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

Selecteer het tabblad **Application settings** → **Mobile mode**.

3. Configureer de updatebronnen. De updatebronnen kunnen Kaspersky-updateservers, andere FTP- en HTTP-servers, lokale mappen of netwerkmappen zijn.

4. Sla uw wijzigingen op.

De updates en programmamodules worden nu geüpdatet op de computers van gebruikers wanneer ze naar de mobiele modus overschakelen.

## Een updatetaak starten en stoppen

U kunt een updatetaak van Kaspersky Endpoint Security altijd starten of stoppen, ongeacht de geselecteerde uitvoermodus voor de updatetaak.

*Zo start of stopt u een updatetaak:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. Klik in de tegel **Update van databases en programmamodules** op de knop **Updaten** als u de updatetaak wilt starten.

Kaspersky Endpoint Security begint met het bijwerken van de programmamodules en databases. Het programma geeft de voortgang van de taak, de grootte van de gedownloade bestanden en de updatebron weer. U kunt de taak op elk moment stoppen door op de knop **Update stoppen** te klikken.


*Zo start of stopt u de updatetaak wanneer u de vereenvoudigde programma-interface gebruikt:*

1. Klik rechts om het contextmenu van het programmapictogram in het systeemvak van de taakbalk te openen.
2. Doe in de vervolgkeuzelijst **Taken** in het contextmenu een van het volgende:
  - selecteer een inactieve updatetaak om die te starten
  - selecteer een actieve updatetaak om die te stoppen
  - selecteer een gepauzeerde updatetaak om die te hervatten of te herstarten

## 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 een updatebron waarvoor authenticatie bij de proxyserver vereist is niet geconfigureerd is. 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. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Klik op **Database-updates met gebruikersrechten starten**.
4. Selecteer in het venster dat opent **Andere gebruiker**.
5. Voer de accountgegevens in van een gebruiker met de benodigde machtigingen voor toegang tot de updatebron.
6. Sla uw wijzigingen op.



## De uitvoermodus van de updatetaak selecteren

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 begintijd 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.

*Zo selecteert u de uitvoermodus van de updatetaak:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Klik op **Uitvoermodus**.
4. Selecteer in het venster dat opent de uitvoermodus van de 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 andere opties als u een schema voor de uitvoering van de updatetaak wilt configureren. Configureer de geavanceerde instellingen om de updatetaak te starten:
    - Geef in het veld **Stel start na programmastart uit met N-minuten** op hoelang u de start van de updatetaak na de opstart van Kaspersky Endpoint Security wilt uitstellen.
    - Selecteer **Start geplande scan de volgende dag als de computer uitgeschakeld is** als u wilt dat Kaspersky Endpoint Security gemiste update-taken bij de eerste gelegenheid uitvoert.
5. Sla uw wijzigingen op.

## Een updatebron toevoegen

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.

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.

Kaspersky Endpoint Security ondersteunt geen updates van HTTPS-servers, tenzij het de updateservers van Kaspersky zijn.

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.

*Zo voegt u een updatebron toe:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Klik op de knop **Updatebronnen selecteren**.
4. Klik in het venster op de knop **Toevoegen**.
5. Geef in het geopende venster het adres op van de FTP- of HTTP-server, de netwerkmap of de lokale map die het updatepakket bevat.

De volgende structuur voor het pad wordt gebruikt voor updatebronnen:

- Voor een FTP- of HTTP-server voert u het webadres of IP-adres in.  
Bijvoorbeeld `http://dn1-01.geo.kaspersky.com/` of `93.191.13.103`.  
Voor een FTP-server kunt u de authenticatie-instellingen in het adres opgeven in de volgende structuur:  
`ftp://<gebruikersnaam>:<wachtwoord>@<node>:<poort>`.
- Voer voor een netwerkmap het UNC-pad in.  
Bijvoorbeeld `\\Server\Share\Update distribution`.
- Voor een lokale map voert u het volledige pad naar de map in.  
Bijvoorbeeld `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Klik op de knop **Selecteren**.
7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.
8. Sla uw wijzigingen op.


## Bijwerken vanuit een gedeelde map configureren

Als u minder internetverkeer wilt verbruiken, kunt u het updaten van databases en programmamodules op computers binnen het bedrijfsnetwerk met behulp van een gedeelde map configureren. In dit geval ontvangt een van de computers in het bedrijfsnetwerk de updatepakketten vanaf Administration Server van Kaspersky Security Center of vanaf de Kaspersky-updateservers en worden de ontvangen updatepakketten naar de gedeelde map gekopieerd. Andere computers in het bedrijfsnetwerk kunnen dan het updatepakket in deze gedeelde map ophalen.


Zo configureert u het updaten van databases en programmamodules vanuit een gedeelde map:

1. Schakel het kopiëren van een updatepakket naar een gedeelde map in op een van de computers in het lokale netwerk.
2. Configureer het ophalen van updates voor databases en programmamodules in de gedeelde map voor de resterende computers in het bedrijfsnetwerk.

*Zo schakelt u het kopiëren van het updatepakket naar de gedeelde map in:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Schakel in het gedeelte **Updates verdelen** het selectievakje **Updates naar map kopiëren** in.
4. Voer het UNC-pad naar de gedeelde map in (bijvoorbeeld \\Server\Share\Update distribution).
5. Sla uw wijzigingen op.


*Zo configureert u het updaten vanuit een gedeelde map:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Klik op de knop **Updatebronnen selecteren**.
4. Klik in het venster op de knop **Toevoegen**.
5. Geef in het venster dat wordt geopend het pad naar de gedeelde map.

Het bronadres moet overeenkomen met het adres dat u eerder hebt opgegeven wanneer u het kopiëren van het updatepakket naar de gedeelde map hebt geconfigureerd (zie *instructies hierboven*).

6. Klik op de knop **Selecteren**.
7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.
8. Sla uw wijzigingen op.

## Programmamodules updaten

Updates voor programmamodules verhelpen fouten, verbeteren de prestaties en voegen nieuwe functies toe. Als er een nieuwe update van de programmamodule beschikbaar komt, moet u de installatie van de update bevestigen. U kunt de installatie van een update van een programmamodule bevestigen in de programma-interface of in Kaspersky Security Center. Waar een update beschikbaar is, geeft het programma een melding in het hoofdvenster van Kaspersky Endpoint Security: . Als voor de updates voor de programmamodules de voorwaarden van de Gebruiksrechtovereenkomst moeten worden doorgenomen en aanvaard, installeert het programma de updates nadat de voorwaarden van de Gebruiksrechtovereenkomst zijn aanvaard. Raadpleeg de [Help van Kaspersky Security Center](#) voor details over het bijhouden van updates van programmamodules en het bevestigen van een update in Kaspersky Security Center.

Na het installeren van een programma-update, moet u mogelijk uw computer opnieuw opstarten.


*Zo configureert u updates voor programmamodules:*

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.
2. U ziet nu de lijst met taken: selecteer de taak en klik op .
3. Schakel in het blok **Updates voor programmamodules downloaden en installeren** het selectievakje **Updates voor programmamodules downloaden** in.
4. Selecteer de programmamodule-updates die u wilt installeren.
  - **Essentiële en goedgekeurde updates installeren.** Als deze optie is geselecteerd en updates voor programmamodules beschikbaar zijn, installeert Kaspersky Endpoint Security essentiële updates automatisch en alle andere updates voor programmamodules pas nadat de installatie ervan lokaal is goedgekeurd via de programma-interface of via Kaspersky Security Center.
  - **Alleen goedgekeurde updates installeren.** Als deze optie is geselecteerd en updates voor programmamodules beschikbaar zijn, installeert Kaspersky Endpoint Security updates pas nadat de installatie ervan lokaal is goedgekeurd via de programma-interface of via Kaspersky Security Center. Deze optie is standaard geselecteerd.
5. Sla uw wijzigingen op.

## Een proxyserver voor updates gebruiken

Mogelijk moet u proxyserverinstellingen opgeven om updates voor databases en programmamodules te downloaden vanaf de updatebron. Als er meerdere updatebronnen zijn, worden de proxyserverinstellingen toegepast voor alle bronnen. In het geval dat geen proxyserver vereist is voor bepaalde updatebronnen, kunt u het gebruik van een proxyserver uitschakelen in de beleidseigenschappen. Kaspersky Endpoint Security gebruikt ook een proxyserver om toegang te krijgen tot Kaspersky Security Network en activeringsservers.

*Zo configureert u een verbinding met updatebronnen via een proxyserver:*

1. Klik op  in het hoofdvenster van de Webconsole.  
U ziet nu het venster met eigenschappen van Administration Server.
2. Ga naar het gedeelte **Configuring Internet access**.
3. Schakel het selectievakje **Use proxy server** in.
4. Configureer de instellingen van de proxyserververbinding: het adres en de poort van de proxyserver en de authenticatie-instellingen (gebruikersnaam en wachtwoord).
5. Sla uw wijzigingen op.

*Zo schakelt u het gebruik van een proxyserver voor een specifieke beheergroep uit:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

U ziet nu het venster met de beleidseigenschappen.


3. Selecteer het tabblad **Application settings**.

4. Ga naar **Algemene instellingen** → **Netwerkinstellingen**.

5. Selecteer in het blok **Proxy server settings** **Bypass proxy server for local addresses**.

6. Sla uw wijzigingen op.

*De instellingen van de proxyserver configureren in de programma-interface:*

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

2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.

3. Klik in het blok **Proxyserver** op de koppeling **Proxyserverinstellingen**.

4. Selecteer in het venster dat opent één van de volgende opties voor het bepalen van het proxyserveradres:

- **Detecteer proxyserverinstellingen automatisch.**

Deze optie is standaard geselecteerd. Kaspersky Endpoint Security gebruikt de proxyserverinstellingen die zijn gedefinieerd in de instellingen van het besturingssysteem.

- **Gebruik opgegeven proxyserverinstellingen.**

Als u deze optie hebt geselecteerd, configureert u de instellingen om verbinding te maken met de proxyserver: proxyserveradres en poort.

5. Als u authenticatie op de proxyserver wilt inschakelen, schakelt u het selectievakje **Gebruik proxyserververificatie** in en geeft u uw gebruikersaccountgegevens op.

6. Als u geen proxyserver wilt gebruiken wanneer u [databases en programmamodules](#) vanuit een gedeelde map bijwerkt, schakelt u het selectievakje **Gebruik geen proxyserver voor lokale adressen** in.

7. Sla uw wijzigingen op.

Als gevolg hiervan zal Kaspersky Endpoint Security de proxyserver gebruiken om de programmamodule en database-updates te downloaden. Kaspersky Endpoint Security gebruikt de proxyserver ook om toegang te krijgen tot KSN-servers en Kaspersky-activeringsservers. Als authenticatie vereist is op de proxyserver, maar de inloggegevens van het gebruikersaccount zijn niet verstrekt of zijn onjuist, vraagt Kaspersky Endpoint Security u om de gebruikersnaam en het wachtwoord.

## Laatste 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. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.

2. Klik in de tegel **Vorige versie van databases terugdraaien** op de knop **Terugdraaien**.

Kaspersky Endpoint Security begint met het terugdraaien van de laatste database-update. Het programma toont de voortgang van het terugdraaien, de grootte van de gedownloadde bestanden en de updatebron. U kunt de taak op elk moment stoppen door op **Update stoppen** te klikken.

*Zo start of stopt u het terugdraaien wanneer u de vereenvoudigde programma-interface gebruikt:*

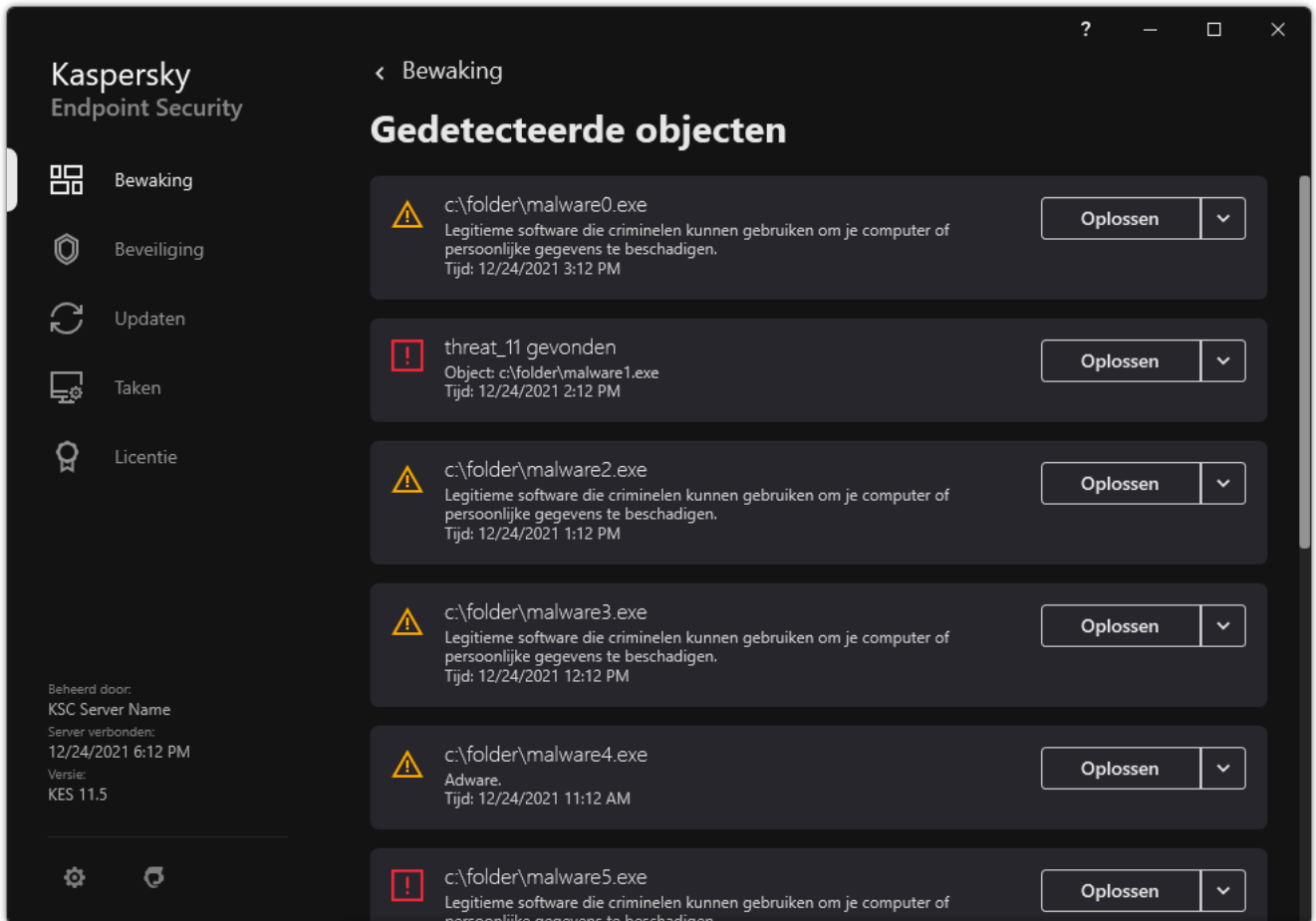
1. Klik rechts om het contextmenu van het programmapictogram in het systeemvak van de taakbalk te openen.

2. Doe in de vervolgkeuzelijst **Taken** in het contextmenu een van het volgende:

- Selecteer een inactieve taak voor terugdraaien om die te starten.
- Selecteer een actieve taak voor terugdraaien om die te stoppen.
- Selecteer een gepauzeerde taak voor terugdraaien om die te hervatten of te herstarten.

## Werken met actieve dreigingen

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 actieve dreigingen vastgelegd (zie de onderstaande afbeelding). Om met actieve dreigingen te werken, gebruikt Kaspersky Endpoint Security de [geavanceerde desinfectietechnologie](#). De geavanceerde desinfectie werkt verschillend voor werkstations en servers. U kunt geavanceerde desinfectie configureren in [Virusscan-taakinstellingen](#) en in [programma-instellingen](#).

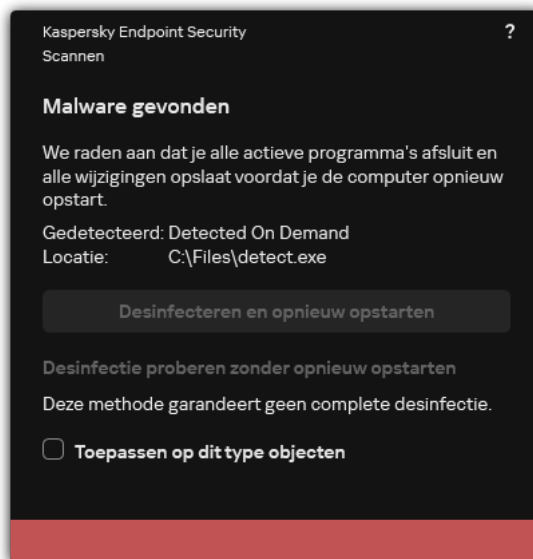


Een lijst met actieve bedreigingen

## Desinfectie van actieve dreigingen op werkstations

Om te werken met actieve dreigingen op werkstations [schakelt u de Geavanceerde desinfectietechnologie](#) in in de programma-instellingen. Configureer vervolgens de gebruikerservaring in de [virusscan](#)-taakeigenschappen. U ziet het selectievakje **Run Advanced Disinfection immediately** in de taakeigenschappen. Als de vlag is ingesteld, voert Kaspersky Endpoint Security desinfectie uit zonder de gebruiker hiervan op de hoogte te stellen. Wanneer de desinfectie voltooid is, wordt de computer opnieuw opgestart. Als de vlag niet is ingesteld, geeft Kaspersky Endpoint Security een melding over actieve dreigingen (zie onderstaande afbeelding). U kunt deze melding niet sluiten zonder het bestand te verwerken.

Een geavanceerde desinfectie tijdens een virusscantaak op een computer wordt alleen uitgevoerd als de functie [Geavanceerde desinfectie is ingeschakeld](#) in de eigenschappen van het beleid dat op deze computer is toegepast.



Melding over actieve dreiging

## Desinfectie van actieve dreigingen op servers

Om met actieve bedreigingen op servers te werken, moet u het volgende doen:

- [De Geavanceerde desinfectietechnologie inschakelen](#) in de programma-instellingen;
- [Onmiddellijke geavanceerde desinfectie inschakelen](#) in de taakeigenschappen van *Virusscan*.

Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Windows for Servers, toont Kaspersky Endpoint Security de melding niet. Daarom kan de gebruiker geen actie selecteren om een actieve dreiging te desinfecteren. Voor de desinfectie van een dreiging moet u [de technologie Geavanceerde desinfectie inschakelen](#) in de programma-instellingen en [directe Geavanceerde desinfectie inschakelen](#) in de instellingen van de taak *Virusscan*. Vervolgens moet u de *virusscantaak* starten.

## Geavanceerde desinfectietechnologie inschakelen of uitschakelen

Als Kaspersky Endpoint Security de malware niet kan tegenhouden, dan kunt u de geavanceerde desinfectietechnologie gebruiken. Geavanceerde desinfectie is standaard uitgeschakeld omdat deze technologie een aanzienlijke hoeveelheid verwerkingsvermogen van de computer gebruikt. Daarom kunt u geavanceerde desinfectie alleen inschakelen [wanneer u met actieve dreigingen werkt](#).

De geavanceerde desinfectie werkt verschillend voor werkstations en servers. Om de technologie op servers te gebruiken, moet u [onmiddellijke geavanceerde desinfectie inschakelen](#) in de eigenschappen van de *virusscantaak*. Deze voorwaarde is niet nodig om de technologie op werkstations te gebruiken.

[Het onderdeel Geavanceerde desinfectietechnologie in- of uitschakelen in de Beheerconsole \(MMC\)](#) 




1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
6. Selecteer of deselecteer in het blok **Uitvoermodus** het selectievakje **Geavanceerde desinfectietechnologie inschakelen** in om de Geavanceerde desinfectietechnologie in of uit te schakelen.
7. Sla uw wijzigingen op.

### [Het onderdeel Geavanceerde desinfectietechnologie in- of uitschakelen in de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Programma-instellingen**.
5. Selecteer of deselecteer in het blok **Operating mode** het selectievakje **Enable Advanced Disinfection technology** in om de Geavanceerde desinfectietechnologie in of uit te schakelen.
6. Sla uw wijzigingen op.

### [Het onderdeel Geavanceerde desinfectietechnologie in de programma-interface in- of uitschakelen](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Selecteer of deselecteer in het blok **Uitvoermodus** het selectievakje **Gebruik Geavanceerde desinfectietechnologie (vereist heel wat computerbronnen)** in om de Geavanceerde desinfectietechnologie in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan kan de gebruiker de meeste functies van het besturingssysteem niet gebruiken terwijl Actieve desinfectie wordt uitgevoerd. Wanneer de desinfectie voltooid is, wordt de computer opnieuw opgestart.



## Verwerking van actieve dreigingen

Een geïnfecteerd bestand wordt beschouwd als *verwerkt* als Kaspersky Endpoint Security het bestand heeft gedesinfecteerd of de dreiging heeft verwijderd als onderdeel van het scannen van de computer op virussen en andere malware.

Kaspersky Endpoint Security verplaatst het bestand naar de lijst met actieve dreigingen als de in de programma-instellingen opgegeven actie om een bepaalde reden niet kan worden uitgevoerd op dit bestand wanneer de computer op virussen en andere dreigingen wordt gescand.

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).
- In de *Virusscan*-taakinstellingen, is de actie voor detectie van bedreigingen ingesteld op **Melden**. Daarna, wanneer de melding van het geïnfecteerde bestand op het scherm werd weergegeven, selecteerde de gebruiker **Over slaan**.

Als er onverwerkte bedreigingen zijn, verandert Kaspersky Endpoint Security het pictogram in: . In het hoofdvenster van het programma wordt de melding van de dreiging weergegeven (zie onderstaande afbeelding). In de Kaspersky Security Center-console wordt de status van de computer gewijzigd in: *Essentieel* - .

### [Een dreiging verwerken in de Beheerconsole \(MMC\)](#)

1. Ga in de Beheerconsole naar de map **Administration Server** → **Extra** → **Opslagplaatsen** → **Actieve dreigingen**.

De lijst met actieve dreigingen wordt geopend.

2. Selecteer het object dat u wilt verwerken.


3. Kies hoe u de dreiging wilt aanpakken:

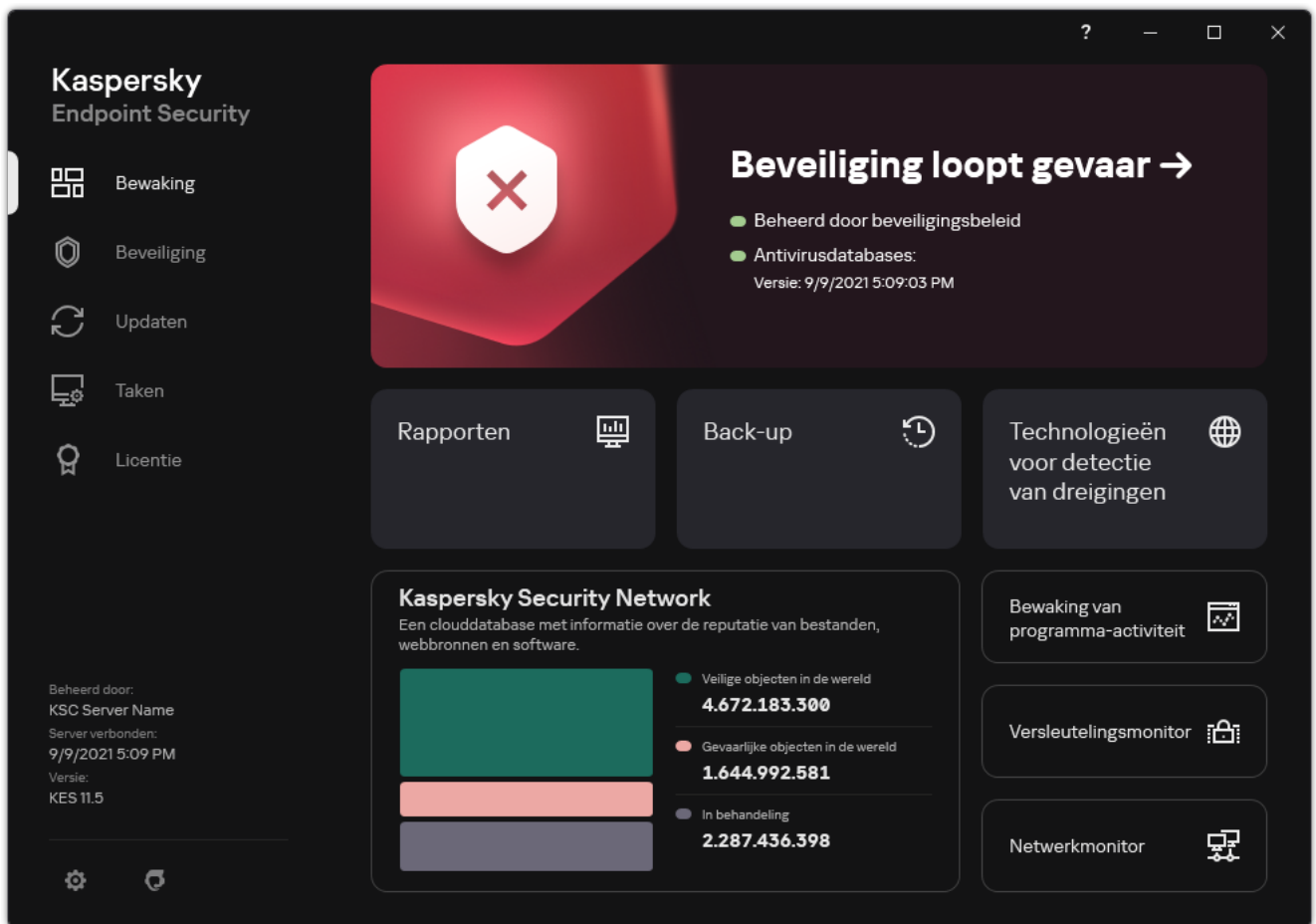
- **Desinfecteren**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.
- **Verwijderen**.

### [Een dreiging verwerken in de Webconsole en de Cloudconsole](#)

1. Selecteer in het hoofdvenster van de webconsole **Activiteiten** → **Opslagplaatsen** → **Actieve dreigingen**.  
De lijst met actieve dreigingen wordt geopend.
2. Selecteer het object dat u wilt verwerken.
3. Kies hoe u de dreiging wilt aanpakken:
  - **Desinfecteren**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.
  - **Verwijderen**.

### Een dreiging verwerken via de programma-interface

1. Ga in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **De bescherming loopt risico**.  
De lijst met actieve dreigingen wordt geopend.
2. Selecteer het object dat u wilt verwerken.
3. Kies hoe u de dreiging wilt aanpakken:
  - **Oplossen**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.
  - **Toevoegen aan uitzonderingen**. Als deze actie is geselecteerd, stelt Kaspersky Endpoint Security voor: [het bestand toevoegen aan de lijst met scanuitsluitingen](#). Instellingen van de uitsluiting worden automatisch geconfigureerd. Als het toevoegen van een uitzondering niet beschikbaar is, betekent dit dat de beheerder het toevoegen van uitzonderingen heeft uitgeschakeld in de beleidsinstellingen.
  - **Negeren**. Als deze optie is geselecteerd, verwijdert Kaspersky Endpoint Security het item uit de lijst met actieve dreigingen. Als er geen actieve dreigingen meer op de lijst staan, wordt de computerstatus gewijzigd in *OK*. Als het object opnieuw wordt gedetecteerd, voegt Kaspersky Endpoint Security een nieuw item toe aan de lijst met actieve dreigingen.
  - **Locatie openen**. Als deze optie wordt geselecteerd, opent Kaspersky Endpoint Security de map met het object in Bestandsverkenner. U kunt het object vervolgens handmatig verwijderen of het object verplaatsen naar een map die niet binnen het beschermd bereik valt.
  - **Meer info**. Als deze optie wordt geselecteerd, opent Kaspersky Endpoint Security de [Kaspersky Virus Encyclopedia website](#) .



Hoofdprogrammavenster wanneer een bedreiging wordt gedetecteerd

# Computerbescherming

## File Threat Protection

Met het onderdeel File Threat Protection voorkomt u dat het bestandssysteem van de computer geïnfecteerd raakt. Standaard bevindt het onderdeel File Threat Protection zich permanent in het RAM van de computer. Het onderdeel scant bestanden op alle schijven van de computer, evenals op aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Het onderdeel scant de bestanden waartoe de gebruiker of het programma toegang heeft. Als een schadelijk bestand wordt gedetecteerd, blokkeert Kaspersky Endpoint Security de bestandsbewerking. Het programma desinfecteert of verwijdert vervolgens het schadelijke bestand, afhankelijk van de instellingen van het onderdeel File Threat Protection.

Als u probeert een bestand te openen waarvan de inhoud is opgeslagen in de OneDrive-cloud, downloadt en scant Kaspersky Endpoint Security de bestandsinhoud.

## File Threat Protection inschakelen en uitschakelen

Het onderdeel File Threat Protection is standaard ingeschakeld en werkt in de modus die door de experts van Kaspersky is aanbevolen. Voor File Threat Protection kan Kaspersky Endpoint Security verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beschermingsniveaus* genoemd: **Hoog**, **Aanbevolen**, **Laag**. De instellingen van het beschermingsniveau **Aanbevolen** worden beschouwd als de optimale instellingen die door experts van Kaspersky worden aanbevolen (zie de onderstaande tabel). 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.

*Zo schakelt u het onderdeel File Threat Protection in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **File Threat Protection** om de component in of uit te schakelen.
4. Als u het onderdeel hebt ingeschakeld, voert u een van de volgende handelingen uit in het blok **Beveiligingsniveau**:
  - Als u een van de vooraf ingestelde beveiligingsniveaus wilt toepassen, selecteer het dan met de schuifregelaar:
    - **Hoog**. Als dit beschermingsniveau is geselecteerd, past het onderdeel File Threat Protection de strikte controle toe op alle bestanden die worden geopend, opgeslagen en gestart. Het onderdeel File Threat Protection scant alle soorten bestanden op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Het onderdeel scant ook archieven, installatiepakketten en ingebedde OLE-objecten.

- **Aanbevolen.** Dit bestandsbeveiligingsniveau wordt aanbevolen door experts van Kaspersky Lab. Het onderdeel File Threat Protection scant alleen de opgegeven soorten bestanden op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer, alsook ingebedde OLE-objecten. Het onderdeel File Threat Protection scant geen archieven of installatiepakketten. De waarden van instellingen voor het aanbevolen beveiligingsniveau staan in de onderstaande tabel.
- **Laag.** De instellingen van dit bestandsbeveiligingsniveau zorgen voor maximale scansnelheid. Het onderdeel File Threat Protection scant alleen bestanden met de opgegeven extensies op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Het onderdeel File Threat Protection scant geen samengestelde bestanden.
- Als u een aangepast beveiligingsniveau wilt configureren, klikt u op de knop **Geavanceerde instellingen** en definieert u uw eigen onderdeelinstellingen.

U kunt de waarden van vooraf ingestelde beschermingsniveaus Aanbevolen beveiligingsniveau herstellen door op de knop Aanbevolen beveiligingsniveau herstellen in het bovenste deel van het venster te klikken.

## 5. Sla uw wijzigingen op.

Instellingen voor File Threat Protection aanbevolen door Kaspersky-experts (aanbevolen beveiligingsniveau)

| Parameter   | Waarde                               | Beschrijving   |
|---|--------------------------------------|--|
| <b>Bestandstypen</b>                              | <b>Bestanden gescand op indeling</b> | Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.  |
| <b>Heuristische analyse</b>                       | <b>Oppervlakkige scan</b>            | 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.<br><br>Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse. |
| <b>Scan alleen nieuwe en gewijzigde bestanden</b> | <b>Aan</b>                           | Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.  |
| <b>iSwift-technologie</b>                         | <b>Aan</b>                           | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.   |
| <b>iChecker-technologie</b>                       | <b>Aan</b>                           | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van   |

|  |   |   |
|--|---|---|
|  |   | de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR). |
| <b>Scan Microsoft Office-bestanden</b>     | <b>Aan</b>  | Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.   |
| <b>Scanmodus</b>                           | <b>Intelligente modus</b>                                   | In deze modus scant File Threat Protection een object op basis van een analyse van acties die zijn uitgevoerd op het object. Wanneer u bijvoorbeeld werkt met een Microsoft Office-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.  |
| <b>Actie bij detectie van een dreiging</b> | <b>Desinfecteren of verwijderen als desinfectie mislukt</b> | Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.  |

## File Threat Protection automatisch pauzeren

U kunt File Threat Protection configureren om automatisch te worden gepauzeerd op een opgegeven tijdstip of wanneer u met specifieke programma's werkt.

U dient File Threat Protection alleen te pauzeren als laatste remedie bij een eventueel conflict met andere programma's. Als er zich conflicten voordoen terwijl een component actief is, wordt u aangeraden contact op te nemen met [Technische Support van Kaspersky](#). De Support-experts zullen u helpen het onderdeel File Threat Protection zodanig te configureren dat u het samen met andere programma's op de computer kunt gebruiken.

*Zo configureert u het automatisch pauzeren van File Threat Protection:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Klik in het blok **File Threat Protection pauzeren** op de koppeling **File Threat Protection pauzeren**.
5. Configureer in het venster dat opent de instellingen voor het pauzeren van File Threat Protection:
  - a. Configureer een schema voor het automatisch pauzeren van File Threat Protection.

- b. Maak een lijst met programma's waarvan de werking ertoe zou moeten leiden dat File Threat Protection zijn activiteiten onderbreekt.

6. Sla uw wijzigingen op.

## De actie wijzigen die het onderdeel File Threat Protection moet uitvoeren op geïnfecteerde bestanden

Standaard probeert het onderdeel File Threat Protection automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Het onderdeel File Threat Protection verwijdert deze bestanden als de desinfectie mislukt.


*Zo wijzigt u de actie die het onderdeel File Threat Protection moet uitvoeren op geïnfecteerde bestanden:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Selecteer in het blok **Actie bij detectie van een dreiging** de relevante optie:
  - **Desinfecteren of verwijderen als desinfectie mislukt.** Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.
  - **Desinfecteren of blokkeren als desinfectie mislukt.** Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.
  - **Blokkeren.** Als deze optie is geselecteerd, blokkeert het onderdeel File Threat Protection automatisch alle geïnfecteerde bestanden zonder eerst te proberen om ze te desinfecteren.

Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt Kaspersky Endpoint Security een reservekopie van het bestand voor het geval u [het bestand moet herstellen of als het in de toekomst kan worden gedesinfecteerd](#).

4. Sla uw wijzigingen op.

## Het beschermd bereik van het onderdeel File Threat Protection instellen




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 het onderdeel File Threat Protection. Standaard scant het onderdeel File Threat Protection alleen [bestanden die mogelijk geïnfecteerd kunnen raken](#)  die vanaf harde schijven, verwisselbare schijven of netwerkschijven worden uitgevoerd.

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



1. Er bestaat een kleine kans dat kwaadaardige code wordt geïntroduceerd in bestanden met bepaalde indelingen en dat deze vervolgens wordt geactiveerd (bijvoorbeeld TXT-indeling). Tegelijkertijd bestaan er ook bestandsindelingen die uitvoerbare code bevatten (zoals .exe, .dll). De uitvoerbare code kan ook opgenomen zijn in bestanden met indelingen die niet voor dit doel bedoeld zijn (bijvoorbeeld het DOC-formaat). Het risico op binnendringing en de activering van schadelijke code in zulke bestanden is groot.
2. Een indringer kan een virus of een ander schadelijk 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 Kaspersky Endpoint Security voor bestanden de bestandsheader, ongeacht de extensie. Als deze analyse aantoont dat het bestand de indeling van een uitvoerbaar bestand heeft (bijvoorbeeld EXE), scant het programma het bestand.

*Zo maakt u het beschermd bereik aan:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Geef in het blok **Bestandstypen** op welke bestanden het onderdeel File Threat Protection moet scannen:
  - **Alle bestanden**. Als deze instelling is ingeschakeld, worden alle bestanden gecontroleerd door Kaspersky Endpoint Security, zonder uitzondering (alle indelingen en extensies).
  - **Bestanden gescand op indeling**. Als deze instelling is ingeschakeld, worden [alleen infecteerbare bestanden](#)  gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.
  - **Bestanden gescand op extensie**. Als deze instelling is ingeschakeld, worden [alleen infecteerbare bestanden](#)  gescand door Kaspersky Endpoint Security. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.
5. Klik op de koppeling **Beschermd bereik bewerken**.
6. Selecteer in het venster dat opent de objecten die u aan het beschermd bereik wilt toevoegen of daarvan wilt uitsluiten.

U kunt geen objecten verwijderen of bewerken die in het standaard beschermd bereik zijn opgenomen.

7. Als u een nieuw object aan het beschermd bereik wilt toevoegen:
  - a. Klik op **Toevoegen**.  
De mappenboom wordt geopend.
  - b. Selecteer een object om toe te voegen aan het beschermd bereik.

U kunt een object van scans uitsluiten zonder het uit de lijst met objecten in het scanbereik te verwijderen. Schakel hiervoor het selectievakje naast het object uit.


8. Sla uw wijzigingen op.

## Scanmethoden gebruiken

Kaspersky Endpoint Security gebruikt de scantechniek Machine learning en een analyse op basis van definities. Tijdens de analyse op basis van definities controleert Kaspersky Endpoint Security of het gevonden object in de database voorkomt. Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.

Om de doeltreffendheid van de bescherming te verhogen, kunt u de heuristische analyse gebruiken. Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.

*Zo configureert u het gebruik van de heuristische analyse door het onderdeel File Threat Protection:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Als u wilt dat het programma heuristische analyse gebruikt voor bescherming tegen bestandsdreigingen, selecteer dan het selectievakje **Heuristische analyse** in het blok **Scanmethoden**. Gebruik dan de schuifregelaar om het niveau van de heuristische analyse in te stellen: **Oppervlakkige scan**, **Gemiddelde scan** of **Gedetailleerde scan**.
5. Sla uw wijzigingen op.

## Scantechnologieën met het onderdeel File Threat Protection gebruiken

*Zo configureert u het gebruik van scantechnologieën door het onderdeel File Threat Protection:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Schakel in het gedeelte **Scantechnologieën** de selectievakjes in naast de namen van de technologieën die u wilt gebruiken voor bescherming tegen bestandsdreigingen.
  - **iSwift-technologie**. Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.

- **iChecker-technologie.** Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).


5. Sla uw wijzigingen op.

## Het scannen van bestanden optimaliseren

U kunt het scannen van bestanden door het onderdeel File Threat Protection optimaliseren door 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.

*Zo optimaliseert u het scannen van bestanden:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Schakel in het blok **Scanoptimalisatie** het selectievakje **Scan alleen nieuwe en gewijzigde bestanden** in.
5. Sla uw wijzigingen op.


## 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.

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

Het onderdeel File Threat Protection desinfecteert samengestelde bestanden met een ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR en ICE-indeling en verwijdert bestanden met alle andere indelingen (behalve e-maildatabases).

Zo configureert u het scannen van samengestelde bestanden:

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Geef in het blok **Scan van samengestelde bestanden** op welke soorten samengestelde bestanden u wilt scannen: archieven, distributiepakketten of Office-bestanden.
5. Als [alleen scannen van nieuwe en gewijzigde bestanden is uitgeschakeld](#), configureer dan de instellingen voor het scannen van elk type samengesteld bestand: scan alle bestanden van dit type of alleen nieuwe bestanden.  
Als het scannen van alleen nieuwe en gewijzigde bestanden is ingeschakeld, scant Kaspersky Endpoint Security alleen nieuwe en gewijzigde bestanden van alle soorten samengestelde bestanden.
6. Configureer de geavanceerde instellingen voor het scannen van samengestelde bestanden.

- **Pak grote samengestelde bestanden niet uit.**

Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde.

Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door Kaspersky Endpoint Security.

Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Pak grote samengestelde bestanden niet uit** is ingeschakeld.

- **Pak samengestelde bestanden op de achtergrond uit.**

Als het selectievakje is ingeschakeld, verleent Kaspersky Endpoint Security toegang tot samengestelde bestanden die groter zijn dan de opgegeven waarde voordat deze bestanden worden gescand. In dit geval zal Kaspersky Endpoint Security samengestelde bestanden op de achtergrond uitpakken en scannen.

Kaspersky Endpoint Security biedt alleen toegang tot samengestelde bestanden die kleiner zijn dan deze waarde na het uitpakken en scannen van deze bestanden.


Als het selectievakje is uitgeschakeld, verleent Kaspersky Endpoint Security pas toegang tot samengestelde bestanden nadat bestanden van elke grootte zijn uitgepakt en gescand.

7. Sla uw wijzigingen op.

## De scanmodus wijzigen

De *scanmodus* verwijst naar de voorwaarde die het scannen van bestanden door het onderdeel File Threat Protection activeert. Standaard scant Kaspersky Endpoint Security bestanden in de intelligente modus. In deze scanmodus beslist het onderdeel File Threat Protection 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **File Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Selecteer in het blok **Scanmodus** de vereiste modus:
  - **Intelligente modus.** In deze modus scant File Threat Protection een object op basis van een analyse van acties die zijn uitgevoerd op het object. Wanneer u bijvoorbeeld werkt met een Microsoft Office-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.
  - **Bij openen en wijzigen.** In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze te openen of te wijzigen.
  - **Bij openen.** In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze te openen.
  - **Bij uitvoeren.** In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze uit te voeren.
5. Sla uw wijzigingen op.

## Web Threat Protection

Het onderdeel Web Threat Protection voorkomt downloads van schadelijke bestanden vanaf het internet en blokkeert ook schadelijke en phishingwebsites. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Kaspersky Endpoint Security scant HTTP-, HTTPS- en FTP-verkeer. Kaspersky Endpoint Security scant URL's en IP-adressen. U kunt [opgeven welke poorten Kaspersky Endpoint Security moet bewaken](#) of gewoon alle poorten selecteren.

Voor de bewaking van HTTPS-verkeer moet u [Versleutelde verbindingen scannen](#) inschakelen.

Wanneer een gebruiker een schadelijke website of phishingwebsite probeert te openen, blokkeert Kaspersky Endpoint Security de toegang en wordt er een waarschuwing weergegeven (zie onderstaande afbeelding).



### Toegang geweigerd

Het opgevraagde webadres kan niet worden weergegeven

[http://kl-test-page.avp.ru/new\\_ksn\\_samples/AVS\\_RISKWARE-KSN\\_BAD.exe](http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe)

**Reden:**

object is geïnfecteerd met [UDS:DangerousObject.Multi.Generic](#)

Bericht gemaakt op: 10/12/2020 7:37:31 PM

kaspersky

Bericht over geweigerde toegang tot website

## Web Threat Protection inschakelen en uitschakelen

Het onderdeel Web Threat Protection is standaard ingeschakeld en werkt in de modus die door de experts van Kaspersky is aanbevolen. Voor Web Threat Protection kan Kaspersky Endpoint Security verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beschermingsniveaus* genoemd: **Hoog, Aanbevolen, Laag**. De instellingen van het beschermingsniveau voor webverkeer **Aanbevolen** worden beschouwd als de optimale instellingen die door experts van Kaspersky worden aanbevolen (zie de onderstaande tabel). U kunt een van de vooraf geïnstalleerde beveiligingsniveaus selecteren voor webverkeer ontvangen of verzonden via de HTTP- en FTP-protocollen, of een aangepast beveiligingsniveau voor webverkeer configureren. Als u de instellingen van het beschermingsniveau voor webverkeer wijzigt, kunt u altijd de aanbevolen instellingen van het beschermingsniveau voor webverkeer herstellen.

Je kunt het beschermingsniveau alleen selecteren of configureren in de beheerconsole (MMC) of de lokale interface van het programma. U kunt het beschermingsniveau in Webconsole of Cloudconsole niet selecteren of configureren.

[Het onderdeel Web Threat Protection in- of uitschakelen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. Gebruik het selectievakje **Web Threat Protection** om het onderdeel in of uit te schakelen.
7. Als u het onderdeel hebt ingeschakeld, voert u een van de volgende handelingen uit in het blok **Beveiligingsniveau**:
  - Als u een van de vooraf ingestelde beveiligingsniveaus wilt toepassen, selecteer het dan met de schuifregelaar:
    - **Hoog**. Het beveiligingsniveau waarmee het internetverkeer dat de computer via de protocollen HTTP en FTP ontvangt zeer grondig wordt gescand door het onderdeel Web Threat Protection. Web Threat Protection scant alle objecten uit het internetverkeer in detail door de complete programmadatabases te gebruiken en voert de meest gedetailleerde [heuristische analyse](#) uit.
    - **Aanbevolen**. Het beschermingsniveau dat het optimale evenwicht tussen prestaties van Kaspersky Endpoint Security en beveiliging van internetverkeer biedt. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit. Dit beschermingsniveau voor internetverkeer wordt door experts van Kaspersky aanbevolen. De waarden van instellingen voor het aanbevolen beveiligingsniveau staan in de onderstaande tabel.
    - **Laag**. De instellingen van dit beschermingsniveau voor webverkeer zorgen voor maximale scansnelheid van webverkeer. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit.


Als u een aangepast beveiligingsniveau wilt configureren, klikt u op de knop **Instellingen** en definieert u uw eigen onderdeelinstellingen.

U kunt de waarden van vooraf ingestelde beschermingsniveaus herstellen door te klikken op de knop **Standaard** onder **Beveiligingsniveau**.
8. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten uit het internetverkeer:
  - **Download blokkeren**. Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, blokkeert het onderdeel Web Threat Protection de toegang tot het object en toont het een bericht in de browser.
  - **Melden**. Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, staat Kaspersky Endpoint Security toe dat het object wordt gedownload naar de computer maar voegt het informatie over het geïnfecteerde object toe aan de lijst met actieve dreigingen.
9. Sla uw wijzigingen op.

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Essential Threat Protection** → **Web Threat Protection** .
5. Gebruik de schakelaar **Web Threat Protection** om de component in of uit te schakelen.
6. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten uit het internetverkeer:
  - **Download blokkeren**. Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, blokkeert het onderdeel Web Threat Protection de toegang tot het object en toont het een bericht in de browser.
  - **Melden**. Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, staat Kaspersky Endpoint Security toe dat het object wordt gedownload naar de computer maar voegt het informatie over het geïnfecteerde object toe aan de lijst met actieve dreigingen.
7. Sla uw wijzigingen op.

[Zo schakelt u het onderdeel Web Threat Protection in en uit](#) 



1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Web Threat Protection** om de component in of uit te schakelen.
4. Als u het onderdeel hebt ingeschakeld, voert u een van de volgende handelingen uit in het blok **Beveiligingsniveau**:
  - Als u een van de vooraf ingestelde beveiligingsniveaus wilt toepassen, selecteer het dan met de schuifregelaar:
    - **Hoog.** Het beveiligingsniveau waarmee het internetverkeer dat de computer via de protocollen HTTP en FTP ontvangt zeer grondig wordt gescand door het onderdeel Web Threat Protection. Web Threat Protection scant alle objecten uit het internetverkeer in detail door de complete programmadatabases te gebruiken en voert de meest gedetailleerde [heuristische analyse](#) uit.
    - **Aanbevolen.** Het beschermingsniveau dat het optimale evenwicht tussen prestaties van Kaspersky Endpoint Security en beveiliging van internetverkeer biedt. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit. Dit beschermingsniveau voor internetverkeer wordt door experts van Kaspersky aanbevolen. De waarden van instellingen voor het aanbevolen beveiligingsniveau staan in de onderstaande tabel.
    - **Laag.** De instellingen van dit beschermingsniveau voor webverkeer zorgen voor maximale scansnelheid van webverkeer. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit.
  - Als u een aangepast beveiligingsniveau wilt configureren, klikt u op de knop **Geavanceerde instellingen** en definieert u uw eigen onderdeelinstellingen.

U kunt de waarden van vooraf ingestelde beschermingsniveaus Aanbevolen beveiligingsniveau herstellen door op de knop Aanbevolen beveiligingsniveau herstellen in het bovenste deel van het venster te klikken.
5. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten uit het internetverkeer:
  - **Download blokkeren.** Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, blokkeert het onderdeel Web Threat Protection de toegang tot het object en toont het een bericht in de browser.
  - **Melden.** Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, staat Kaspersky Endpoint Security toe dat het object wordt gedownload naar de computer maar voegt het informatie over het geïnfecteerde object toe aan de lijst met actieve dreigingen.
6. Sla uw wijzigingen op.

Instellingen voor Web Threat Protection aanbevolen door Kaspersky-experts (aanbevolen beveiligingsniveau)

| Parameter   | Waarde     | Beschrijving  |
|---|------------|---|
| <b>Controleer of het webadres voorkomt in de database met</b> | <b>Aan</b> | Door de koppelingen te scannen om te bepalen of ze zijn opgenomen in de database met kwaadaardige webadressen, kunt u websites volgen die aan de denylist zijn toegevoegd. De database van kwaadaardige webadressen wordt door Kaspersky onderhouden, bij het |

|  |                           |   |
|--|---------------------------|---|
| <b>schadelijke webadressen</b>   |                           | installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security geüpdatet.  |
| <b>Controleer of het webadres voorkomt in de database met phishingadressen</b> | <b>Aan</b>                | De database van phishing-webadressen bevat de webadressen van bekende websites die voor phishing-aanvallen worden gebruikt. Kaspersky vult deze database met phishing-koppelingen aan met adressen die zijn verkregen van de internationale organisatie gekend als Anti-Phishing Working Group. De database van phishing-adressen wordt bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security bijgewerkt.   |
| <b>Gebruik heuristische analyse (Web Threat Protection)</b>                    | <b>Gemiddelde scan</b>    | 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.<br><br>Wanneer webverkeer wordt gescand op virussen en andere toepassingen die een bedreiging vormen, voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse. |
| <b>Gebruik heuristische analyse (anti-phishing)</b>                            | <b>Aan</b>                | 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.   |
| <b>Actie bij detectie van een dreiging</b>                                     | <b>Download blokkeren</b> | Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, blokkeert het onderdeel Web Threat Protection de toegang tot het object en toont het een bericht in de browser.   |

## Methoden voor het detecteren van schadelijke webadressen configureren

Web Threat Protection detecteert kwaadaardige webadressen met behulp van anti-virusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

U kunt detectiemethoden voor schadelijke webadressen alleen selecteren in de beheerconsole (MMC) of de lokale interface van het programma. U kunt geen detectiemethoden voor schadelijke webadressen selecteren in Webconsole of Cloudconsole. De standaardoptie vergelijkt webadressen met de database van kwaadaardige adressen met heuristische analyse (medium scan).

### Scannen met behulp van de database van kwaadaardige adressen


Door de koppelingen te scannen om te bepalen of ze zijn opgenomen in de database met kwaadaardige webadressen, kunt u websites volgen die aan de denylist zijn toegevoegd. De database van kwaadaardige webadressen wordt door Kaspersky onderhouden, bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security geüpdatet.

Kaspersky Endpoint scant alle koppelingen om te bepalen of ze worden vermeld in databases met kwaadaardige webadressen. [De scaninstellingen van het programma](#) voor beveiligde verbindingen hebben geen invloed op de scanfunctionaliteit van koppelingen. Als dus de scan van versleutelde verbindingen is uitgeschakeld, controleert Kaspersky Endpoint Security of koppelingen voorkomen in databases met schadelijke webadressen, zelfs als het netwerkverkeer via een geëncrypte verbinding gaat.

### [Het in- of uitschakelen van het controleren van webadressen in de database van kwaadaardige webadressen met behulp van de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. Klik in het venster **Beveiligingsniveau** op de knop **instellingen**.
7. Dit opent een venster. Selecteer of deselecteer in dat venster onder **Scanmethoden** het selectievakje **Controleer of het webadres voorkomt in de database met schadelijke webadressen** om het controleren van adressen aan de hand van de database met kwaadaardige webadressen in of uit te schakelen.
8. Sla uw wijzigingen op.

### [Het in- of uitschakelen van het controleren van adressen aan de hand van de database met schadelijke adressen in de programmainterface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Selecteer of deselecteer onder **Scanmethoden** het selectievakje **Controleer of het webadres voorkomt in de database met schadelijke webadressen** om adressen te controleren aan de hand van de database met kwaadaardige webadressen.
5. Sla uw wijzigingen op.

## Heuristische analyse

Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van programma's in het besturingssysteem. De heuristische analyse kan dreigingen vinden die momenteel niet voorkomen in de databases van Kaspersky Endpoint Security.

Wanneer webverkeer wordt gescand op virussen en andere toepassingen die een bedreiging vormen, voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.

### [Het gebruik van heuristische analyse in- of uitschakelen in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. Klik in het venster **Beveiligingsniveau** op de knop **instellingen**.
7. Schakel in het blok **Scanmethoden** het selectievakje **Gebruik heuristische analyse** in als u wilt dat het programma heuristische analyse gebruikt bij het scannen van webverkeer op virussen en andere malware.
8. Gebruik de schuifregelaar om het niveau van de heuristische analyse in te stellen: **Oppervlakkige scan**, **Gemiddelde scan** of **Gedetailleerde scan**.

Wanneer webverkeer wordt gescand op virussen en andere toepassingen die een bedreiging vormen, voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.

9. Sla uw wijzigingen op.

### [Het gebruik van heuristische analyse in de programma-interface in- of uitschakelen](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Schakel in het blok **Scanmethoden** het selectievakje **Gebruik heuristische analyse** in als u wilt dat het programma heuristische analyse gebruikt bij het scannen van webverkeer op virussen en andere malware.  
Wanneer webverkeer wordt gescand op virussen en andere toepassingen die een bedreiging vormen, voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.
5. Sla uw wijzigingen op.

## Anti-Phishing

Web Threat Protection controleert koppelingen om te zien of ze behoren tot phishing-webadressen. Dit helpt *phishing-aanvallen* voorkomen. Een phishingaanval kan bijvoorbeeld vermomd zijn als een vermeend 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 messengers, monitort het onderdeel Web Threat Protection pogingen tot het openen van een phishingwebsite tijdens het scannen 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.

U kunt Anti-Phishing alleen configureren in de beheerconsole (MMC) of de lokale interface van het programma. U kunt Anti-Phishing niet configureren in Webconsole of Cloudconsole. Standaard is Anti-Phishing met heuristische analyse ingeschakeld.

[Anti-Phishing inschakelen of uitschakelen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. Klik in het venster **Beveiligingsniveau** op de knop **instellingen**.
7. Dit opent een venster. Selecteer of deselecteer in dat venster, onder **Anti-Phishing-instellingen** het selectievakje **Controleer of het webadres voorkomt in de database met phishingadressen** om Anti-Phishing in of uit te schakelen.

De database van phishing-webadressen bevat de webadressen van bekende websites die voor phishing-aanvallen worden gebruikt. Kaspersky vult deze database met phishing-koppelingen aan met adressen die zijn verkregen van de internationale organisatie gekend als Anti-Phishing Working Group. De database van phishing-adressen wordt bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security bijgewerkt.

8. Selecteer het selectievakje **Gebruik heuristische analyse** in als u wilt dat de toepassing heuristische analyse gebruikt bij het scannen van webpagina's op phishing-koppelingen.

Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van programma's in het besturingssysteem. De heuristische analyse kan dreigingen vinden die momenteel niet voorkomen in de databases van Kaspersky Endpoint Security.

Om koppelingen te scannen, kunt u naast anti-virusdatabase en heuristische analyse, reputatiedatabases gebruiken van [Kaspersky Security Network](#).

9. Sla uw wijzigingen op.

[Het onderdeel Anti-Phishing in de programma-interface in- of uitschakelen](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Als u wilt dat het onderdeel Web Threat Protection controleert of koppelingen voorkomen in de databases met phishingwebadressen, schakelt u in het blok Controleer of het webadres voorkomt in de database met phishingadressen het selectievakje in het blok **Anti-Phishing**. De database van phishing-webadressen bevat de webadressen van bekende websites die voor phishing-aanvallen worden gebruikt. Kaspersky vult deze database met phishing-koppelingen aan met adressen die zijn verkregen van de internationale organisatie gekend als Anti-Phishing Working Group. De database van phishing-adressen wordt bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security bijgewerkt.
5. Schakel het selectievakje **Gebruik heuristische analyse** in als u wilt dat het programma heuristische analyse gebruikt bij het scannen van webpagina's op phishing-koppelingen.

Tijdens de heuristische analyse analyseert Kaspersky Endpoint Security de activiteit van programma's in het besturingssysteem. De heuristische analyse kan dreigingen vinden die momenteel niet voorkomen in de databases van Kaspersky Endpoint Security.

Om koppelingen te scannen, kunt u naast anti-virusdatabase en heuristische analyse, reputatiedatabases gebruiken van [Kaspersky Security Network](#).
6. Sla uw wijzigingen op.

## De lijst met vertrouwde webadressen aanmaken

Naast kwaadaardige en phishing-websites kan Web Threat Protection ook andere websites blokkeren. Web Threat Protection blokkeert bijvoorbeeld HTTP-verkeer dat niet aan de RFC-normen voldoet. U kunt een lijst met URL's maken waarvan u de inhoud vertrouwt. Het onderdeel Web Threat Protection analyseert geen informatie van vertrouwde webadressen om ze te controleren op virussen of andere dreigingen. Deze optie kan bijvoorbeeld nuttig zijn wanneer het onderdeel Web Threat Protection 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.

[Een vertrouwd webadres toevoegen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. Klik in het blok **Beschermingsniveau** op de knop **Instellingen**.
7. Selecteer in het venster dat opent het tabblad **Vertrouwde webadressen**.
8. Selecteer het selectievakje **Scan geen internetverkeer van vertrouwde URL's**.

Als het selectievakje is ingeschakeld, wordt de inhoud van webpagina's of websites waarvan de adressen voorkomen in de lijst met vertrouwde webadressen niet gescand door het onderdeel Web Threat Protection. U kunt zowel het specifieke adres als het adresmasker van een webpagina of website toevoegen aan de lijst met vertrouwde webadressen.
9. Maak een lijst met URL's / webpagina's waarvan u de inhoud vertrouwt.

Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens \* en ? bij de invoer van een masker.

U kunt ook [een lijst met vertrouwde webadressen exporteren vanuit een XML-bestand](#).
10. Sla uw wijzigingen op.

### [Een vertrouwd webadres toevoegen in de Webconsole en de Cloudconsole](#)



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Essential Threat Protection** → **Web Threat Protection**.
5. Selecteer onder **Vetrouwde webadressen** het selectievakje **Scan geen internetverkeer van vertrouwde webadressen**.  
Als het selectievakje is ingeschakeld, wordt de inhoud van webpagina's of websites waarvan de adressen voorkomen in de lijst met vertrouwde webadressen niet gescand door het onderdeel Web Threat Protection. U kunt zowel het specifieke adres als het adresmasker van een webpagina of website toevoegen aan de lijst met vertrouwde webadressen.
6. Maak een lijst met URL's / webpagina's waarvan u de inhoud vertrouwt.  
Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens \* en ? bij de invoer van een masker.  
U kunt ook [een lijst met vertrouwde webadressen exporteren vanuit een XML-bestand](#).
7. Sla uw wijzigingen op.

### [Een vertrouwd webadres maken in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Selecteer het selectievakje **Scan geen internetverkeer van vertrouwde URL's**.  
Als het selectievakje is ingeschakeld, wordt de inhoud van webpagina's of websites waarvan de adressen voorkomen in de lijst met vertrouwde webadressen niet gescand door het onderdeel Web Threat Protection. U kunt zowel het specifieke adres als het adresmasker van een webpagina of website toevoegen aan de lijst met vertrouwde webadressen.
5. Maak een lijst met URL's / webpagina's waarvan u de inhoud vertrouwt.  
Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens \* en ? bij de invoer van een masker.  
U kunt ook [een lijst met vertrouwde webadressen exporteren vanuit een XML-bestand](#).
6. Sla uw wijzigingen op.

Als gevolg hiervan scant Web Threat Protection geen verkeer van vertrouwde webadressen. De gebruiker kan altijd een vertrouwde website openen en een bestand van die website downloaden. Als u geen toegang kon krijgen tot de website, controleer dan de instellingen van de onderdelen [Scan van geëncrypte verbindingen](#), [Webcontrole](#), en [Netwerkpoorten bewaken](#). Als Kaspersky Endpoint Security een bestand gedownload van een vertrouwde website als kwaadaardig detecteert, [kunt u dit bestand toevoegen aan uitzonderingen](#).

U kunt ook [een algemene lijst maken van uitzonderingen van versleutelde verbindingen](#). In dit geval scant Kaspersky Endpoint Security geen HTTPS-verkeer van vertrouwde webadressen wanneer de onderdelene Web Threat Protection, Mail Threat Protection, Webcontrole hun werk doen.

## De lijst met vertrouwde webadressen exporteren en importeren

U kunt de lijst met vertrouwde webadressen exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal webadressen van hetzelfde type toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijst met vertrouwde webadressen of om de lijst naar een andere server te migreren.

[Een lijst met vertrouwde webadressen exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
6. In het blok **Beschermingsniveau**, klikt u op de knop **Instellingen**.
7. Selecteer in het venster dat opent het tabblad **Vertrouwde webadressen**.
8. De lijst met vertrouwde webadressen exporteren:
  - a. Selecteer de vertrouwde webadressen die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen vertrouwd webadres hebt geselecteerd, exporteert Kaspersky Endpoint Security alle webadressen.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met vertrouwde webadressen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met vertrouwde webadressen naar het XML-bestand.
9. De lijst met vertrouwde webadressen importeren:
  - a. Klik op de link **Import**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met vertrouwde adressen wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met vertrouwde adressen heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of of u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.
10. Sla uw wijzigingen op.

[Een lijst met vertrouwde webadressen exporteren en importeren in de Webconsole en Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Essential Threat Protection** → **Web Threat Protection**.
5. De lijst met uitzonderingen in het blok **Trusted web addresses** exporteren:
  - a. Selecteer de vertrouwde webadressen die u wilt exporteren.
  - b. Klik op de link **Export**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met vertrouwde webadressen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met vertrouwde webadressen naar het XML-bestand.
6. De lijst met uitzonderingen in het blok **Trusted web addresses** importeren:
  - a. Klik op de koppeling **Import**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met vertrouwde adressen wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met vertrouwde adressen heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of of u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.
7. Sla uw wijzigingen op.

## Mail Threat Protection

Het onderdeel Mail Threat Protection scant de bijlagen van inkomende en uitgaande e-mailberichten op virussen en andere dreigingen. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Mail Threat Protection kan zowel inkomende als uitgaande berichten scannen. Het programma ondersteunt POP3, SMTP, IMAP en NNTP in de volgende e-mailprogramma's:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express
- Windows Mail

Mail Threat Protection ondersteunt geen andere protocollen en e-mailprogramma's.

Mail Threat Protection kan niet altijd toegang op *protocol-niveau* verkrijgen tot berichten (bijvoorbeeld bij gebruik van de Microsoft Exchange-oplossing). Daarom bevat Mail Threat Protection een [extensie voor Microsoft Office Outlook](#). De extensie maakt het scannen van berichten mogelijk op het *niveau van het e-mailprogramma*. De extensie Mail Threat Protection ondersteunt bewerkingen met Outlook 2010, 2013, 2016 en 2019.

Het onderdeel Mail Threat Protection scant geen berichten als de e-mailclient in een browser is geopend.

Wanneer een schadelijk bestand in een bijlage wordt gedetecteerd, hernoemt Kaspersky Endpoint Security het onderwerp van het bericht als volgt: [Bericht heeft uw deelname nodig voor verwerking] <onderwerp bericht> of [Bericht is verwerkt] <onderwerp bericht>.

## Mail Threat Protection inschakelen en uitschakelen

Het onderdeel Mail Threat Protection is standaard ingeschakeld en werkt in de modus die door de experts van Kaspersky is aanbevolen. Voor Mail Threat Protection past Kaspersky Endpoint Security verschillende groepen instellingen toe. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beschermingsniveaus* genoemd: **Hoog**, **Aanbevolen**, **Laag**. De instellingen van het mailbeschermingsniveau **Aanbevolen** worden beschouwd als de optimale instellingen die door experts van Kaspersky worden aanbevolen (zie de onderstaande tabel). U kunt een van de vooraf geïnstalleerde e-mailbeveiligingsniveaus selecteren of een aangepast e-mailbeveiligingsniveau configureren. Als u de instellingen van een mailbeschermingsniveau hebt gewijzigd, kunt u altijd de aanbevolen instellingen van het e-mailbeschermingsniveau herstellen.

*Zo schakelt u het onderdeel Mail Threat Protection in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Mail Threat Protection** om de component in of uit te schakelen.
4. Als u het onderdeel hebt ingeschakeld, voert u een van de volgende handelingen uit in het blok **Beveiligingsniveau**:
  - Als u een van de vooraf ingestelde beveiligingsniveaus wilt toepassen, selecteer het dan met de schuifregelaar:
    - **Hoog**. Als dit beveiligingsniveau voor e-mails is geselecteerd, worden e-mailberichten zeer grondig gescand door het onderdeel Mail Threat Protection. Het onderdeel Mail Threat Protection scant inkomende en uitgaande e-mailberichten en voert een gedetailleerde heuristische analyse uit. Het hoge e-mailbeveiligingsniveau wordt aanbevolen voor omgevingen met een hoog risico. Een voorbeeld van zulk een omgeving is een verbinding met een gratis e-mailservice vanaf een thuisnetwerk dat niet is beveiligd door een centrale e-mailbescherming.
    - **Aanbevolen**. Het beveiligingsniveau voor e-mails dat het optimale evenwicht tussen prestaties van Kaspersky Endpoint Security en e-mailbeveiliging biedt. Het onderdeel Mail Threat Protection scant inkomende en uitgaande e-mailberichten en voert een normale heuristische analyse uit. Dit beveiligingsniveau voor e-mails wordt door experts van Kaspersky aanbevolen. De waarden van instellingen voor het aanbevolen beveiligingsniveau staan in de onderstaande tabel.

- **Laag.** Als dit beveiligingsniveau voor e-mails is geselecteerd, scant het onderdeel Mail Threat Protection alleen inkomende e-mailberichten, voert het een oppervlakkige heuristische analyse uit en scant het geen archieven die aan e-mailberichten zijn toegevoegd. Met dit beveiligingsniveau voor e-mails scant het onderdeel Mail Threat Protection e-mailberichten op maximale snelheid en gebruikt het zeer weinig bronnen van het besturingssysteem. Het beveiligingsniveau voor e-mails Laag wordt aanbevolen voor gebruik in een goed beveiligde omgeving. Een voorbeeld van zo'n omgeving is een bedrijfsnetwerk met een centrale e-mailbeveiliging.
- Als u een aangepast beveiligingsniveau wilt configureren, klikt u op de knop **Geavanceerde instellingen** en definieert u uw eigen onderdeelinstellingen.

U kunt de waarden van vooraf ingestelde beschermingsniveaus Aanbevolen beveiligingsniveau herstellen door op de knop Aanbevolen beveiligingsniveau herstellen in het bovenste deel van het venster te klikken.

## 5. Sla uw wijzigingen op.

Instellingen voor Mail Threat Protection aanbevolen door Kaspersky-experts (aanbevolen beveiligingsniveau)

| Parameter                                 | Waarde  | Beschrijving  |
|---|---|---|
| <b>Beschermd bereik</b>                   | <b>Inkomende en uitgaande berichten</b>               | <p>Het <i>beschermd bereik</i> omvat objecten die door het onderdeel worden gecontroleerd wanneer het wordt uitgevoerd: inkomende en uitgaande berichten of alleen inkomende berichten.</p> <p>Om uw computers te beschermen, hoeft u alleen inkomende berichten te scannen. U kunt het scannen op uitgaande berichten inschakelen om te voorkomen dat geïnfecteerde bestanden in archieven worden verzonden. U kunt ook het scannen van uitgaande berichten inschakelen als u wilt voorkomen dat bestandformaten worden verzonden, zoals audio- en videobestanden.</p> |
| <b>Verbind Microsoft Outlook-extensie</b> | <b>Aan</b>  | <p>Als het selectievakje is ingeschakeld, worden de e-mailberichten die via de POP3-, SMTP-, NNTP- en IMAP-protocollen worden verstuurd gescand met behulp van de extensie die in Microsoft Outlook is geïntegreerd.</p> <p>Als e-mail wordt gescand met de extensie voor Microsoft 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 <a href="#">Microsoft Knowledge Base</a>.</p>                                   |
| <b>Scan toegevoegde archieven</b>         | <b>Aan</b>  | ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling   |
| <b>Scan Microsoft Office-bijlagen</b>     | <b>Aan</b>  | Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.   |
| <b>Filter voor bijlagen</b>               | <b>Naam van geselecteerde typen bijlagen wijzigen</b> | Als deze optie geselecteerd is, zal het onderdeel Mail Threat Protection het laatste extensie-teken in de bijgevoegde bestanden van de gespecificeerde types vervangen door het onderstrepingssteken (bijvoorbeeld bijlage.doc_). Dus om het bestand te openen, moet de gebruiker het bestand hernoemen.  |
| <b>Heuristische analyse</b>               | <b>Gemiddelde scan</b>                                | 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.   |

|  |   |  |
|--|---|--|
|  |   | Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.    |
| <b>Actie bij detectie van een dreiging</b> | <b>Desinfecteren of verwijderen als desinfectie mislukt</b> | Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. De gebruiker krijgt dan toegang tot het bericht met een veilige bijlage. Als het object niet kan worden gedesinfecteerd, verwijdert Kaspersky Endpoint Security het geïnfecteerde object. Kaspersky Endpoint Security voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht: [Bericht is verwerkt] <onderwerp van bericht>. |

## De uit te voeren actie op geïnfecteerde e-mailberichten wijzigen

Standaard probeert het onderdeel Mail Threat Protection automatisch om alle gevonden geïnfecteerde e-mailberichten te desinfecteren. Het onderdeel Mail Threat Protection verwijdert de geïnfecteerde e-mailberichten als de desinfectie mislukt.

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

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het venster met de programma-instellingen.
3. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren wanneer een geïnfecteerd bericht wordt gevonden:
  - **Desinfecteren of verwijderen als desinfectie mislukt.** Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. De gebruiker krijgt dan toegang tot het bericht met een veilige bijlage. Als het object niet kan worden gedesinfecteerd, verwijdert Kaspersky Endpoint Security het geïnfecteerde object. Kaspersky Endpoint Security voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht: [Bericht is verwerkt] <onderwerp van bericht>.
  - **Desinfecteren of blokkeren als desinfectie mislukt.** Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. De gebruiker krijgt dan toegang tot het bericht met een veilige bijlage. Als het object niet kan worden gedesinfecteerd, voegt Kaspersky Endpoint Security een waarschuwing toe aan het onderwerp van het bericht: [Bericht heeft uw medewerking nodig voor verwerking] <onderwerp van bericht>. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert Kaspersky Endpoint Security de verzending van het bericht en toont het e-mailprogramma een fout.


- **Blokkeren.** Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt Kaspersky Endpoint Security een waarschuwing toe aan het onderwerp van het bericht: [Bericht heeft uw deelname nodig voor verwerking] <onderwerp van bericht>. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert Kaspersky Endpoint Security de verzending van het bericht en toont het e-mailprogramma een fout.

4. Sla uw wijzigingen op.

## Het beschermd bereik van het onderdeel Mail Threat Protection instellen

Onder *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 het onderdeel Mail Threat Protection omvatten de instellingen voor de integratie van het onderdeel Mail Threat Protection in e-mailprogramma's en het type e-mailberichten en het verkeer van de e-mailprotocollen die door het onderdeel Mail Threat Protection 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 stelt u het beschermd bereik van het onderdeel Mail Threat Protection in:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Selecteer in het blok **Beschermd bereik** de berichten die u wilt scannen:
  - **Inkomende en uitgaande berichten.**
  - **Alleen inkomende berichten.**

Om uw computers te beschermen, hoeft u alleen inkomende berichten te scannen. U kunt het scannen op uitgaande berichten inschakelen om te voorkomen dat geïnfecteerde bestanden in archieven worden verzonden. U kunt ook het scannen van uitgaande berichten inschakelen als u wilt voorkomen dat bestandformaten worden verzonden, zoals audio- en videobestanden.

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.

5. In het blok **Connectiviteit** doet u het volgende:

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



Schakel het selectievakje **Scan POP3-, SMTP-, NNTP- en IMAP-verkeer** uit als u niet wilt dat Mail Threat Protection berichten scant die zijn verstuurd via de protocollen POP3, SMTP, NNTP en IMAP voordat ze op de computer van de gebruiker terechtkomen. In dit geval worden berichten gescand door de Mail Threat Protection-extensie 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 **Verbind Microsoft Outlook-extensie** is ingeschakeld.

Als u een ander e-mailprogramma dan Microsoft Office Outlook gebruikt, scant Mail Threat Protection geen berichten die zijn verstuurd via de protocollen POP3, SMTP, NNTP en IMAP wanneer het selectievakje **Scan POP3-, SMTP-, NNTP- en IMAP-verkeer** is uitgeschakeld.

- Als u de instellingen van Mail Threat Protection 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 **Verbind Microsoft Outlook-extensie** in.

Als u de toegang tot de instellingen van Mail Threat Protection 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 **Verbind Microsoft Outlook-extensie** uit.

De extensie van Mail Threat Protection wordt tijdens de installatie van Kaspersky Endpoint Security ingesloten in Microsoft Office Outlook.

6. Sla uw wijzigingen op.

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

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.

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

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer in het venster met programma-instellingen **Essential Threat Protection** → **Mail Threat Protection**.
3. Klik op **Geavanceerde instellingen**.
4. Configureer de scaninstellingen in het blok **Scan van samengestelde bestanden**:
  - **Scan bijgevoegde bestanden van Microsoft Office-formaten.** Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.
  - **Scan bijgevoegde archieven.** ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling

Als Kaspersky Endpoint Security tijdens de scan een wachtwoord voor een archief in de tekst van het bericht detecteert, wordt dit wachtwoord gebruikt om de inhoud van het archief te scannen op kwaadaardige programma's. In dit geval wordt het wachtwoord niet opgeslagen. Een archief wordt tijdens het scannen uitgepakt. Als er een programmafout optreedt tijdens het uitpakken, kunt u de uitgepakte bestanden handmatig verwijderen. Deze bestanden worden opgeslagen in het volgende pad: %systemroot%\temp. De bestanden hebben het voorvoegsel PR.

- **Scan geen archieven die groter zijn dan N MB.** Als dit selectievakje is ingeschakeld, worden archieven die aan e-mailberichten zijn toegevoegd en die groter dan de opgegeven waarde zijn niet gescand door het onderdeel Mail Threat Protection. Als het selectievakje is uitgeschakeld, worden toegevoegde archieven van elke grootte gescand door het onderdeel Mail Threat Protection.
- **Beperk de tijd voor het controleren van archieven tot N sec.** Als het selectievakje is ingeschakeld, is de toegestane scanduur voor archieven die aan e-mailberichten zijn toegevoegd beperkt tot de opgegeven tijd.

5. Sla uw wijzigingen op.

## Filteren van bijlagen van e-mailberichten

De functionaliteit voor het filteren van bijlagen wordt niet toegepast op uitgaande e-mailberichten.

Schadelijke 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 schadelijk programma.

*Zo configureert u een filter voor bijlagen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Doe in het blok **Filter voor bijlagen** een van het volgende:
  - **Filteren uitschakelen.** Als deze optie is geselecteerd, worden bestanden die aan e-mailberichten zijn toegevoegd niet gefilterd door het onderdeel Mail Threat Protection.
  - **Naam van geselecteerde typen bijlagen wijzigen.** Als deze optie geselecteerd is, zal het onderdeel Mail Threat Protection het laatste extensie-teken in de bijgevoegde bestanden van de gespecificeerde types vervangen door het onderstrepingssteken (bijvoorbeeld bijlage.doc\_). Dus om het bestand te openen, moet de gebruiker het bestand hernoemen.
  - **Geselecteerde typen bijlagen verwijderen.** Als deze optie is geselecteerd, verwijdert het onderdeel Mail Threat Protection de opgegeven soorten toegevoegde bestanden uit e-mailberichten.
5. Als u tijdens de vorige stap de opties **Naam van geselecteerde typen bijlagen wijzigen** of **Geselecteerde typen bijlagen verwijderen** hebt geselecteerd, schakelt u de selectievakjes naast de relevante typen

bestanden in.

6. Sla uw wijzigingen op.

## Extensies exporteren en importeren voor het filteren van bijlagen

U kunt de lijst met filterextensies voor bijlagen exporteren naar een XML-bestand. U kunt de export/import-functie gebruiken om een back-up te maken van de lijst met extensies of om de lijst naar een andere server te migreren.

### [Een lijst met filterextensies voor bijlagen exporteren en importeren in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het beleidsvenster.
6. In het blok **Beschermingsniveau**, klikt u op de knop **Instellingen**.
7. Selecteer in het venster dat opent het tabblad **Filter voor bijlagen**.
8. De lijst met extensies exporteren:
  - a. Selecteer de extensies die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met extensies wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.

Kaspersky Endpoint Security exporteert de volledige lijst met extensies naar het XML-bestand.
9. De lijst met extensies importeren:
  - a. Klik op de link **Import**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met extensies wilt importeren.
  - c. Open het bestand.

Als de computer al een lijst met extensies heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of of u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.
10. Sla uw wijzigingen op.

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Essential Threat Protection** → **Mail Threat Protection**.
5. De lijst met extensies in het blok **Attachment filter** exporteren:
  - a. Selecteer de extensies die u wilt exporteren.
  - b. Klik op de link **Export**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met extensies wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met extensies naar het XML-bestand.
6. De lijst met extensies in het blok **Attachment filter** importeren:
  - a. Klik op de koppeling **Import**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met extensies wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met extensies heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of of u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.
7. Sla uw wijzigingen op.

## E-mails in Microsoft Office Outlook scannen

Tijdens de installatie van Kaspersky Endpoint Security wordt de Mail Threat Protection-extensie ingesloten in Microsoft Office Outlook (hierna ook Outlook genoemd). Hiermee kunt u de instellingen van Mail Threat Protection vanuit Outlook openen en kunt u opgeven welke e-mailberichten moeten worden gescand op virussen en andere dreigingen. De extensie van Mail Threat Protection voor Outlook kan inkomende en uitgaande berichten scannen die via de protocollen POP3, SMTP, NNTP, IMAP en MAPI worden verstuurd en ontvangen. Kaspersky Endpoint Security ondersteunt ook het werken met andere e-mailclients (inclusief Microsoft Outlook Express®, Windows Mail en Mozilla™ Thunderbird™).

De extensie Mail Threat Protection ondersteunt bewerkingen met Outlook 2010, 2013, 2016 en 2019.

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

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

De instellingen van het onderdeel Mail Threat Protection kunnen rechtstreeks in Outlook worden geconfigureerd als [Microsoft Office Outlook-extensie is aangesloten](#) in de interface van Kaspersky Endpoint Security is ingeschakeld.

Uitgaande berichten worden eerst gescand door de Mail Threat Protection-extensie voor Outlook en dan door het onderdeel Mail Threat Protection.

Als e-mail wordt gescand met de extensie voor Mail Threat Protection 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](#).

*De uitvoermodus van de extensie Mail Threat Protection-extensie voor Outlook configureren met Kaspersky Security Center:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het beleidsvenster.
6. In het blok **Beschermingsniveau**, klikt u op de knop **Instellingen**.
7. In het blok **Connectiviteit**, klikt u op de knop **Instellingen**.
8. In het venster **E-mailbescherming** doet u het volgende:
  - Schakel het selectievakje **Scannen bij ontvangen** in als u wilt dat de Mail Threat Protection-extensie voor Outlook inkomende berichten scant zodra ze in de mailbox aankomen.
  - Schakel het selectievakje **Scannen bij lezen** in als u wilt dat de Mail Threat Protection-extensie voor Outlook inkomende berichten scant wanneer de gebruiker ze opent.
  - Schakel het selectievakje **Scannen bij verzenden** in als u wilt dat de Mail Threat Protection-extensie voor Outlook uitgaande berichten scant wanneer ze worden verzonden.
9. Sla uw wijzigingen op.

## Network Threat Protection

Het onderdeel Network Threat Protection scant inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Wanneer Kaspersky Endpoint Security een poging tot netwerkaanval op de computer van een gebruiker detecteert, blokkeert het de netwerkverbinding met de aanvallende computer. 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 Threat Protection wordt bijgewerkt wanneer [de databases en de modules van het programma worden bijgewerkt](#).

## Network Threat Protection inschakelen en uitschakelen

Network Threat Protection is standaard ingeschakeld en werkt in de optimale modus. U kunt indien nodig Network Threat Protection uitschakelen.


*Zo schakelt u Network Threat Protection in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Network Threat Protection** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan scant Kaspersky Endpoint Security, als Network Threat Protection is ingeschakeld, inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Wanneer Kaspersky Endpoint Security een poging tot netwerkaanval op de computer van een gebruiker detecteert, blokkeert het de netwerkverbinding met de aanvallende computer.

## Een aanvallende computer blokkeren

*Een aanvallende computer te blokkeren:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het venster met de programma-instellingen.
3. Selecteer het selectievakje **Voeg een aanvallende computer toe aan de lijst met geblokkeerde computers gedurende N min.**

Als het selectievakje is ingeschakeld, voegt Network Threat Protection de aanvallende computer toe aan de lijst met geblokkeerde computers. Dit betekent dat de netwerkverbinding met de aanvallende computer na de eerste netwerkaanval een bepaalde tijd wordt geblokkeerd door het onderdeel Network Threat Protection. Deze blokkering beschermt de gebruiker automatisch tegen mogelijke nieuwe netwerkaanvallen vanaf hetzelfde adres.

De minimale tijd die een aanvallende computer in de blokkeerlijst moet doorbrengen, is één minuut. De maximale tijd is 32 768 minuten.

U kunt de blokkeerlijst bekijken in het venster van het [Netwerkmonitor-tool](#).

Kaspersky Endpoint Security wist de blokkeerlijst wanneer het programma opnieuw wordt opgestart en wanneer de instellingen voor Network Threat Protection worden gewijzigd.


1. Stel een andere blokkeringsduur in voor een aanvallende computer in het veld rechts van het selectievakje **Voeg een aanvallende computer toe aan de lijst met geblokkeerde computers gedurende N min.**
2. Sla uw wijzigingen op.

Wanneer Kaspersky Endpoint Security hierdoor een poging tot netwerkaanval tegen de computer van een gebruiker detecteert, blokkeert het alle netwerkverbindingen met de aanvallende computer.

## Adressen configureren die niet moeten worden geblokkeerd

Kaspersky Endpoint Security kan een netwerkaanval herkennen en een onbeveiligde netwerkverbinding blokkeren die een groot aantal pakketten verzendt (bijvoorbeeld van bewakingscamera's). Om met vertrouwde apparaten te werken, kunt u de IP-adressen van deze apparaten toevoegen aan de lijst met uitzonderingen.

*Zo configureert u adressen die niet moeten worden geblokkeerd:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het venster met de programma-instellingen.
3. Klik op de koppeling **Uitzonderingen beheren**.
4. Klik in het geopende venster op de knop **Toevoegen**.
5. Voer het IP-adres van de computer dat niet moet worden geblokkeerd als er netwerkaanvallen vanaf dat adres plaatsvinden.
6. Sla uw wijzigingen op.

Als gevolg hiervan volgt Kaspersky Endpoint Security de activiteit van apparaten op de lijst met uitzonderingen niet.

## De lijst met uitzonderingen voor blokkeren exporteren en importeren

U kunt de lijst met uitzonderingen exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal adressen van hetzelfde type toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijst met uitzonderingen of om de lijst naar een andere server te migreren.

[Een lijst met uitzonderingen exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het beleidsvenster.
6. In het blok **Instellingen van Network Threat Protection**, klikt u op de knop **Uitzonderingen**.
7. De lijst met regels exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen uitzonderingen hebt geselecteerd, exporteert Kaspersky Endpoint Security alle uitzonderingen.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
8. De lijst met uitzonderingen importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
9. Sla uw wijzigingen op.

[Een lijst met uitzonderingen exporteren en importeren in de Webconsole en Cloudconsole](#) 



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Essential Threat Protection** → **Network Threat Protection**.
5. Klik in het blok **Network Threat Protection settings** op de koppeling **Exclusions**.  
De lijst met uitzonderingen wordt geopend.
6. De lijst met regels exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde uitzonderingen wilt exporteren of de volledige lijst met uitzonderingen wilt exporteren.
  - d. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - e. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
7. De lijst met uitzonderingen importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

## Beveiliging tegen netwerkaanvallen configureren op type

Met Kaspersky Endpoint Security kunt u de bescherming tegen de volgende soorten netwerkaanvallen beheren:

- *Network Flooding* is een aanval op netwerkbronnen van een organisatie (zoals webservers). Deze aanval bestaat uit het verzenden van een groot aantal verzoeken om de bandbreedte van netwerkbronnen te overbelasten. Wanneer dit gebeurt, hebben gebruikers geen toegang meer tot de netwerkbronnen van de organisatie.
- Een *Port Scanning*-aanval bestaat uit het scannen van de UDP-poorten, TCP-poorten en netwerkservices op de computer. Met deze aanval kan de aanvaller de mate van kwetsbaarheid van de computer bepalen voordat hij


gevaarlijkere netwerkaanvallen uitvoert. Met Port Scanning kan de aanvaller ook het besturingssysteem op de computer identificeren en de juiste netwerkaanvallen voor dit besturingssysteem kiezen.

- Bij een *MAC-spoofing-aanval* wordt het MAC-adres van een netwerkapparaat (netwerkaart) gewijzigd. Als gevolg hiervan kan een aanvaller gegevens die naar een apparaat zijn verzonden, omleiden naar een ander apparaat en toegang krijgen tot deze gegevens. Via Kaspersky Endpoint Security kunt u MAC-adresvervalsing blokkeren en meldingen over deze aanvallen ontvangen.

U kunt de detectie van dit soort aanvallen uitschakelen voor het geval dat sommige van uw toegestane programma's bewerkingen uitvoeren die typisch zijn voor dit soort aanvallen. Dit helpt om vals alarm te voorkomen.


Kaspersky Endpoint Security bewaakt standaard niet tegen Network Flooding, Port Scanning en MAC-spoofing-aanvallen.

*Beveiliging tegen netwerkaanvallen configureren op type:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Behandel poortscans en flooding als aanvallen** om detectie van deze aanvallen in of uit te schakelen.
4. Gebruik de schakelaar **MAC spoofing-bescherming**.
5. Selecteer in het blok **Bij detectie van een MAC-spoofingaanval** een van de volgende opties:
  - **Alleen melden.**
  - **Melden en blokkeren.**
6. Sla uw wijzigingen op.

## Firewall

De Firewall blokkeert ongeautoriseerde verbindingen met de computer tijdens het werken op internet of een lokaal netwerk. De Firewall controleert ook de netwerkactiviteit van programma's op de computer. Hierdoor kunt u uw bedrijfs-LAN beschermen tegen identiteitsdiefstal en andere aanvallen. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en vooraf gedefinieerde *netwerkregels*.

Network Agent wordt gebruikt voor interactie met Kaspersky Security Center. Firewall maakt automatisch netwerkregels die nodig zijn voor de werking van het programma en de netwerkagent. Als gevolg hiervan opent de firewall verschillende poorten op de computer. Welke poorten worden geopend, is afhankelijk van de rol van de computer (bijvoorbeeld distributiepunt). Raadpleeg de [help van Kaspersky Security Center](#)  voor meer informatie over de poorten die op de computer worden geopend.

## Netwerkregels

U kunt netwerkregels op de volgende niveaus configureren:

- *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. Kaspersky Endpoint Security heeft vooraf gedefinieerde netwerkpakketregels met machtigingen die worden aanbevolen door Kaspersky-experts.
- *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.

Beheerde toegang van programma's tot bronnen, processen en persoonlijke gegevens van het besturingssysteem wordt geleverd door het [Host Intrusion Prevention-onderdeel](#) met behulp van *programmarechten*.

Wanneer een programma voor de eerste keer wordt opgestart, voert de Firewall de volgende acties uit:

1. Controleert de beveiliging van het programma aan de hand van gedownloadte antivirusdatabases.
2. Controleert in Kaspersky Security Network of de website veilig is.

Het wordt aanbevolen [deel te nemen aan Kaspersky Security Network](#) zodat het onderdeel Firewall efficiënter kan werken.

3. Zet het programma in één van de *vertrouwensgroepen*: Vertrouwd, Deels beperkt, Zeer beperkt, of Niet vertrouwd.

Een [vertrouwensgroep definieert de rechten](#) die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd. Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep, afhankelijk van het risico dat dit programma voor de computer kan opleveren.

Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep voor de onderdelen Firewall en Host Intrusion Prevention. U kunt de vertrouwensgroep niet uitsluitend voor de firewall of voor Host Intrusion Prevention wijzigen.

Als deelname aan KSN hebt geweigerd of als er geen netwerk is, plaatst Kaspersky Endpoint Security het programma in een vertrouwensgroep, afhankelijk van de [instellingen van het Host Intrusion Prevention-onderdeel](#). Nadat de reputatie van het programma is ontvangen van KSN, kan de vertrouwensgroep automatisch worden gewijzigd.

4. Dit blokkeert de netwerkactiviteit van het programma, afhankelijk van de vertrouwensgroep. Programma's in de vertrouwensgroep 'Zeer beperkt' mogen bijvoorbeeld geen netwerkverbindingen gebruiken.

De volgende keer dat het programma wordt gestart, controleert Kaspersky Endpoint Security de integriteit van het programma. Als het programma niet is gewijzigd, gebruikt het onderdeel de huidige netwerkregels ervoor. Als het programma is gewijzigd, analyseert Kaspersky Endpoint Security het programma alsof het voor het eerst wordt gestart.

## Prioriteiten voor netwerkregels

Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als netwerkactiviteit aan meerdere regels wordt toegevoegd, regelt de Firewall de netwerkactiviteit volgens de regel met de hoogste prioriteit.

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.

## Status van netwerkverbinding

U kunt met de Firewall de netwerkactiviteit beheren, afhankelijk van de status van de netwerkverbinding. Kaspersky Endpoint Security ontvangt de netwerkverbindingstatus van het besturingssysteem van de computer. De status van de netwerkverbinding in het besturingssysteem wordt door de gebruiker ingesteld bij het opzetten van de verbinding. U kunt [de status van de netwerkverbinding wijzigen in de instellingen van Kaspersky Endpoint Security](#). De firewall controleert de netwerkactiviteit afhankelijk van de netwerkstatus in de Kaspersky Endpoint Security-instellingen en niet in het besturingssysteem.

De netwerkverbinding kan de volgende status hebben:

- **Openbaar netwerk.** Het netwerk wordt niet beschermd door antivirusprogramma's, firewalls of filters (zoals wifi in een café). 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.** Netwerk voor gebruikers met beperkte toegang tot bestanden en printers op deze computer (zoals voor een bedrijfsnetwerk of thuisnetwerk).
- **Vertrouwd netwerk.** 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.

## Firewall inschakelen en uitschakelen

Firewall is standaard ingeschakeld en werkt in de optimale modus.

*Zo schakelt u Firewall in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met programma-instellingen.

3. Gebruik de schakelaar **Firewall** om het onderdeel in of uit te schakelen.

4. Sla uw wijzigingen op.

Daarom, als de firewall is ingeschakeld, controleert Kaspersky Endpoint Security de netwerkactiviteit en blokkeert onbevoegde netwerkverbindingen met uw computer en blokkeert onbevoegde netwerkactiviteit van programma's op uw computer. Netwerkactiviteit wordt ook gecontroleerd door het onderdeel [Network Threat Protection](#). Het onderdeel Network Threat Protection scant inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen.

Kaspersky Endpoint Security registreert netwerkaanvallen in rapporten, ongeacht de firewall-instellingen. Zelfs als de firewall de netwerkverbinding blokkeert met behulp van regels en zo een netwerkaanval voorkomt, registreert het onderdeel Network Threat Protection toch netwerkaanvallen. Het is vereist om statistische informatie te genereren over netwerkaanvallen op de computers in uw organisatie.

## Status van de netwerkverbinding wijzigen

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

*Zo wijzigt u de status van de netwerkverbinding:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Beschikbare netwerken**.
4. Selecteer de netwerkverbinding waarvan u de status wilt wijzigen.
5. Selecteer in de kolom **Netwerktipe** de status van de netwerkverbinding:
  - **Openbaar netwerk**. Het netwerk wordt niet beschermd door antivirusprogramma's, firewalls of filters (zoals wifi in een café). 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.
  - **Lokaal netwerk**. Netwerk voor gebruikers met beperkte toegang tot bestanden en printers op deze computer (zoals voor een bedrijfsnetwerk of thuisnetwerk).
  - **Vertrouwd netwerk**. 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.
6. Sla uw wijzigingen op.

## 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 maken

U kunt op de volgende manieren een netwerkpakketregel maken:

- Gebruik de tool [Netwerkmonitor](#).

*Netwerkmonitor* is een tool ontworpen voor de realtime weergave van informatie over de netwerkactiviteit van de computer van een gebruiker. Dit is handig omdat u niet alle regelinstellingen hoeft te configureren. Sommige Firewall-instellingen worden automatisch ingevoegd vanuit Netwerkmonitor-gegevens. Netwerkmonitor is alleen beschikbaar in de programma-interface.

- De instellingen van Firewall configureren:

Hiermee kunt u de Firewall-instellingen verfijnen. U kunt regels maken voor elke netwerkactiviteit, zelfs als er momenteel geen netwerkactiviteit is.

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

## De tool Netwerkmonitor gebruiken om een netwerkpakketregel in de programma-interface te maken

1. Ga in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **Netwerkmonitor**.
2. Selecteer het tabblad **Netwerkactiviteit**.

Op het tabblad **Netwerkactiviteit** ziet u alle huidige actieve netwerkverbindingen van de computer. Zowel uitgaande als inkomende netwerkverbindingen worden weergegeven.
3. Selecteer in het contextmenu van een netwerkverbinding de optie **Regel voor netwerkpakketten maken**.

Dit opent de eigenschappen van de netwerkregel.
4. Stel de status **Actief** in voor de pakketregel.
5. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
6. Configureer de netwerkregelinstellingen (zie onderstaande tabel).

U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Sjabloon voor netwerkregel** te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.

Alle instellingen voor netwerkregels worden automatisch ingevuld.
7. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
8. Klik op **Opslaan**.


De nieuwe netwerkregel wordt aan de lijst toegevoegd.
9. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
10. Sla uw wijzigingen op.

## Firewall-instellingen gebruiken om een netwerkpakketregel in de programma-interface te maken

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Pakketregels**.  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
4. Klik op **Toevoegen**.  
Dit opent de eigenschappen van de netwerkregel.
5. Stel de status **Actief** in voor de pakketregel.
6. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
7. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Sjabloon voor netwerkregel** te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.
8. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
9. Klik op **Opslaan**.  
De nieuwe netwerkregel wordt aan de lijst toegevoegd.
10. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
11. Sla uw wijzigingen op.

[Een netwerkpakketregel maken in de Beheerconsole \(MMC\)](#) 



1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.
6. In het blok **Firewall-instellingen**, klikt u op de knop **Instellingen**.  
Dit opent de lijst met netwerkpakketregels en de lijst met netwerkregels voor programma's.
7. Selecteer het tabblad **Regels voor netwerkpakketten**.  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
8. Klik op **Toevoegen**.  
Dit opent de pakketregeleigenschappen.
9. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
10. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de knop  te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.
11. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
12. Sla de netwerkregel op.
13. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
14. Sla uw wijzigingen op.

De Firewall controleert netwerkpakketten volgens de regel. U kunt een pakketregel uitschakelen via Firewall zonder deze uit de lijst te verwijderen. Schakel hiervoor het selectievakje naast het object uit.

[Een regel voor netwerkpakketten maken in de webconsole en de cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Selecteer **Essential Threat Protection** → **Firewall**.
5. Klik in het blok **Instellingen van Firewall** op de koppeling **Regels voor netwerkpakketten** .  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
6. Klik op de knop **Add**.  
Dit opent de pakketregeleigenschappen.
7. Voer de naam van de netwerkservice handmatig in het veld **Name** in.
8. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Select template** klikken.  
Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.
9. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Log events** in.
10. Sla de netwerkregel op.  
De nieuwe netwerkregel wordt aan de lijst toegevoegd.
11. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
12. Sla uw wijzigingen op.

De Firewall controleert netwerkpakketten volgens de regel. U kunt een pakketregel uitschakelen via Firewall zonder deze uit de lijst te verwijderen. Gebruik de schakelaar in de kolom **Status** om de regel in of uit te schakelen.


Het tabblad Regels voor netwerkpakketten

| Parameter       | Beschrijving   |
|-----------------|--|
| <b>Actie</b>    | <p><b>Toestaan.</b></p> <p><b>Blokkeren.</b></p> <p><b>Volgens programmaregels.</b> Als deze optie is geselecteerd, past Firewall de <a href="#">Netwerkregels voor programma's</a> toe op de netwerkverbinding.</p>   |
| <b>Protocol</b> | <p>Beheer de netwerkactiviteit via het geselecteerde protocol: TCP, UDP, ICMP, ICMPv6, IGMP en GRE.</p> <p>Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode definiëren.</p> <p>Als TCP of UDP als het type protocol is geselecteerd, kunt u de door komma's gescheiden poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden bewaakt.</p> |

|                           |  |
|---------------------------|--|
| <b>Richting</b>           | <p><b>Inkomend (pakket).</b> Firewall past de netwerkregel toe op alle inkomende netwerkpakketten.</p> <p><b>Inkomend.</b> De netwerkregel wordt door Firewall toegepast op alle netwerkpakketten die door een externe computer geactiveerd zijn.</p> <p><b>Inkomend / Uitgaand.</b> De netwerkregel wordt door Firewall toegepast op zowel inkomende als uitgaande netwerkpakketten, ongeacht of de computer van de gebruiker of een externe computer de netwerkverbinding tot stand heeft gebracht.</p> <p><b>Uitgaand (pakket).</b> Firewall past de netwerkregel toe op alle uitgaande netwerkpakketten.</p> <p><b>Uitgaand.</b> De netwerkregel wordt door Firewall toegepast op alle netwerkpakketten die door de computer van de gebruiker tot stand is gebracht.</p>   |
| <b>Netwerkadapters</b>    | <p>Netwerkadapters die netwerkpakketten kunnen verzenden en/of ontvangen. Door de instellingen van netwerkadapters op te geven kunnen de netwerkpakketten die zijn verstuurd en ontvangen met netwerkadapters met identieke IP-adressen worden onderscheiden.</p>  |
| <b>Time to live (TTL)</b> | <p>Beperk de controle over netwerkpakketten op basis van hun time to live (TTL).</p>   |
| <b>Extern adres</b>       | <p>Netwerkadressen van externe computers die netwerkpakketten kunnen verzenden en/of ontvangen. Firewall past een netwerkregel toe op het opgegeven bereik van externe netwerkadressen. U kunt alle IP-adressen aan een netwerkregel toevoegen, een aparte lijst met IP-adressen maken, een bereik met IP-adressen opgeven of een subnet selecteren (vertrouwde netwerken, lokale netwerken, openbare netwerken). U kunt ook een DNS-naam van een computer opgeven in plaats van het IP-adres ervan. U doet er goed aan om DNS-namen alleen te gebruiken voor computers in een netwerk of interne services. De interactie met cloudservices (zoals Microsoft Azure) en andere internetbronnen moet door het onderdeel Webcontrole gebeuren.</p> <div data-bbox="421 1106 1493 1263" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security ondersteunt DNS-namen vanaf versie 11.7.0. Als u een DNS-naam opgeeft voor versie 11.6.0 of ouder, kan Kaspersky Endpoint Security de relevante regel toepassen op alle adressen.</p> </div> |
| <b>Lokaal adres</b>       | <p>Geef de netwerkadressen van computers die netwerkpakketten kunnen verzenden en/of ontvangen. Firewall past een netwerkregel toe op het opgegeven bereik van lokale netwerkadressen. U kunt alle IP-adressen aan een netwerkregel toevoegen, een aparte lijst met IP-adressen maken of een bereik van IP-adressen opgeven.</p> <div data-bbox="421 1505 1493 1662" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security ondersteunt DNS-namen vanaf versie 11.7.0. Als u een DNS-naam opgeeft voor versie 11.6.0 of ouder, kan Kaspersky Endpoint Security de relevante regel toepassen op alle adressen.</p> </div> <div data-bbox="421 1706 1493 1827" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Soms kan het lokale adres voor programma's niet worden verkregen. Als dit het geval is, wordt deze parameter genegeerd.</p> </div>   |

## Een regel voor netwerkpakketten inschakelen of uitschakelen

*Zo schakelt u een regel voor netwerkpakketten in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Pakketregels**.  
Dit opent een lijst met standaardregels voor netwerkpakketten die door Firewall zijn ingesteld.
4. Selecteer in de lijst de noodzakelijke regel voor netwerkpakketten.
5. Gebruik de schakelaar in de kolom **Status** om de regel in of uit te schakelen.
6. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Pakketregels**.  
Dit opent een lijst met standaardregels voor netwerkpakketten die door Firewall zijn ingesteld.
4. Selecteer het in de lijst met regels voor netwerkpakketten en klik u op de knop **Bewerken**.
5. Selecteer in de vervolgkeuzelijst **Actie** de actie die Firewall moet uitvoeren bij de detectie van deze soort netwerkactiviteit:
  - **Toestaan**.
  - **Blokkeren**.
  - **Volgens programmaregels**. Als deze optie is geselecteerd, past Firewall de [Netwerkregels voor programma's](#) toe op de netwerkverbinding.
6. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Pakketregels**.  
Dit opent een lijst met standaardregels voor netwerkpakketten die door Firewall zijn ingesteld.
4. Selecteer in de lijst de regel voor netwerkpakketten waarvan u de prioriteit wilt wijzigen.
5. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
6. Sla uw wijzigingen op.

## Netwerkpakketregels exporteren en importeren

U kunt de lijst met netwerkpakketregels exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal regels van hetzelfde type toe te voegen. U kunt de export/import-functie gebruiken om een back-up te maken van de lijst met netwerkpakketregels of om de lijst naar een andere server te migreren.

[Een lijst met netwerkpakketregels exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.
6. In het blok **Firewall-instellingen**, klikt u op de knop **Instellingen**.  
Dit opent de lijst met netwerkpakketregels en de lijst met netwerkregels voor programma's.
7. Selecteer het tabblad **Regels voor netwerkpakketten**.
8. De lijst met netwerkpakketregels exporteren:
  - a. Selecteer de regels die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen regel hebt geselecteerd, exporteert Kaspersky Endpoint Security alle regels.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met regels wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.
9. Een lijst met netwerkpakketregels importeren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
10. Sla uw wijzigingen op.

[Een lijst met netwerkpakketregels exporteren en importeren in de Webconsole en Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Selecteer **Essential Threat Protection** → **Firewall**.
5. Klik op de link **Regels voor netwerkpakketten**.
6. De lijst met netwerkpakketregels exporteren:
  - a. Selecteer de regels die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde regels wilt exporteren of de volledige lijst wilt exporteren.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar een XML-bestand in de standaard downloadmap.
7. Een lijst met netwerkpakketregels importeren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

## 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.

Net als het onderdeel [Host Intrusion Prevention](#) past het onderdeel Firewall standaard de netwerkregels voor een programmagroep toe wanneer de netwerkactiviteit van alle programma's in de groep wordt gefilterd. 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 hogere prioriteit dan de netwerkregel van de groep waartoe het programma behoort.

## Een netwerkregel voor programma's maken

Standaard wordt de programma-activiteit beheerd door netwerkregels 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 netwerkregels maken voor een hele vertrouwensgroep, voor een individueel programma of voor een groep van programma's in een vertrouwensgroep.

Handmatig gedefinieerde netwerkregels hebben een hogere prioriteit dan netwerkregels die zijn bepaald voor een vertrouwensgroep. Als handmatig gedefinieerde programmaregels met andere woorden verschillen van de programmaregels die zijn ingesteld voor een vertrouwensgroep, controleert Firewall de programma-activiteit volgens de handmatig gedefinieerde regels voor programma's.

Firewall maakt standaard de volgende netwerkregels voor elk programma:

- Alle netwerkactiviteit in vertrouwde netwerken.
- Alle netwerkactiviteit in lokale netwerken.
- Alle netwerkactiviteit in openbare netwerken.

Kaspersky Endpoint Security controleert als volgt de netwerkactiviteit van programma's volgens vooraf gedefinieerde netwerkregels:

- Vertrouwd en deels beperkt: alle netwerkactiviteit is toegestaan.
- Zeer beperkt en niet vertrouwd: alle netwerkactiviteit is geblokkeerd.

Vooraf gedefinieerde programmaregels kunnen niet worden bewerkt of verwijderd.

U kunt op de volgende manieren een netwerkregel voor programma's maken:

- Gebruik de tool [Netwerkmonitor](#).

*Netwerkmonitor* is een tool ontworpen voor de realtime weergave van informatie over de netwerkactiviteit van de computer van een gebruiker. Dit is handig omdat u niet alle regelinstellingen hoeft te configureren. Sommige Firewall-instellingen worden automatisch ingevoegd vanuit Netwerkmonitor-gegevens. Netwerkmonitor is alleen beschikbaar in de programma-interface.

- De instellingen van Firewall configureren:

Hiermee kunt u de Firewall-instellingen verfijnen. U kunt regels maken voor elke netwerkactiviteit, zelfs als er momenteel geen netwerkactiviteit is.



Houd er bij het maken van netwerkregels voor programma's rekening mee dat netwerkpakketregels voorrang hebben op netwerkregels voor programma's.

### [De tool Netwerkmonitor gebruiken om een netwerkregel voor programma's te maken in de programma-interface](#)

1. Ga in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **Netwerkmonitor**.
2. Selecteer het tabblad **Netwerkactiviteit** of **Open poorten**.

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.
3. Selecteer in het contextmenu van een netwerkverbinding de optie **Netwerkregel voor programma's maken**.

Het venster met toepassingsregels en eigenschappen wordt geopend.
4. Selecteer het tabblad **Netwerkregels**.

Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
5. Klik op **Toevoegen**.


Dit opent de eigenschappen van de netwerkregel.
6. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
7. Configureer de netwerkregelinstellingen (zie onderstaande tabel).

U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Sjabloon voor netwerkregel** te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.


Alle instellingen voor netwerkregels worden automatisch ingevuld.
8. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
9. Klik op **Opslaan**.

De nieuwe netwerkregel wordt aan de lijst toegevoegd.
10. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
11. Sla uw wijzigingen op.

### [Instellingen van Firewall gebruiken om een netwerkregel voor programma's te maken in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Regels voor programma's**.  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
4. Selecteer in de lijst met programma's het programma of de groep programma's waarvoor u een netwerkregel wilt aanmaken.
5. Klik rechts om het contextmenu te openen en selecteer **Details en regels**.  
Het venster met toepassingsregels en eigenschappen wordt geopend.
6. Selecteer het tabblad **Netwerkregels**.
7. Klik op **Toevoegen**.  
Dit opent de eigenschappen van de netwerkregel.
8. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
9. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Sjabloon voor netwerkregel** te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.
10. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
11. Klik op **Opslaan**.  
De nieuwe netwerkregel wordt aan de lijst toegevoegd.
12. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
13. Sla uw wijzigingen op.

[Een netwerkregel voor programma's maken in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.
6. In het blok **Firewall-instellingen**, klikt u op de knop **Instellingen**.  
Dit opent de lijst met netwerkpakketregels en de lijst met netwerkregels voor programma's.
7. Selecteer het tabblad **Netwerkregels voor programma's**.
8. Klik op **Toevoegen**.
9. Selecteer in het venster dat opent de criteria om te zoeken naar het programma waarvoor u een netwerkregel wilt maken.  
U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.
10. Klik op de knop **Vernieuwen**.  
Kaspersky Endpoint Security zoekt naar het programma in de geconsolideerde lijst met programma's die op beheerde computers zijn geïnstalleerd. Kaspersky Endpoint Security toont een lijst met programma's die voldoen aan uw zoekcriteria.
11. Selecteer het noodzakelijke programma.
12. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de optie **Standaardgroepen** en klik op **OK**.  
Het programma wordt toegevoegd aan de standaard groep.
13. Selecteer het relevante programma en vervolgens **Programmarechten** in het contextmenu van het programma.  
Het venster met toepassingsregels en eigenschappen wordt geopend.
14. Selecteer het tabblad **Netwerkregels**.  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
15. Klik op de knop **Add**.  
Dit opent de eigenschappen van de netwerkregel.
16. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.
17. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de knop  te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.

18. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Gebeurtenissen registreren** in.
19. Sla de netwerkregel op.
20. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
21. Sla uw wijzigingen op.

[Een netwerkregel voor programma's maken in de webconsole en de cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Selecteer **Essential Threat Protection** → **Firewall**.
5. Klik in het blok **Instellingen van Firewall** op de koppeling **Netwerkregels voor programma's**.  
Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.
6. Selecteer het tabblad **Programmarechten**.  
U ziet een lijst met vertrouwensgroepen aan de linkerkant van het venster en hun eigenschappen aan de rechterkant.
7. Klik op de knop **Add**.  
Hiermee start u de wizard voor het toevoegen van een programma aan een vertrouwensgroep.
8. Selecteer de relevante vertrouwensgroep voor het programma.
9. Selecteer het type **Programma**. Klik op de knop **Next**.  
Als u een netwerkregel wil maken voor meerdere programma's, selecteert u het type **Groep** en definieert u een naam voor de programmagroep.
10. Selecteer in de geopende lijst met programma's de programma's waarvoor u een netwerkregel wilt maken.  
Gebruik een filter. U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.
11. Sluit de wizard af door op **OK** te klikken.  
Het programma wordt toegevoegd aan de vertrouwensgroep.
12. Selecteer links in het venster het relevante programma.
13. Selecteer in het rechterdeel van het venster **Netwerkregels** uit de vervolgkeuzelijst.  
Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
14. Klik op de knop **Add**.  
Dit opent de eigenschappen voor programmaregels.
15. Voer de naam van de netwerkservice handmatig in het veld **Name** in.
16. Configureer de netwerkregelinstellingen (zie onderstaande tabel).  
U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Select template** te klikken. Regelsjablonen beschrijven de meest frequent gebruikte netwerkverbindingen.  
Alle instellingen voor netwerkregels worden automatisch ingevuld.
17. Als u wilt dat de acties van de netwerkregel worden opgenomen in het [rapport](#), schakelt u het selectievakje **Log events** in.
18. Sla de netwerkregel op.

De nieuwe netwerkregel wordt aan de lijst toegevoegd.

19. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.

20. Sla uw wijzigingen op.

#### Instellingen Netwerkregels voor programma's

| Parameter           | Beschrijving  |
|---------------------|---|
| <b>Actie</b>        | <b>Toestaan.</b><br><b>Blokkeren.</b>   |
| <b>Protocol</b>     | Beheer de netwerkactiviteit via het geselecteerde protocol: TCP, UDP, ICMP, ICMPv6, IGMP en GRE.<br><br>Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode definiëren.<br><br>Als TCP of UDP als het type protocol is geselecteerd, kunt u de door komma's gescheiden poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden bewaakt.   |
| <b>Richting</b>     | <b>Inkomend.</b><br><b>Inkomend / Uitgaand.</b><br><b>Uitgaand.</b>   |
| <b>Extern adres</b> | Netwerkadressen van externe computers die netwerkpakketten kunnen verzenden en/of ontvangen. Firewall past een netwerkregel toe op het opgegeven bereik van externe netwerkadressen. U kunt alle IP-adressen aan een netwerkregel toevoegen, een aparte lijst met IP-adressen maken, een bereik met IP-adressen opgeven of een subnet selecteren (vertrouwde netwerken, lokale netwerken, openbare netwerken). U kunt ook een DNS-naam van een computer opgeven in plaats van het IP-adres ervan. U doet er goed aan om DNS-namen alleen te gebruiken voor computers in een netwerk of interne services. De interactie met cloudservices (zoals Microsoft Azure) en andere internetbronnen moet door het onderdeel Webcontrole gebeuren.<br><br>Kaspersky Endpoint Security ondersteunt DNS-namen vanaf versie 11.7.0. Als u een DNS-naam opgeeft voor versie 11.6.0 of ouder, kan Kaspersky Endpoint Security de relevante regel toepassen op alle adressen. |
| <b>Lokaal adres</b> | Geef de netwerkadressen van computers die netwerkpakketten kunnen verzenden en/of ontvangen. Firewall past een netwerkregel toe op het opgegeven bereik van lokale netwerkadressen. U kunt alle IP-adressen aan een netwerkregel toevoegen, een aparte lijst met IP-adressen maken of een bereik van IP-adressen opgeven.<br><br><div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">Kaspersky Endpoint Security ondersteunt DNS-namen vanaf versie 11.7.0. Als u een DNS-naam opgeeft voor versie 11.6.0 of ouder, kan Kaspersky Endpoint Security de relevante regel toepassen op alle adressen.</div><br><div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">Soms kan het lokale adres voor programma's niet worden verkregen. Als dit het geval is, wordt deze parameter genegeerd.</div>   |

## Een netwerkregel voor programma's inschakelen en uitschakelen

*Zo schakelt u een netwerkregel voor programma's in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Regels voor programma's**.  
Dit opent de lijst met toepassingsregels.
4. Selecteer in de lijst met programma's het programma of de groep programma's waarvoor u een netwerkregel wilt aanmaken of bewerken.
5. Klik rechts om het contextmenu te openen en selecteer **Details en regels**.  
Het venster met toepassingsregels en eigenschappen wordt geopend.
6. Selecteer het tabblad **Netwerkregels**.
7. Selecteer de relevante netwerkregel in de lijst met netwerkregels voor een programmagroep.  
Het venster Netwerkregeleigenschappen opent.
8. Stel de status **Actief** of **Inactief** voor de netwerkregel.  
U kunt een netwerkregel voor een programmagroep die standaard is aangemaakt door Firewall niet uitschakelen.
9. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Regels voor programma's**.  
Dit opent de lijst met toepassingsregels.
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 met de rechtermuisknop om het contextmenu te openen, selecteer **Netwerkregels** en selecteer vervolgens de actie die u wilt toewijzen:
  - **Overnemen.**
  - **Toestaan.**
  - **Blokkeren.**

6. Sla uw wijzigingen op.

*Zo wijzigt u het antwoord van Firewall voor één netwerkregel voor een programma of een programmagroep:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Regels voor programma's**.  
Dit opent de lijst met toepassingsregels.
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 **Details en regels**.  
Het venster met toepassingsregels en eigenschappen wordt geopend.
6. Selecteer 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:
  - **Overnemen.**
  - **Toestaan.**
  - **Weigeren.**
  - **Gebeurtenissen registreren.**
9. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **Firewall** in het venster met de programma-instellingen.
3. Klik op **Regels voor programma's**.



Dit opent de lijst met toepassingsregels.

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 **Details en regels**.  
Het venster met toepassingsregels en eigenschappen wordt geopend.
6. Selecteer het tabblad **Netwerkregels**.
7. Selecteer de netwerkregel waarvan u de prioriteit wilt wijzigen.
8. Gebruik de knoppen **Omhoog/Omlaag** om de prioriteit van de netwerkregel in te stellen.
9. Sla uw wijzigingen op.

## Netwerkmonitor

*Netwerkmonitor* is een tool ontworpen voor de realtime weergave van informatie over de netwerkactiviteit van de computer van een gebruiker.

*Zo start u Netwerkmonitor:*

Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **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 dit tabblad kunt u ook [netwerkpakketregels maken](#) voor de werking van de firewall.
- Op het tabblad **Open poorten** ziet u alle open netwerkpoorten van de computer. Op dit tabblad kunt u ook [netwerkpakketregels](#) en [programmaregels](#) maken voor de werking van de firewall.
- 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 waarvoor de netwerkactiviteit is geblokkeerd door het onderdeel Network Threat Protection nadat een netwerkaanval vanaf die IP-adressen is gedetecteerd.

## 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. Als gevolg hiervan kan het virus opdrachten uitvoeren onder uw gebruikersaccount om bijvoorbeeld malware te downloaden.

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 besturingssysteem 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 het [Schermtoetsenbord \(als dit beschikbaar is\)](#) (zie onderstaande afbeelding). Deze procedure noemen we de toetsenbordautorisatie.

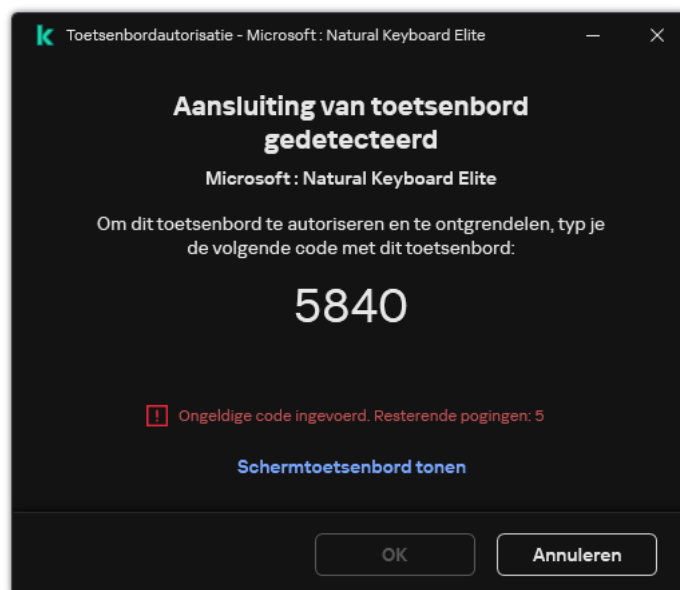
Als de code juist is ingevoerd, slaat het programma de identificatieparameters op (VID/PID van het toetsenbord en het nummer van de poort waarop het is aangesloten) in de lijst met geautoriseerde toetsenborden. U hoeft de toetsenbordautorisatie niet te herhalen wanneer het toetsenbord opnieuw wordt aangesloten 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 kunt [het aantal pogingen voor de invoer van de numerieke code configureren](#). Als de numerieke code meermaals verkeerd wordt ingevoerd of als het venster voor de toetsenbordautorisatie wordt gesloten (zie onderstaande afbeelding), blokkeert het programma de invoer van dit toetsenbord. Wanneer de tijd voor de blokkering van het USB-apparaat verstrijkt of het besturingssysteem opnieuw wordt opgestart, wordt de gebruiker door het programma gevraagd om de toetsenbordautorisatie opnieuw uit te voeren.

Het programma staat het gebruik van een geautoriseerd toetsenbord toe en blokkeert een toetsenbord dat niet is geautoriseerd.

Het onderdeel BadUSB Attack Prevention wordt niet standaard geïnstalleerd. Als u het onderdeel BadUSB Attack Prevention nodig hebt, kunt u het onderdeel toevoegen aan de eigenschappen van het [installatiepakket](#) voordat u het programma installeert of [de beschikbare programmaonderdelen wijzigen](#) nadat u het programma hebt geïnstalleerd.



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.

*Zo schakelt u BadUSB Attack Prevention in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **BadUSB Attack Prevention** om de component in of uit te schakelen.
4. Pas in het blok **Autorisatie van USB-toetsenbord bij aansluiting** de beveiligingsinstellingen voor de invoer van de autorisatiecode aan:
  - **Maximaal aantal pogingen tot autorisatie van USB-apparaten.** Het USB-apparaat wordt automatisch geblokkeerd als de autorisatiecode het opgegeven aantal keer verkeerd wordt ingevoerd. Geldige waarden zijn 1 tot en met 10. Als u dus 5 pogingen voor de invoer van de autorisatiecode invoert, wordt het USB-apparaat na de vijfde poging geblokkeerd. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd hebt u weer 5 pogingen om de autorisatiecode in te voeren.
  - **Time-out als het maximale aantal pogingen is bereikt.** De duur van de blokkering van het USB-apparaat na het opgegeven aantal mislukte pogingen om de autorisatiecode in te voeren. Geldige waarden zijn 1 tot en met 180 (minuten).
5. Sla uw wijzigingen op.

Als gevolg hiervan, als BadUSB Attack Prevention is ingeschakeld, vereist Kaspersky Endpoint Security autorisatie van een aangesloten USB-apparaat dat door het besturingssysteem als toetsenbord wordt geïdentificeerd. De gebruiker kan een ongeautoriseerd toetsenbord pas gebruiken wanneer het wordt geautoriseerd.

## Schermttoetsenbord gebruiken voor autorisatie van USB-apparaten

Schermttoetsenbord mag alleen worden gebruikt voor de autorisatie van USB-apparaten die de invoer van willekeurige tekens niet ondersteunen (bijvoorbeeld barcodescanners). U wordt afgeraden om Schermttoetsenbord te gebruiken voor de autorisatie van onbekende USB-apparaten.

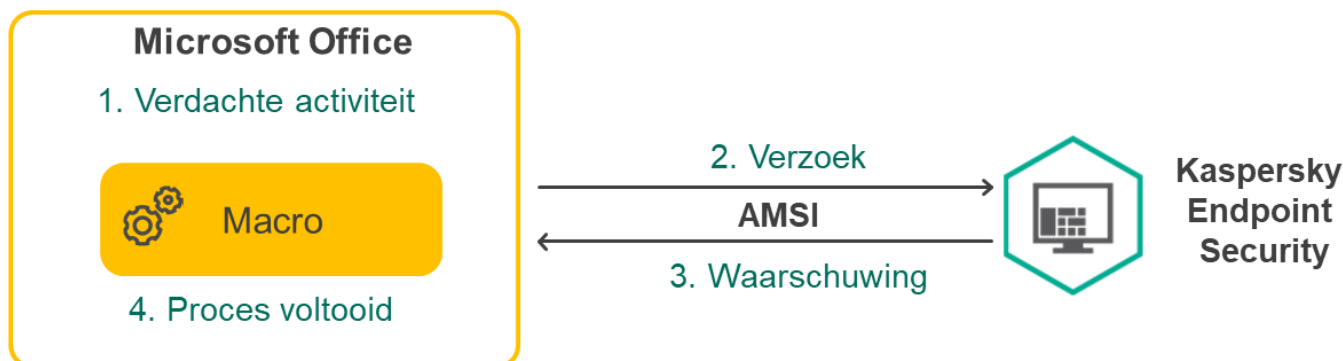
*Zo staat u het gebruik van Schermttoetsenbord voor autorisaties al dan niet toe:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het venster met de programma-instellingen.
3. Gebruik het selectievakje **Gebruik van Schermttoetsenbord voor autorisatie van USB-apparaten verbieden** als u het gebruik van Schermttoetsenbord voor autorisaties wilt blokkeren of toestaan.
4. Sla uw wijzigingen op.

## AMSI-bescherming

AMSI-beschermingsonderdeel is ontwikkeld als ondersteuning voor de Antimalware Scan Interface van Microsoft. Dankzij de *Antimalware Scan Interface (AMSI)* kunnen programma's van andere leveranciers met AMSI-ondersteuning objecten (bijvoorbeeld PowerShell-scripts) versturen naar Kaspersky Endpoint Security om ze te laten scannen en om vervolgens de resultaten van de scans voor deze objecten te ontvangen. Programma's van andere leveranciers zijn bijvoorbeeld Microsoft Office-programma's (zie onderstaande afbeelding). Voor meer informatie over AMSI raadpleegt u de [Microsoft-documentatie](#).

De AMSI-bescherming kan alleen dreigingen detecteren en meldingen over dreigingen versturen naar programma's van andere leveranciers. Nadat het andere programma een melding heeft ontvangen, kunnen geen schadelijke acties worden uitgevoerd (bijvoorbeeld een beëindiging van een proces).



Voorbeeld van AMSI-werking

AMSI-bescherming kan een verzoek van een ander programma weigeren als dit programma bijvoorbeeld het maximale aantal verzoeken binnen een bepaalde tijd overschrijdt. Kaspersky Endpoint Security stuurt informatie over een geweigerd verzoek van een ander programma naar Administration Server. De AMSI Protection-component weigert geen verzoeken van programma's van derden waarvoor: [continue integratie met de AMSI Protection-component](#) is ingeschakeld.


AMSI-bescherming is beschikbaar voor de volgende besturingssystemen voor werkstations en servers:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

## AMSI-bescherming inschakelen en uitschakelen

De AMSI-bescherming is standaard ingeschakeld.

*De AMSI-bescherming in- of uitschakelen:*


1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **AMSI-bescherming** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **AMSI-bescherming** om de component in of uit te schakelen.

4. Sla uw wijzigingen op.

## AMSI-bescherming gebruiken om samengestelde bestanden te scannen

Een vaak gebruikte techniek voor het verbergen van virussen en andere malware is de insluiting ervan in samengestelde bestanden, zoals archieven. 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.

*Het scannen van samengestelde bestanden configureren:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Essential Threat Protection** → **AMSI-bescherming** in het venster met de programma-instellingen.
3. Geef in het blok **Scan van samengestelde bestanden** op welke soorten samengestelde bestanden u wilt scannen: archieven, distributiepakketten of Office-bestanden.
4. Doe in het blok **Beperking van grootte** een van het volgende:
  - Om het AMSI-beschermingsonderdeel geen grote samengestelde bestanden te laten uitpakken, schakelt u het selectievakje **Pak grote samengestelde bestanden niet uit** in en voert u de vereiste waarde in het veld **Maximale bestandsgrootte** in. Het AMSI-beschermingsonderdeel pakt geen samengestelde bestanden uit die groter zijn dan de opgegeven grootte.
  - Om het AMSI-beschermingsonderdeel grote samengestelde bestanden te laten uitpakken, schakelt u het selectievakje **Pak grote samengestelde bestanden niet uit** uit.

Het AMSI-beschermingsonderdeel scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Pak grote samengestelde bestanden niet uit** is ingeschakeld.

5. Sla uw wijzigingen op.

## Exploit-preventie

Het onderdeel Exploit-preventie detecteert programmacode die kwetsbaarheden op de computer uitbuit om bevoegdheden van beheerders te misbruiken of om schadelijke activiteit uit te voeren. Exploits kunnen bijvoorbeeld aanvallen met bufferoverschrijdingen gebruiken. Hiervoor verstuurt de exploit een grote hoeveelheid gegevens naar een kwetsbaar programma. Wanneer deze gegevens worden verwerkt, voert het kwetsbare programma schadelijke code uit. Door deze aanval kan de exploit een onbevoegde installatie van malware starten. Wanneer er zonder medeweten van de gebruiker wordt geprobeerd om een uitvoerbaar bestand te starten met een kwetsbaar programma, belet Kaspersky Endpoint Security dat het bestand wordt gestart en brengt het de gebruiker op de hoogte.

## Exploit-preventie inschakelen en uitschakelen

Exploit-preventie is standaard ingeschakeld en werkt in de modus die door experts van Kaspersky is aanbevolen. U kunt indien nodig Exploit-preventie uitschakelen.

*Zo schakelt u Exploit-preventie in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Exploit-preventie** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Exploit-preventie** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan controleert Kaspersky Endpoint Security, als Exploit-preventie is ingeschakeld, uitvoerbare bestanden die worden uitgevoerd door kwetsbare programma's. Als Kaspersky Endpoint Security detecteert dat een uitvoerbaar bestand van een kwetsbaar programma door iets anders dan de gebruiker is gestart, dan voert Kaspersky Endpoint Security de geselecteerde actie uit (bijvoorbeeld, de bewerking blokkeren).

## Een actie selecteren die moet worden uitgevoerd wanneer een exploit wordt gedetecteerd

Wanneer een exploit wordt gedetecteerd, blokkeert Kaspersky Endpoint Security standaard de bewerkingen die de exploit probeert uit te voeren.

*Zo kiest u een actie die bij de detectie van een exploit moet worden uitgevoerd:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Exploit-preventie** in het venster met de programma-instellingen.
3. Selecteer de relevante actie in het blok **Bij detectie van exploit**:
  - **Bewerking blokkeren**. Als deze optie wordt geselecteerd wanneer een exploit is gedetecteerd, blokkeert Kaspersky Endpoint Security de bewerkingen van deze exploit en registreert het informatie over deze exploit.
  - **Melden**. Als deze optie wordt geselecteerd wanneer een exploit wordt gedetecteerd, registreert Kaspersky Endpoint Security informatie over de exploit en voegt het informatie over deze exploit toe aan de [lijst met actieve dreigingen](#).
4. Sla uw wijzigingen op.

## Bescherming voor systeemprocessen in geheugen

De bescherming van systeemprocessen in het geheugen is standaard ingeschakeld.

*Zo schakelt u de bescherming van systeemprocessen in het geheugen in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Exploit-preventie** in het venster met de programma-instellingen.

3. Gebruik de schakelaar **Bescherming voor systeemprocessen in geheugen inschakelen** om deze functie in of uit te schakelen.

4. Sla uw wijzigingen op.

Als gevolg hiervan blokkeert Kaspersky Endpoint Security externe processen die proberen toegang te krijgen tot systeemprocessen.

## Gedragsdetectie


Het onderdeel Gedragsdetectie ontvangt gegevens over de acties van programma's op de computer en geeft deze gegevens door aan andere beschermingsonderdelen om hun prestaties te verbeteren. Het onderdeel Gedragsdetectie gebruikt definities van gedragspatronen (BSS) voor programma's. Als een programma-activiteit overeenkomt met een behavior stream signature, voert Kaspersky Endpoint Security de geselecteerde responsieve actie uit. De functionaliteit van Kaspersky Endpoint Security op basis van de definities van gedragspatronen levert een proactieve bescherming voor de computer.

## Gedragsdetectie inschakelen en uitschakelen

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

Het is niet aangeraden om Gedragsdetectie uit te schakelen omdat de beschermingsonderdelen hierdoor minder efficiënt zullen zijn, tenzij het absoluut noodzakelijk is. Voor de detectie van dreigingen kunnen beschermingsonderdelen gegevens opvragen die door het onderdeel Gedragsdetectie zijn verzameld.

*Zo schakelt u Gedragsdetectie in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Gedragsdetectie** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan, als gedragsdetectie is ingeschakeld, gebruikt Kaspersky Endpoint Security handtekeningen van gedragsstromen om de activiteit van programma's in het besturingssysteem te analyseren.

## De actie selecteren die moet worden genomen bij het detecteren van malwareactiviteit

*Voer de volgende stappen uit om te kiezen wat u wilt doen als een programma schadelijke activiteit vertoont:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met de programma-instellingen.
3. Selecteer de relevante actie in het blok **Bij detectie van malware-activiteit**:

- **Bestand verwijderen.** Als deze optie is geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, verwijdert Kaspersky Endpoint Security het uitvoerbare bestand van het schadelijke programma en maakt het een back-up van het bestand in Back-up.
- **Programma beëindigen.** Als deze optie wordt geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, beëindigt Kaspersky Endpoint Security dit programma.
- **Melden.** Als deze optie is geselecteerd wanneer malware-activiteit van een programma wordt gedetecteerd, voegt Kaspersky Endpoint Security informatie over de malware-activiteit van het programma toe aan de lijst met actieve dreigingen.

4. Sla uw wijzigingen op.

## Bescherming van gedeelde mappen tegen externe encryptie

Alleen bewerkingen met bestanden op apparaten voor massaopslag met het NTFS-bestandssysteem en die niet met EFS zijn geëncrypt, worden door het onderdeel gemonitord.

De bescherming van gedeelde mappen tegen externe encryptie analyseert de activiteit in gedeelde mappen. Als deze activiteit overeenkomt met een definitie van gedragspatronen die kenmerkend is voor externe encryptie, voert Kaspersky Endpoint Security de geselecteerde actie uit.


De bescherming van gedeelde mappen tegen externe encryptie is standaard uitgeschakeld.

Na de installatie van Kaspersky Endpoint Security zal de bescherming van gedeelde mappen tegen externe encryptie beperkt zijn totdat de computer opnieuw wordt opgestart.

## Bescherming van gedeelde mappen tegen externe encryptie inschakelen en uitschakelen

Na de installatie van Kaspersky Endpoint Security zal de bescherming van gedeelde mappen tegen externe encryptie beperkt zijn totdat de computer opnieuw wordt opgestart.


*Zo schakelt u de bescherming van gedeelde mappen tegen externe encryptie in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Bescherming van gedeelde mappen tegen externe encryptie inschakelen** om de detectie van activiteit die typisch is voor externe encryptie in of uit te schakelen.
4. Sla uw wijzigingen op.



## De actie selecteren die u wilt uitvoeren bij de detectie van externe encryptie van gedeelde mappen

Zo selecteert u de actie die u wilt uitvoeren bij de detectie van externe encryptie van gedeelde mappen:

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met programma-instellingen.
3. Selecteer de relevante actie in het blok **Bescherming van gedeelde mappen tegen externe encryptie**:

- **Blokkeer verbinding voor N min. (van 1 tot 43800)**. Als deze optie is geselecteerd en Kaspersky Endpoint Security detecteert een poging tot wijziging van bestanden in gedeelde mappen, onderneemt het de volgende acties:
  - Blokkeert de toegang tot bestandswijzigingen voor de sessie die de kwaadaardige activiteit heeft gestart (het bestand is alleen-lezen).
  - Het maakt back-ups van bestanden die worden gewijzigd.
  - Het voegt een vermelding toe aan [lokale rapporten over de programma-interface](#).
  - Het verstuurt informatie over de gedetecteerde schadelijke activiteit naar Kaspersky Security Center.

In het geval dat het onderdeel Remediation Engine is ingeschakeld, worden gewijzigde bestanden ook teruggezet vanuit de back-ups.

- **Melden**. Als deze optie is geselecteerd en Kaspersky Endpoint Security detecteert een poging tot wijziging van bestanden in gedeelde mappen, onderneemt het de volgende acties:
  - Het voegt een vermelding toe aan [lokale rapporten over de programma-interface](#).
  - Voegt een item toe aan de lijst met actieve dreigingen.
  - Het verstuurt informatie over de gedetecteerde schadelijke activiteit naar Kaspersky Security Center.

4. Sla uw wijzigingen op.

## Een uitzondering voor bescherming van gedeelde mappen tegen externe encryptie maken:

Het uitsluiten van een map kan foutieve identificaties verminderen als uw organisatie gegevensencryptie gebruikt bij het uitwisselen van bestanden met behulp van gedeelde mappen. Gedragsdetectie kan bijvoorbeeld foutieve identificatie opleveren wanneer de gebruiker werkt met bestanden met de ENC-extensie in een gedeelde map. Dergelijke activiteit komt overeen met een gedragspatroon dat typisch is voor externe versleuteling. Als u bestanden in een gedeelde map hebt versleuteld om gegevens te beschermen, voegt u die map toe aan uitzonderingen.

[Een uitzondering maken voor de bescherming van gedeelde mappen met behulp van de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Exclusions** in het beleidsvenster.
6. Klik in het venster **Scanuitzonderingen en vertrouwde programma's** op de knop **instellingen**.
7. Selecteer in het geopende venster het tabblad **Scanuitzonderingen**.

Met een klik op deze koppeling opent u een venster waarin u een lijst met uitzonderingen vindt.

8. Schakel het selectievakje **Merge values when inheriting** in als u een geconsolideerde lijst met uitzonderingen voor alle computers in het bedrijf wilt maken. De lijsten met uitzonderingen in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Uitzonderingen van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Uitzonderingen van het bovenliggende beleid wijzigen of verwijderen is niet mogelijk.
9. Schakel het selectievakje **Allow use of local trusted applications** in als u wilt dat de gebruiker een lokale lijst met uitzonderingen kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met uitzonderingen maken naast de algemene lijst met uitzonderingen die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.

Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met uitzonderingen die in het beleid is gegenereerd.

10. Klik op **Toevoegen**.
11. Schakel in het blok **Eigenschappen** het selectievakje **Bestand of map** in.
12. Klik op de link **Bestand of map selecteren** in het blok **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** om het venster **Naam van bestand of map** te openen.
13. Klik op **Bladeren** en selecteer de gedeelde map.

U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security ondersteunt de tekens \* en ? bij de invoer van een masker.

- Het teken \* (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes \*\* stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Map\\*\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker C:\\*\*\\*.txt is geen geldig masker.

- Het teken ? (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

14. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.
15. Klik op een koppeling in het blok **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** om de koppeling **Selecteer onderdelen** te activeren.
16. Klik op de koppeling **Selecteer onderdelen** om het venster **Beschermingsonderdelen** te openen.
17. Schakel het selectievakje naast het onderdeel **Gedragsdetectie** in.
18. Sla uw wijzigingen op.

[Een uitzondering maken voor de bescherming van gedeelde mappen met behulp van de Webconsole en Cloudconsole](#) 


1. Selecteer **Devices** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Exclusions**.
5. Klik in het blok **Scan exclusions and trusted applications** op de koppeling **Scan exclusions**.
6. Schakel het selectievakje **Merge values when inheriting** in als u een geconsolideerde lijst met uitzonderingen voor alle computers in het bedrijf wilt maken. De lijsten met uitzonderingen in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Uitzonderingen van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Uitzonderingen van het bovenliggende beleid wijzigen of verwijderen is niet mogelijk.
7. Schakel het selectievakje **Allow use of local trusted applications** in als u wilt dat de gebruiker een lokale lijst met uitzonderingen kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met uitzonderingen maken naast de algemene lijst met uitzonderingen die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.  
  
Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met uitzonderingen die in het beleid is gegenereerd.
8. Klik op de knop **Add**.
9. Selecteer hoe u de uitzondering wil toevoegen **File or folder**.
10. Klik op **Bladeren** en selecteer de gedeelde map.  
U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security ondersteunt de tekens \* en ? bij de invoer van een masker.
  - Het teken \* (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
  - Twee opeenvolgende sterretjes \*\* stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Map\\*\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker C:\\*\*\\*.txt is geen geldig masker.
  - Het teken ? (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
11. Selecteer in het blok **Beschermingsonderdelen** het onderdeel **Gedragsdetectie**.
12. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

13. Selecteer de status **Actief** voor de uitzondering.

U kunt de schakelaar gebruiken [om een uitzondering](#) op elk moment te [stoppen](#).

14. Sla uw wijzigingen op.

## [Een uitzondering maken voor de bescherming van gedeelde mappen in de programma-interface](#)

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

2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.

3. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

4. Klik op **Toevoegen**.

5. Klik op **Bladeren** en selecteer de gedeelde map.

U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security ondersteunt de tekens \* en ? bij de invoer van een masker.

- Het teken \* (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes \*\* stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Map\\*\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker C:\\*\*\\*.txt is geen geldig masker.
- Het teken ? (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

6. Selecteer in het blok **Beschermingsonderdelen** het onderdeel **Gedragsdetectie**.

7. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

8. Selecteer de status **Actief** voor de uitzondering.

U kunt de schakelaar gebruiken [om een uitzondering](#) op elk moment te [stoppen](#).


9. Sla uw wijzigingen op.

## Adressen van gedeelde mappen configureren die niet moeten worden beschermd tegen externe encryptie

De service Aanmelden controleren moet zijn ingeschakeld om adressen te kunnen uitsluiten van de bescherming van gedeelde mappen tegen externe encryptie. Standaard is de service Aanmelden controleren uitgeschakeld (voor gedetailleerde informatie over de inschakeling van de service Aanmelden controleren gaat u naar de website van Microsoft).

Adressen uitsluiten van de bescherming voor gedeelde mappen werkt niet op een externe computer als die externe computer werd ingeschakeld voordat Kaspersky Endpoint Security werd gestart. U kunt deze externe computer opnieuw opstarten nadat Kaspersky Endpoint Security is gestart om te verzekeren dat het uitsluiten van adressen van de bescherming voor gedeelde mappen op deze externe computer werkt.

*Zo sluit u externe computers uit die gedeelde mappen op afstand encrypten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Configureer adressen van uitzonderingen**.
4. Klik op de knop **Toevoegen** als u een IP-adres of computer wilt toevoegen aan de lijst met uitzonderingen.
5. Voer het IP-adres van de computer in waarvoor geen pogingen tot externe encryptie moeten worden behandeld.
6. Sla uw wijzigingen op.

## Een lijst van uitzonderingen die niet moeten worden beschermd tegen externe encryptie exporteren en importeren:

U kunt de lijst met uitzonderingen exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal adressen van hetzelfde type toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijst met uitzonderingen of om de lijst naar een andere server te migreren.

[Een lijst met uitzonderingen exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het beleidsvenster.
6. In het blok **Instellingen van Network Threat Protection**, klikt u op de knop **Uitzonderingen**.
7. De lijst met regels exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen uitzonderingen hebt geselecteerd, exporteert Kaspersky Endpoint Security alle uitzonderingen.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
8. De lijst met uitzonderingen importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
9. Sla uw wijzigingen op.

[Een lijst met uitzonderingen exporteren en importeren in de Webconsole en Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Gedragsdetectie**.
5. De lijst met uitzonderingen in het blok **Exclusions** exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde uitzonderingen wilt exporteren of de volledige lijst met uitzonderingen wilt exporteren.
  - d. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - e. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
6. De lijst met uitzonderingen importeren in het blok **Exclusions**:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
7. Sla uw wijzigingen op.

## Host Intrusion Prevention

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

Het onderdeel Host Intrusion Prevention voorkomt dat programma's acties uitvoeren die mogelijk gevaarlijk zijn voor het besturingssysteem en controleert de toegang tot bronnen van het besturingssysteem en persoonlijke gegevens. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases en de Kaspersky Security Network-cloudservice.



Het onderdeel regelt de werking van programma's door gebruik te maken van *programmarechten*. Programmarechten omvatten de volgende toegangsparemeters:

- Toegang tot besturingssteebronnen (bijvoorbeeld automatische-opstartopties, registersleutels)
- Toegang tot persoonlijke gegevens (zoals bestanden en programma's)

De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.

Wanneer een programma voor de eerste keer wordt opgestart, voert het Host Intrusion Prevention-onderdeel de volgende acties uit:

1. Controleert de beveiliging van het programma aan de hand van gedownloade antivirusdatabases.
2. Controleert in Kaspersky Security Network of de website veilig is.

U wordt aanbevolen [deel te nemen aan Kaspersky Security Network](#) zodat het onderdeel Host Intrusion Prevention efficiënter kan werken.

3. Zet het programma in één van de *vertrouwensgroepen*: Vertrouwd, Deels beperkt, Zeer beperkt, of Niet vertrouwd.

Een [vertrouwensgroep definieert de rechten](#) die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd. Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep, afhankelijk van het risico dat dit programma voor de computer kan opleveren.

Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep voor de onderdelen Firewall en Host Intrusion Prevention. U kunt de vertrouwensgroep niet uitsluitend voor de firewall of voor Host Intrusion Prevention wijzigen.

Als deelname aan KSN hebt geweigerd of als er geen netwerk is, plaatst Kaspersky Endpoint Security het programma in een vertrouwensgroep, afhankelijk van de [instellingen van het Host Intrusion Prevention-onderdeel](#). Nadat de reputatie van het programma is ontvangen van KSN, kan de vertrouwensgroep automatisch worden gewijzigd.

4. Blokkeert acties van programma's afhankelijk van de vertrouwensgroep. Programma's uit de vertrouwensgroep 'Zeer beperkt' krijgen bijvoorbeeld geen toegang tot de modules van het besturingsstee.

De volgende keer dat het programma wordt gestart, controleert Kaspersky Endpoint Security de integriteit van het programma. Als het programma niet is gewijzigd, gebruikt het onderdeel de huidige programmarechten ervoor. Als het programma is gewijzigd, analyseert Kaspersky Endpoint Security het programma alsof het voor het eerst wordt gestart.

## Host Intrusion Prevention inschakelen en uitschakelen

Het onderdeel Host Intrusion Prevention is standaard ingeschakeld en werkt in de modus die door de experts van Kaspersky is aanbevolen.


[Het onderdeel Host Intrusion Prevention in- of uitschakelen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. Gebruik het selectievakje **Host Intrusion Prevention** om het onderdeel in of uit te schakelen.
7. Sla uw wijzigingen op.

### [Het onderdeel Host Intrusion Prevention in- of uitschakelen in de webconsole en cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Gebruik de schakelaar **Host Intrusion Prevention** om de component in of uit te schakelen.
6. Sla uw wijzigingen op.

### [Het onderdeel Host Intrusion Prevention in de programma-interface in- of uitschakelen](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Host Intrusion Prevention** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als het onderdeel Host Intrusion Prevention is ingeschakeld, dan plaatst Kaspersky Endpoint Security een programma in een [vertrouwensgroep](#), afhankelijk van het risico dat dit programma voor de computer kan opleveren. Kaspersky Endpoint Security blokkeert vervolgens de acties van het programma, afhankelijk van de vertrouwensgroep.

## Vertrouwensgroepen voor programma's beheren

Wanneer een programma voor het eerst wordt gestart, controleert het onderdeel Host Intrusion Prevention de beveiliging van het programma en plaatst het het programma in een van de [vertrouwensgroepen](#).

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 dan 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 [Onderdeelinstellingen Host Intrusion Prevention](#) is opgegeven.

Voor programma's die vóór Kaspersky Endpoint Security zijn gestart, wordt alleen de netwerkactiviteit gecontroleerd. De controle wordt uitgevoerd met de netwerkregels [die in de instellingen van Firewall zijn ingesteld](#).

## De vertrouwensgroep van een programma wijzigen

Wanneer een programma voor het eerst wordt gestart, controleert het onderdeel Host Intrusion Prevention de beveiliging van het programma en plaatst het het programma in een van de [vertrouwensgroepen](#).

Experts van Kaspersky raden aan dat u geen programma's verplaatst van de automatisch toegewezen vertrouwensgroep naar een andere vertrouwensgroep. In plaats daarvan kunt u, indien gewenst, [de rechten voor een afzonderlijk programma wijzigen](#).


[De vertrouwensgroep van een programma activeren in de Beheerconsole \(MMC\)](#) 


1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. In het blok **Programmarenchten en beschermde bronnen**, klikt u op de knop **Instellingen**.  
Dit opent het venster voor configuratie van programmarenchten en de lijst met beschermde bronnen.
7. Selecteer het tabblad **Programmarenchten**.
8. Klik op **Toevoegen**.
9. Voer in het venster dat opent de criteria in om te zoeken naar het programma waarvan u de vertrouwensgroep wilt wijzigen.  
U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.
10. Klik op de knop **Vernieuwen**.  
Kaspersky Endpoint Security zoekt naar het programma in de geconsolideerde lijst met programma's die op beheerde computers zijn geïnstalleerd. Kaspersky Endpoint Security toont een lijst met programma's die voldoen aan uw zoekcriteria.
11. Selecteer het noodzakelijke programma.
12. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de benodigde vertrouwensgroep voor het programma.
13. Sla uw wijzigingen op.

[De vertrouwensgroep van een programma veranderen in de Webconsole en Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de link **Programmaren rechten en beschermde bronnen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
6. Selecteer het tabblad **Application rights**.  
U ziet een lijst met vertrouwensgroepen aan de linkerkant van het venster en hun eigenschappen aan de rechterkant.
7. Klik op **Add**.  
Hiermee start u de wizard voor het toevoegen van een programma aan een vertrouwensgroep.
8. Selecteer de relevante vertrouwensgroep voor het programma.
9. Selecteer het type **Programma**. Klik op de knop **Next**.  
Als u de vertrouwensgroep voor meerdere programma's wilt wijzigen, selecteert u het type **Groep** en definieert u een naam voor de programmagroep.
10. Selecteer in de geopende lijst met programma's de programma's waarvan u de vertrouwensgroep wilt veranderen.  
Gebruik een filter. U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.
11. Sluit de wizard af door op **OK** te klikken.  
Het programma wordt toegevoegd aan de vertrouwensgroep.
12. Sla uw wijzigingen op.

[De vertrouwensgroep van een programma veranderen in de programma-interface](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Klik op de knop **Programma's beheren**.  
Dit opent de lijst met geïnstalleerde programma's.
4. Selecteer het noodzakelijke programma.
5. Klik in het contextmenu van het programma op **Beperkingen** → **<vertrouwensgroep>**.
6. Sla uw wijzigingen op.

Als gevolg hiervan wordt het programma in de andere vertrouwensgroep geplaatst. Kaspersky Endpoint Security blokkeert vervolgens de acties van het programma, afhankelijk van de vertrouwensgroep. De  (door de gebruiker gedefinieerde) status wordt toegewezen aan het programma. Als de reputatie van het programma wordt gewijzigd in Kaspersky Security Network, laat het onderdeel Host Intrusion Prevention de vertrouwensgroep van dit programma ongewijzigd.

## Rechten van vertrouwensgroep configureren

De [optimale programmarechten](#) worden standaard aangemaakt voor verschillende vertrouwensgroepen. De instellingen voor programmagroepen die zich in een vertrouwensgroep bevinden nemen de waarden over van de instellingen van de rechten van de vertrouwensgroep.

[De rechten van een vertrouwensgroep veranderen in de beheerconsole \(MMC\)](#) 


1. Open de Beheerconsole van Kaspersky Security Center.
  2. Open in de map **Managed devices** 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 **Policies**.
  4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
  5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
  6. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de knop **Instellingen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
  7. Selecteer het tabblad **Programmaren rechten**.
  8. Selecteer de nodige vertrouwensgroep.
  9. Selecteer in het contextmenu de vertrouwensgroep **Groepsrechten**.  
Dit opent de eigenschappen van de vertrouwensgroep.
  10. Doe een van de volgende acties:
    - Selecteer het tabblad **Bestanden en systeemregister** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
    - Als u vertrouwensgroeprrechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan het tabblad **Rechten**.
- De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.
11. Voor de relevante bron klikt u in de kolom van de bijbehorende actie met de rechtermuisknop om het contextmenu te openen en selecteert u de benodigde optie: **Overnemen**, **Toestaan** (✓) of **Blokkeren** (⊘).
  12. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** (✓ / ⊘).  
Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.
  13. Sla uw wijzigingen op.

## [Rechten van vertrouwensgroep maken in de Webconsole en Cloudconsole](#)




1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
  2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
  3. Selecteer het tabblad **Application settings**.
  4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
  5. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de link **Programmaren rechten en beschermde bronnen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
  6. Selecteer het tabblad **Application rights**.  
U ziet een lijst met vertrouwensgroepen aan de linkerkant van het venster en hun eigenschappen aan de rechterkant.
  7. Selecteer links in het venster de relevante vertrouwensgroep.
  8. Voer in de vervolgkeuzelijst rechts in het venster een van de volgende handelingen uit:
    - Selecteer **Files and system registry** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
    - Als u vertrouwensgroeprchten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan **Rights**.
- De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.
9. Voor de relevante bron klikt u in de kolom van de bijbehorende actie de benodigde optie: **Overnemen**, **Toestaan** (✓) of **Verbieden** (✗).
  10. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** (✓ / ✗).  
Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.
  11. Sla uw wijzigingen op.


## [De rechten van een vertrouwensgroep veranderen in de programma-interface](#)



1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Klik op de knop **Programma's beheren**.  
Dit opent de lijst met geïnstalleerde programma's.
4. Selecteer de nodige vertrouwensgroep.
5. Selecteer in het contextmenu de vertrouwensgroep **Details en regels**.  
Dit opent de eigenschappen van de vertrouwensgroep.
6. Doe een van de volgende acties:
  - Selecteer het tabblad **Bestanden en systeemregister** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
  - Als u vertrouwensgroeprechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan het tabblad **Rechten**.

De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.

7. Voor de relevante bron klikt u in de kolom van de bijbehorende actie met de rechtermuisknop om het contextmenu te openen en selecteert u de benodigde optie: **Overnemen**, **Toestaan**  of **Weigeren** .
8. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** .  
Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.
9. Sla uw wijzigingen op.

De rechten van de vertrouwensgroep worden gewijzigd. Kaspersky Endpoint Security blokkeert vervolgens de acties van het programma, afhankelijk van de vertrouwensgroep. De  status (*gebruikersinstellingen*) wordt toegewezen aan de vertrouwensgroep.

## Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security worden gestart

Voor programma's die vóór Kaspersky Endpoint Security zijn gestart, wordt alleen de netwerkactiviteit gecontroleerd. De controle wordt uitgevoerd met de [netwerkregels](#) die in de instellingen van Firewall zijn ingesteld. U moet een vertrouwensgroep selecteren om op te geven welke netwerkregels u wilt toepassen op de monitoring van de netwerkactiviteit van deze programma's.


## [Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security zijn gestart in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Bewerken**.
7. Selecteer voor de instelling **Vertrouwensgroep voor programma's die starten voordat Kaspersky Endpoint Security voor Windows begint te werken** selecteert u de gepaste [vertrouwensgroep](#).
8. Sla uw wijzigingen op.

## [Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security zijn gestart in de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Selecteer voor de instelling **Vertrouwensgroep voor programma's die starten voordat Kaspersky Endpoint Security voor Windows begint te werken** selecteert u de gepaste [vertrouwensgroep](#).
6. Sla uw wijzigingen op.

## [Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security zijn gestart in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. In het blok **Vertrouwensgroep voor programma's die starten voordat Kaspersky Endpoint Security voor Windows begint te werken** selecteert u de gepaste [vertrouwensgroep](#).
4. Sla uw wijzigingen op.

Als gevolg hiervan wordt een programma dat wordt gestart voordat Kaspersky Endpoint Security in de andere vertrouwensgroep geplaatst. Kaspersky Endpoint Security blokkeert vervolgens de acties van het programma, afhankelijk van de vertrouwensgroep.

## Een vertrouwensgroep selecteren voor onbekende programma's

Tijdens de eerste keer opstarten van een programma, bepaalt het onderdeel Host Intrusion Prevention de [vertrouwensgroep](#) voor het programma. Als u geen internettoegang heeft of als Kaspersky Security Network geen informatie over dit programma heeft, dan plaatst Kaspersky Endpoint Security het programma standaard in de groep Deels beperkt. Wanneer informatie over een eerder onbekend programma wordt gedetecteerd in KSN, werkt Kaspersky Endpoint Security de rechten van dit programma bij. U kunt vervolgens de [programmarechten handmatig bewerken](#).

### [Een vertrouwensgroep selecteren voor onbekende programma's in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. Gebruik in het blok **Regels voor programmaverwerking** de vervolgkeuzelijst **Vertrouwensgroep voor programma's die niet aan bestaande groepen kunnen worden toegevoegd** om de benodigde vertrouwensgroep te selecteren.  

Als 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 ontvangen antwoord kan het programma worden verplaatst naar een vertrouwensgroep die verschilt van de opgegeven groep in de instellingen van het onderdeel Host Intrusion Prevention.
7. Gebruik het selectievakje **Update rechten voor eerder onbekende programma's uit KSN-database** om de automatische update te configureren van de rechten van onbekende programma's.
8. Sla uw wijzigingen op.

### [Een vertrouwensgroep selecteren voor onbekende programma's in de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Gebruik in het blok **Regels voor programmaverwerking** de vervolgkeuzelijst **Vertrouwensgroep voor programma's die niet aan bestaande groepen kunnen worden toegevoegd** om de benodigde vertrouwensgroep te selecteren.  
Als 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 ontvangen antwoord kan het programma worden verplaatst naar een vertrouwensgroep die verschilt van de opgegeven groep in de instellingen van het onderdeel Host Intrusion Prevention.
6. Gebruik het selectievakje **Update rechten voor eerder onbekende programma's uit KSN-database** om de automatische update te configureren van de rechten van onbekende programma's.
7. Sla uw wijzigingen op.

### [Een vertrouwensgroep selecteren voor onbekende programma's in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Selecteer in het blok **Regels voor programmaverwerking** de benodigde vertrouwensgroep.  
Als 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 ontvangen antwoord kan het programma worden verplaatst naar een vertrouwensgroep die verschilt van de opgegeven groep in de instellingen van het onderdeel Host Intrusion Prevention.
4. Gebruik het selectievakje **Werk regels voor eerder onbekende programma's bij vanaf KSN** om de automatische update te configureren van de rechten van onbekende programma's.
5. Sla uw wijzigingen op.

## Een vertrouwensgroep selecteren voor digitaal ondertekende programma's

Kaspersky Endpoint Security plaatst programma's ondertekend door Microsoft- of Kaspersky-certificaten altijd in de groep Vertrouwd.

### [Een vertrouwensgroep selecteren voor digitaal ondertekende programma's in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. Gebruik in het blok **Regels voor programmaverwerking** het selectievakje **Vertrouw digitaal ondertekende programma's** om de automatische toewijzing aan de vertrouwde groep in- of uit te schakelen voor programma's met digitale handtekeningen van vertrouwde leveranciers.  
*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](#).  
Als dit selectievakje is uitgeschakeld, beschouwt het onderdeel Host Intrusion Prevention digitaal ondertekende programma's niet als vertrouwd en gebruikt het andere parameters om de [vertrouwensgroep](#) van die programma's te bepalen.
7. Sla uw wijzigingen op.

#### [Een vertrouwensgroep selecteren voor digitaal ondertekende programma's in de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Gebruik in het blok **Regels voor programmaverwerking** het selectievakje **Vertrouw digitaal ondertekende programma's** om de automatische toewijzing aan de vertrouwde groep in- of uit te schakelen voor programma's met digitale handtekeningen van vertrouwde leveranciers.  
*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](#).  
Als dit selectievakje is uitgeschakeld, beschouwt het onderdeel Host Intrusion Prevention digitaal ondertekende programma's niet als vertrouwd en gebruikt het andere parameters om de [vertrouwensgroep](#) van die programma's te bepalen.
6. Sla uw wijzigingen op.

#### [Een vertrouwensgroep selecteren voor digitaal ondertekende programma's in de programma-interface](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Gebruik in het blok **Regels voor programmaverwerking** het selectievakje **Vertrouw digitaal ondertekende programma's** om de automatische toewijzing aan de vertrouwde groep in- of uit te schakelen voor programma's met digitale handtekeningen van vertrouwde leveranciers.  
*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](#).  
Als dit selectievakje is uitgeschakeld, beschouwt het onderdeel Host Intrusion Prevention digitaal ondertekende programma's niet als vertrouwd en gebruikt het andere parameters om de [vertrouwensgroep](#) van die programma's te bepalen.
4. Sla uw wijzigingen op.

## Programmarechten beheren

Standaard wordt de programma-activiteit beheerd op basis van de programmarechten die zijn gedefinieerd voor de specifieke [vertrouwensgroep](#) waaraan Kaspersky Endpoint Security het programma heeft toegewezen wanneer dat programma voor het eerst werd gestart. U kunt indien nodig [de programmarechten bewerken voor een hele vertrouwensgroep](#), voor een individueel programma of voor een groep van programma's in een vertrouwensgroep.

Handmatig gedefinieerde programmarechten hebben een hogere prioriteit dan programmarechten die zijn gedefinieerd voor een vertrouwensgroep. Als handmatig gedefinieerde programmarechten met andere woorden verschillen van de programmarechten die zijn gedefinieerd voor een vertrouwensgroep, dan controleert het onderdeel Host Intrusion Prevention de programma-activiteit volgens de handmatig gedefinieerde programmarechten.

De regels die u aanmaakt voor programma's worden door de onderliggende processen overgenomen. Als u bijvoorbeeld alle netwerkactiviteit voor cmd.exe blokkeert, wordt alle netwerkactiviteit ook geblokkeerd voor notepad.exe als dat programma wordt gestart via cmd.exe. Wanneer een programma geen onderliggend proces is van een ander programma dat het heeft gestart, worden regels niet overgenomen.

[Programmarechten toevoegen of verwijderen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de knop **Instellingen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
7. Selecteer het tabblad **Programmaren rechten**.
8. Klik op **Toevoegen**.
9. Voer in het venster dat opent de criteria in om te zoeken naar het programma waarvan u de programmaren rechten wilt wijzigen.  
U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.
10. Klik op de knop **Vernieuwen**.  
Kaspersky Endpoint Security zoekt naar het programma in de geconsolideerde lijst met programma's die op beheerde computers zijn geïnstalleerd. Kaspersky Endpoint Security toont een lijst met programma's die voldoen aan uw zoekcriteria.
11. Selecteer het noodzakelijke programma.
12. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de optie **Standaardgroepen** en klik op **OK**.  
Het programma wordt toegevoegd aan de standaard groep.
13. Selecteer het relevante programma en vervolgens **Programmaren rechten** in het contextmenu van het programma.  
Dit opent de programma-eigenschappen.
14. Doe een van de volgende acties:
  - Selecteer het tabblad **Bestanden en systeemregister** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
  - Als u vertrouwensgroepr rechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan het tabblad **Rechten**.

De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.

15. Voor de relevante bron klikt u in de kolom van de bijbehorende actie met de rechtermuisknop om het contextmenu te openen en selecteert u de benodigde optie: **Overnemen**, **Toestaan** (✓) of **Blokkeren** (⊘).

16. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** (✓ / ✗).

Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.

17. Sla uw wijzigingen op.

### [Programmarechten veranderen in de Webconsole en Cloudconsole](#)







1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
  2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
  3. Selecteer het tabblad **Application settings**.
  4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
  5. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de link **Programmaren rechten en beschermde bronnen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
  6. Selecteer het tabblad **Application rights**.  
U ziet een lijst met vertrouwensgroepen aan de linkerkant van het venster en hun eigenschappen aan de rechterkant.
  7. Klik op **Add**.  
Hiermee start u de wizard voor het toevoegen van een programma aan een vertrouwensgroep.
  8. Selecteer de relevante vertrouwensgroep voor het programma.
  9. Selecteer het type **Programma**. Klik op de knop **Next**.  
Als u de vertrouwensgroep voor meerdere programma's wilt wijzigen, selecteert u het type **Groep** en definieert u een naam voor de programmagroep.
  10. Selecteer in de geopende lijst met programma's de programma's waarvan u de programmaren rechten wilt veranderen.  
Gebruik een filter. U kunt de naam van het programma of de naam van de leverancier invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de **\*** en **?**-tekens bij het invoeren van een masker.
  11. Sluit de wizard af door op **OK** te klikken.  
Het programma wordt toegevoegd aan de vertrouwensgroep.
  12. Selecteer links in het venster het relevante programma.
  13. Voer in de vervolgkeuzelijst rechts in het venster een van de volgende handelingen uit:
    - Selecteer **Files and system registry** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
    - Als u vertrouwensgroeprchten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan **Rights**.
- De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.
14. Voor de relevante bron klikt u in de kolom van de bijbehorende actie de benodigde optie: **Overnemen**, **Toestaan** (✓) of **Verbieden** (✗).
  15. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** (✓ / ✗).

Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.

16. Sla uw wijzigingen op.

[Programmarechten wijzigen in de programma-interface](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Klik op de knop **Programma's beheren**.  
Dit opent de lijst met geïnstalleerde programma's.
4. Selecteer het noodzakelijke programma.
5. Selecteer in het contextmenu van het programma de optie **Details en regels**.  
Dit opent de programma-eigenschappen.
6. Doe een van de volgende acties:
  - Selecteer het tabblad **Bestanden en systeemregister** als u rechten van vertrouwensgroepen wilt bewerken die de werking regelen met het register van het besturingssysteem, gebruikersbestanden en programma-instellingen beheren.
  - Als u vertrouwensgroeprechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan het tabblad **Rechten**.
7. Voor de relevante bron klikt u in de kolom van de bijbehorende actie met de rechtermuisknop om het contextmenu te openen en selecteert u de benodigde optie: **Overnemen**, **Toestaan**  of **Weigeren** .
8. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Gebeurtenissen registreren** .  
Kaspersky Endpoint Security legt informatie vast over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.
9. Selecteer het tabblad **Uitzonderingen** en configureer de geavanceerde instellingen van het programma (zie de onderstaande tabel).
10. Sla uw wijzigingen op.

Geavanceerde instellingen van het programma

| Parameter   | Beschrijving  |
|---|---|
| <b>Scan geen geopende bestanden</b>                                   | Alle bestanden die door het programma worden geopend, worden uitgesloten van scans door Kaspersky Endpoint Security. Als u bijvoorbeeld programma's gebruikt om een back-up van bestanden te maken, dan helpt deze functie het verbruik van bronnen door Kaspersky Endpoint Security te verminderen.  |
| <b>Bewaak de programma-activiteit niet</b>                            | Kaspersky Endpoint Security controleert de bestands- en netwerkactiviteit van het programma in het besturingssysteem niet. De programma/activiteit wordt gecontroleerd door de volgende componenten: <a href="#">Gedragsdetectie</a> , <a href="#">Exploit-preventie</a> , <a href="#">Host Intrusion Prevention</a> , <a href="#">Remediation Engine</a> en <a href="#">Firewall</a> . |
| <b>Neem geen beperkingen van bovenliggend proces (programma) over</b> | De beperkingen die voor het bovenliggende proces zijn geconfigureerd, worden door Kaspersky Endpoint Security niet toegepast op een onderliggend proces. Het bovenliggende proces wordt gestart door een toepassing waarvoor <a href="#">programmamachtigingen</a> (Host Intrusion Prevention) en <a href="#">netwerkregels voor programma's</a> (Firewall) zijn geconfigureerd.        |

|   |   |
|---|---|
| <b>Bewaak geen activiteit van onderliggende processen</b>       | Kaspersky Endpoint Security bewaakt de bestands- of netwerkactiviteit van programma's die worden gestart door het programma niet.   |
| <b>Sta interactie met de programma-interface toe</b>            | <a href="#">Kaspersky Endpoint Security Self-Defense</a> blokkeert alle pogingen om services van programma's te beheren vanaf een externe computer. Als het selectievakje is ingeschakeld, mag het programma voor externe toegang de instellingen van Kaspersky Endpoint Security beheren via de interface van Kaspersky Endpoint Security. |
| <b>Scan geen versleuteld verkeer / Scan niet al het verkeer</b> | Netwerkverkeer dat wordt gestart door het programma, wordt uitgesloten van scans door Kaspersky Endpoint Security. U kunt alle verkeer of alleen versleuteld verkeer van scans uitsluiten. U kunt ook individuele IP-adressen en poortnummers uitsluiten van scans.   |

## Bronnen van het besturingssysteem en persoonsgegevens beschermen

Het onderdeel Host Intrusion Prevention beheert de rechten van programma's om acties uit te voeren op diverse categorieën van bronnen van het besturingssysteem en persoonlijke gegevens. Kaspersky-experts hebben vooraf ingestelde categorieën van beschermde bronnen gemaakt. De categorie *besturingssysteem* heeft bijvoorbeeld een subcategorie *Opstartinstellingen* die alle registersleutels geven in verband met het automatisch starten van programma's. U kunt de vooraf ingestelde categorieën van beschermde bronnen of de beschermde bronnen in deze categorieën niet bewerken of verwijderen.

Om bronnen van besturingssystemen te beschermen in het register `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`, moet u registersleutels toevoegen in `\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???`. Bijvoorbeeld `\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???\services\*\`. Dit komt door specifieke kenmerken van de werking van het Windows-register.

### [Een beschermde bron toevoegen in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. In het blok **Programmarenchten en beschermde bronnen**, klikt u op de knop **Instellingen**.  
Dit opent het venster voor configuratie van programmarenchten en de lijst met beschermde bronnen.
7. Selecteer het tabblad **Beschermde bronnen**.  
U ziet een lijst met beschermde bronnen in het linkerdeel van het venster en de bijbehorende rechten voor toegang tot deze bronnen, afhankelijk van de specifieke vertrouwensgroep.
8. Selecteer de categorie van beschermde bronnen waaraan u een nieuwe beschermde bron wilt toevoegen.  
Als u een subcategorie wilt toevoegen, klik dan op **Toevoegen** → **Categorie** .
9. Klik op de knop **Toevoegen**. Selecteer in de vervolgkeuzelijst het type bron dat u wilt toevoegen: **Bestand of map** of **Registersleutel**.
10. Selecteer een bestand, map of registersleutel in het venster dat opent.  
U kunt de rechten van programma's bekijken om toegang te krijgen tot de toegevoegde bronnen. Hiervoor selecteert u een toegevoegde bron in het linkerdeel van het venster en Kaspersky Endpoint Security toont de toegangsrechten voor elke vertrouwensgroep. U kunt de controle over programma-activiteit met bronnen ook uitschakelen met het selectievakje naast een nieuwe bron.
11. Sla uw wijzigingen op.

[Een beschermde bron toevoegen in de Webconsole en de Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. In het blok **Programmaren rechten en beschermde bronnen**, klikt u op de link **Programmaren rechten en beschermde bronnen**.  
Dit opent het venster voor configuratie van programmaren rechten en de lijst met beschermde bronnen.
6. Selecteer het tabblad **Protected resources**.  
U ziet een lijst met beschermde bronnen in het linkerdeel van het venster en de bijbehorende rechten voor toegang tot deze bronnen, afhankelijk van de specifieke vertrouwensgroep.
7. Klik op de knop **Add**.  
De wizard Nieuwe bron wordt gestart.
8. Klik op de categorie **Groepsnaam** om de categorie van beschermde bronnen te selecteren waaraan u een nieuwe beschermde bron wil toevoegen.  
Als u een subcategorie wilt toevoegen, selecteert u de optie **Categorie van beschermde bronnen**.
9. Selecteer het type bron dat u wilt toevoegen: **Bestand of map** of **Registersleutel**.
10. Selecteer een bestand, map of registersleutel.
11. Sluit de wizard af door op **OK** te klikken.  
U kunt de rechten van programma's bekijken om toegang te krijgen tot de toegevoegde bronnen. Hiervoor selecteert u een toegevoegde bron in het linkerdeel van het venster en Kaspersky Endpoint Security toont de toegangsrechten voor elke vertrouwensgroep. U kunt ook het selectievakje in de kolom **Status** om de controle over programma-activiteit met bronnen uit te schakelen.
12. Sla uw wijzigingen op.

[Een beschermde bron maken in de programma-interface](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.
3. Klik op de knop **Bronnen beheren**.  
De lijst met beschermde bronnen wordt geopend.
4. Selecteer de categorie van beschermde bronnen waaraan u een nieuwe beschermde bron wilt toevoegen.  
Als u een subcategorie wilt toevoegen, klik dan op **Toevoegen** → **Categorie**.
5. Klik op de knop **Add**. Selecteer in de vervolgkeuzelijst het type bron dat u wilt toevoegen: **Bestand of map** of **Registersleutel**.
6. Selecteer een bestand, map of registersleutel in het venster dat opent.  
U kunt de rechten van programma's bekijken om toegang te krijgen tot de toegevoegde bronnen. Hiervoor selecteert u een toegevoegde bron in het linkerdeel van het venster en Kaspersky Endpoint Security toont een lijst van programma's en de toegangsrechten voor elk programma. U kunt de controle over programma-activiteit met bronnen ook uitschakelen met de knop  **Controle uitschakelen** in de kolom **Status**.
7. Sla uw wijzigingen op.

Kaspersky Endpoint Security beheert de toegang tot de toegevoegde bronnen van het besturingssysteem en tot persoonlijke gegevens. Kaspersky Endpoint Security controleert de toegang van een programma tot bronnen op basis van de vertrouwensgroep die aan het programma is toegewezen. U kunt [de vertrouwensgroep van een programma wijzigen](#).

## Informatie over ongebruikte programma's verwijderen

Kaspersky Endpoint Security gebruikt programmarechten om de activiteiten van programma's te controleren. Programmarechten worden bepaald door hun vertrouwensgroep. Kaspersky Endpoint Security plaatst een programma in een [vertrouwensgroep](#) wanneer het programma voor de eerste keer wordt gestart. U kunt [de vertrouwensgroep van een toepassing handmatig wijzigen](#). U kunt [de rechten van een individueel programma ook handmatig configureren](#). Kaspersky Endpoint Security slaat de volgende informatie over een programma op: de vertrouwensgroep van het programma en de rechten van het programma.

Kaspersky Endpoint Security verwijdert automatisch informatie over ongebruikte programma's om computerbronnen te sparen. Kaspersky Endpoint Security verwijdert programma-informatie volgens de volgende regels:

- Als de vertrouwensgroep en rechten van een programma automatisch zijn bepaald, verwijdert Kaspersky Endpoint Security na 30 dagen informatie over dit programma. Het is niet mogelijk om de opslagduur voor programma-informatie te wijzigen of om de automatische verwijdering uit te schakelen.
- Als u een programma handmatig in een vertrouwensgroep plaatst of de toegangsrechten ervan configureert, verwijdert Kaspersky Endpoint Security informatie over dit programma na 60 dagen (standaard opslagtermijn). U kunt de opslagtermijn voor programma-informatie wijzigen of automatisch verwijderen uitschakelen (zie onderstaande instructies).

Wanneer u een programma start waarvan de informatie is verwijderd, analyseert Kaspersky Endpoint Security het programma alsof het voor de eerste keer wordt gestart.

## [Automatische verwijdering van informatie over ongebruikte programma's configureren in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.
6. Doe in het blok **Regels voor programmaverwerking** een van het volgende:
  - Als u de automatische verwijdering wilt configureren, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** in en voert u het aantal dagen in.  
Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt na het opgegeven aantal dagen door Kaspersky Endpoint Security verwijderd. Informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch zijn bepaald, wordt na 30 dagen ook door Kaspersky Endpoint Security verwijderd.
  - Als u de automatische verwijdering wilt uitschakelen, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** uit.  
Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt voor onbepaalde tijd door Kaspersky Endpoint Security opgeslagen, zonder enige opslaglimiet. Kaspersky Endpoint Security verwijdert alleen informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch na 30 dagen zijn bepaald.
7. Sla uw wijzigingen op.

## [Automatisch verwijderen van informatie over ongebruikte programma's configureren in de Webconsole en Cloudconsole](#)



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.

2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar **Advanced Threat Protection** → **Host Intrusion Prevention**.

5. Doe in het blok **Regels voor programmaverwerking** een van het volgende:

- Als u de automatische verwijdering wilt configureren, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** in en voert u het aantal dagen in.


Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt na het opgegeven aantal dagen door Kaspersky Endpoint Security verwijderd. Informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch zijn bepaald, wordt na 30 dagen ook door Kaspersky Endpoint Security verwijderd.

- Als u de automatische verwijdering wilt uitschakelen, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** uit.

Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt voor onbepaalde tijd door Kaspersky Endpoint Security opgeslagen, zonder enige opslaglimiet. Kaspersky Endpoint Security verwijdert alleen informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch na 30 dagen zijn bepaald.

6. Sla uw wijzigingen op.

[Automatisch verwijderen van informatie over ongebruikte programma's in de programma-interface](#) 

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

2. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het venster met de programma-instellingen.

3. Doe in het blok **Regels voor programmaverwerking** een van het volgende:

- Als u de automatische verwijdering wilt configureren, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** in en voert u het aantal dagen in.

Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt na het opgegeven aantal dagen door Kaspersky Endpoint Security verwijderd. Informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch zijn bepaald, wordt na 30 dagen ook door Kaspersky Endpoint Security verwijderd.

- Als u de automatische verwijdering wilt uitschakelen, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen** uit.

Informatie over de programma's die u handmatig in een vertrouwensgroep plaatst of waarvan u de toegangsrechten handmatig hebt geconfigureerd, wordt voor onbepaalde tijd door Kaspersky Endpoint Security opgeslagen, zonder enige opslaglimiet. Kaspersky Endpoint Security verwijdert alleen informatie over programma's waarvan de vertrouwensgroep en programmarechten automatisch na 30 dagen zijn bepaald.

4. Sla uw wijzigingen op.

## Host Intrusion Prevention volgen

U kunt rapporten ontvangen over de werking van het onderdeel Host Intrusion Prevention. Rapporten bevatten informatie over bewerkingen met computerbronnen die door het programma worden uitgevoerd (toegestaan of verboden). Rapporten bevatten ook informatie over de programma's die elke bron gebruiken.

Om de werking van Host Intrusion Prevention te volgen moet u het schrijven van rapporten inschakelen. U kunt bijvoorbeeld [het doorsturen van rapporten voor individuele programma's inschakelen in de onderdeelinstellingen van Host Intrusion Prevention](#).

Houd bij het configureren van Host Intrusion Prevention-monitoring rekening met de mogelijke netwerkbelasting bij het doorsturen van gebeurtenissen naar Kaspersky Security Center. U kunt het opslaan van rapporten ook alleen inschakelen in het lokale logboek van Kaspersky Endpoint Security.

## Toegang tot audio en video beveiligen

Cybercriminelen kunnen speciale programma's gebruiken om toegang te proberen krijgen tot apparaten die audio en video opnemen (zoals microfoons of webcams). Kaspersky Endpoint Security controleert wanneer programma's een audiostream of videostream ontvangen en beschermt gegevens tegen ongeautoriseerde onderschepping.

Standaard controleert Kaspersky Endpoint Security de toegang van programma's tot audio- en videostreams als volgt:

- Vertrouwde en deels beperkte programma's mogen standaard de audiostream en videostream van apparaten ontvangen.
- Zeer beperkte en Niet vertrouwde programma's mogen standaard de audiostream en videostream van apparaten niet ontvangen.

U kunt [programma's handmatig toestaan om de audiostream en videostream te ontvangen](#).

## Speciale kenmerken van audiostreambeveiliging

De bescherming van audiostreams heeft de volgende speciale kenmerken:

- Het [onderdeel Host Intrusion Prevention moet ingeschakeld zijn](#) opdat deze functionaliteit zou werken.
- Als het programma de audiostream al ontving voordat het onderdeel Host Intrusion Prevention 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 het programma tot geluidsopnameapparaten (u hebt bijvoorbeeld [ingesteld dat het programma geen audiostreams mag ontvangen](#)), moet dit programma opnieuw worden gestart zodat het geen audiostreams meer ontvangt.
- 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.
- 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.

## Speciale functies van de webcamtoegangsbescherming van het programma

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 programma controleert alleen webcams die via USB of IEEE1394 zijn aangesloten en die als Beeldapparaten in Windows Apparaatbeheer worden weergegeven.
- 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 in deze lijst staan niet verzekeren.

## Remediation Engine

Via Remediation Engine kan Kaspersky Endpoint Security acties van malware in het besturingssysteem terugdraaien.

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

- **Bestandsactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het verwijdert uitvoerbare bestanden die door malware zijn aangemaakt (op alle media behalve netwerkschijven).
- Het verwijdert uitvoerbare bestanden die zijn gemaakt door programma's die door malware zijn geïnfecteerd.
- Het herstelt bestanden die door malware zijn gewijzigd of verwijderd.

De functie voor bestandsherstel heeft een [aantal beperkingen](#).

- **Registeractiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het verwijdert registersleutels die door malware zijn aangemaakt.
- Het herstelt geen registersleutels die door malware zijn gewijzigd of verwijderd.

- **Systeemactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het beëindigt processen die door malware zijn gestart.
- Het beëindigt processen waarin een schadelijk programma is binnengedrongen.
- Het hervat geen processen die door malware zijn gestopt.

- **Netwerkactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het blokkeert de netwerkactiviteit van malware.
- het blokkeert de netwerkactiviteit van processen waarin malware is binnengedrongen.

Het terugdraaien van malwareacties kan door het onderdeel [File Threat Protection](#) of [Gedragsdetectie](#) worden gestart, of tijdens een [virusscan](#).

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.


### [Het onderdeel Remediation Engine in- of uitschakelen in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Advanced Threat Protection** → **Remediation Engine** in het beleidsvenster.
6. Gebruik het selectievakje **Remediation Engine** om het onderdeel in of uit te schakelen.
7. Sla uw wijzigingen op.

### [Het onderdeel Remediation Engine in- of uitschakelen in de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Remediation Engine** .
5. Gebruik de schakelaar **Remediation Engine** om de component in of uit te schakelen.
6. Sla uw wijzigingen op.

### [Het onderdeel Remediation Engine in de programma-interface in- of uitschakelen](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Remediation Engine** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Remediation Engine** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan zal Kaspersky Endpoint Security, als Remediation Engine is ingeschakeld, de acties genomen door kwaadaardige programma's in het besturingssysteem terugdraaien.

## Kaspersky Security Network

Voor een efficiëntere bescherming van uw computer gebruikt Kaspersky Endpoint Security gegevens die het van gebruikers over de hele wereld ontvangt. Kaspersky Security Network is ontworpen om deze 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 dreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. Als u deelneemt aan Kaspersky Security Network, ontvangt Kaspersky Endpoint Security van de KSN-services informatie over de categorie en reputatie van gescande bestanden, alsook informatie over de reputatie van gescande webadressen.

Het gebruik van Kaspersky Security Network is vrijwillig. U wordt tijdens de initiële configuratie van het programma gevraagd om aan KSN deel te nemen. Gebruikers kunnen hun deelname aan KSN op elk moment starten of stoppen.

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 Kaspersky Security Network-verklaring wordt bij het [distributiepakket](#) van het programma meegeleverd.

Om de belasting van de KSN-servers te verminderen, kunnen Kaspersky-experts programma-updates beschikbaar maken die verzoeken aan Kaspersky Security Network tijdelijk uitschakelen of deels beperken. In dit geval is de status van de verbinding met KSN in de lokale interface van het programma *Ingeschakeld met beperkingen*.

## Infrastructuur van KSN

Kaspersky Endpoint Security ondersteunt de volgende infrastructurele KSN-oplossingen:


- *Wereldwijd KSN* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky Security Network en sturen Kaspersky informatie over objecten die op hun computers worden gedetecteerd. Dankzij deze informatie worden de objecten dan verder onderzocht door Kaspersky-analisten en worden ze toegevoegd aan de Kaspersky Security Network-databases die reputatie-informatie en statistische gegevens bevatten.
- *Privaat KSN* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang verkrijgen tot reputatiedatabases van Kaspersky Security Network en tot andere statistische gegevens zonder gegevens naar KSN te versturen vanaf hun eigen computers. Privaat KSN is ontworpen voor bedrijven die niet kunnen deelnemen aan Kaspersky Security Network wegens een van de volgende redenen:
  - De lokale werkstations zijn niet verbonden met internet.
  - De verzending van gegevens naar het buitenland of andere netwerken dan het bedrijfsnetwerk is wettelijk verboden of beperkt door het beveiligingsbeleid van het bedrijf.

Kaspersky Security Center gebruikt standaard Wereldwijd KSN. U kunt het gebruik van Privaat KSN configureren in de Beheerconsole (MMC) en de Webconsole van Kaspersky Security Center en in de [opdrachtregel](#). U kunt het gebruik van Privaat KSN niet in de Cloudconsole van Kaspersky Security Center configureren.

Voor meer informatie over Privaat KSN raadpleegt u de documentatie van Kaspersky Private Security Network.

## Het gebruik van Kaspersky Security Network inschakelen en uitschakelen

*Het gebruik van Kaspersky Security Network in- of uitschakelen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het venster met de programma-instellingen.

3. Gebruik de schakelaar **Kaspersky Security Network** om de component in of uit te schakelen.

Als u het gebruik van KSN hebt ingeschakeld, geeft Kaspersky Endpoint Security de Kaspersky Security Network-verklaring weer. Lees en accepteer de gebruiksvoorwaarden van de Kaspersky Security Network-verklaring (KSN) als u ermee akkoord gaat.

Kaspersky Endpoint Security gebruikt standaard de uitgebreide KSN-modus. De *uitgebreide KSN-modus* is een modus waarin Kaspersky Endpoint Security [aanvullende gegevens](#) naar Kaspersky verstuurt.

4. Zet indien nodig de schakelaar **Uitgebreide KSN-modus inschakelen** uit.
5. Sla uw wijzigingen op.

Als het gebruik van KSN is ingeschakeld, gebruikt Kaspersky Endpoint Security daarom informatie over de reputatie van bestanden, webbronnen en applicaties die zijn ontvangen van Kaspersky Security Network.

## Beperkingen van Privaat KSN

Met Privaat KSN (hierna ook wel KPSN genoemd) kunt u uw eigen lokale reputatiedatabase gebruiken om de reputatie van objecten (bestanden of webadressen) te controleren. De reputatie van een object dat is toegevoegd aan de lokale reputatiedatabase, heeft een hogere prioriteit dan een object dat is toegevoegd aan KSN/KPSN. Stel bijvoorbeeld dat Kaspersky Endpoint Security een computer scant en de reputatie van een bestand in KSN/KPSN opvraagt. Als het bestand de reputatie 'niet-vertrouwd' heeft in de lokale reputatiedatabase, maar de reputatie 'vertrouwd' in KSN/KPSN, detecteert Kaspersky Endpoint Security het bestand als 'niet-vertrouwd' en voert de actie uit die is gedefinieerd voor gedetecteerde dreigingen.

In sommige gevallen vraagt Kaspersky Endpoint Security echter niet de reputatie van een object op in KSN/KPSN. Als dit het geval is, ontvangt Kaspersky Endpoint Security geen gegevens uit de lokale reputatiedatabase van KPSN. Kaspersky Endpoint Security vraagt om de volgende redenen mogelijk niet de reputatie op van een object in KSN/KPSN:


- Kaspersky-programma's gebruiken offline reputatiedatabases. Offline reputatiedatabases zijn ontworpen om bronnen te optimaliseren tijdens het gebruik van Kaspersky-programma's en om cruciale objecten op de computer te beschermen. Offline reputatiedatabases worden gemaakt door Kaspersky-experts op basis van gegevens van Kaspersky Security Network. Kaspersky-programma's werken offline reputatiedatabases bij met antivirusdatabases van het specifieke programma. Als offline reputatiedatabases informatie bevatten over een object dat wordt gescand, vraagt het programma niet de reputatie van dit object op in KSN/KPSN.
- Scanuitzonderingen ([vertrouwde zone](#)) worden geconfigureerd in de programma-instellingen. Als dit het geval is, houdt het programma geen rekening met de reputatie van het object in de lokale reputatiedatabase.
- Het programma gebruikt technologieën voor scanoptimalisatie, zoals iSwift of iChecker, of plaatst reputatieaanvragen voor KSN / KPSN in de cache. Als dit het geval is, vraagt het programma mogelijk niet de reputatie op van eerder gescande objecten.
- Het programma scant bestanden van een bepaalde indeling en grootte voor een optimale werklust. De lijst met relevante indelingen en grootte wordt bepaald door Kaspersky-experts. Deze lijst wordt bijgewerkt met de antivirusdatabases van het programma. U kunt ook instellingen voor scanoptimalisatie configureren in de programma-interface, bijvoorbeeld voor het [onderdeel File Threat Protection](#).

## Cloudmodus voor beschermingsonderdelen inschakelen en uitschakelen

*Cloudmodus* verwijst naar de modus waarin Kaspersky Endpoint Security een beperkte versie van de antivirusdatabases gebruikt. Kaspersky Security Network ondersteunt de werking van het programma wanneer een beperkte versie van de antivirusdatabases worden gebruikt. Met de beperkte versie van de antivirusdatabases verbruikt u ongeveer de helft van het RAM van de computer dat anders met de normale databases zou worden gebruikt. Als u niet deelneemt aan Kaspersky Security Network of als de cloudmodus is uitgeschakeld, downloadt Kaspersky Endpoint Security de volledige versie van de antivirusdatabases vanaf de Kaspersky-servers.

Wanneer u Kaspersky Security Network gebruikt, is de cloudmodus beschikbaar vanaf versie 3.0 van Kaspersky Private Security Network.

*Zo schakelt u de cloudmodus voor beschermingsonderdelen in en uit:*

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



2. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Cloudmodus inschakelen** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan downloadt Kaspersky Endpoint Security bij de volgende update een lichte versie of volledige versie van antivirusdatabases.

Als de beperkte versie van de antivirusdatabases niet kunnen worden gebruikt, schakelt Kaspersky Endpoint Security automatisch over naar de Premium versie van de antivirusdatabases.

## Instellingen voor KSN-proxy

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.
- De service KSN-proxy plaatst verwerkte gegevens in de cache waardoor de externe netwerkcommunicatie minder belast raakt en de informatie die gevraagd wordt door de computer van de gebruiker sneller ontvangen wordt.

Nadat KSN is ingeschakeld en de KSN-verklaring is geaccepteerd, gebruikt het programma standaard een proxyserver om verbinding te maken met Kaspersky Security Network. De proxyserver die door het programma wordt gebruikt, is de Kaspersky Security Center Administration Server via TCP-poort 13111. Als KSN Proxy niet beschikbaar is, moet u daarom het volgende controleren:

- De service *ksnproxy* wordt uitgevoerd op de Administration Server.
- De firewall op de computer blokkeert poort 13111 niet.

U kunt het gebruik van KSN Proxy als volgt configureren: KSN Proxy in- of uitschakelen en de poort voor de verbinding configureren. Om dit te doen, moet u de eigenschappen van de Administration Server openen. Voor meer informatie over de configuratie van KSN-proxy raadpleegt u de Help van Kaspersky Security Center. U kunt KSN Proxy ook in- of uitschakelen voor individuele computers in het Kaspersky Endpoint Security-beleid.

[Anti-Phishing inschakelen of uitschakelen in de Beheerconsole \(MMC\)](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het venster met de programma-instellingen.
3. Gebruik in het blok **Instellingen voor KSN-proxy** het selectievakje **KSN-proxy gebruiken** om KSN-proxy in of uit te schakelen.
4. Schakel indien nodig het selectievakje **KSN-servers gebruiken als KSN-proxy niet beschikbaar is** in.  
Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN-proxyservice niet beschikbaar is. KSN-servers kunnen eigendom van zowel Kaspersky (wanneer wereldwijd KSN wordt gebruikt) als derden (wanneer privaat KSN wordt gebruikt) zijn.
5. Sla uw wijzigingen op.

### [KSN-proxy inschakelen of uitschakelen in de webconsole](#)

1. Selecteer **Devices** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Advanced Threat Protection** → **Kaspersky Security Network**.
5. Gebruik het selectievakje **Use KSN Proxy** om KSN-proxy in of uit te schakelen.
6. Schakel indien nodig het selectievakje **Use KSN servers when KSN Proxy is not available** in.  
Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN-proxyservice niet beschikbaar is. KSN-servers kunnen eigendom van zowel Kaspersky (wanneer wereldwijd KSN wordt gebruikt) als derden (wanneer privaat KSN wordt gebruikt) zijn.
7. Sla uw wijzigingen op.

Het adres van de KSN-proxy komt overeen met het adres van de Administration Server. Wanneer de domeinnaam van de beheerserver gewijzigd is, moet u het KSN-proxyadres handmatig bijwerken.

*Het KSN Proxy-adres configureren:*

1. Ga in de Beheerconsole naar de map **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.
2. Selecteer in het contextmenu van het de map met het **Installation packages** de optie **Properties**.
3. Op het tabblad **General** in het geopende venster, specificeert u het nieuwe adres van de KSN-proxyserver.
4. Sla uw wijzigingen op.

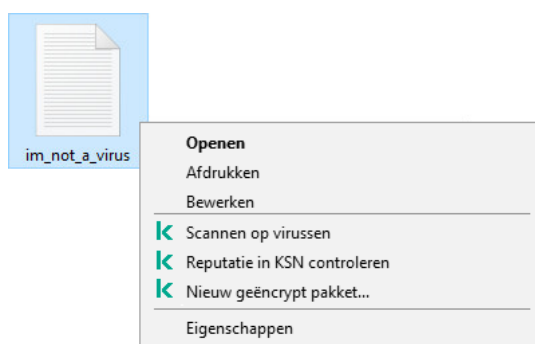
## De reputatie van een bestand in Kaspersky Security Network controleren

Als u twijfelt aan de veiligheid van een bestand, kunt u de reputatie ervan controleren in Kaspersky Security Network.

U kunt de reputatie van een bestand controleren als u de voorwaarden van de [Kaspersky Security Network-verklaring](#) hebt geaccepteerd.

Zo controleert u de reputatie van een bestand in Kaspersky Security Network:

Open het bestandscontextmenu en selecteer de optie **Reputatie in KSN controleren** (zie de onderstaande afbeelding).




Contextmenu van bestand

Kaspersky Endpoint Security geeft de bestandsreputatie weer:

 **Vertrouwd (Kaspersky Security Network).** De meeste gebruikers van Kaspersky Security Network hebben bevestigd dat het bestand te vertrouwen is.

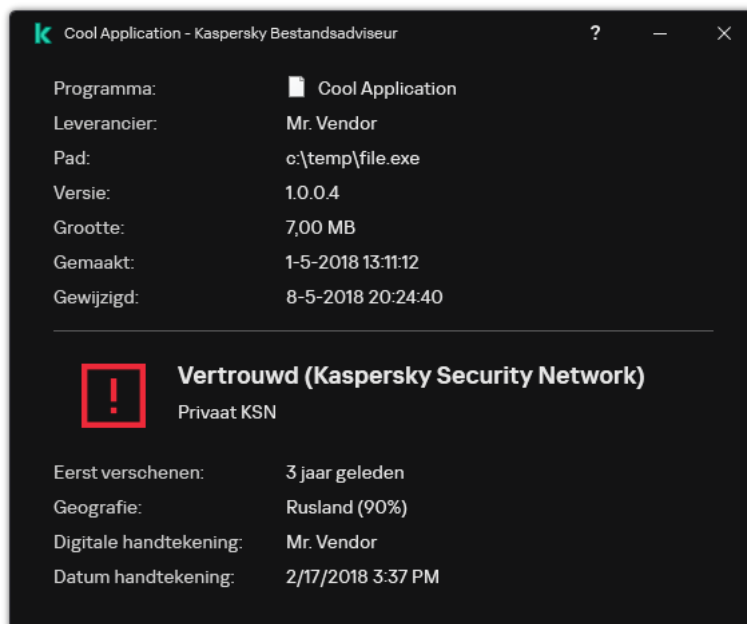
 **Legitieme software die criminelen kunnen gebruiken om je computer of persoonlijke gegevens te beschadigen.** Hoewel ze geen kwaadaardige functies hebben, kunnen dit soort programma's door indringers worden gebruikt als een hulpmiddel. Voor informatie over legitieme software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen, raadpleegt u de [website van de IT-encyclopedie van Kaspersky](#). U kunt [deze programma's toevoegen aan de vertrouwde lijst](#).

 **Vertrouwd (Kaspersky Security Network).** Een virus of ander programma dat [een bedreiging vormt](#).

 **Onbekend (Kaspersky Security Network).** Kaspersky Security Network heeft geen informatie over het bestand. U kunt een bestand scannen met behulp van anti-virusdatabases (de optie **Scannen op virussen** in het contextmenu).

Kaspersky Endpoint Security geeft de KSN-oplossing weer die werd gebruikt om de reputatie van het bestand te bepalen: *Wereldwijd KSN* of *Privaat KSN*.

Kaspersky Endpoint Security geeft ook aanvullende informatie over het bestand weer (zie onderstaande afbeelding).



De reputatie van een bestand in Kaspersky Security Network

## Versleutelde verbindingen scannen

Na installatie voegt Kaspersky Endpoint Security een Kaspersky-certificaat toe aan de systeemopslag voor vertrouwde certificaten (Windows-certificaatarchief). Kaspersky Endpoint Security gebruikt dit certificaat om versleutelde verbindingen te scannen. Kaspersky Endpoint Security omvat ook het gebruik van systeemopslag van vertrouwde certificaten in Firefox en Thunderbird om het verkeer van deze programma's te scannen.

De onderdelen [Webcontrole](#), [Mail Threat Protection](#) en [Web Threat Protection](#) decrypten en scannen netwerkverkeer van geëncrypte verbindingen die met de volgende protocollen tot stand zijn gebracht:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

## Versleutelde verbindingen scannen inschakelen

*Om het scannen van versleutelde verbindingen mogelijk te maken:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Selecteer in het blok **Versleutelde verbindingen scannen** de modus voor het scannen van versleutelde verbindingen:
  - **Versleutelde verbindingen niet scannen.** Kaspersky Endpoint Security heeft geen toegang tot de inhoud van websites waarvan het adres begint met `https://`.
  - **Versleutelde verbindingen scannen op verzoek van beschermingsonderdelen.** Kaspersky Endpoint Security scant versleuteld verkeer alleen wanneer daarom wordt gevraagd door de onderdelen File Threat

Protection, Mail Threat Protection en Web Control.

- **Versleutelde verbindingen altijd scannen.** Kaspersky Endpoint Security scant versleuteld netwerkverkeer, zelfs als de beschermingsonderdelen zijn uitgeschakeld.

Kaspersky Endpoint Security scant geen versleutelde verbindingen die tot stand zijn gebracht door [vertrouwde programma's waarvoor het scannen van verkeer is uitgeschakeld](#). Kaspersky Endpoint Security scant geen versleutelde verbindingen uit de vooraf gedefinieerde lijst met vertrouwde websites. De vooraf gedefinieerde lijst met vertrouwde websites is gemaakt door Kaspersky-experts. Deze lijst wordt bijgewerkt met de antivirusdatabases van het programma. U kunt de vooraf gedefinieerde lijst met vertrouwde websites alleen in de Kaspersky Endpoint Security-interface bekijken. U kunt de lijst niet bekijken in de Kaspersky Security Center Console.

4. Voeg indien nodig [scanuitsluitingen toe: vertrouwde adressen en programma's](#).
5. Configureer de instellingen voor het scannen van versleutelde verbindingen (zie onderstaande tabel).
6. Sla uw wijzigingen op.

Instellingen voor het scannen van versleutelde verbindingen

| Parameter   | Beschrijving   |
|---|--|
| <b>Vetrouwde rootcertificaten</b>                                       | Lijst met vertrouwde rootcertificaten. Met Kaspersky Endpoint Security kunt u vertrouwde rootcertificaten op gebruikerscomputers installeren als u bijvoorbeeld een nieuw certificeringscentrum moet implementeren. Met het programma kunt u een certificaat toevoegen aan een speciaal Kaspersky Endpoint Security-certificaatarchief. In dit geval wordt het certificaat alleen als vertrouwd beschouwd voor de Kaspersky Endpoint Security-programma. De gebruiker kan met andere woorden toegang krijgen tot een website met het nieuwe certificaat in de browser. Als een ander programma toegang probeert te krijgen tot de website, kunt u een verbindingfout krijgen vanwege een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.  |
| <b>Bij een bezoek aan een domein met een niet-vertrouwd certificaat</b> | <ul style="list-style-type: none"><li>• <b>Toestaan.</b> Wanneer een domein met een niet-vertrouwd certificaat wordt bezocht, staat Kaspersky Endpoint Security <a href="#">de netwerkverbinding niet toe</a>. Wanneer een domein met een niet-vertrouwd certificaat wordt geopend in een browser, toont Kaspersky Endpoint Security een HTML-pagina met een waarschuwing en de reden waarom een bezoek aan dat domein niet wordt aanbevolen. Een gebruiker kan klikken op de koppeling op de HTML-waarschuwingpagina om toegang tot de opgevraagde webbron te krijgen. Als een programma of dienst van derden een verbinding tot stand brengt met een domein met een niet-vertrouwd certificaat, maakt Kaspersky Endpoint Security een eigen certificaat om verkeer te scannen. Het nieuwe certificaat heeft de status <i>Niet vertrouwd</i>. Dit is nodig om het programma van derden te waarschuwen voor de niet-vertrouwde verbinding, omdat de HTML-pagina in dit geval niet kan worden weergegeven en de verbinding in de achtergrondmodus kan worden gemaakt.</li><li>• <b>Verbinding blokkeren.</b> Wanneer een domein met een niet-vertrouwd certificaat wordt bezocht, staat Kaspersky Endpoint Security de netwerkverbinding niet toe. Wanneer een domein met een niet-vertrouwd certificaat wordt geopend in een browser, toont Kaspersky Endpoint Security een HTML-pagina met de reden waarom dat domein is geblokkeerd.</li></ul> |
| <b>Bij fouten</b>   |  |

|  |  |
|--|--|
| <p>tijdens het scannen van geëncrypte verbindingen</p>                                       | <ul style="list-style-type: none"> <li>• <b>Verbinding blokkeren.</b> Als deze optie is geselecteerd wanneer een fout tijdens het scannen van een beveiligde verbinding optreedt, blokkeert Kaspersky Endpoint Security de netwerkverbinding.</li> <li>• <b>Domein toevoegen aan uitzonderingen.</b> Als deze optie is geselecteerd wanneer een fout tijdens het scannen van een geëncrypte verbinding optreedt, zal Kaspersky Endpoint Security het domein dat aan de basis lag van de fout toevoegen aan de lijst met domeinen met scanfouten en zal het geen geëncrypt netwerkverkeer bewaken wanneer dit domein wordt bezocht. Alleen in de lokale interface van het programma kunt u een lijst met domeinen zien waarvoor fouten tijdens het scannen van de geëncrypte verbindingen zijn opgetreden. Als u de inhoud van de lijst wilt wissen, moet u <b>Verbinding blokkeren</b> selecteren. Kaspersky Endpoint Security genereert ook een gebeurtenis voor de fout bij het scannen van de versleutelde verbinding.</li> </ul> |
| <p>Blokkeer SSL 2.0-verbindingen (aanbevolen)</p>  | <p>Als het selectievakje is ingeschakeld, blokkeert Kaspersky Endpoint Security netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht.</p> <p>Als het selectievakje is uitgeschakeld, blokkeert Kaspersky Endpoint Security geen netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht en bewaakt het geen netwerkverkeer dat via deze verbindingen wordt verstuurd of ontvangen.</p>  |
| <p>Ontsleutel een versleutelde verbinding met de website die een EV-certificaat gebruikt</p> | <p>EV-certificaten (Certificaten voor uitgebreide validatie) bevestigen de authenticiteit van websites en verbeteren de beveiliging van de verbinding. Browsers tonen een hangslot in de adresbalk om aan te geven dat een website een EV-certificaat heeft. Browsers kunnen de adresbalk ook volledig of gedeeltelijk in een groene kleur weergeven.</p> <p>Als het selectievakje is ingeschakeld, decrypt en bewaakt Kaspersky Endpoint Security geëncrypte verbindingen met websites die een EV-certificaat gebruiken.</p> <p>Als het selectievakje is uitgeschakeld, heeft Kaspersky Endpoint Security geen toegang tot de inhoud van HTTPS-verkeer. Om deze reden bewaakt het programma HTTPS-verkeer alleen op basis van het webadres, zoals <code>https://bing.com</code>.</p> <p>Als u een website met een EV-certificaat voor het eerst opent, wordt de beveiligde verbinding gedecrypt ongeacht of het selectievakje is ingeschakeld.</p>  |

## Vertrouwde rootcertificaten installeren.

Met Kaspersky Endpoint Security kunt u vertrouwde rootcertificaten op gebruikerscomputers installeren als u bijvoorbeeld een nieuw certificeringscentrum moet implementeren. Met het programma kunt u een certificaat toevoegen aan een speciaal Kaspersky Endpoint Security-certificaatarchief. In dit geval wordt het certificaat alleen als vertrouwd beschouwd voor de Kaspersky Endpoint Security-programma. De gebruiker kan met andere woorden toegang krijgen tot een website met het nieuwe certificaat in de browser. Als een ander programma toegang probeert te krijgen tot de website, kunt u een verbindingfout krijgen vanwege een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.


[Hoe installeer ik vertrouwde rootcertificaten in de Beheerconsole \(MMC\)?](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
6. In het blok **Vertrouwde rootcertificaten** klikt u op **Toevoegen**.
7. Dit opent een venster; selecteer in dat venster een vertrouwd rootcertificaat.  
Kaspersky Endpoint Security ondersteunt certificaten met PEM-, der- en CRT-extensies.
8. Sla uw wijzigingen op.

### [Vertrouwde rootcertificaten installeren in Webconsole en Cloud Console](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Netwerkinstellingen**.
5. Klik op **Certificaten weergeven**.
6. Dit opent een venster, klik in dat venster op **Toevoegen** en selecteer een vertrouwd rootcertificaat.  
Kaspersky Endpoint Security ondersteunt certificaten met PEM-, der- en CRT-extensies.
7. Sla uw wijzigingen op.

### [Vertrouwde rootcertificaten in de programma-interface installeren](#)

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Klik in het blok **Versleutelde verbindingen scannen** op **certificaten weergeven**.
4. Dit opent een venster, klik in dat venster op **Toevoegen** en selecteer een vertrouwd rootcertificaat.  
Kaspersky Endpoint Security ondersteunt certificaten met PEM-, der- en CRT-extensies.
5. Sla uw wijzigingen op.

Als gevolg hiervan gebruikt Kaspersky Endpoint Security bij het scannen van verkeer, naast het systeemcertificaatarchief, een eigen certificaatarchief.

## Versleutelde verbindingen scannen met een niet-vertrouwd certificaat

Na installatie voegt Kaspersky Endpoint Security een Kaspersky-certificaat toe aan de systeemopslag voor vertrouwde certificaten (Windows-certificaatarchief). Kaspersky Endpoint Security gebruikt dit certificaat om versleutelde verbindingen te scannen. Wanneer u een domein bezoekt met een niet-vertrouwd certificaat, kunt u de toegang van gebruikers tot dat domein toestaan of weigeren (zie de onderstaande instructies).

Als u de gebruiker toestemming hebt gegeven om domeinen met niet-vertrouwde certificaten te bezoeken, voert Kaspersky Endpoint Security de volgende acties uit:

- Wanneer u een domein bezoekt met een niet-vertrouwd certificaat in de *browser*, gebruikt Kaspersky Endpoint Security het Kaspersky-certificaat om verkeer te scannen. Kaspersky Endpoint Security geeft een HTML-pagina weer met een waarschuwing en informatie over de reden waarom het niet wordt aanbevolen om het betreffende domein te bezoeken (zie onderstaande afbeelding). Een gebruiker kan klikken op de koppeling op de HTML-waarschuwingpagina om toegang tot de opgevraagde webbron te krijgen. Na het klikken op deze koppeling zal Kaspersky Endpoint Security één uur lang geen waarschuwingen over een niet-vertrouwd certificaat tonen wanneer andere bronnen binnen hetzelfde domein worden bezocht. Kaspersky Endpoint Security genereert ook een gebeurtenis over het maken van een versleutelde verbinding met een niet-vertrouwd certificaat.
- Als *een programma of dienst van derden* een verbinding tot stand brengt met een domein met een niet-vertrouwd certificaat, maakt Kaspersky Endpoint Security een eigen certificaat om verkeer te scannen. Het nieuwe certificaat heeft de status *Niet vertrouwd*. Dit is nodig om het programma van derden te waarschuwen voor de niet-vertrouwde verbinding, omdat de HTML-pagina in dit geval niet kan worden weergegeven en de verbinding in de achtergrondmodus kan worden gemaakt. Daarom kan de verbinding worden verbroken als een programma van derden over ingebouwde hulpprogramma's voor certificaatverificatie beschikt. In dat geval moet u contact opnemen met de eigenaar van het domein en een vertrouwde verbinding instellen. Als er geen vertrouwde verbinding kan worden ingesteld, kunt u dat [programma van derden toevoegen aan de lijst met vertrouwde programma's](#). Kaspersky Endpoint Security genereert ook een gebeurtenis over het maken van een versleutelde verbinding met een niet-vertrouwd certificaat.

### [Het scannen van versleutelde verbindingen configureren met een niet-vertrouwd certificaat in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
6. Klik in het blok **Versleutelde verbindingen scannen** op de knop **Geavanceerde instellingen**.
7. Dit opent een venster; in dat venster selecteert u de bedrijfsmodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Verbinding toestaan** of **Verbinding blokkeren**.
8. Sla uw wijzigingen op.



## Het scannen van versleutelde verbindingen configureren met een niet-vertrouwd certificaat in Webconsole en Cloudconsole

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Netwerkinstellingen** .
5. Selecteer onder **Versleutelde verbindingen scannen**, selecteer de uitvoermodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Verbinding toestaan** of **Verbinding blokkeren**.
6. Sla uw wijzigingen op.

## Het scannen van versleutelde verbindingen configureren met een niet-vertrouwd certificaat in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Selecteer onder **Versleutelde verbindingen scannen**, selecteer de uitvoermodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Verbinding toestaan** of **Verbinding blokkeren**.
4. Sla uw wijzigingen op.



### Bezoek aan een domein met een niet-vertrouwd certificaat

De verbinding is niet veilig. Criminelen kunnen proberen uw privégegevens te onderscheppen. U wordt aanbevolen de website niet langer te gebruiken.

revoked.badssl.com

#### Reden:

Dit certificaat of een van de certificaten in de keten wordt niet langer vertrouwd.

[Certificaat weergeven](#)

[Ik begrijp het risico maar wil toch doorgaan](#)

kaspersky

Waarschuwing over een bezoek aan een domein met een niet-vertrouwd certificaat

## Versleutelde verbindingen scannen in Firefox en Thunderbird

Na installatie voegt Kaspersky Endpoint Security een Kaspersky-certificaat toe aan de systeemopslag voor vertrouwde certificaten (Windows-certificaatarchief). Firefox en Thunderbird gebruiken standaard hun eigen Mozilla-certificaatopslag in plaats van de Windows-certificaatopslag. Als Kaspersky Security Center is geïmplementeerd in uw organisatie en er wordt beleid toegepast op een computer, maakt Kaspersky Endpoint Security automatisch het gebruik van de Windows-certificaatopslag in Firefox en Thunderbird mogelijk om het verkeer van deze programma's te scannen. Als er geen beleid op de computer wordt toegepast, kunt u de certificaatopslag kiezen die wordt gebruikt door Mozilla-programma's. Als u de Mozilla-certificaatopslag hebt geselecteerd, voegt u er handmatig een Kaspersky-certificaat aan toe. Dit helpt fouten te voorkomen bij het werken met HTTPS-verkeer.

Om verkeer in de Mozilla Firefox-browser en de Thunderbird-mailclient te scannen, moet u de [versleutelde verbindingen scannen inschakelen](#). Als Versleutelde verbindingen scannen ingeschakeld is, scant Kaspersky Endpoint Security geen versleuteld verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient.

Voordat u een certificaat toevoegt aan de Mozilla-opslag, exporteert u het Kaspersky-certificaat via het Configuratiescherm van Windows (browsereigenschappen). Voor informatie over het exporteren van het Kaspersky-certificaat raadpleegt u de [Knowledge Base van de Technische Support](#). Bezoek de [website voor technische support van Mozilla](#) voor meer informatie over het toevoegen van een certificaat aan de opslag.

U kunt de certificaatopslag alleen in de lokale interface van het programma kiezen.

*Een certificaatopslag kiezen voor het scannen van versleutelde verbindingen in Firefox en Thunderbird:*

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

2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Schakel in het blok **Mozilla Firefox en Thunderbird** het selectievakje **Beveiligd verkeer in Mozilla-apps scannen** in.
4. Selecteer een certificaatarchief:
  - **Windows-certificaatarchief gebruiken (aanbevolen)**. Het Kaspersky-rootcertificaat wordt aan deze opslag toegevoegd tijdens de installatie van Kaspersky Endpoint Security.
  - **Mozilla-certificaatarchief gebruiken**. Mozilla Firefox en Thunderbird gebruiken hun eigen certificaatopslag. Als de Mozilla-certificaatopslag is geselecteerd, moet u het Kaspersky-rootcertificaat handmatig aan deze opslag toevoegen via de browsereigenschappen.
5. Sla uw wijzigingen op.

## Versleutelde verbindingen uitsluiten van scannen

De meeste webbronnen gebruiken versleutelde verbindingen. Kaspersky-experts raden u aan om [Versleutelde verbindingen scannen](#) in te schakelen. Als het scannen van geëncrypte verbindingen uw werk verstoort, kunt u een website toevoegen aan de uitzonderingen die *vertrouwde adressen* worden genoemd. Als een vertrouwde toepassing een versleutelde verbinding gebruikt, kunt u [u het scannen van versleutelde verbindingen voor dit programma uitschakelen](#). U kunt bijvoorbeeld het scannen van versleutelde verbindingen uitschakelen voor programma's met cloudopslag die tweefactorauthenticatie gebruiken met hun eigen certificaat.

*Een webadres uitsluiten van de scan van versleutelde verbindingen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. In het blok **Versleutelde verbindingen scannen**, klikt u op de knop **Vertrouwde adressen**.
4. Klik op **Toevoegen**.
5. Voer een domeinnaam of een IP-adres in als u niet wilt dat Kaspersky Endpoint Security de versleutelde verbinding scant bij een bezoek aan dat domein.  
Kaspersky Endpoint Security ondersteunt het teken \* voor de invoer van een masker in de domeinnaam.

Kaspersky Endpoint Security ondersteunt geen maskers voor IP-adressen. U kunt een bereik van IP-adressen invoeren in de lokale programma-interface (bijvoorbeeld 198.51.100.0/24). U kunt geen bereik van IP-adressen invoeren in de Kaspersky Security Center-console.

Voorbeelden:

- **domein.nl**: – de record bevat de volgende adressen: <https://domein.nl>, <https://www.domein.nl>, <https://domein.nl/pagina123>. De record bevat geen subdomeinen (bijvoorbeeld [subdomein.domein.nl](https://subdomein.domein.nl)).
- **subdomein.domein.nl** – de record bevat de volgende adressen: <https://subdomein.domein.nl>, <https://subdomein.domein.nl/pagina123>. De record bevat niet het domein [domein.nl](https://domein.nl).

- \*.domein.nl – de record bevat de volgende adressen: https://films.domein.nl, https://afbeeldingen.domein.nl/pagina123. De record bevat niet het domein domein.nl.

6. Sla uw wijzigingen op.

Kaspersky Endpoint Security scant standaard geen versleutelde verbindingen als er fouten optreden en voegt de website toe aan een speciale lijst met *domeinen met scanfouten*. Kaspersky Endpoint Security stelt voor elke gebruiker een aparte lijst samen en stuurt geen gegevens naar Kaspersky Security Center. U kunt [het blokkeren van de verbinding inschakelen wanneer er een scanfout optreedt](#). Alleen in de lokale interface van het programma kunt u een lijst met domeinen zien waarvoor fouten tijdens het scannen van de geëncrypte verbindingen zijn opgetreden.

*De lijst met domeinen met scanfouten bekijken:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. In het blok **Versleutelde verbindingen scannen**, klikt u op de knop **Domeinen met scanfouten**.

Er wordt een lijst met domeinen met scanfouten geopend. Als u de lijst opnieuw wilt instellen, schakelt u in het beleid het blokkeren van verbindingen in wanneer er scanfouten optreden. Pas vervolgens het beleid toe, stel de parameter opnieuw in op de oorspronkelijke waarde en pas het beleid opnieuw toe.

Kaspersky-specialisten maken een lijst met *wereldwijde uitzonderingen*: vertrouwde websites die Kaspersky Endpoint Security niet controleert, ongeacht de programma-instellingen.

*Zo bekijkt u wereldwijde uitzonderingen voor scans van geëncrypte verkeer:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Klik in het blok **Versleutelde verbindingen scannen** op de link naar de lijst met vertrouwde websites.

Dit opent een lijst met websites samengesteld door Kaspersky-experts. Kaspersky Endpoint Security scant geen beveiligde verbindingen voor websites op de lijst. De lijst kan worden geüpdatet wanneer de databases en modules van Kaspersky Endpoint Security worden geüpdatet.

## Gegevens wissen

Met Kaspersky Endpoint Security kunt u een taak gebruiken om gegevens op computers van gebruikers op afstand te verwijderen.

Zo verwijdert Kaspersky Endpoint Security de gegevens:

- In de stille modus;
- Op harde schijven en verwisselbare schijven;
- Voor alle gebruikersaccounts op de computer.

Kaspersky Endpoint Security voert de taak *Gegevens wissen* uit ongeacht het type licentie dat wordt gebruikt, zelfs nadat de licentie is verlopen.

## Modi van Gegevens wissen

Met deze taak kunt u gegevens verwijderen in de volgende modi:

- Directe gegevensverwijdering.

In deze modus kunt u bijvoorbeeld verouderde gegevens verwijderen om schijfruimte vrij te maken.

- Uitgestelde gegevensverwijdering.

Deze modus is bedoeld om bijvoorbeeld gegevens op een laptop te beschermen bij diefstal of verlies van de laptop. U kunt een automatische gegevensverwijdering configureren die wordt uitgevoerd als de laptop het bedrijfsnetwerk verlaat en al lange tijd niet meer is gesynchroniseerd met Kaspersky Security Center.

Het is niet mogelijk om in de taakeigenschappen een schema voor gegevensverwijdering in te stellen. U kunt gegevens alleen net na de handmatige start van de taak verwijderen of u kunt een vertraagde gegevensverwijdering configureren als er geen verbinding Kaspersky Security Center is.

## Beperkingen

De functie 'Gegevens wissen' heeft de volgende beperkingen:

- Alleen een Kaspersky Security Center-beheerder kan de taak *Gegevens wissen* beheren. U kunt geen taak in de lokale interface van Kaspersky Endpoint Security configureren of starten.
- Bij het NTFS-bestandssysteem verwijdert Kaspersky Endpoint Security alleen de namen van de belangrijkste gegevensstromen. Namen van alternatieve gegevensstromen kunnen niet worden verwijderd.
- Wanneer u een bestand met een symbolische koppeling verwijdert, zal Kaspersky Endpoint Security ook de bestanden waarvan de paden zijn opgegeven in de symbolische koppeling verwijderen.

## Een 'Gegevens wissen'-taak aanmaken

*Zo verwijdert u gegevens op computers van gebruikers:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

- a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

- b. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Gegevens wissen**.

c. Typ in het veld **Task name** een korte omschrijving, zoals *Gegevens wissen (Anti-Diefstal)*.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Ga naar de volgende stap.

Als nieuwe computers worden toegevoegd aan een beheergroep binnen het bereik van de taak, wordt de taak voor directe gegevensverwijdering alleen uitgevoerd op de nieuwe computers als de taak binnen 5 minuten na het toevoegen van de nieuwe computers wordt voltooid.

5. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de lijst met taken.

6. Klik op de taak **Gegevens wissen** voor Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

7. Selecteer het tabblad **Application settings**.

8. Selecteer de methode voor de verwijdering van de gegevens:

- **Delete by means of the operating system.** Kaspersky Endpoint Security gebruikt de bronnen van het besturingssysteem om bestanden te verwijderen zonder ze naar de prullenbak te verplaatsen.
- **Delete completely, no recovery possible.** Kaspersky Endpoint Security overschrijft bestanden met willekeurige gegevens. Het is vrijwel onmogelijk om gegevens te herstellen nadat ze zijn verwijderd.

9. Als u de gegevensverwijdering wilt uitstellen, schakelt u het selectievakje **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days** in. Geef het aantal dagen op.

De taak voor de uitgestelde gegevensverwijdering wordt uitgevoerd telkens als geen verbinding met Kaspersky Security Center is gemaakt gedurende de ingestelde tijd.

Bij de configuratie van de uitgestelde gegevensverwijdering moet u wel rekening houden dat werknemers hun computer kunnen afsluiten voordat ze op vakantie gaan. In dat geval kan de tijd dat er geen verbinding is gemaakt overschreden worden en worden de gegevens verwijderd. Houd ook rekening met het werkschema van offline gebruikers. Voor meer informatie over het werken met offline computers en gebruikers die niet op kantoor zijn, raadpleegt u de [Help van Kaspersky Security Center](#).

Als het selectievakje is uitgeschakeld, wordt de taak meteen na de synchronisatie met Kaspersky Security Center uitgevoerd.

10. Zo maakt u een lijst met te verwijderen objecten:

- **Mappen.** Kaspersky Endpoint Security verwijdert alle bestanden in de map en de submappen ervan. Kaspersky Endpoint Security ondersteunt geen maskers en omgevingsvariabelen voor de invoer van een pad naar een map.
- **Bestanden op extensie.** Kaspersky Endpoint Security zoekt bestanden met de opgegeven extensies op alle schijven van de computer, inclusief verwisselbare schijven. Gebruik de tekens ';' of ',' om meerdere extensies op te geven.
- **Vooraf gedefinieerd bereik.** Kaspersky Endpoint Security verwijdert bestanden uit de volgende gebieden:

- **Documenten.** Bestanden in de standaardmap *Documenten* van het besturingssysteem, en de submappen ervan.
- **Cookies.** Bestanden waarin de browser gegevens bewaart van websites die de gebruiker bezoekt (zoals gegevens over gebruikersautorisaties).
- **Bureaublad.** Bestanden in de standaardmap *Bureaublad* van het besturingssysteem, en de submappen ervan.
- **Temporary Internet Explorer files.** Tijdelijke bestanden voor de werking van Internet Explorer, zoals exemplaren van webpagina's, afbeeldingen en mediabestanden.
- **Tijdelijke bestanden.** Tijdelijke bestanden voor de werking van op de computer geïnstalleerde programma's. Microsoft Office-programma's maken bijvoorbeeld tijdelijke bestanden aan die back-ups van documenten bevatten.
- **Outlook-bestanden.** Bestanden voor de werking van het e-mailprogramma Outlook: gegevensbestanden (PST), offline gegevensbestanden (OST), offline adresboekbestanden (OAB) en persoonlijk-adresboekbestanden (PAB).
- **User profile.** Een aantal bestanden en mappen met instellingen van het besturingssysteem voor het lokale gebruikersaccount.

Op elk tabblad kunt u een lijst met te verwijderen objecten maken. Kaspersky Endpoint Security maakt een geconsolideerde lijst aan en verwijdert bestanden van deze lijst wanneer een taak is voltooid.

U kunt geen bestanden verwijderen die vereist zijn voor de werking van Kaspersky Endpoint Security.

11. Sla uw wijzigingen op.
12. Schakel het selectievakje naast de taak in.
13. Klik op de knop **Run**.

De gegevens op computers van gebruikers worden nu verwijderd volgens de geselecteerde modus: direct of als er geen verbinding is. Als Kaspersky Endpoint Security een bestand niet kan verwijderen, zoals wanneer een gebruiker het bestand momenteel gebruikt, probeert het programma het niet opnieuw te verwijderen. Start de taak opnieuw om de gegevensverwijdering te voltooien.

# Computerbeheer

## Webcontrole

Webcontrole beheert de toegang van gebruikers tot webbronnen. Het onderdeel helpt zo het verkeersvolume en het misbruik van werkuren verminderen. Wanneer een gebruiker een website probeert te openen die wordt beperkt door Webcontrole, dan blokkeert Kaspersky Endpoint Security de toegang of wordt er een waarschuwing weergegeven (zie onderstaande afbeelding).

Kaspersky Endpoint Security bewaakt alleen HTTP- en HTTPS-verkeer.

Voor de bewaking van HTTPS-verkeer moet u [Versleutelde verbindingen scannen](#) inschakelen.

## Methoden voor het beheer van de toegang tot websites

Met Webcontrole kunt u de toegang tot websites configureren met de volgende methoden:

- **Websitecategorie.** Websites worden gecategoriseerd volgens de Kaspersky Security Network-cloudservice, heuristische analyse en de database van bekende websites (een onderdeel van de programmadatabases). U kunt bijvoorbeeld de gebruikerstoegang beperken tot de categorie "Sociale netwerken" of tot [andere categorieën](#).
- **Gegevenstype.** U kunt de toegang van gebruikers beperken voor gegevens op websites en bijvoorbeeld afbeeldingen verbergen. Kaspersky Endpoint Security bepaalt het gegevenstype op basis van de bestandsindeling en niet op basis van de extensie.

Kaspersky Endpoint Security scant geen bestanden in archieven. Als een archief bijvoorbeeld afbeeldingen bevat, identificeert Kaspersky Endpoint Security de gegevens als 'Archieven' en niet als 'Grafische bestanden'.

- **Individueel adres.** U kunt een webadres invoeren of [maskers gebruiken](#).

U kunt meerdere methoden tegelijk gebruiken om de toegang tot websites te regelen. Zo kunt u bijvoorbeeld de toegang tot het gegevenstype 'Office-bestanden' alleen beperken voor de categorie 'Webmail'.

## Regels voor toegang tot websites

Webcontrole beheert de toegang van gebruikers tot websites met behulp van *toegangsregels*. U kunt de volgende geavanceerde instellingen configureren voor een regel voor toegang tot websites:

- Gebruikers waarop de regel van toepassing is.  
U kunt bijvoorbeeld de internettoegang via een browser beperken voor alle gebruikers van het bedrijf, behalve voor de IT-afdeling.
- Regelplanning.  
U kunt bijvoorbeeld de internettoegang via een browser tijdens de werkuren beperken.



## Prioriteiten voor toegangsregels

Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als een website is toegevoegd aan meerdere regels, regelt Webcontrole de toegang tot de website volgens de regel met de hoogste prioriteit. Kaspersky Endpoint Security kan bijvoorbeeld een bedrijfsportal identificeren als een sociaal netwerk. Wilt u de toegang tot sociale netwerken verbieden maar toch toegang tot de webportal van het bedrijf verlenen, dan maakt u twee regels: een regel die de websitecategorie 'Sociale netwerken' blokkeert en een regel die de webportal van het bedrijf toestaat. De toegangsregel voor de webportal van het bedrijf moet een hogere prioriteit hebben dan de toegangsregel voor sociale netwerken.



De gevraagde webpagina kan niet worden geopend.

Adres: <http://kaspersky.ru/>.

De webpagina is geblokkeerd door de regel test\_block.

Reden: de webbron behoort tot de Onbepaald inhoudscategorie(ën) en de Onbepaald gegevenscategorie(ën).

Deze webbron is verboden binnen het bedrijf. Als je vindt dat de blokkering een vergissing is of als je toegang tot deze webbron nodig hebt, neem je contact op met de beheerder van het lokale bedrijfsnetwerk ([Toegang vragen](#)).

Bericht gemaakt op: 10/29/2020 4:16:12 AM



De opgevraagde webpagina is mogelijk onveilig of verboden door het bedrijfsbeleid.

Adres: <http://kaspersky.com/>.

De webpagina is geblokkeerd door de regel test\_warning.

Reden: de webbron behoort tot de inhoudscategorieën Onbepaald en de gegevenscategorieën Onbepaald.

Klik op de koppeling <http://kaspersky.com/> om de opgevraagde webpagina te openen.

Klik op de koppeling <http://kaspersky.com/> om toegang te krijgen tot de volledige inhoud van de website, waarvan de webpagina deel uitmaakt.

Klik op de koppeling [\\*://\\*.kaspersky.com/](http://*.kaspersky.com/) om toegang te krijgen tot alle bestaande domeinen van een niveau dat lager is dan of gelijk is aan het niveau met het "\*".

De toegang tot de hierboven vermelde webbronnen wordt tijdens de huidige sessie van het programma toegestaan.

Als je een waarschuwing ziet die berust op een vergissing, neem je contact op met de beheerder van het lokale bedrijfsnetwerk ([Toegang vragen](#)).


Bericht gemaakt op: 10/29/2020 4:20:00 AM

Berichten van Webcontrole

## Webcontrole inschakelen en uitschakelen

Webcontrole is standaard ingeschakeld.

*Zo schakelt u Webcontrole in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Webcontrole** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

## Bewerkingen voor toegangsregels voor webbronnen

Het is niet aanbevolen om meer dan 1000 toegangsregels voor webbronnen aan te maken omdat het systeem hierdoor instabiel kan worden.

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 inhoud en gegevens, die behoren tot de typen gedefinieerd door deze 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 gebruikers.** U kunt de namen van gebruikers en/of groepen 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 'Scripts en opmaakmodellen' 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>.

- Standaardregel. Deze regel wordt toegepast op alle webbronnen waarop geen andere regels van toepassing zijn en staat de toegang tot deze webbronnen al dan niet toe voor alle gebruikers.

## Een toegangsregel voor webbronnen toevoegen

*Zo voegt u een toegangsregel voor webbronnen toe en bewerkt u er een:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. In het blok **Instellingen**, klikt u op de knop **Toegangsregels voor webbronnen**.
4. Klik in het venster op de knop **Toevoegen**.  
Het venster **Regel voor toegang tot webbronnen** wordt geopend.
5. Typ in het veld **Regelnaam** de naam van de regel.
6. Selecteer de status **Aan** voor de toegangsregel voor webbronnen.  
U kunt de schakelaar gebruiken [om de toegangsregel voor webbronnen op elk gewenst moment uit te schakelen](#).
7. Selecteer in het blok **Actie** de relevante 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.
8. Selecteer in het blok **Inhoud van de filter** het relevante filter voor de inhoud:
  - **Op inhoudscategorieën**. U kunt gebruikerstoegang tot webbronnen per [categorie](#)  beheren (bijvoorbeeld de categorie *Sociale netwerken*).
  - **Op gegevenstypen**. U kunt de gebruikerstoegang tot webbronnen beheren op basis van het specifieke gegevenstype van de gepubliceerde gegevens (bijvoorbeeld *grafische afbeeldingen*).

Het inhoudsfilter configureren:

- a. Klik op de link **Instellingen**.
- b. 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.
- c. Keer terug naar het venster voor het configureren van de toegangsregel voor webbronnen.

9. Selecteer in het blok **Adressen** het relevante filter voor adres van de webbron:

- **Op alle adressen.** Webcontrole filtert webbronnen niet op adres.
- **Op individuele adressen.** Webcontrole filtert alleen adressen van webbronnen uit de lijst. Een lijst met vertrouwde adressen van webbronnen maken:
  - a. Klik op de knop **Adres** of **Adresgroep** .
  - b. Maak in het venster dat opent een lijst met adressen van webbronnen. U kunt een webadres invoeren of [maskers gebruiken](#). U kunt ook [een lijst met webbronadressen exporteren vanuit een TXT-bestand](#).
  - c. Keer terug naar het venster voor het configureren van de toegangsregel voor webbronnen.

Als de [Scan van versleutelde verbindingen is uitgeschakeld](#), kunt u voor het HTTPS-protocol alleen op servernaam filteren.

10. Selecteer in het blok **Gebruikers** het relevante filter voor gebruikers:

- **Op alle gebruikers.** Webcontrole filtert geen webbronnen voor specifieke gebruikers.
- **Op individuele gebruikers en/of groepen.** Webcontrole filtert webbronnen alleen voor specifieke gebruikers. Een lijst met gebruikers maken waarop u de regel wilt toepassen:
  - a. Klik op **Toevoegen**.
  - b. Selecteer in het venster dat opent de gebruikers of groep gebruikers waarop u de toegangsregel voor webbronnen wilt toepassen.
  - c. Keer terug naar het venster voor het configureren van de toegangsregel voor webbronnen.

11. 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:

- a. Klik op **Bewerken of nieuw toevoegen**.
- b. Klik in het geopende venster op de knop **Toevoegen**.
- c. Voer in het venster dat opent de naam van de regelplanning in.
- d. Configureer het toegangsschema voor webbronnen voor gebruikers.
- e. Keer terug naar het venster voor het configureren van de toegangsregel voor webbronnen.


12. Sla uw wijzigingen op.

## Prioriteiten aan toegangsregels voor webbronnen toewijzen

Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als een website is toegevoegd aan meerdere regels, regelt Webcontrole de toegang tot de website volgens de regel met de hoogste prioriteit. Kaspersky Endpoint Security kan bijvoorbeeld een bedrijfsportal identificeren als een sociaal netwerk. Wilt u de toegang tot sociale netwerken verbieden maar toch toegang tot de webportal van het bedrijf verlenen, dan maakt u twee regels: een regel die de websitecategorie 'Sociale netwerken' blokkeert en een regel die de webportal van het bedrijf toestaat. De toegangsregel voor de webportal van het bedrijf moet een hogere prioriteit hebben dan de toegangsregel voor sociale netwerken.

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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. In het blok **Instellingen**, klikt u op de knop **Toegangsregels voor webbronnen**.
4. Selecteer in het venster dat opent de regel waarvan u de prioriteit wilt wijzigen.
5. Gebruik de knoppen **Omhoog** en **Omlaag** om de regel naar de relevante plaats in de lijst met toegangsregels van webbronnen te bewegen.
6. Sla uw wijzigingen op.

## Een toegangsregel voor webbronnen inschakelen en uitschakelen

*Zo schakelt u een toegangsregel voor webbronnen in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. In het blok **Instellingen**, klikt u op de knop **Toegangsregels voor webbronnen**.
4. Selecteer in het geopende venster rechts de regel die u wilt in- of uitschakelen.
5. 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.
6. Sla uw wijzigingen op.

## De lijst met vertrouwde webadressen exporteren en importeren

U kunt de lijst met regels van Webcontrole exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal adressen van hetzelfde type toe te voegen. U kunt de export- en importfunctie gebruiken om een back-up te maken van de lijst met regels van Webcontrole of om de lijst naar een andere server te migreren.

## Een lijst met regels van Webcontrole exporteren en importeren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
6. Zo exporteert u de lijst met regels van Webcontrole:
  - a. Selecteer de regels die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen regel hebt geselecteerd, exporteert Kaspersky Endpoint Security alle regels.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met regels wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.
7. Zo importeert u de lijst met regels van Webcontrole:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

## Een lijst met regels van Webconsole exporteren en importeren via de Webconsole en Cloudconsole

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Security Controls** → **Webcontrole**.
5. U exporteert de lijst met regels door het volgende te doen in het blok **Rule List**:
  - a. Selecteer de regels die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde regels wilt exporteren of de volledige lijst wilt exporteren.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar een XML-bestand in de standaard downloadmap.
6. U importeert de lijst met regels door het volgende te doen in het blok **Rule List**:
  - a. Klik op de koppeling **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
7. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. Klik in het blok **Instellingen** op de koppeling **Diagnose van regels**.  
Het venster **Diagnose van regels** wordt geopend.
4. 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.

5. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot webbronnen te controleren voor opgegeven gebruikers en/of groepen gebruikers, geeft u een lijst met gebruikers en/of groepen gebruikers op.
6. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot webbronnen van bepaalde inhoudscategorieën en/of categorieën van gegevenstypen te controleren, schakelt u het selectievakje **Filter inhoud** in en kiest u de relevante optie uit de vervolgkeuzelijst (**Op inhoudscategorieën**, **Op gegevenstypen** of **Op inhoudscategorieën en gegevenstypen**).
7. 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.
8. Klik op **Scannen**.

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 verkrijgen van toegang tot de opgegeven webbron (toestaan, blokkeren of waarschuwing). 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 **Scannen** 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.

## 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.

*Een lijst met adressen van webbronnen naar een bestand importeren of exporteren:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. In het blok **Instellingen**, klikt u op de knop **Toegangsregels voor webbronnen**.
4. Selecteer de regel waarvan u de lijst met adressen van webbronnen wilt exporteren of importeren.
5. Om de lijst met vertrouwde webadressen te exporteren, doet u het volgende in het blok **Adressen**:
  - a. Selecteer de items die u wilt exporteren.  
Als u geen enkel adres hebt geselecteerd, dan exporteert Kaspersky Endpoint Security alle adressen.
  - b. Klik op **Exporteren**.
  - c. Voer in het venster dat opent de naam in van het TXT-bestand waarnaar u de lijst met adressen van webbronnen wilt exporteren, en selecteer de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met adressen van webbronnen naar een TXT-bestand.



6. Om de lijst met webbronnen te importeren, doet u het volgende in het blok **Adressen**:

a. Klik op **Importeren**.

Selecteer in het geopende venster het TXT-bestand waaruit u de lijst met webbronnen wilt importeren.

b. Open het bestand.

Als de computer al een lijst met adressen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het TXT-bestand.

7. Sla uw wijzigingen op.

## Activiteit van gebruikers op internet bewaken

Met Kaspersky Endpoint Security kunt u gegevens registreren over bezoeken aan websites, waaronder toegestane websites. Op deze manier krijgt u een compleet overzicht van de browseractiviteit. Kaspersky Endpoint Security stuurt gebeurtenissen over gebruikersactiviteit naar Kaspersky Security Center, naar [het lokale logboek van Kaspersky Endpoint Security](#) en naar het Windows-gebeurtenislogboek. Voor het ontvangen van gebeurtenissen in Kaspersky Security Center moet u de instellingen van gebeurtenissen configureren in een beleid in Beheerconsole of Webconsole. U kunt ook de overdracht van Webcontrole-gebeurtenissen per e-mail configureren, alsook de weergave van meldingen op het computerscherm van de gebruiker.

Browsers die de bewakingsfunctie ondersteunen: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Bewaking van gebruikersactiviteiten werkt niet in andere browsers.

Kaspersky Endpoint Security maakt de volgende gebeurtenissen over de activiteit van gebruikers op internet:

- Blokkering van de website (status *Kritieke gebeurtenissen* .
- Bezoek aan een niet-aanbevolen website (status *Waarschuwingen* .
- Bezoek aan een toegestane website (status *Informatieve berichten* .

Voordat u bewaking van de internetactiviteit van gebruikers inschakelt, moet u het volgende doen:

- Injecteer een webpagina-interactiescript in het webverkeer (zie onderstaande instructies). Het script maakt de registratie van Webcontrole-gebeurtenissen mogelijk.
- Voor de bewaking van HTTPS-verkeer moet u [Versleutelde verbindingen scannen](#) inschakelen.

*Een interactiescript voor een webpagina in het webverkeer injecteren:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Schakel in het blok **Verkeersverwerking** het selectievakje **Injecteer script in internetverkeer voor interactie met webpagina's** in.
4. Sla uw wijzigingen op.

Als gevolg hiervan zal Kaspersky Endpoint Security een webpagina-interactiescript in het webverkeer injecteren. Met dit script kunnen Webcontrole-gebeurtenissen voor het programmeergebeurtenislogboek, het OS-gebeurtenislogboek en [rapporten](#) worden geregistreerd.

*Zo configureert u de registratie van Webcontrole-gebeurtenissen op de computer van de gebruiker:*


1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
3. In het blok **Meldingen**, klikt u op de knop **Instellingen voor meldingen**.
4. Selecteer in het geopende venster het gedeelte **Webcontrole**.  
U ziet nu de tabel met Webcontrole-gebeurtenissen en methoden voor meldingen.
5. Configureer de methode voor het melden van elke gebeurtenis: **Opslaan in lokaal rapport** of **Opslaan in Windows-gebeurtenislogboek**.  
Voor het registreren van bezoeken aan toegestane websites moet u ook Webcontrole configureren (raadpleeg de onderstaande instructies).  
In de tabel met gebeurtenissen kunt u ook instellen dat een melding op het scherm moet worden weergegeven en dat een melding per e-mail moet worden verstuurd. Voor het versturen van meldingen per e-mail moet u de instellingen van de SMTP-server configureren. Voor meer informatie over het versturen van meldingen per e-mail raadpleegt u de [Help van Kaspersky Security Center](#) .
6. Sla uw wijzigingen op.

Kaspersky Endpoint Security begint nu gebeurtenissen voor de activiteit van de gebruiker op internet te registreren.

Webcontrole stuurt gebeurtenissen van gebruikersactiviteiten als volgt naar Kaspersky Security Center:

- Als u Kaspersky Security Center gebruikt, verzendt Webcontrole gebeurtenissen voor alle objecten waaruit de webpagina bestaat. Daarom kunnen meerdere gebeurtenissen worden aangemaakt wanneer een webpagina wordt geblokkeerd. Voorbeeld: bij de blokkering van de webpagina <http://www.voorbeeld.nl>, zal Kaspersky Endpoint Security gebeurtenissen voor de volgende objecten vastleggen: <http://www.voorbeeld.nl>, <http://www.voorbeeld.nl/icon.ico>, <http://www.voorbeeld.nl/file.js>, etc.
- Als u de Kaspersky Security Center Cloud Console gebruikt, groepeert Webcontrole gebeurtenissen en verzendt alleen het protocol en het domein van de website. Als een gebruiker bijvoorbeeld niet-aanbevolen webpagina's <http://www.example.com/main>, <http://www.example.com/contact> en <http://www.example.com/gallery> bezoekt, verzendt Kaspersky Endpoint Security slechts één gebeurtenis met het object <http://www.example.com>.

*Zo schakelt u de registratie van gebeurtenissen voor bezoeken aan toegestane websites in:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. In het blok **Extra**, klikt u op de knop **Geavanceerde instellingen**.
4. Selecteer in het venster dat opent het selectievakje **Registreer het openen van toegestane pagina's**.
5. Sla uw wijzigingen op.

U kunt nu de volledige browsergeschiedenis bekijken.


## 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):

- **Waarschuwing** 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 waarschuwingbericht als de optie **Waarschuwen** is geselecteerd 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 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 waarschuwingbericht, 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.
3. Configureer in het blok **Sjablonen** de sjablonen voor Webcontrole-berichten:
  - **Waarschuwing** Het invoerveld bestaat uit een sjabloon van het bericht dat wordt weergegeven als een regel voor een waarschuwing over pogingen tot toegang tot een ongewenste webbron wordt geactiveerd.
  - **Bericht over blokkering** Het invoerveld bevat het sjabloon van het bericht dat wordt weergegeven als een regel die de toegang tot een webbron blokkeert wordt geactiveerd.
  - **Bericht aan beheerder** Sjabloon van het bericht dat naar de netwerkbeheerder wordt verstuurd als de gebruiker vindt dat de blokkering een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: **Bericht over blokkering van toegang tot webpagina aan beheerder**. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie **User requests**. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.
4. Sla uw wijzigingen op.

## 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 die de reeks `abc` bevatten. Voorbeeld: `http://www.voorbeeld.com/pagina_0-9abcdef.html`.

2. Een reeks van `*.` tekens (ook wel *domeinmasker genoemd*) laat u alle domeinen van een adres selecteren. Het `*.` domeinmasker vertegenwoordigt een domeinnaam, subdomeinnaam of een lege regel.

Voorbeeld: het masker `*.example.com` staat voor de volgende adressen:

- `http://pictures.example.com`. Het domeinmasker `*.` vertegenwoordigt `afbeeldingen`.
- `http://user.pictures.example.com`. Het domeinmasker `*.` vertegenwoordigt `afbeeldingen` en `gebruiker`.
- `http://voorbeeld.com`. Het domeinmasker `*.` wordt geïnterpreteerd als een lege regel.

3. De tekenreeks `www.` bij het begin van het adresmasker wordt beschouwd als een `*.`-reeks.

Voorbeeld: het adresmasker `www.voorbeeld.com` wordt behandeld als `*.voorbeeld.com`. Dit masker bedekt de adressen `www2.example.com` en `www.pictures.example.com`.

4. Als een adresmasker niet begint met het teken `*`, is de inhoud van het adresmasker gelijk aan dezelfde inhoud met het voorvoegsel `*.`

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.example.com/abc`, waarbij `a`, `b`, and `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.nl` omvat de adressen `http://voorbeeld.nl` en `https://voorbeeld.nl`.

- 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 2.   |
| 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 3, 2, 1.  |
| 7   | www.voorbeeld.com            | https://www.voorbeeld.com                              | Ja                              | Zie regels 3, 2, 1.  |
| 8   | http://www.*.voorbeeld.com   | http://123.voorbeeld.com                               | Ja                              | Zie regels 3, 4, 1.  |
| 9   | www.voorbeeld.com            | http://www.voorbeeld.com/abc                           | Ja                              | Zie regels 3, 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;<br>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. |

Toegangsregels voor webbronnen migreren vanaf oudere versies van het programma

Wanneer Kaspersky Endpoint Security 10 Service Pack 2 voor Windows of een oudere versie van het programma wordt bijgewerkt naar Kaspersky Endpoint Security 11.9.0 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 'Chats en forums', 'Webmail' en 'Sociale netwerken' worden naar de inhoudscategorie 'Online communicatie' 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 'Online winkels, banken, betaalsystemen' 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.

## Apparaatcontrole

Apparaatcontrole beheert de toegang van gebruikers tot apparaten die zijn geïnstalleerd in of aangesloten op de computer (bijvoorbeeld harde schijven, camera's of wifi-apparaten). Met dit onderdeel kunt u de computer beschermen tegen infecties en datalekken voorkomen wanneer zulke apparaten worden aangesloten.

### Niveaus voor toegang tot apparaten

Apparaatcontrole beheert de toegang op de volgende niveaus:

- **Apparaattype.** Bijvoorbeeld printers, verwisselbare schijven en cd-/dvd-stations.

Zo kunt u de toegang tot apparaten configureren:

- Toestaan – ✓.
- Blokkeren – ✗.
- Afhankelijk van de verbindingbus (behalve wifi) – 🌐.
- Blokkeren met uitzonderingen (alleen wifi) – 🚫.

- **Verbindingbus.** Een *verbindingbus* is een interface voor de aansluiting van apparaten op de computer (bijvoorbeeld USB of FireWire). U kunt dus de aansluiting van alle apparaten beperken, bijvoorbeeld via USB.

Zo kunt u de toegang tot apparaten configureren:

- Toestaan – ✓.
- Blokkeren – ✗.

- **Vertrouwde apparaten.** *Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

U kunt vertrouwde apparaten toevoegen op basis van de volgende gegevens:

- **Apparaten per ID.** Elk apparaat heeft een uniek ID (Hardware-ID of HWID). U kunt het ID in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Voorbeeld van een apparaat-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Apparaten toevoegen per ID is handig als u meerdere specifieke apparaten wilt toevoegen.
- **Apparaten per model.** Elk apparaat heeft een leverancier-ID (VID) en een product-ID (PID). U kunt de ID's in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Sjabloon voor de invoer van het VID en PID: `VID_1234&PID_5678`. Apparaten toevoegen per model is handig als u een bepaald model apparaten in uw bedrijf gebruikt. Op deze manier kunt u alle apparaten van dit model toevoegen.
- **Apparaten per ID-masker.** Als u meerdere apparaten met vergelijkbare ID's gebruikt, kunt u maskers gebruiken om apparaten toe te voegen aan de lijst met vertrouwde apparaten. Het teken `*` vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken `?` bij de invoer van een masker. Bijvoorbeeld `WDC_C*`.
- **Apparaten per modelmasker.** Als u meerdere apparaten met vergelijkbare VID's of PID's gebruikt (bijvoorbeeld apparaten van dezelfde fabrikant), kunt u maskers gebruiken om apparaten aan de lijst met vertrouwde apparaten toe te voegen. Het teken `*` vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken `?` bij de invoer van een masker. Bijvoorbeeld `VID_05AC & PID_*`.

Apparaatcontrole beheert de toegang van gebruikers tot apparaten met behulp van [toegangsregels](#). Via Apparaatcontrole kunt u ook gebeurtenissen zoals het aansluiten of loskoppelen van apparaten opslaan. Voor het opslaan van gebeurtenissen moet u in een beleid de registratie van gebeurtenissen configureren.

Als de toegang tot een apparaat afhangt van de aansluitbus (de status 🌈), slaat Kaspersky Endpoint Security geen informatie over het aansluiten of loskoppelen van apparaten op. Als u wilt dat Kaspersky Endpoint Security informatie over het aansluiten of loskoppelen van apparaten opslaat, staat u de toegang tot het desbetreffende soort apparaat toe (de status ✓) of voegt u het apparaat aan de vertrouwde lijst toe.

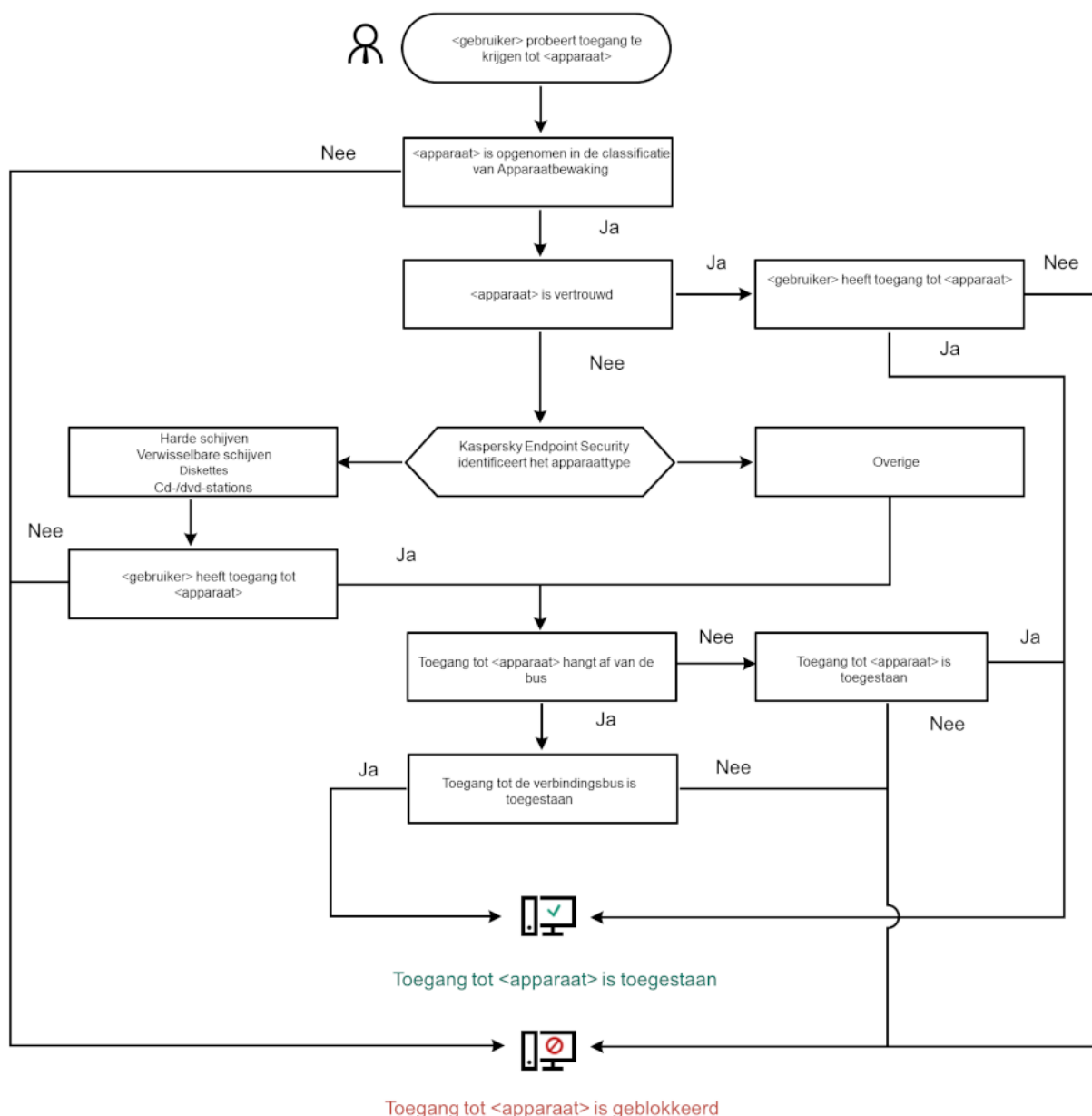
Wanneer een apparaat dat wordt geblokkeerd door Apparaatcontrole wordt aangesloten op de computer, blokkeert Kaspersky Endpoint Security de toegang en toont het een melding (zie onderstaande afbeelding).



Melding van Apparaatcontrole

Algoritme voor werking van Apparaatcontrole

Kaspersky Endpoint Security beslist of de toegang tot een apparaat moet worden verleend nadat de gebruiker het apparaat op de computer heeft aangesloten (zie onderstaande afbeelding).



Algoritme voor werking van Apparaatcontrole

Als een apparaat wordt aangesloten en de toegang wordt verleend, kunt u de toegangsregel bewerken om de toegang te blokkeren. In dit geval blokkeert Kaspersky Endpoint Security de toegang de volgende keer dat iemand probeert toegang te krijgen tot het apparaat (bewerkingen zoals het weergeven van de mapstructuur of het lezen of schrijven van data). 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](#).

## Apparaatcontrole inschakelen en uitschakelen

Apparaatcontrole is standaard ingeschakeld.



Zo schakelt u Apparaatcontrole in of uit:

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Apparaatcontrole** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan, als Apparaatbeheer is ingeschakeld, stuurt het programma informatie over aangesloten apparaten door naar Kaspersky Security Center. U kunt de lijst met aangesloten apparaten bekijken in Kaspersky Security Center in de map **Geavanceerd** → **Opslag** → **Hardware**.

## Over toegangsregels

*Toegangsregels* zijn een groep instellingen die bepalen welke gebruikers toegang krijgen tot apparaten die zijn geïnstalleerd in of aangesloten op de computer. U kunt geen apparaten toevoegen die niet door Apparaatcontrole kunnen worden geclassificeerd. De toegang tot zulke apparaten is voor alle gebruikers toegestaan.

### Toegangsregels voor apparaten

De groep instellingen van een toegangsregel hangt af van het type apparaat (zie onderstaande tabel).

Instellingen van toegangsregels

| Apparaten                           | Toegangsbeheer | Schema voor toegang tot een apparaat | Toewijzing van gebruikers en/of groepen gebruikers | Prioriteit | Lees- en schrijfmachtiging |
|-------------------------------------|----------------|--------------------------------------|--|------------|----------------------------|
| Harde schijven                      | ✓              | ✓                                    | ✓  | ✓          | ✓                          |
| Verwisselbare schijven              | ✓              | ✓                                    | ✓  | ✓          | ✓                          |
| Printers                            | ✓              | –                                    | –  | –          | –                          |
| Diskettes                           | ✓              | ✓                                    | ✓  | ✓          | ✓                          |
| Cd-/dvd-stations                    | ✓              | ✓                                    | ✓  | ✓          | ✓                          |
| Modems                              | ✓              | –                                    | –  | –          | –                          |
| Tapeapparaten                       | ✓              | –                                    | –  | –          | –                          |
| Multifunctionele apparaten          | ✓              | –                                    | –  | –          | –                          |
| Smartcardlezers                     | ✓              | –                                    | –  | –          | –                          |
| Windows CE USB ActiveSync-apparaten | ✓              | –                                    | –  | –          | –                          |
| Externe netwerkadapters             | ✓              | –                                    | –  | –          | –                          |


|                           |   |   |   |   |   |
|---------------------------|---|---|---|---|---|
| Draagbare apparaten (MTP) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bluetooth                 | ✓ | – | – | – | – |
| Camera's en scanners      | ✓ | – | – | – | – |

## Toegangsregels voor mobiele apparaten




Mobiele Android- of iOS-apparaten worden als draagbare apparaten (MTP) gecategoriseerd. Wanneer een mobiel apparaat wordt aangesloten op de computer, bepaalt het besturingssysteem het type van het apparaat. Als Android Debug Bridge (ADB), iTunes of een equivalent programma is geïnstalleerd op de computer, identificeert het besturingssysteem mobiele apparaten als ADB- of iTunes-apparaten. In alle andere gevallen kan het besturingssysteem het type van het mobiele apparaat identificeren als een draagbaar apparaat (MTP) voor bestandsoverdrachten, een PTP-apparaat (camera) voor de overdracht van afbeeldingen of een ander apparaat. Het type apparaat hangt af van het model van het mobiele apparaat.

Houd rekening met de volgende aandachtspunten voor toegang tot ADB- of iTunes-apparaten:



- U kunt geen toegangsschema voor apparaten configureren. Als de toegang tot apparaten is beperkt door regels (ze hebben de status ) , zijn ADB- en iTunes-apparaten altijd toegankelijk.
- U kunt de toegang tot apparaten niet configureren voor individuele gebruikers of toegangsmachtigingen (lezen/schrijven) configureren. Als de toegang tot apparaten is beperkt door regels (ze hebben de status ) , zijn ADB- en iTunes-apparaten toegankelijk voor alle gebruikers met alle machtigingen.
- U kunt de toegang tot ADB- of iTunes-apparaten niet configureren voor individuele gebruikers. Als het apparaat wordt vertrouwd, zijn ADB- en iTunes-apparaten toegankelijk voor alle gebruikers.
- Als u de ADB- of iTunes-programma's hebt geïnstalleerd nadat u een apparaat op de computer hebt aangesloten, wordt het unieke ID van het apparaat mogelijk opnieuw ingesteld. Dan zal Kaspersky Endpoint Security dit apparaat identificeren als een nieuw apparaat. Als u het apparaat vertrouwt, voegt u het apparaat opnieuw toe aan de lijst met vertrouwde apparaten.

Standaard geven toegangsregels alle gebruikers altijd volledige toegang tot de apparaten als de toegang tot de verbindingusbussen voor de overeenkomstige soorten apparaten is toegestaan (de status ) .

## Toegangsregels voor wifinetwerken

Een toegangsregel voor wifinetwerken bepaalt of het gebruik van wifinetwerken is toegestaan (de status ) of verboden (de status ) . U kunt een *vertrouwd wifinetwerk* (de status ) toevoegen aan een regel. Bij het gebruik van een vertrouwd wifinetwerk zijn er geen beperkingen. Standaard staat een toegangsregel voor wifinetwerken de toegang tot elk wifinetwerk toe.


## Toegangsregels voor verbindingusbussen

Toegangsregels voor verbindingusbussen bepalen of de aansluiting van apparaten is toegestaan (de status ) of verboden (de status ) . Regels die de toegang tot bussen toestaan, worden standaard aangemaakt voor alle verbindingusbussen in de classificatie van het onderdeel Apparaatcontrole.

## Een regel voor toegang tot apparaten bewerken

*Regels voor toegang tot apparaten* zijn een groep instellingen die bepalen hoe gebruikers toegang krijgen tot apparaten die zijn geïnstalleerd of aangesloten op de computer. Deze instellingen omvatten toegang tot een specifiek apparaat, een toegangsschema en lees- of schrijfmachtigingen.

*Zo bewerkt u een regel voor toegang tot apparaten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.

3. In het blok **Toegangsinstellingen**, klikt u op de knop **Apparaten en wifinetwerken**.

Het geopende venster toont toegangsregels voor alle apparaten die zijn opgenomen in de componentclassificatie Apparaatcontrole.

4. Selecteer in het blok **Toegang tot opslagapparaten** de toegangsregel die u wilt bewerken. Het blok bevat apparaten met een bestandssysteem waarvoor u aanvullende toegangsinstellingen kunt configureren. Standaard geeft een regel voor toegang tot apparaten alle gebruikers op elk moment volledige toegang tot het opgegeven type van apparaten.

a. In het blok **Toegang**, selecteert u de gepaste optie voor toegang tot het apparaat:

- **Toestaan.**
- **Blokkeren.**
- **Afhankelijk van verbindingbus.**

[Configureer de toegang tot de verbindingbus](#) om de toegang tot een apparaat te blokkeren of toe te staan.

- **Beperken volgens regels.**

Met deze optie kunt u gebruikersrechten, machtigingen en een schema voor apparaattoegang configureren.

- b. Klik in het venster **Gebruikersrechten** op de knop **Toevoegen**.

Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot apparaten.

- c. Wijs een prioriteit aan de *regel/toe*. Een regel bevat de volgende kenmerken: gebruikersaccount, planning, machtigingen (lezen/schrijven) en prioriteit.

Een regel heeft een specifieke prioriteit. Als een gebruiker aan meerdere groepen is toegevoegd, regelt Kaspersky Endpoint Security de apparaattoegang op basis van de regel met de hoogste prioriteit. U kunt in Kaspersky Endpoint Security een prioriteit toekennen van 0 tot 10.000. Hoe hoger de waarde, hoe hoger de prioriteit. Met andere woorden, een invoer met de waarde 0 heeft de laagste prioriteit.

U kunt bijvoorbeeld de machtiging alleen-lezen verlenen aan de groep Iedereen en de machtiging lezen/schrijven aan de groep Administratoren. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep Administratoren en een prioriteit van 0 voor de groep Iedereen.


De prioriteit van een Blokkeren-regel is hoger dan die van een Toestaan-regel. Als een gebruiker met andere woorden aan meerdere groepen is toegevoegd en de prioriteit van alle regels hetzelfde is, dan regelt Kaspersky Endpoint Security de toegang tot het apparaat op basis van een bestaande blokkeringsregel.

- d. Selecteer de status **Ingeschakeld** voor de regel voor apparaattoegang.

- e. Configureer de machtigingen voor apparaattoegang van gebruikers: lezen en/of schrijven.
  - f. Selecteer de gebruikers of groep gebruikers waarop u de regel voor apparaattoegang wilt toepassen.
  - g. Configureer een apparaattoegangsschema voor gebruikers.
  - h. Klik op de knop **Add**.
5. Selecteer in het blok **Toegang tot externe apparaten** de regel en configureer de toegang: **Toestaan**, **Blokkeren** of **Afhankelijk van verbindingbus** indien nodig. [Configureer indien nodig de verbindingbus](#).
  6. Klik in het blok **Toegang tot wifinetwerken** op de koppeling **Wifi** en configureer de toegang: **Toestaan**, **Blokkeren**, of **Blokkeren met uitzonderingen**. Voeg indien nodig [wifinetwerken toe aan de vertrouwde lijst](#).
  7. Sla uw wijzigingen op.

## Een toegangsregel voor verbindingsbussen bewerken

*Zo bewerkt u een toegangsregel voor verbindingsbussen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Verbindingsbussen**.  
Het geopende venster toont toegangsregels voor alle verbindingsbussen die zijn opgenomen in de onderdeelclassificatie Apparaatcontrole.
4. Selecteer de toegangsregel die u wilt bewerken.
5. Selecteer in de kolom **Toegang** of u al dan niet toegang tot de verbindingbus wilt toestaan: **Toestaan** of **Blokkeren**.
6. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Apparaten en wifinetwerken**.

Het geopende venster toont toegangsregels voor alle apparaten die zijn opgenomen in de componentclassificatie Apparaatcontrole.

4. Klik in het blok **Toegang tot wifinetwerken** op de koppeling **Wifi**.

Het geopende venster toont de toegangsregels voor het wifinetwerk.

5. Selecteer in het blok **Toegang Blokkeren met uitzonderingen**.

6. In het blok **Vertrouwde wifinetwerken**, klikt u op de knop **Toevoegen**.

7. Doe in het venster dat opent het volgende:

- a. Geef in het veld **Netwerknaam** de naam van het wifinetwerk op dat u aan de lijst Vertrouwd wilt toevoegen.
- b. Selecteer in de vervolgkeuzelijst **Authenticatietype** het gebruikte type authenticatie voor de verbinding met het vertrouwde wifinetwerk.
- c. Selecteer in de vervolgkeuzelijst **Encryptietype** het gebruikte type encryptie voor de beveiliging van het verkeer van het vertrouwde wifinetwerk.
- d. 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.

8. Sla uw wijzigingen op.

## Bewaking op het gebruik van verwisselbare schijven

De bewaking van het gebruik van verwisselbare schijven omvat:

- De bewaking van bewerkingen met bestanden op verwisselbare schijven.
- De bewaking van de aansluiting en verwijdering van vertrouwde verwisselbare schijven.

Met Kaspersky Endpoint Security kunt u de aansluiting en verwijdering van alle vertrouwde apparaten bewaken, en niet alleen verwisselbare schijven. U kunt de registratie van gebeurtenissen inschakelen in [Instellingen voor meldingen](#) voor het onderdeel Apparaatcontrole. Gebeurtenissen hebben de ernst *Informatieve berichten*.

*Bewaking op het gebruik van verwisselbare schijven inschakelen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Apparaten en wifinetwerken**.  
Het geopende venster toont toegangsregels voor alle apparaten die zijn opgenomen in de componentclassificatie Apparaatcontrole.
4. Selecteer **Toegang tot opslagapparaten** in het blok **Verwisselbare schijven**.
5. Selecteer in het geopende venster het tabblad **Registratie**.

6. Zet de schakelaar **Registratie** aan.
7. Selecteer in het blok **Bestandsbewerkingen** de bewerkingen die u wilt bewaken: **Schrijven, Verwijderen**.
8. Selecteer in het blok **Filteren op bestandsindelingen** de bestandsindelingen waarvan de bijbehorende bewerkingen door apparaatcontrole moeten worden geregistreerd.
9. Selecteer de gebruikers of groep gebruikers waarvan u het gebruik van verwisselbare schijven wilt controleren.
10. Sla uw wijzigingen op.

Als resultaat, wanneer 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 Kaspersky Security Center. 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.

## De cacheduur wijzigen

Het onderdeel Apparaatbeheer registreert gebeurtenissen die verband houden met bewaakte apparaten, zoals het verbinden van een apparaat en het verbreken van de verbinding met een apparaat, het lezen van een bestand van een apparaat, het schrijven van een bestand naar een apparaat en andere gebeurtenissen. Apparaatbeheer staat vervolgens de actie toe of blokkeert deze op basis van de instellingen van Kaspersky Endpoint Security.

Apparaatbeheer slaat informatie over gebeurtenissen op voor een specifieke periode, de *cacheperiode genoemd*. Als informatie over een gebeurtenis in de cache wordt opgeslagen en deze gebeurtenis wordt herhaald, is het niet nodig om Kaspersky Endpoint Security hiervan op de hoogte te stellen of om een andere prompt weer te geven voor het verlenen van toegang tot de overeenkomstige actie, zoals het verbinden van een apparaat. Hierdoor wordt het handiger om met een apparaat te werken.

Een gebeurtenis wordt als een dubbele gebeurtenis beschouwd als alle volgende gebeurtenisinstellingen overeenkomen met het record in de cache:

- apparaat-ID
- SID van het gebruikersaccount dat toegang probeert te krijgen
- Apparaatcategorie
- Actie ondernomen met het apparaat
- Toestemming van programma voor deze actie: toegestaan of geweigerd
- Pad naar het proces dat wordt gebruikt om de actie uit te voeren
- Bestand waartoe toegang wordt verkregen

[Schakel Zelfbescherming van Kaspersky Endpoint Security uit](#) voordat u de cacheperiode wijzigt. Schakel Zelfbescherming in nadat u de cacheperiode hebt gewijzigd.

*De cacheperiode wijzigen:*

1. Open de registereditor op de computer.
2. Ga in de registereditor naar het volgende gedeelte:
  - Voor 64-bits besturingssystemen:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
  - Voor 32-bits besturingssystemen:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]
3. Open `DeviceControlEventsCachePeriod` om het te bewerken.
4. Definieer het aantal minuten dat Apparaatbeheer informatie over een gebeurtenis moet opslaan voordat deze informatie wordt verwijderd.

## Bewerkingen met vertrouwde apparaten

*Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

Om met vertrouwde apparaten te werken, kunt u toegang verlenen aan een individuele gebruiker, een groep gebruikers of aan alle gebruikers van de organisatie.

Als uw organisatie bijvoorbeeld het gebruik van verwisselbare schijven niet toestaat, maar beheerders verwisselbare schijven voor hun werk gebruiken, kunt u verwisselbare schijven alleen toestaan voor een groep beheerders. U doet dit door verwisselbare schijven toe te voegen aan de vertrouwde lijst en de toegangsrechten voor gebruikers te configureren.

Het wordt niet aanbevolen om meer dan 1000 vertrouwde apparaten toe te voegen, omdat dit systeeminstabiliteit kan veroorzaken.

Met Kaspersky Endpoint Security kunt u op de volgende manieren een apparaat aan de vertrouwde lijst toevoegen:

- Als Kaspersky Security Center niet in uw organisatie is geïmplementeerd, kunt u het apparaat op de computer aansluiten en het [toevoegen aan de vertrouwde lijst in de programma-instellingen](#). Als u de lijst met vertrouwde apparaten naar alle computers in uw organisatie wilt distribueren, kunt u het samenvoegen van de lijsten met vertrouwde apparaten in een beleid inschakelen of de [export-/importprocedure gebruiken](#).
- Als Kaspersky Security Center in uw organisatie is geïmplementeerd, kunt u alle verbonden apparaten op afstand detecteren en [een lijst met vertrouwde apparaten in het beleid maken](#). De lijst met vertrouwde apparaten is beschikbaar op alle computers waarop het beleid wordt toegepast.

Met Kaspersky Endpoint Security kunt u het gebruik van vertrouwde apparaten beheren (aansluiting en verwijdering). U kunt de registratie van gebeurtenissen inschakelen in [Instellingen voor meldingen](#) voor het onderdeel Apparaatcontrole. Gebeurtenissen hebben het urgentieniveau *Informatief*.

Kaspersky Endpoint Security heeft de volgende beperkingen bij het werken met vertrouwde apparaten:

- Beheerplug-ins van Kaspersky Endpoint Security versie 11.0.0-11.2.0 kunnen niet werken met een lijst met vertrouwde apparaten die is gemaakt in Kaspersky Endpoint Security versie 11.3.0 en 11.4.0. Wanneer u met een lijst met vertrouwde apparaten uit deze versies wilt kunnen werken, moet de beheerplug-in worden geüpgraded naar respectievelijk versie 11.3.0 en 11.4.0.

- Beheerplug-ins van Kaspersky Endpoint Security versie 11.3.0-11.4.0 kunnen niet werken met een lijst met vertrouwde apparaten die is gemaakt in Kaspersky Endpoint Security versie 11.2.0 of eerder. Om te zorgen dat deze versies kunnen werken met een lijst met vertrouwde apparaten, moet het programma worden geüpgraded naar respectievelijk versie 11.3.0 en 11.4.0. U kunt ook een verzoek sturen met een beschrijving van uw situatie naar de [Technische Support sturen via Kaspersky CompanyAccount](#).
- Wanneer u een lijst met vertrouwde apparaten wil migreren van Kaspersky Endpoint Security versie 11.2.0 naar versie 11.3.0, stuurt u een verzoek met een beschrijving van uw situatie naar de [Technische Support via Kaspersky CompanyAccount](#).

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Vertrouwde apparaten**.  
Dit opent de lijst met vertrouwde apparaten.
4. Klik op **Selecteren**.  
Dit opent de lijst met aangesloten apparaten. De lijst Apparaten hangt af van de geselecteerde waarde in de vervolkeuzelijst **Toon aangesloten apparaten**.
5. Selecteer in de lijst met apparaten het apparaat dat u aan de vertrouwde lijst wilt toevoegen.
6. In het veld **Opmerking** kunt u alle relevante informatie over het vertrouwde apparaat opgeven.
7. Selecteer de gebruikers of groep gebruikers waarvoor u toegang tot vertrouwde apparaten wilt toestaan.
8. Sla uw wijzigingen op.

## Een apparaat vanuit Kaspersky Security Center toevoegen aan de Vertrouwde lijst

Kaspersky Security Center ontvangt informatie over apparaten als Kaspersky Endpoint Security op de computers is geïnstalleerd en [Apparaatcontrole is ingeschakeld](#). Het is niet mogelijk om een apparaat aan de vertrouwde lijst toe te voegen, tenzij informatie over dat apparaat beschikbaar is in Kaspersky Security Center.

U kunt een apparaat aan de vertrouwde lijst toevoegen op basis van de volgende gegevens:

- **Apparaten per ID.** Elk apparaat heeft een uniek ID (Hardware-ID of HWID). U kunt het ID in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Voorbeeld van een apparaat-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Apparaten toevoegen per ID is handig als u meerdere specifieke apparaten wilt toevoegen.



- **Apparaten per model.** Elk apparaat heeft een leverancier-ID (VID) en een product-ID (PID). U kunt de ID's in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Sjabloon voor de invoer van het VID en PID: VID\_1234&PID\_5678. Apparaten toevoegen per model is handig als u een bepaald model apparaten in uw bedrijf gebruikt. Op deze manier kunt u alle apparaten van dit model toevoegen.
- **Apparaten per ID-masker.** Als u meerdere apparaten met vergelijkbare ID's gebruikt, kunt u maskers gebruiken om apparaten toe te voegen aan de lijst met vertrouwde apparaten. Het teken \* vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken ? bij de invoer van een masker. Bijvoorbeeld WDC\_C\*.
- **Apparaten per modelmasker.** Als u meerdere apparaten met vergelijkbare VID's of PID's gebruikt (bijvoorbeeld apparaten van dezelfde fabrikant), kunt u maskers gebruiken om apparaten aan de lijst met vertrouwde apparaten toe te voegen. Het teken \* vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken ? bij de invoer van een masker. Bijvoorbeeld VID\_05AC & PID\_ \*.

*Apparaten aan de lijst met vertrouwde apparaten toevoegen.*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkrimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
6. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.
7. Schakel het selectievakje **Waarden samenvoegen bij overname** in als u een geconsolideerde lijst met vertrouwde apparaten wilt maken voor alle computers in het bedrijf.  
De lijsten met vertrouwde apparaten in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Vertrouwde apparaten van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Het is niet mogelijk om vertrouwde apparaten van het bovenliggende beleid te wijzigen of verwijderen.
8. Klik op de knop **Toevoegen** en selecteer een methode om een apparaat aan de vertrouwde lijst toe te voegen.
9. Om apparaten te filteren, selecteert u een apparaattype in de vervolgkeuzelijst **Apparaattype** (bijvoorbeeld **Verwisselbare schijven**).
10. Voer in het veld **Naam / model** de apparaat-ID, het model (VID en PID) of het masker in, afhankelijk van de geselecteerde toevoegingsmethode.

Apparaten toevoegen per modelmasker (VID en PID) werkt als volgt: als u een modelmasker invoert dat niet overeenkomt met een model, dan controleert Kaspersky Endpoint Security of de apparaat-ID (HWID) overeenkomt met het masker. Kaspersky Endpoint Security controleert alleen het deel van de apparaat-ID dat de fabrikant en het type apparaat bepaalt (SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000). Als het modelmasker overeenkomt met dit deel van de apparaat-ID, dan worden de apparaten die overeenkomen met het masker toegevoegd aan de lijst met vertrouwde apparaten op de computer. Tegelijkertijd blijft de lijst met apparaten in Kaspersky Security Center leeg wanneer u op de knop **Vernieuwen** klikt. Om de lijst met apparaten correct weer te geven, kunt u apparaten toevoegen op apparaat-ID-masker.

11. Om apparaten te filteren, voert u in het veld **Computernaam** de computernaam of een masker in voor de naam van de computer waarmee het apparaat is verbonden.  
Het teken  \* vervangt een willekeurige reeks tekens. Het teken  ? vervangt elk willekeurig teken.
12. Klik op de knop **Vernieuwen**.  
De tabel toont een lijst met apparaten die voldoen aan de gedefinieerde filtercriteria.
13. Schakel de selectievakjes in naast de namen van de apparaten die u aan de lijst met vertrouwde apparaten wilt toevoegen.
14. Voer in het veld **Opmerking** een beschrijving in van de reden voor het toevoegen van apparaten aan de vertrouwde lijst.
15. Klik op de knop **Selecteren** aan de rechterkant van het veld **Sta toe aan gebruikers en/of groepen gebruikers**.
16. Selecteer een gebruiker of een groep in Active Directory en bevestig uw selectie.  
Standaard is toegang tot vertrouwde apparaten toegestaan voor de groep ledereen.
17. Sla uw wijzigingen op.

Wanneer een apparaat wordt aangesloten, controleert Kaspersky Endpoint Security naar een geautoriseerde gebruiker in de lijst met vertrouwde apparaten. Als het apparaat vertrouwd is, geeft Kaspersky Endpoint Security toegang tot het apparaat met alle machtigingen, zelfs als toegang tot het apparaattype of de verbindingbus wordt geweigerd. Als het apparaat niet vertrouwd is en de toegang wordt geweigerd, dan kunt u [toegang tot het vergrendelde apparaat aanvragen](#).


## Zo importeert en exporteert u de lijst met vertrouwde apparaten

Om de lijst met vertrouwde apparaten naar alle computers in uw organisatie te distribueren, kunt u de export-/importprocedure gebruiken.

Als u bijvoorbeeld een lijst met vertrouwde verwisselbare schijven wilt verspreiden, moet u het volgende doen:

1. Sluit achtereenvolgens verwisselbare schijven aan op uw computer.
2. Voeg in de instellingen van Kaspersky Endpoint Security [de verwisselbare schijven toe aan de vertrouwde lijst](#). Configureer indien nodig machtigingen voor gebruikerstoegang. Geef bijvoorbeeld alleen beheerders toegang tot verwisselbare schijven.
3. Exporteer de lijst met vertrouwde apparaten in de Kaspersky Endpoint Security-instellingen (zie onderstaande instructies).
4. Distribueer het bestand met de lijst met vertrouwde apparaten naar andere computers in uw organisatie. Plaats het bestand bijvoorbeeld in een gedeelde map.
5. Importeer de lijst met vertrouwde apparaten in de Kaspersky Endpoint Security-instellingen op andere computers in de organisatie (zie onderstaande instructies).

*Zo exporteert of importeert u de lijst met vertrouwde apparaten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.

3. In het blok **Toegangsinstellingen**, klikt u op de knop **Vertrouwde apparaten**.

Dit opent de lijst met vertrouwde apparaten.

4. Zo exporteert u de lijst met vertrouwde apparaten:

a. Selecteer de vertrouwde apparaten in de lijst die u wilt exporteren.

b. Klik op **Exporteren**.

c. Voer in het geopende venster de naam in van het XML-bestand waarnaar u de lijst met vertrouwde apparaten wilt exporteren, en selecteer de map waarin u dit bestand wilt opslaan.

d. Sla het bestand op.

Kaspersky Endpoint Security exporteert de volledige lijst met vertrouwde apparaten naar het XML-bestand.

5. Zo importeert u de lijst met vertrouwde apparaten:

a. In de vervolgkeuzelijst **Importeren** selecteert u de relevante actie: **Importeren en toevoegen aan bestaande** of **Importeren en bestaande vervangen**.

b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met vertrouwde apparaten wilt importeren.

c. Open het bestand.

Als de computer al een lijst met vertrouwde apparaten heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.

6. Sla uw wijzigingen op.

Wanneer een apparaat wordt aangesloten, controleert Kaspersky Endpoint Security naar een geautoriseerde gebruiker in de lijst met vertrouwde apparaten. Als het apparaat vertrouwd is, geeft Kaspersky Endpoint Security toegang tot het apparaat met alle machtigingen, zelfs als toegang tot het apparaattype of de verbindingbus wordt geweigerd.

## Toegang tot een geblokkeerd apparaat verkrijgen

Wanneer u Apparaatcontrole configureert, kunt u de toegang tot een apparaat voor uw werk per ongeluk blokkeren.

Als Kaspersky Security Center niet in uw bedrijf is geïmplementeerd, kunt u toegang tot een apparaat verlenen via de instellingen van Kaspersky Endpoint Security. U kunt bijvoorbeeld [het apparaat aan de lijst Vertrouwd toevoegen](#) of [Apparaatcontrole tijdelijk uitschakelen](#).

Als Kaspersky Security Center in uw bedrijf is geïmplementeerd en er is een beleid toegepast op de computers, kunt u toegang tot een apparaat verlenen via de Beheerconsole.

### Online modus voor het verlenen van toegang

U kunt alleen toegang verlenen tot een geblokkeerd apparaat in de online modus als Kaspersky Security Center in het bedrijf is geïmplementeerd en een beleid op de computer is toegepast. De computer moet verbinding kunnen maken met de Administration Server.

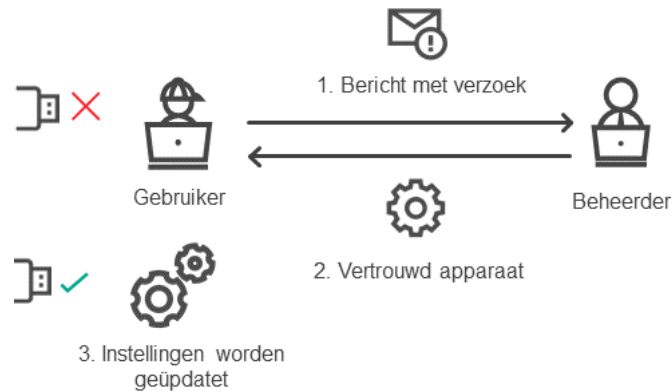
Met deze stappen kunt u toegang in de online modus verlenen:

1. De gebruiker stuurt de beheerder een bericht met een verzoek om toegang te krijgen.

2. De beheerder voegt het apparaat aan de lijst Vertrouwd toe.

U kunt een vertrouwd apparaat toevoegen in een beleid voor de beheergroep of in de lokale programma-instellingen voor een individuele computer.

3. De beheerder updatet de instellingen van Kaspersky Endpoint Security op de computer van de gebruiker.



Schema voor het verlenen van toegang tot een apparaat in de online modus

## Offline modus voor het verlenen van toegang

U kunt alleen toegang verlenen tot een geblokkeerd apparaat in de offline modus als Kaspersky Security Center in het bedrijf is geïmplementeerd en een beleid op de computer is toegepast. In het gedeelte **Apparaatcontrole** van de beleidsinstellingen moet het selectievakje **Allow requests for temporary access** ingeschakeld zijn.

Als u tijdelijke toegang tot een geblokkeerd apparaat moet verlenen maar het is niet mogelijk om [het apparaat aan de lijst Vertrouwd toe te voegen](#), kunt u toegang tot het apparaat in de offline modus verlenen. Op deze manier kunt u toegang tot een geblokkeerd apparaat verlenen, zelfs als de computer geen netwerktoegang heeft of als de computer zich niet in het bedrijfsnetwerk bevindt.

Met deze stappen kunt u toegang in de offline modus verlenen:

1. De gebruiker maakt een bestand met de toegangs aanvraag aan en verstuurt het naar de beheerder.

2. De beheerder maakt een toegangssleutel op basis van het bestand met de toegangs aanvraag en verstuurt deze sleutel naar de gebruiker.

3. De gebruiker activeert de toegangssleutel.



Schema voor het verlenen van toegang tot een apparaat in de offline modus

## Online modus voor het verlenen van toegang

U kunt alleen toegang verlenen tot een geblokkeerd apparaat in de online modus als Kaspersky Security Center in het bedrijf is geïmplementeerd en een beleid op de computer is toegepast. De computer moet verbinding kunnen maken met de Administration Server.

*Een gebruiker vraagt als volgt toegang tot een geblokkeerd apparaat:*

1. Sluit het apparaat aan op de computer.

Kaspersky Endpoint Security toont een melding met het bericht dat de toegang tot het apparaat wordt geblokkeerd (zie onderstaande afbeelding).

2. Klik op de koppeling **Toegang vragen**.

Dit opent een venster met een bericht voor de beheerder. Dit bericht bevat informatie over het geblokkeerde apparaat.

3. Klik op **Versturen**.

De beheerder ontvangt een bericht met een verzoek om toegang te verlengen, bijvoorbeeld per e-mail. Voor meer informatie over de verwerking van verzoeken van gebruikers raadpleegt u de [Help van Kaspersky Security Center](#). Na het [toevoegen van het apparaat aan de lijst Vertrouwd](#) en het updaten van de Kaspersky Endpoint Security-instellingen op de computer ontvangt de gebruiker toegang tot het apparaat.



Melding van Apparaatcontrole

## Offline modus voor het verlenen van toegang

U kunt alleen toegang verlenen tot een geblokkeerd apparaat in de offline modus als Kaspersky Security Center in het bedrijf is geïmplementeerd en een beleid op de computer is toegepast. In het gedeelte **Apparaatcontrole** van de beleidsinstellingen moet het selectievakje **Aanvraag voor tijdelijke toegang toestaan** ingeschakeld zijn.

*Een gebruiker vraagt als volgt toegang tot een geblokkeerd apparaat:*

1. Sluit het apparaat aan op de computer.  
Kaspersky Endpoint Security toont een melding met het bericht dat de toegang tot het apparaat wordt geblokkeerd (zie onderstaande afbeelding).
2. Klik op de koppeling **Tijdelijke toegang aanvragen**.  
Dit opent u een venster waarin u een lijst met aangesloten apparaten vindt.
3. Selecteer in de lijst met aangesloten apparaten het apparaat waartoe u toegang wilt krijgen.
4. Klik op **Bestand met toegangsaanvraag genereren**.
5. Geef in het veld **Duur van toegang** op hoelang u toegang tot het apparaat wilt hebben.
6. Sla het bestand op de computer op.

Een bestand met de toegangsaanvraag wordt naar de computer gedownload. Dit bestand heeft de extensie \*.akey. Gebruik een beschikbare methode om het bestand met de toegangsaanvraag te versturen naar de beheerder van het bedrijfsnetwerk.



Melding van Apparaatcontrole

[Hoe de beheerder een toegangssleutel kan maken voor het geblokkeerde apparaat in de Administration Console \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer in de lijst met clientcomputers de computer waarvan de gebruiker tijdelijke toegang tot een geblokkeerd apparaat moet krijgen.
5. Selecteer in het contextmenu van de computer het item **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster het tabblad **Apparaatcontrole**.
7. Klik op de knop **Bladeren** en download het bestand met de toegangsaanvraag dat u van de gebruiker hebt gekregen.  
U ziet informatie over het geblokkeerde apparaat waartoe de gebruiker toegang wilt.
8. Wijzig indien nodig de waarde van de instelling **Duur van toegang**.  
Standaard heeft de instelling **Duur van toegang** de waarde die de gebruiker heeft opgegeven wanneer deze het bestand met de toegangsaanvraag heeft gemaakt.
9. Geef de waarde van de instelling **Activeren voor** op.  
Deze instelling definieert de tijd die de gebruiker heeft om de toegang tot het geblokkeerde apparaat te activeren met de verstrekte toegangssleutel.
10. Sla het bestand met een toegangssleutel op de computer op.

[Hoe de beheerder een toegangssleutel kan maken voor het geblokkeerde apparaat in Web Console en Cloud Console](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer in de lijst met clientcomputers de computer waarvan de gebruiker tijdelijke toegang tot een geblokkeerd apparaat moet krijgen.
3. Klik op de ellipsisknop ( ) boven de lijst met computers en klik vervolgens op het **Grant access to the device in offline mode** knop.
4. Selecteer in het geopende venster het gedeelte **Device Control**.
5. Klik op de knop **Browse** en download het bestand met de toegangs aanvraag dat u van de gebruiker hebt gekregen.  
U ziet informatie over het geblokkeerde apparaat waartoe de gebruiker toegang wilt.
6. Wijzig indien nodig de waarde van de instelling **Access duration (hours)**.  
Standaard heeft de instelling **Access duration (hours)** de waarde die de gebruiker heeft opgegeven wanneer deze het bestand met de toegangs aanvraag heeft gemaakt.
7. Geef de tijdsperiode op waarin de toegangssleutel op het apparaat kan worden geactiveerd.  
Deze instelling definieert de tijd die de gebruiker heeft om de toegang tot het geblokkeerde apparaat te activeren met de verstrekte toegangssleutel.
8. Sla het bestand met een toegangssleutel op de computer op.

De toegangssleutel voor het geblokkeerde apparaat wordt nu naar de computer gedownload. Een bestand met een toegangssleutel heeft de extensie \*.acode. Gebruik een beschikbare methode om de toegangssleutel voor het geblokkeerde apparaat te versturen naar de gebruiker.

*Zo activeert de gebruiker de toegangssleutel:*

1. Klik in het [hoofdvenster van het programma](#) op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangs aanvraag**, klikt u op de knop **Toegang tot apparaat vragen**.
4. Klik in het venster op de knop **Toegangssleutel activeren**.
5. Selecteer in het venster dat opent het bestand met de apparaattoegangssleutel dat u van de beheerder van het bedrijfsnetwerk hebt ontvangen.  
U ziet nu een venster met informatie over de verstrekking van de toegang.
6. Klik op **OK**.

De gebruiker krijgt nu toegang tot het apparaat gedurende de periode die door de beheerder is ingesteld. De gebruiker ontvangt alle rechten voor de toegang tot het apparaat (lezen en schrijven). Wanneer de code verloopt, wordt de toegang tot het apparaat weer geblokkeerd. Als de gebruiker permanente toegang tot het apparaat nodig heeft, [voegt u het apparaat aan de lijst met vertrouwde apparaten toe](#).


## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. Configureer in het blok **Berichtsjablonen** de sjablonen voor berichten over apparaatcontrole:
  - **Bericht over blokkering** Sjabloon van het bericht dat verschijnt wanneer een geblokkeerd apparaat toegang tot een geblokkeerd apparaat probeert te krijgen. Dit bericht verschijnt ook wanneer een gebruiker een bewerking met inhoud op een apparaat probeert uit voeren wanneer die bewerking werd geblokkeerd voor die gebruiker.
  - **Bericht aan beheerder** Een sjabloon van het bericht dat naar de netwerkbeheerder wordt verstuurd als de gebruiker vindt dat de geblokkeerde toegang tot het apparaat of het verboden gebruik van de inhoud op het apparaat een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: **Bericht over blokkering van toegang tot apparaat aan beheerder**. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie **User requests**. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.
4. Sla uw wijzigingen op.

## Anti-Bridging

Anti-Bridging belet het maken van netwerkbruggen door het gelijktijdig maken van meerdere netwerkverbindingen op een computer te voorkomen. Hiermee kunt u een bedrijfsnetwerk beschermen tegen aanvallen via onbeveiligde, onbevoegde netwerken.

Anti-Bridging regelt het maken van netwerkverbindingen met behulp van *verbindingsregels*.

Voor de volgende vooraf gedefinieerde soorten apparaten worden verbindingsregels aangemaakt:

- Netwerkadapters;
- Wifi-adapters;
- Modems.


Als een verbindingsregel is ingeschakeld, doet Kaspersky Endpoint Security het volgende:

- De actieve verbinding wordt geblokkeerd bij het maken van een nieuwe verbinding als het opgegeven soort apparaat in de regel wordt gebruikt voor beide verbindingen;
- Verbindingen die worden gemaakt met de soorten apparaten waarvoor regels met een lagere prioriteit worden gebruikt, worden geblokkeerd.

## Anti-Bridging inschakelen

Anti-Bridging is standaard uitgeschakeld.

*Anti-Bridging inschakelen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Anti-Bridging**.
4. Gebruik de schakelaar **Anti-Bridging inschakelen** om deze functie in of uit te schakelen.
5. Sla uw wijzigingen op.

Nadat Anti-Bridging is ingeschakeld, blokkeert Kaspersky Endpoint Security al gemaakte verbindingen overeenkomstig de verbindingsregels.


## De status van een verbindingsregel wijzigen

*Zo wijzigt u de status van een verbindingsregel:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. In het blok **Toegangsinstellingen**, klikt u op de knop **Anti-Bridging**.
4. Selecteer in het blok **Regels voor apparaten** de regel waarvan u de status wilt wijzigen.
5. Gebruik de schakelaars in de kolom **Controleren** om de regel in of uit te schakelen.
6. Sla uw wijzigingen op.

## De prioriteit van een verbindingsregel wijzigen

*Zo wijzigt u de prioriteit van een verbindingsregel:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.

3. In het blok **Toegangsinstellingen**, klikt u op de knop **Anti-Bridging**.

4. Selecteer in het blok **Regels voor apparaten** de regel waarvan u de prioriteit wilt wijzigen.

5. Gebruik de knoppen **Omhoog** / **Omlaag** om de prioriteit van de verbindingsregel in te stellen.

Hoe hoger de regel in de tabel met regels staat, hoe hoger de prioriteit van de regel. Anti-Bridging blokkeert alle verbindingen behalve één verbinding die tot stand is gebracht met het type apparaat waarvoor de regel met de hoogste prioriteit wordt gebruikt.

6. Sla uw wijzigingen op.

## Adaptieve controle op afwijkingen

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

Het onderdeel Adaptieve controle op afwijkingen bewaakt en blokkeert acties die niet kenmerkend zijn voor de computers in het bedrijfsnetwerk. Adaptieve controle op afwijkingen gebruikt een aantal regels om afwijkend gedrag bij te houden (bijvoorbeeld de regel *Start van Windows PowerShell via Office-programma*). Regels worden door Kaspersky-experts gemaakt op basis van kenmerkende scenario's van malware-activiteit. U kunt configureren hoe Adaptieve controle op afwijkingen elke regel moet gebruiken en bijvoorbeeld toestaan dat PowerShell-scripts voor de automatisering van bepaalde workflows worden uitgevoerd. Kaspersky Endpoint Security updatet de reeks regels samen met de programmadatabases. Updates voor deze regels moeten [handmatig worden bevestigd](#).

### Instellingen van Adaptieve controle op afwijkingen

De configuratie van Adaptieve controle op afwijkingen bestaat uit de volgende stappen:

#### 1. Adaptieve controle op afwijkingen trainen.

Nadat u Adaptieve controle op afwijkingen hebt ingeschakeld, werken de regels ervan in de *trainingsmodus*. Tijdens de training bewaakt Adaptieve controle op afwijkingen de activering van regels en verstuurt het activeringsgebeurtenissen naar Kaspersky Security Center. Elke regel heeft een eigen trainingsduur. De duur van de trainingsmodus is door experts van Kaspersky vastgelegd. Normaal is de trainingsmodus twee weken actief.

Als een regel tijdens de training niet één keer is geactiveerd, zal Adaptieve controle op afwijkingen de acties die zijn gekoppeld aan deze regel als niet typisch beschouwen. Kaspersky Endpoint Security blokkeert dan alle acties die aan die regel zijn gekoppeld.

Als een regel tijdens de training is geactiveerd, registreert Kaspersky Endpoint Security gebeurtenissen in het [rapport over de activering van regels](#) en de opslagplaats **Triggering of rules in Smart Training state**.

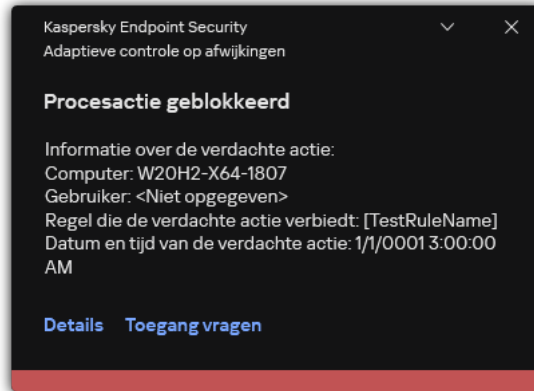
#### 2. Rapport over activering van regels analyseren.

De beheerder analyseert het [rapport over de activering van regels](#) of de inhoud van de opslagplaats **Triggering of rules in Smart Training state**. Daarna kan de beheerder het gedrag van Adaptieve controle op afwijkingen selecteren wanneer de regel wordt geactiveerd: blokkeren of toestaan. De beheerder kan ook verder bewaken hoe de regel werkt en de duur van de training verlengen. Als de beheerder geen actie onderneemt, blijft het programma ook werken in de trainingsmodus. De periode van de trainingsmodus wordt dan herstart.

Adaptieve controle op afwijkingen wordt in realtime geconfigureerd. Adaptieve controle op afwijkingen wordt via de volgende kanalen geconfigureerd:

- Adaptieve controle op afwijkingen begint automatisch de acties te blokkeren voor de regels die nooit zijn geactiveerd in de trainingsmodus.
- Kaspersky Endpoint Security voegt nieuwe regels toe of verwijdert oude regels.
- De beheerder configureert de werking van Adaptieve controle op afwijkingen na de controle van het rapport over de activering van regels en de inhoud van de opslagplaats **Triggering of rules in Smart Training state**. U wordt aanbevolen het rapport over de activering van regels en de inhoud van de opslagplaats **Triggering of rules in Smart Training state** te controleren.

Wanneer een schadelijk programma een actie probeert uit te voeren, blokkeert Kaspersky Endpoint Security de actie en toont het een melding (zie onderstaande afbeelding).



Melding van Adaptieve controle op afwijkingen

## Algoritme voor de werking van Adaptieve controle op afwijkingen

Op basis van het volgende algoritme (zie onderstaande afbeelding) beslist Kaspersky Endpoint Security of een actie van een regel al dan niet mag worden uitgevoerd.




Algoritme voor de werking van Adaptieve controle op afwijkingen

## Adaptieve controle op afwijkingen inschakelen en uitschakelen

Adaptieve controle op afwijkingen is standaard ingeschakeld.

Zo schakelt u Adaptieve controle op afwijkingen in of uit:


1. Klik in het [hoofdvenster van het programma](#) op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Adaptieve controle op afwijkingen** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan schakelt Adaptieve controle op afwijkingen over naar de trainingsmodus. Tijdens de training bewaakt Adaptieve controle op afwijkingen het activeren van regels. Wanneer de training voltooid is, begint Adaptieve Anomaly Control acties te blokkeren die niet typisch zijn voor de computers in het netwerk van een bedrijf.

Als uw organisatie een aantal nieuwe hulpprogramma's is gaan gebruiken en Adaptieve controle op afwijkingen de acties van die hulpprogramma's blokkeert, kunt u de resultaten van de trainingsmodus opnieuw instellen en de training herhalen. Om dit te doen moet u [de actie wijzigen die wordt uitgevoerd wanneer de regel wordt geactiveerd](#) (stel het bijvoorbeeld in op **Melden**). Vervolgens moet u de trainingsmodus opnieuw inschakelen (stel de waarde **Slim** in).


## Een regel van Adaptieve controle op afwijkingen inschakelen en uitschakelen

*Zo schakelt u een regel van Adaptieve controle op afwijkingen in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. In het blok **Regels**, klikt u op de knop **Regels bewerken**.  
Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend.
4. Selecteer in de tabel een set regels (bijvoorbeeld *Activiteit van Office-programma's*) en vouw de set uit.
5. Selecteer een regel (bijvoorbeeld *Start Windows PowerShell vanuit Office-programma's*).
6. Gebruik de schakelaar in de kolom **Status** om de regel voor Adaptieve controle op afwijkingen in of uit te schakelen.
7. Sla uw wijzigingen op.

## Actie bij de activering van een regel van Adaptieve controle op afwijkingen wijzigen

*Zo wijzigt u de actie die wordt uitgevoerd wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. In het blok **Regels**, klikt u op de knop **Regels bewerken**.  
Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend.
4. Selecteer een regel in de tabel.

5. Klik op **Bewerken**.

Het venster eigenschappen van Regel voor Adaptieve controle op afwijkingen wordt geopend.

6. Selecteer in het blok **Actie** een van de volgende opties:

- **Slim**. Als deze optie is geselecteerd, werkt een regel voor Adaptieve controle op afwijkingen in de Slimme training-modus gedurende de door de Kaspersky-experts ingestelde tijd. Wanneer in deze modus een regel voor Adaptieve controle op afwijkingen wordt geactiveerd, staat Kaspersky Endpoint Security de activiteit toe die in de regel is vastgelegd en registreert het informatie in de opslagplaats **Activering van regels in de Smart training-modus** van de Administration Server van Kaspersky Security Center. Wanneer de ingestelde tijdsperiode voor het werken in de Smart training-modus is afgelopen, blokkeert Kaspersky Endpoint Security de activiteit die in de regel voor Adaptieve controle op afwijkingen is vastgelegd en registreert het informatie over de activiteit.
- **Blokkeren**. Als deze actie is geselecteerd wanneer een regel voor Adaptieve controle op afwijkingen wordt geactiveerd, blokkeert Kaspersky Endpoint Security de activiteit die in de regel is vastgelegd en registreert het informatie over de activiteit.
- **Melden**. Als deze actie is geselecteerd wanneer een regel voor Adaptieve controle op afwijkingen wordt geactiveerd, staat Kaspersky Endpoint Security de activiteit toe die in de regel is vastgelegd en registreert het informatie over de activiteit.


7. Sla uw wijzigingen op.

## Een uitzondering maken voor een regel van Adaptieve controle op afwijkingen:

U kunt maximaal 1.000 uitzonderingen voor regels voor Adaptieve controle op afwijkingen maken. U wordt aanbevolen om maximaal 200 uitzonderingen te maken. Om het aantal gebruikte uitzonderingen zo laag mogelijk te houden, raden we u aan maskers in de instellingen van de uitzonderingen te gebruiken.

Een uitzondering voor een regel voor Adaptieve controle op afwijkingen bevat een beschrijving van de bron- en doelobjecten. Het *bronobject* is het object dat de acties uitvoert. Het *doelobject* is het object waarop de acties worden uitgevoerd. Voorbeeld: u hebt het bestand `bestand.xlsx` geopend. Door deze actie uit te voeren hebt u een bibliotheekbestand met een DLL-extensie in het geheugen van de computer geladen. Deze bibliotheek wordt gebruikt door een browser (uitvoerbaar bestand met de naam `browser.exe`). In dit voorbeeld is `bestand.xlsx` het bronobject, Excel het bronproces, `browser.exe` het doelobject en Browser het doelproces.

*Een uitzondering voor een regel van Adaptieve controle op afwijkingen aanmaken:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. In het blok **Regels**, klikt u op de knop **Regels bewerken**.  
Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend.
4. Selecteer een regel in de tabel.
5. Klik op **Bewerken**.

Het venster eigenschappen van Regel voor Adaptieve controle op afwijkingen wordt geopend.

6. Klik in het blok **Uitzonderingen** op de knop **Toevoegen**.

U ziet nu het venster met de eigenschappen van de uitzondering.

7. Selecteer de gebruiker waarvoor u een uitzondering wilt configureren.

Adaptieve controle op afwijkingen ondersteunt geen uitzonderingen voor gebruikersgroepen. Als u een gebruikersgroep selecteert, past Kaspersky Endpoint Security de uitsluiting niet toe.

8. Voer in het veld **Beschrijving** een beschrijving van de uitzondering in.

9. Definieer de instellingen van het bronobject of het bronproces dat door het object is gestart:

- **Bronproces.** Pad of masker van het pad naar het bestand of de map met bestanden (bijvoorbeeld `C:\Dir\Bestand.exe` of `Dir\*.exe`).
- **Hash van bronproces.** Hash-code van bestanden.
- **Bronobject.** Pad of masker van het pad naar het bestand of de map met bestanden (bijvoorbeeld `C:\Dir\Bestand.exe` of `Dir\*.exe`). Voorbeeld: het bestandspad `document.docm` dat een script of macro gebruikt om de doelprocessen te starten.  
U kunt ook andere objecten opgeven die u wilt uitsluiten, zoals een webadres, macro, opdracht in de opdrachtregel, registerpad, enzovoort. Geef het object op met behulp van de volgende sjabloon:  
`object://<object>`, waarbij `<object>` verwijst naar de naam van het object. Enkele voorbeelden:  
`object://web.site.voorbeeld.nl`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. U kunt ook maskers gebruiken, zoals `object://*C:\Windows\temp\*`.
- **Hash van bronobject.** Hash-code van bestanden.

De regel voor Adaptieve controle op afwijkingen wordt niet toegepast op acties die door het object worden uitgevoerd of op processen die door het object worden gestart.

10. Definieer de instellingen van het doelobject of de doelprocessen die door het object zijn gestart.

- **Doelproces.** Pad of masker van het pad naar het bestand of de map met bestanden (bijvoorbeeld `C:\Dir\Bestand.exe` of `Dir\*.exe`).
- **Hash van doelproces.** Hash-code van bestanden.
- **Doelobject.** De opdracht om het doelproces te starten. Geef de opdracht op in de volgende structuur:  
`object://<opdracht>`. Voorbeeld: `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage txt' "`. U kunt ook maskers gebruiken, zoals `object://*C:\Windows\temp\*`.
- **Hash van doelobject.** Hash-code van bestanden.


De regel voor Adaptieve controle op afwijkingen wordt niet toegepast op acties die worden uitgevoerd op het object of op processen die door het object zijn gestart.

11. Sla uw wijzigingen op.



## Uitzonderingen voor regels van Adaptieve controle op afwijkingen exporteren en importeren:

*De lijst met uitzonderingen voor geselecteerde regels exporteren of importeren:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. In het blok **Regels**, klikt u op de knop **Regels bewerken**.  
Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend.
4. De lijst met regels exporteren:
  - a. De regels selecteren waarvan u de uitzonderingen wilt exporteren.
  - b. Klik op **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Bevestig dat u alleen de geselecteerde uitzonderingen wilt exporteren of de volledige lijst met uitzonderingen wilt exporteren.
  - e. Sla het bestand op.
5. De lijst met regels importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wil importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
6. Sla uw wijzigingen op.

## Updates voor regels van Adaptieve controle op afwijkingen toepassen

Nieuwe regels van Adaptieve controle op afwijkingen kunnen aan de tabel met regels worden toegevoegd en bestaande regels van Adaptieve controle op afwijkingen kunnen uit de tabel met regels worden verwijderd wanneer de antivirusdatabases worden bijgewerkt. Kaspersky Endpoint Security onderscheidt regels van Adaptieve controle op afwijkingen die moeten worden verwijderd uit of toegevoegd aan de tabel als een update voor deze regels niet is toegepast.

Pas wanneer de update wordt toegepast, toont Kaspersky Endpoint Security de regels voor Adaptieve controle op afwijkingen die worden verwijderd door de update in de tabel met regels en wijst het de status *Uitgeschakeld* aan deze regels toe. Het is niet mogelijk om de instellingen van deze regels te wijzigen.

*Zo past u updates voor regels van Adaptieve controle op afwijkingen toe:*


1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. In het blok **Regels**, klikt u op de knop **Regels bewerken**.  
Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend.
4. Klik in het venster op de knop **Updates goedkeuren**.  
De knop **Updates goedkeuren** is beschikbaar wanneer een update voor de regels van Adaptieve controle op afwijkingen beschikbaar is.
5. Sla uw wijzigingen op.

## Berichtsjablonen van Adaptieve controle op afwijkingen bewerken

Wanneer een gebruiker een actie probeert uit te voeren die door regels van Adaptieve controle op afwijkingen wordt geblokkeerd, toont Kaspersky Endpoint Security een bericht dat mogelijk schadelijke acties zijn geblokkeerd. Als de gebruiker vindt dat een actie 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 berichten over de blokkering van mogelijk schadelijke acties en voor berichten die naar de beheerder worden verstuurd. U kunt de berichtsjablonen wijzigen.

*Zo bewerkt u een berichtsjabloon:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het venster met de programma-instellingen.
3. Configureer in het blok **Sjablonen** de sjablonen voor berichten over Adaptieve controle op afwijkingen.
  - **Bericht over blokkering** Sjabloon van het bericht dat wordt weergegeven aan een gebruiker wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd voor de blokkering van een afwijkende actie.
  - **Bericht aan beheerder** Sjabloon van het bericht dat een gebruiker kan versturen naar de beheerder van het lokale bedrijfsnetwerk als de gebruiker vindt dat de blokkering een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: **Bericht over blokkering van programma-activiteit aan beheerder**. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie **User requests**. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.
4. Sla uw wijzigingen op.

# Rapporten van Adaptieve controle op afwijkingen bekijken

Zo bekijkt u rapporten van Adaptieve controle op afwijkingen:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het beleidsvenster.  
De instellingen van het onderdeel Adaptieve controle op afwijkingen ziet u rechts in het venster.
6. Doe een van de volgende acties:
  - Klik op **Rapport over de status van de regels van Adaptieve controle op afwijkingen** als u een rapport over de instellingen van de regels van Adaptieve controle op afwijkingen wilt bekijken.
  - Klik op **Rapport over geactiveerde regels van Adaptieve controle op afwijkingen** als u een rapport over de activering van de regels van Adaptieve controle op afwijkingen wilt bekijken.
7. Het rapport wordt gemaakt.

Het rapport wordt in een nieuw venster weergegeven.

## Programmacontrole

Programmacontrole beheert het opstarten van applicaties op de computers van gebruikers. Hiermee kunt u een bedrijfsbeveiligingsbeleid implementeren bij het gebruik van programma's. Programmacontrole vermindert ook het risico op computerinfectie door de toegang tot programma's te beperken.

De configuratie van programmacontrole bestaat uit de volgende stappen:

### 1. [Categorieën van programma's aanmaken](#).

De beheerder maakt categorieën applicaties die de beheerder wil beheren. Programmacategorieën zijn bedoeld voor alle computers in het bedrijfsnetwerk, ongeacht de beheergroepen. Om een categorie aan te maken, kunt u de volgende criteria gebruiken: KL-categorie (bijvoorbeeld, *Browsers*), bestandshash, programmaverkoper en andere criteria.

### 2. [Regels van programmacontrole maken](#).

De beheerder maakt regels van programmacontrole in het beleid voor de beheergroep. De regel omvat de categorieën van programma's en de opstartstatus van programma's uit deze categorieën: geblokkeerd of toegestaan.

### 3. [De modus van Programmacontrole selecteren](#).

De beheerder kiest de modus voor het werken met programma's die niet zijn opgenomen in een van de regels (programma denylist en allowlist).

Wanneer een gebruiker probeert een verboden programma te starten, blokkeert Kaspersky Endpoint Security het starten van het programma en wordt er een melding weergegeven (zie de onderstaande afbeelding).

Er is een *testmodus* beschikbaar om de configuratie van programmacontrole te controleren. In deze modus doet Kaspersky Endpoint Security het volgende:

- Staat het opstarten van programma's toe, inclusief verboden programma's.
- Geeft een melding weer over het opstarten van een verboden programma en voegt informatie toe aan het rapport op de computer van de gebruiker.
- Stuurt gegevens over het opstarten van verboden programma's naar Kaspersky Security Center.



Melding van programmacontrole

## Over de uitvoermodi van programmacontrole

Het onderdeel Programmacontrole werkt in twee modi:

- **Denylist.** In deze modus staat programmacontrole toe dat alle gebruikers alle programma's starten, behalve de programma's die verboden zijn in programmacontrole. Deze modus van Programmacontrole is standaard ingeschakeld.

- **Allowlist.** In deze modus staat Programmacontrole niet toe dat de gebruikers alle programma's starten, behalve de programma's die toegestaan zijn en niet verboden zijn in de regels van Programmacontrole.

Als de Toestaan-regels van Programmacontrole 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.

U kunt de [aanbevelingen voor de configuratie van regels voor programmacontrole in de modus allowlist](#) lezen.

De werking van Programmacontrole 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.](#)

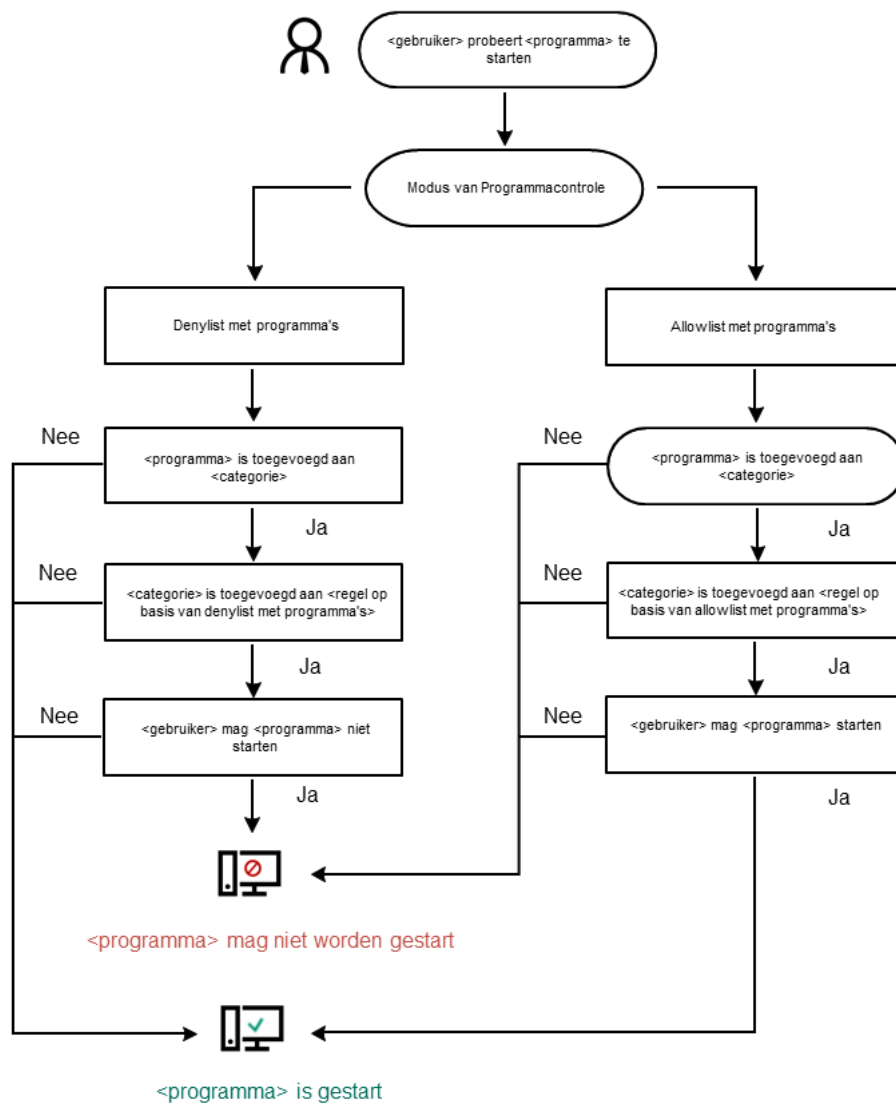
De regels van Programmacontrole die worden aangemaakt in de Beheerconsole van Kaspersky Security Center zijn gebaseerd op aangepaste categorieën van programma's en niet op uitvoerings- of uitzonderingsvoorwaarden zoals in de lokale interface van Kaspersky Endpoint Security.

- [Informatie over geïnstalleerde programma's op netwerkcomputers ontvangen.](#)

Dit is de reden waarom u wordt aanbevolen om Kaspersky Security Center te gebruiken voor de configuratie van de werking van het onderdeel Programmacontrole.

### Algoritme voor werking van programmacontrole

Kaspersky Endpoint Security gebruikt een algoritme om een beslissing te nemen over het starten van een programma (zie onderstaande afbeelding).



Algoritme voor werking van programmacontrole

### Beperkingen van de functionaliteit van Programmacontrole

In de volgende gevallen is de werking van het onderdeel Programmacontrole beperkt:

- Wanneer de versie van het programma wordt geüpgraded, wordt de import van de instellingen van het onderdeel Programmacontrole niet ondersteund.
- Wanneer een upgrade van de programmaversie wordt uitgevoerd, wordt de import van de instellingen van het onderdeel Programmacontrole alleen ondersteund als Kaspersky Endpoint Security 10 Service Pack 2 voor Windows of hoger wordt geüpgraded naar Kaspersky Endpoint Security 11.9.0 voor Windows.

Wanneer andere programmaversies dan Kaspersky Endpoint Security 10 Service Pack 2 voor Windows worden geüpgraded, moeten de instellingen van Programmacontrole opnieuw worden geconfigureerd om de werking van dit onderdeel te herstellen.

- Zonder verbinding met KSN-servers krijgt Kaspersky Endpoint Security alleen van de lokale databases informatie over de reputatie van programma's en hun modules.

De lijst met programma's die Kaspersky Endpoint Security benoemt als KL-categorie **Overige programma's \ Programma's, vertrouwd op basis van hun reputatie in KSN** kan verschillen afhankelijk van een eventuele verbinding met de KSN-servers.

- 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 Programmacontrole, blokkeert het onderdeel de opstart van een script vanaf deze interpreter niet.

Als ten minste één van de opgegeven scripts niet via de opdrachtregel voor de interpreter kan worden gestart wegens de regels van Programmacontrole, blokkeert het onderdeel alle scripts die op de opdrachtregel voor de interpreter worden opgegeven.

- 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:

- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;

- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

## Programmacontrole inschakelen en uitschakelen

Programmacontrole is standaard ingeschakeld.

*Zo schakelt u Programmacontrole in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Programmacontrole** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Als gevolg hiervan, als Programmacontrole is ingeschakeld, stuurt het programma informatie over het uitvoeren van uitvoerbare bestanden naar Kaspersky Security Center. U kunt de lijst met actieve uitvoerbare bestanden bekijken in Kaspersky Security Center in de map **Uitvoerbare bestanden**. Om informatie over alle uitvoerbare bestanden te ontvangen in plaats van alleen uitvoerbare bestanden uit te voeren, voert u de [Inventarisatie taak uit](#).

## De modus van Programmacontrole selecteren

Zo selecteert u de modus van Programmacontrole:

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Kies in het gedeelte **Modus van Controle van programma-opstart** een van de volgende opties:
  - **Denylist**. Als deze optie is geselecteerd, staat Programmacontrole toe dat alle gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de blokkeringsregels van Programmacontrole is voldaan.
  - **Allowlist**. Als deze optie is geselecteerd, staat Programmacontrole niet toe dat gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de uitvoeringsregels van Programmacontrole is voldaan.

De **Golden Image**-regel en de **Vertrouwde updaters**-regel zijn aanvankelijk gedefinieerd voor de Allowlist-modus. Deze Application Control-regels komen overeen met KL-categorieën. De KL-categorie 'Golden Image' bevat programma's die de normale werking van het besturingssysteem verzekeren. De KL-categorie 'Vertrouwde updaters' bevat updaters voor de meest bekende softwareleveranciers. U kunt deze regels niet verwijderen. De instellingen van deze regels kunnen niet worden bewerkt. Standaard is de **Golden Image**-regel ingeschakeld en is de **Vertrouwde updaters**-regel 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 weer te gaan gebruiken, hoeft u alleen maar de benodigde modus te selecteren.

4. Selecteer in het blok **Actie bij starten van geblokkeerde programma's** de actie die door het onderdeel moet worden uitgevoerd wanneer een gebruiker een programma probeert te starten dat door de regels van programmacontrole is geblokkeerd.

5. Schakel het selectievakje **Laden van DLL-modules controleren** in als u wilt dat Kaspersky Endpoint Security het laden van DLL-modules bewaakt wanneer programma's worden gestart door gebruikers.

Informatie over de module en het programma dat de module heeft geladen wordt in een rapport opgeslagen.

Kaspersky Endpoint Security bewaakt alleen DLL-modules en stuurprogramma's die zijn geladen nadat het selectievakje werd ingeschakeld. Start de computer opnieuw op nadat u het selectievakje hebt ingeschakeld als u wilt dat Kaspersky Endpoint Security alle DLL-modules en stuurprogramma's bewaakt, inclusief deze die worden geladen voordat Kaspersky Endpoint Security wordt gestart.

Wanneer u de controle over het laden van DLL-modules en stuurprogramma's inschakelt, moet u in de instellingen van programmacontrole controleren of een van de volgende regels is ingeschakeld: de standaard **Golden Image**-regel of een andere regel die de KI-categorie "Vertrouwde certificaten" bevat en ervoor zorgt dat vertrouwde DLL-modules en stuurprogramma's worden geladen voordat Kaspersky Endpoint Security wordt gestart. Als u de controle van het laden van DLL-modules en stuurprogramma's inschakelt wanneer de regel **Golden Image** is uitgeschakeld, kan het besturingssysteem instabiel worden.



We raden aan dat u de [wachtwoordbeveiliging](#) voor de configuratie van programma-instellingen inschakelt zodat u de regels die essentiële DLL-modules en stuurprogramma's vanaf het begin blokkeren kunt uitschakelen, zonder de instellingen van het Kaspersky Security Center-beleid te wijzigen.

6. Sla uw wijzigingen op.

## Werken met regels van programmacontrole in de applicatie-interface

Kaspersky Endpoint Security gebruikt regels om de start van programma's door gebruikers te controleren. Een regel van programmacontrole bevat de activeringsvoorwaarden en de actie die door programmacontrole wordt uitgevoerd wanneer de regel wordt geactiveerd (de start van het programma door gebruikers wordt toegestaan of geblokkeerd).

### Voorwaarden voor activering van regel

Een regel-activerende voorwaarde heeft de volgende correlatie: "voorwaarde type - criterium - waarde". Op basis van de voorwaarden voor de activering van de regel past Kaspersky Endpoint Security (al dan niet) een regel op een programma toe.

In regels worden de volgende soorten voorwaarden gebruikt:

- *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 activering 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 Programmacontrole 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 Programmacontrole.

Als u een certificaat hebt geselecteerd als een regel-triggerende voorwaarde, moet u ervoor zorgen dat dit certificaat wordt toegevoegd aan de vertrouwde systeemopslag op de computer, en controleer de [vertrouwde systeemopslaggebruikersinstellingen in het programma](#).

## Beslissingen van het onderdeel Programmacontrole bij de activering van een regel

Wanneer een regel wordt geactiveerd, worden gebruikers (of groepen gebruikers) door Programmacontrole toegestaan om programma's te starten of wordt de start van die programma's geblokkeerd volgens de regel. U kunt individuele gebruikers of groepen 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 Programmacontrole is toegewezen aan een gebruikersgroep terwijl een Blokkeren-regel van Programmacontrole is toegewezen aan één gebruiker in deze gebruikersgroep, kan deze gebruiker het programma niet starten.

## Status van werking van regel

Regels voor programmacontrole kunnen de volgende status hebben:

- **Ingeschakeld.** Deze status geeft aan dat de regel wordt gebruikt als het onderdeel Programmacontrole actief is.
- **Uitgeschakeld.** Deze status geeft aan dat de regel wordt genegeerd als het onderdeel Programmacontrole actief is.
- **Testen.** Deze status geeft aan dat Kaspersky Endpoint Security de opstart van programma's toestaat waarop de regels van toepassing zijn maar informatie over de opstart van zulke programma's in het rapport registreert.

## Een regel van programmacontrole toevoegen

*Een regel van Programmacontrole toevoegen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Klik op de knop **Geblokkeerde programma's** of **Toegestane programma's**.  
Hiermee wordt de lijst met regels van programmacontrole geopend.
4. Klik op **Toevoegen**.  
U ziet nu het venster Regel van Programmacontrole.

5. Definieer op het tabblad **Algemene instellingen** de belangrijkste instellingen van de regel:

- a. Typ in het veld **Regelnaam** de naam van de regel.
- b. Voer in het veld **Beschrijving** een beschrijving van de regel in.
- c. Maak of bewerk een lijst met gebruikers en/of groepen 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 **Houders en hun rechten**.

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.

- d. Gebruik in de tabel **Houders en hun rechten** de schakelaar om het recht in te stellen van gebruikers om programma's te starten.
- e. Selecteer het vakje **Weigeren voor andere gebruikers** als u wilt dat de toepassing voorkomt dat programma's die voldoen aan de voorwaarden voor het activeren van regels worden uitgevoerd voor alle gebruikers die niet vermeld staan in de lijst **Houders en hun rechten** en die geen lid zijn van gebruikersgroepen vermeld in de tabel **Houders en hun rechten**.

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 **Houders en hun rechten** en die niet behoren tot opgegeven groepen gebruikers in de tabel **Houders en hun rechten**.

- f. Selecteer het vakje **Vertrouwde updaters** als u wenst dat Kaspersky Endpoint Security programma's die voldoen aan de triggervoorwaarden van de regel beschouwt als vertrouwde updaters. *Vertrouwde updaters* zijn programma's die andere uitvoerbare bestanden mogen maken die daarna mogen worden uitgevoerd.

Als een programma meerdere regels activeert, stelt Kaspersky Endpoint Security de optie "Vertrouwde updaters" in als aan de volgende voorwaarden is voldaan:

- Alle regels staan het uitvoeren van het programma toe.
- Minstens een regel heeft het selectievakje **Vertrouwde updaters** ingeschakeld.

6. [Maak](#) of bewerk op het tabblad **Voorwaarden** de lijst met inclusievoorwaarden voor activering van de regel.


7. Maak of bewerk op het tabblad **Uitzonderingen** de lijst met exclusievoorwaarden voor activering van de regel.

Wanneer de instellingen van Kaspersky Endpoint Security worden gemigreerd, wordt de lijst met uitvoerbare bestanden die wordt gemaakt door vertrouwde updaters ook gemigreerd.

8. Sla uw wijzigingen op.

## Een activeringsvoorwaarde voor een regel van Programmacontrole toevoegen

*Zo voegt u een nieuwe activeringsvoorwaarde voor een regel van Programmacontrole toe:*

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

2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.

3. Klik op de knop **Geblokkeerde programma's** of **Toegestane programma's**.

Hiermee wordt de lijst met regels van programmacontrole geopend.

4. Selecteer de regel waarvoor u een activeringsvoorwaarde wilt configureren.

De eigenschappen van de regel van programmacontrole wordt geopend.

5. Selecteer het tabblad **Voorwaarden** of **Uitzonderingen** en klik op de knop **Toevoegen**.

6. Selecteer de activeringsvoorwaarden voor een regel van programmacontrole toevoegen:

- **Voorwaarden uit eigenschappen van gestarte programma's.** In de lijst met actieve applicaties kunt u de applicaties selecteren waarop de regel van programmacontrole wordt toegepast. Kaspersky Endpoint Security vermeldt ook de programma's die eerder op de computer werden uitgevoerd. U moet het criterium selecteren dat u wilt gebruiken om eenof meer activeringsvoorwaarden voor de regel te maken: **Bestandshash, Certificaat, KL-categorie, Metagegevens** of **Pad naar bestand of map**.
- **Voorwaarden "KL-categorie".** Een *KL-categorie* is een lijst met programma's die dezelfde themakenmerken hebben. De lijst wordt door experts van Kaspersky geüpdatet. De KL-categorie 'Office-programma's' bevat bijvoorbeeld programma's uit de Microsoft Office-suite, Adobe® Acrobat® en andere.
- **Aangepaste voorwaarde.** U kunt het programmabestand selecteren en een van de activeringsvoorwaarden voor de regel selecteren: **Bestandshash, Certificaat, Metagegevens** of **Pad naar bestand of map**.
- **Voorwaarde op basis van station (verwisselbare schijf).** De regel van programmacontrole wordt alleen toegepast op bestanden die op een verwisselbare schijf worden uitgevoerd.
- **Voorwaarden uit eigenschappen van bestanden in de opgegeven map.** De regel van Programmacontrole wordt alleen toegepast op bestanden die zich in de opgegeven map bevinden. U kunt ook bestanden opnemen in of uitsluiten van submappen. U moet het criterium selecteren dat u wilt gebruiken om eenof meer activeringsvoorwaarden voor de regel te maken: **Bestandshash, Certificaat, KL-categorie, Metagegevens** of **Pad naar bestand of map**.


7. Sla uw wijzigingen op.

Houd bij het toevoegen van voorwaarden rekening met de volgende speciale overwegingen voor programmacontrole:

- Kaspersky Endpoint Security ondersteunt geen MD5 hash 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.
- U wordt afgeraden om alleen de criteria **Verlener** en **Houder** als activeringsvoorwaarden voor regels te gebruiken. Het gebruik van deze criteria is onbetrouwbaar.
- Als u een symbolische koppeling in het veld **Pad naar bestand of map** gebruikt, doet u er goed aan de symbolische koppeling om te zetten opdat de regel van Programmacontrole correct zou werken. Klik hiertoe op de knop **Symbolische koppeling omzetten**.

## De status van een regel van Programmacontrole wijzigen

*Zo wijzigt u de status van een regel van Programmacontrole:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Klik op de knop **Geblokkeerde programma's** of **Toegestane programma's** .  
Hiermee wordt de lijst met regels van programmacontrole geopend.
4. Klik met de rechtermuisknop in de kolom **Status** om het contextmenu weer te geven en selecteer een van de volgende opties:
  - **Ingeschakeld.** Deze status geeft aan dat de regel wordt gebruikt als het onderdeel Programmacontrole actief is.
  - **Uitgeschakeld.** Deze status geeft aan dat de regel wordt genegeerd als het onderdeel Programmacontrole actief is.
  - **Testen.** Deze status geeft aan dat Kaspersky Endpoint Security altijd de opstart van programma's toestaat waarop deze regel van toepassing is maar informatie over de opstart van zulke programma's in het rapport registreert.
5. Sla uw wijzigingen op.

## Regels van programmacontrole beheren in Kaspersky Security Center

Kaspersky Endpoint Security gebruikt regels om de start van programma's door gebruikers te controleren. Een regel van programmacontrole bevat de activeringsvoorwaarden en de actie die door programmacontrole wordt uitgevoerd wanneer de regel wordt geactiveerd (de start van het programma door gebruikers wordt toegestaan of geblokkeerd).

### Voorwaarden voor activering van regel

Een regel-activerende voorwaarde heeft de volgende correlatie: "voorwaarde type - criterium - waarde". Op basis van de voorwaarden voor de activering van de regel past Kaspersky Endpoint Security (al dan niet) een regel op een programma toe.

In regels worden de volgende soorten voorwaarden gebruikt:

- *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 activering 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 Programmacontrole 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 Programmacontrole.

Als u een certificaat hebt geselecteerd als een regel-triggerende voorwaarde, moet u ervoor zorgen dat dit certificaat wordt toegevoegd aan de vertrouwde systeemopslag op de computer, en controleer de [vertrouwde systeemopslaggebruiksinstellingen in het programma](#).

## Beslissingen van het onderdeel Programmacontrole bij de activering van een regel

Wanneer een regel wordt geactiveerd, worden gebruikers (of groepen gebruikers) door Programmacontrole toegestaan om programma's te starten of wordt de start van die programma's geblokkeerd volgens de regel. U kunt individuele gebruikers of groepen 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 Programmacontrole is toegewezen aan een gebruikersgroep terwijl een Blokkeren-regel van Programmacontrole is toegewezen aan één gebruiker in deze gebruikersgroep, kan deze gebruiker het programma niet starten.

## Status van werking van regel

Regels voor programmacontrole kunnen de volgende status hebben:

- **Ingeschakeld.** Deze status geeft aan dat de regel wordt gebruikt als het onderdeel Programmacontrole actief is.
- **Uitgeschakeld.** Deze status geeft aan dat de regel wordt genegeerd als het onderdeel Programmacontrole actief is.
- **Testen.** Deze status geeft aan dat Kaspersky Endpoint Security de opstart van programma's toestaat waarop de regels van toepassing zijn maar informatie over de opstart van zulke programma's in het rapport registreert.

## Informatie over geïnstalleerde programma's op computers van gebruikers ontvangen

Om optimale regels van Programmacontrole aan te maken, moet u eerst weten welke programma's op de computers in het bedrijfsnetwerk 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 **Applications registry** en **Executable files**. De map **programmaregister** en **Uitvoerbare bestanden** bevinden zich in de map **Programmabeheer** in de structuur van de Kaspersky Security Center Administration Console.

De map **Applications registry** bevat de lijst met programma's die zijn gevonden door [Netwerkagent](#) dat op de clientcomputer is geïnstalleerd.

De map **Executable files** 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 **Applications registry** of **Executable files**.

*Het venster openen met eigenschappen van programma's in de map Applications registry:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Additional** → **Application management** → **Applications registry**.
3. Selecteer een programma.
4. Selecteer in het contextmenu van het programma de optie **Properties**.

*Zo opent u het venster met eigenschappen voor een uitvoerbaar bestand in de map Executable files:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Additional** → **Application management** → **Executable files**.
3. Selecteer een uitvoerbaar bestand.
4. Selecteer in het contextmenu van het uitvoerbare bestand de optie **Properties**.

## Programmacategorieën aanmaken

Voor meer gebruiksgemak tijdens het maken van regels van Programmacontrole kunt u programmacategorieën aanmaken.

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 Beheerconsole de map **Extra** → **Programmabeheer** → **Programmacategorieën**.
3. Klik op de knop **New category** 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.

### Stap 1. Een soort categorie selecteren

Tijdens deze stap selecteert u een van de volgende soorten programmacategorieën:

- **Category with content added manually.** Als u deze soort categorie hebt geselecteerd, kunt u tijdens de stappen 'Voorwaarden configureren om programma's toe te voegen aan een categorie' en 'Voorwaarden configureren om programma's uit te sluiten van een categorie' de criteria bepalen waarbij uitvoerbare bestanden worden toegevoegd aan de categorie.
- **Category that includes executable files from selected devices.** Als u deze soort categorie hebt geselecteerd, kunt u tijdens de stap "Instellingen" een computer opgeven waarvan de uitvoerbare bestanden moeten worden toegevoegd aan de categorie.
- **Category that includes executable files from a specific folder.** Als u deze soort categorie hebt geselecteerd, kunt u tijdens de stap 'Opslagmap' een map opgeven waarvan de uitvoerbare bestanden automatisch worden toegevoegd aan de categorie.

Wanneer u een categorie met automatisch toegevoegde inhoud maakt, inventariseert Kaspersky Security Center de bestanden met de volgende indelingen: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX en SCR.

### Stap 2. Een aangepaste categorienaam invoeren

Tijdens deze stap geeft u een naam voor de programmacategorie op.

### Stap 3. Voorwaarden configureren om programma's toe te voegen aan een categorie



Deze stap is beschikbaar als u **Category with content added manually** als soort categorie hebt geselecteerd.

Tijdens deze stap selecteert u in de vervolgkeuzelijst **Add** een van de volgende voorwaarden voor het opnemen van programma's in de categorie:

- **From the list of executable files.** Voeg programma's uit de lijst met uitvoerbare bestanden op het clientapparaat toe aan de aangepaste categorie.
- **From file properties.** Geef gedetailleerde gegevens van uitvoerbare bestanden op als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Metadata from files in folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat. Kaspersky Security Center geeft de metagegevens van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Checksums of the files in the folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat. Kaspersky Security Center geeft de hashes van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Certificates for the files from the folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat die met certificaten ondertekend zijn. Kaspersky Security Center geeft de certificaten van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.

Als de parameter **Certificate thumbprint** niet is opgegeven in de eigenschappen van de voorwaarden, wordt u aanbevolen deze voorwaarden niet te gebruiken.

- **MSI installer files metadata.** Selecteer het MSI-pakket. Kaspersky Security Center geeft de metagegevens van uitvoerbare bestanden in dit MSI-pakket aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Checksums of the files from the MSI installer of the application.** Selecteer het MSI-pakket. Kaspersky Security Center geeft de hashes van uitvoerbare bestanden in dit MSI-pakket aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **From KL category.** Geef een KL-categorie op als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie. Een *KL-categorie* is een lijst met programma's die dezelfde themakenmerken hebben. De lijst wordt door experts van Kaspersky geüpdatet. De KL-categorie 'Office-programma's' bevat bijvoorbeeld programma's uit de Microsoft Office-suite, Adobe Acrobat en andere.

U kunt alle KL-categorieën selecteren om een uitgebreide lijst met vertrouwde programma's te genereren.

- **Specify path to application.** Selecteer een map op het clientapparaat. Kaspersky Security Center voegt de uitvoerbare bestanden in deze map toe aan de aangepaste categorie.
- **Select certificate from repository.** Selecteer certificaten die zijn gebruikt om uitvoerbare bestanden te ondertekenen als voorwaarde om programma's aan de aangepaste categorie toe te voegen.

Als de parameter **Certificate thumbprint** niet is opgegeven in de eigenschappen van de voorwaarden, wordt u aanbevolen deze voorwaarden niet te gebruiken.

- **Drive type.** Selecteer het type opslagapparaat (alle harde schijven en verwisselbare schijven, of alleen verwisselbare schijven) als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.

## Stap 4. Voorwaarden configureren om programma's uit te sluiten van een categorie

Deze stap is beschikbaar als u **Category with content added manually** als soort categorie hebt geselecteerd.

Programma's die tijdens deze stap worden opgegeven, worden uitgesloten van de categorie zelfs als deze programma's tijdens de stap 'Voorwaarden configureren om programma's toe te voegen aan een categorie' werden opgegeven.

Tijdens deze stap selecteert u in de vervolgkeuzelijst **Add** een van de volgende voorwaarden die als basis worden gebruikt om programma's uit te sluiten van de categorie:

- **From the list of executable files.** Voeg programma's uit de lijst met uitvoerbare bestanden op het clientapparaat toe aan de aangepaste categorie.
- **From file properties.** Geef gedetailleerde gegevens van uitvoerbare bestanden op als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Metadata from files in folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat. Kaspersky Security Center geeft de metagegevens van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Checksums of the files in the folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat. Kaspersky Security Center geeft de hashes van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Certificates for the files from the folder.** Selecteer een map op het clientapparaat dat uitvoerbare bestanden bevat die met certificaten ondertekend zijn. Kaspersky Security Center geeft de certificaten van deze uitvoerbare bestanden aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **MSI installer files metadata.** Selecteer het MSI-pakket. Kaspersky Security Center geeft de metagegevens van uitvoerbare bestanden in dit MSI-pakket aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **Checksums of the files from the MSI installer of the application.** Selecteer het MSI-pakket. Kaspersky Security Center geeft de hashes van uitvoerbare bestanden in dit MSI-pakket aan als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.
- **From KL category.** Geef een KL-categorie op als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie. Een *KL-categorie* is een lijst met programma's die dezelfde themakenmerken hebben. De lijst wordt door experts van Kaspersky geüpdatet. De KL-categorie 'Office-programma's' bevat bijvoorbeeld programma's uit de Microsoft Office-suite, Adobe Acrobat en andere.  
U kunt alle KL-categorieën selecteren om een uitgebreide lijst met vertrouwde programma's te genereren.
- **Specify path to application.** Selecteer een map op het clientapparaat. Kaspersky Security Center voegt de uitvoerbare bestanden in deze map toe aan de aangepaste categorie.
- **Select certificate from repository.** Selecteer certificaten die zijn gebruikt om uitvoerbare bestanden te ondertekenen als voorwaarde om programma's aan de aangepaste categorie toe te voegen.
- **Drive type.** Selecteer het type opslagapparaat (alle harde schijven en verwisselbare schijven, of alleen verwisselbare schijven) als een voorwaarde voor het toevoegen van programma's aan de aangepaste categorie.

## Stap 5. Instellingen

Deze stap is beschikbaar als u **Category that includes executable files from selected devices** als soort categorie hebt geselecteerd.

Klik in deze stap op de knop **Add** en geef de computers op waarvan de uitvoerbare bestanden door Kaspersky Security Center aan de programmacategorie worden toegevoegd. Alle uitvoerbare bestanden van de opgegeven computers die in de map **Executable files** worden weergegeven, worden door Kaspersky Security Center toegevoegd aan de programmacategorie.

Tijdens deze stap kunt u ook de volgende instellingen configureren:

- Algoritme voor berekening van hashfunctie. Om een algoritme te selecteren, moet u ten minste een van de volgende selectievakjes inschakelen:
  - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions).**
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**
- Het selectievakje **Synchronize data with Administration Server repository**. Schakel dit selectievakje in als Kaspersky Security Center de programmacategorie periodiek moet wissen en daarna alle uitvoerbare bestanden van de opgegeven computers die in de map **Executable files** worden weergegeven, aan de categorie moet toevoegen.

Als het selectievakje **Synchronize data with Administration Server repository** is uitgeschakeld, brengt Kaspersky Security Center geen wijzigingen aan een programmacategorie aan nadat deze is gemaakt.

- Het veld **Scan period (h)**. U kunt in dit veld opgeven na hoeveel tijd (in uren) Kaspersky Security Center de programmacategorie moet wissen en alle uitvoerbare bestanden van de opgegeven computers die in de map **Executable files** worden weergegeven, aan die categorie moet toevoegen.

Dit veld is beschikbaar als het selectievakje **Synchronize data with Administration Server repository** is ingeschakeld.

## Stap 6. Opslagmap

Deze stap is beschikbaar als u **Category that includes executable files from a specific folder** als soort categorie hebt geselecteerd.

Kies tijdens deze stap de map waarin Kaspersky Security Center moet zoeken naar uitvoerbare bestanden om programma's automatisch toe te voegen aan de programmacategorie.

Tijdens deze stap kunt u ook de volgende instellingen configureren:

- Het selectievakje **Include dynamic-link libraries (DLL) in this category**. Schakel dit selectievakje in als u dynamische-link-bibliotheken (DLL-bestanden) wilt opnemen in de programmacategorie.

Het toevoegen van DLL-bestanden aan de programmacategorie kan leiden tot mindere prestaties van Kaspersky Security Center.

- Het selectievakje **Include script data in this category**. Schakel dit selectievakje in als u scripts wilt opnemen in de programmacategorie.

Het toevoegen van scripts aan de programmacategorie kan leiden tot mindere prestaties van Kaspersky Security Center.

- Algoritme voor berekening van hashfunctie. Om een algoritme te selecteren, moet u ten minste een van de volgende selectievakjes inschakelen:
  - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- Het selectievakje **Force folder scan for changes**. Schakel dit selectievakje in als u wilt dat Kaspersky Security Center periodiek moet zoeken naar uitvoerbare bestanden in de map die wordt gebruikt om uitvoerbare bestanden automatisch toe te voegen aan de programmacategorie.

Als het selectievakje **Force folder scan for changes** is uitgeschakeld, zoekt Kaspersky Security Center naar uitvoerbare bestanden in de map die wordt gebruikt om uitvoerbare bestanden automatisch toe te voegen aan de programmacategorie pas als wijzigingen in de map zijn gemaakt, bestanden aan de map zijn toegevoegd of bestanden uit de map zijn verwijderd.
- Het veld **Scan period (h)**. In dit veld kunt u opgeven na hoeveel tijd (in uren) Kaspersky Security Center moet zoeken naar uitvoerbare bestanden in de map die wordt gebruikt om uitvoerbare bestanden automatisch toe te voegen aan de programmacategorie.

Dit veld is beschikbaar als het selectievakje **Force folder scan for changes** is ingeschakeld.

## Stap 7. Een aangepaste categorie maken

Verlaat de wizard verlaten.

## Uitvoerbare bestanden uit de map Uitvoerbare bestanden toevoegen aan de programmacategorie

In de map **Executable files** ziet u de lijst met uitvoerbare bestanden die op computers zijn gevonden. Kaspersky Endpoint Security genereert een lijst met uitvoerbare bestanden nadat de inventarisatie is gedaan.

*Zo voegt u uitvoerbare bestanden uit de map Executable files toe aan de programmacategorie:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Additional** → **Application management** → **Executable files**.
3. Selecteer in de werkrumte de uitvoerbare bestanden die u wilt toevoegen aan de programmacategorie.
4. Klik rechts om het contextmenu voor de geselecteerde uitvoerbare bestanden te openen en selecteer **Add to category**.
5. Doe in het venster dat opent het volgende:

- Kies boven in het venster één van de volgende opties:
  - **Add to a new application category.** Kies deze optie als u een nieuwe programmacategorie wilt aanmaken en uitvoerbare bestanden wilt toevoegen aan die categorie.
  - **Add to an existing application category.** Kies deze optie als u een bestaande programmacategorie wilt selecteren en uitvoerbare bestanden wilt toevoegen aan die categorie.
- Kies in het gedeelte **Type regel** een van de volgende opties:
  - **Rules for adding to inclusions.** Selecteer deze optie als u een voorwaarde wilt aanmaken die uitvoerbare bestanden toevoegt aan de programmacategorie.
  - **Rules for adding to exclusions.** Selecteer deze optie als u een voorwaarde wilt aanmaken die uitvoerbare bestanden uitsluit van de programmacategorie.
- Selecteer in het blok **Parameter used as a condition** een van de volgende opties:
  - **Certificate details (or SHA-256 hashes for files without a certificate).**
  - **Certificate details (files without a certificate will be skipped).**
  - **Only SHA-256 (files without a hash will be skipped).**
  - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version).**

6. Sla uw wijzigingen op.

## Uitvoerbare bestanden die zijn gerelateerd aan gebeurtenissen toevoegen aan de programmacategorie

*Zo kunt u uitvoerbare bestanden die zijn gerelateerd aan gebeurtenissen van Programmacontrole toevoegen aan de programmacategorie:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Events**.
3. Selecteer gebeurtenissen die zich voordeden tijdens de werking van het onderdeel Programmacontrole ([Gebeurtenissen die zich voordeden tijdens de werking van het onderdeel Programmacontrole weergeven](#), [Gebeurtenissen die zich voordeden tijdens de geteste werking van het onderdeel Programmacontrole weergeven](#)) in de vervolgkeuzelijst **Event selections**.
4. Klik op de knop **Run selection**.
5. Selecteer de gebeurtenissen waarvan u de gerelateerde uitvoerbare bestanden wilt toevoegen aan de programmacategorie.
6. Klik rechts om het contextmenu voor de geselecteerde gebeurtenissen te openen en selecteer **Add to category**.
7. Configureer in het venster dat opent de instellingen van de programmacategorie:

- Kies boven in het venster één van de volgende opties:
  - **Add to a new application category.** Kies deze optie als u een nieuwe programmacategorie wilt aanmaken en uitvoerbare bestanden wilt toevoegen aan die categorie.
  - **Add to an existing application category.** Kies deze optie als u een bestaande programmacategorie wilt selecteren en uitvoerbare bestanden wilt toevoegen aan die categorie.
- Kies in het gedeelte **Type regel** een van de volgende opties:
  - **Rules for adding to inclusions.** Selecteer deze optie als u een voorwaarde wilt aanmaken die uitvoerbare bestanden toevoegt aan de programmacategorie.
  - **Rules for adding to exclusions.** Selecteer deze optie als u een voorwaarde wilt aanmaken die uitvoerbare bestanden uitsluit van de programmacategorie.
- Selecteer in het blok **Parameter used as a condition** een van de volgende opties:
  - **Certificate details (or SHA-256 hashes for files without a certificate).**
  - **Certificate details (files without a certificate will be skipped).**
  - **Only SHA-256 (files without a hash will be skipped).**
  - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version).**

8. Sla uw wijzigingen op.

## Een regel van Programmacontrole toevoegen en wijzigen via Kaspersky Security Center

*Zo kunt u een regel van Programmacontrole toevoegen of wijzigen via Kaspersky Security Center:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkrimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.  
Rechts in het venster ziet u de instellingen van het onderdeel Programmacontrole.
6. Doe een van de volgende acties:
  - 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 Programmacontrole** wordt geopend.

7. Doe een van de volgende acties:

- Als u een nieuwe categorie wilt maken:
  - a. Klik op **Categorie maken**.  
De wizard voor het aanmaken van een gebruikerscategorie wordt gestart.
  - b. Volg de instructies van de wizard voor het aanmaken van een gebruikerscategorie.
  - c. Selecteer in de vervolgkeuzelijst **Categorie** de aangemaakte programmacategorie.
- Als u een bestaande categorie wilt bewerken:
  - a. Selecteer in de vervolgkeuzelijst **Categorie** de aangemaakte programmacategorie die u wilt bewerken.
  - b. Klik op **Eigenschappen**.
  - c. Wijzig de instellingen van de geselecteerde programmacategorie.
  - d. Sla uw wijzigingen op.
  - e. Selecteer in de vervolgkeuzelijst **Categorie** de aangemaakte programmacategorie die u als basis wilt gebruiken om een regel aan te maken.

8. Klik in de tabel **Houders en hun rechten** op de knop **Toevoegen**.

9. Geef in het venster dat opent de lijst met gebruikers en/of groepen gebruikers op waarvoor u wilt instellen dat ze programma's uit de geselecteerde categorie mogen starten.

10. In de tabel **Houders en hun rechten** doet u het volgende:

- Als u wilt toestaan dat gebruikers en/of groepen gebruikers programma's uit de geselecteerde categorie mogen starten, schakelt u het selectievakje **Toestaan** bij de relevante rijen in.
- Als u niet wilt toestaan dat gebruikers en/of groepen gebruikers programma's uit de geselecteerde categorie mogen starten, schakelt u het selectievakje **Weigeren** bij de relevante rijen uit.

11. Schakel het selectievakje **Weigeren voor andere gebruikers** in als u wilt instellen dat alle gebruikers die niet in de kolom **Houder** verschijnen en die geen lid zijn van de opgegeven groep gebruikers in de kolom **Houder** geen programma's mogen starten die tot de geselecteerde categorie behoren.

12. Als u wilt dat Kaspersky Endpoint Security programma's uit de geselecteerde programmacategorie beschouwt als vertrouwde updaters die andere uitvoerbare bestanden mogen aanmaken die daarna mogen worden uitgevoerd, schakelt u het selectievakje **Vertrouwde updaters** in.

Wanneer de instellingen van Kaspersky Endpoint Security worden gemigreerd, wordt de lijst met uitvoerbare bestanden die wordt gemaakt door vertrouwde updaters ook gemigreerd.

13. Sla uw wijzigingen op.

## De status van een regel van Programmacontrole wijzigen via Kaspersky Security Center

Zo wijzigt u de status van een regel van Programmacontrole:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.  
Rechts in het venster ziet u de instellingen van het onderdeel Programmacontrole.
6. Klik in de kolom **Status** om het contextmenu weer te geven en selecteer een van de volgende opties:
  - **Aan.** Deze status geeft aan dat de regel wordt gebruikt als programmacontrole actief is.
  - **Uit.** Deze status geeft aan dat de regel wordt genegeerd als programmacontrole actief is.
  - **Testen.** Deze status geeft aan dat Kaspersky Endpoint Security altijd de opstart van programma's toestaat waarop de regel van toepassing is maar informatie over de opstart van zulke programma's in het rapport registreert.
7. Sla uw wijzigingen op.

## Regels voor programmabeheer exporteren en importeren

U kunt de lijst met regels van programmacontrole exporteren naar een XML-bestand. U kunt de export/import-functie gebruiken om een back-up te maken van de lijst met regels van programmacontrole of om de lijst naar een andere server te migreren.

Houd bij het exporteren en importeren van regels voor programmacontrole rekening met de volgende speciale overwegingen:

- Kaspersky Endpoint Security exporteert de lijst met regels alleen voor de actieve Programmacontrole-modus. Met andere woorden, als Programmacontrole in de denylist-modus werkt, exporteert Kaspersky Endpoint Security alleen regels voor deze modus. Om de lijst met regels voor de allowlist-modus te exporteren, moet u de modus wijzigen en de exportbewerking opnieuw uitvoeren.
- Kaspersky Endpoint Security gebruikt applicatiecategorieën om de regels voor programmacontrole te laten werken. Wanneer u de lijst met regels voor programmacontrole naar een andere server migreert, moet u ook de lijst met programmacategorieën migreren. Voor meer informatie over het exporteren of importeren van programmacategorieën, raadpleegt u [Kaspersky Security Center Help](#).

[Een lijst met regels van programmacontrole exporteren en importeren in de Beheerconsole \(MMC\)](#)



1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.
6. Zo wijzigt u de status van een regel voor programmacontrole:
  - a. Selecteer de regels die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen regel hebt geselecteerd, exporteert Kaspersky Endpoint Security alle regels.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met regels wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.
7. Een lijst met regels van programmacontrole exporteren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

[Een lijst met regels van programmacontrole exporteren en importeren in de Webconsole en de Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Security Controls** → **Programmacontrole**.
5. Klik op de koppeling **Rules Lists Settings**.
6. Selecteer een lijst met regels: denylist of allowlist voor programma's.
7. Zo wijzigt u de status van een regel voor programmacontrole:
  - a. Selecteer de regels die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde regels wilt exporteren of de volledige lijst wilt exporteren.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar een XML-bestand in de standaard downloadmap.
8. Een lijst met regels van programmacontrole exporteren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
9. Sla uw wijzigingen op.

## Regels voor programmacontrole testen via Kaspersky Security Center

Als u ervoor wilt zorgen dat regel van Programmacontrole geen programma's blokkeren die u nodig hebt voor uw werk, wordt u aanbevolen om het testen van de regels van Programmacontrole in te schakelen en hun werking na de aanmaak van nieuwe regels te analyseren. Wanneer het testen van de regels van Programmacontrole is ingeschakeld, blokkeert Kaspersky Endpoint Security geen programma's waarvan de opstart verboden is door regels van Programmacontrole maar stuurt het wel meldingen over de opstart ervan naar de Administration Server.

Voor een analyse van de werking van de regels van Programmacontrole moeten de resulterende gebeurtenissen van Programmacontrole die worden gerapporteerd aan Kaspersky Security Center worden onderzocht. Als de testen aangeven dat alle benodigde programma's voor het werk van de gebruiker kunnen worden gestart, betekent dit dat de juiste regels zijn aangemaakt. In het andere geval wordt u aanbevolen de instellingen van de aangemaakte regels bij te werken, extra regels aan te maken of de bestaande regels te verwijderen.

Kaspersky Endpoint Security staat standaard het opstarten van alle programma's toe, behalve de programma's die volgens de regels verboden zijn.

*Zo schakelt u het testen voor regels van Programmacontrole in Kaspersky Security Center in of uit:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.  
Rechts in het venster ziet u de instellingen van het onderdeel Programmacontrole.
6. Selecteer in de vervolgkeuzelijst **Controlemodus** een van de volgende opties:
  - **Denylist**. Als deze optie is geselecteerd, staat Programmacontrole toe dat alle gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de blokkeringsregels van Programmacontrole is voldaan.
  - **Allowlist**. Als deze optie is geselecteerd, staat Programmacontrole niet toe dat gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de uitvoeringsregels van Programmacontrole is voldaan.
7. Doe een van de volgende acties:
  - Als u het testen voor regels van programmacontrole wilt inschakelen, selecteert u de optie **Regels testen** in de vervolgkeuzelijst **Actie**.
  - Als u wilt dat Programmacontrole de opstart van programma's op computers van gebruikers beheert, selecteert u **Regels toepassen** in de vervolgkeuzelijst.
8. Sla uw wijzigingen op.

## Gebeurtenissen die zich voordeden tijdens de geteste werking van het onderdeel Programmacontrole weergeven

*Zo geeft u testgebeurtenissen van Programmacontrole weer die door Kaspersky Security Center zijn ontvangen:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Events**.
3. Klik op de knop **Create a selection**.
4. Selecteer in het geopende venster het gedeelte **Gebeurtenissen**.
5. Klik op de knop **Clear all**.

6. Schakel in de tabel de selectievakjes **Gebeurtenissen Programma mag niet worden gestart in testmodus** en **Programma mag worden gestart in testmodus** in.
7. Sla uw wijzigingen op.
8. Selecteer in de vervolgkeuzelijst **Event selections** de aangemaakte selectie.
9. Klik op de knop **Run selection**.

## Zo geeft u het rapport over geblokkeerde programma's in de testmodus weer

*Zo geeft u het rapport over geblokkeerde programma's in de testmodus weer:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Reports**.
3. Klik op de knop **New report template**.  
De wizard Nieuwe rapportsjabloon wordt gestart.
4. Volg de instructies van de wizard Sjabloon voor rapport. Tijdens de stap **Selecting the report template type** selecteert u achtereenvolgens **Other** → **Report on prohibited applications in test mode**.  
Wanneer u de wizard Nieuwe rapportsjabloon hebt voltooid, verschijnt de nieuwe rapportsjabloon in de tabel op het tabblad **Reports**.
5. Dubbelklik op het rapport om het te openen.

Het rapport wordt gemaakt. Het rapport wordt in een nieuw venster weergegeven.

## Gebeurtenissen die zich voordeden tijdens de werking van het onderdeel Programmacontrole weergeven

*Zo bekijkt u de resultaten van de werking van het onderdeel Programmacontrole die door Kaspersky Security Center zijn ontvangen:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Events**.
3. Klik op de knop **Create a selection**.
4. Selecteer in het geopende venster het gedeelte **Gebeurtenissen**.
5. Klik op de knop **Clear all**.
6. Schakel in de tabel **Gebeurtenissen** het selectievakje **Programma mag niet worden gestart in**.
7. Sla uw wijzigingen op.

8. Selecteer in de vervolgkeuzelijst **Event selections** de aangemaakte selectie.
9. Klik op de knop **Run selection**.

## Een rapport over geblokkeerde programma's weergeven

*Zo geeft u het rapport over geblokkeerde programma's weer:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer bij het knooppunt **Administration Server** in de structuur van de Beheerconsole het tabblad **Reports**.
3. Klik op de knop **New report template**.  
De wizard Nieuwe rapportsjabloon wordt gestart.
4. Volg de instructies van de wizard Sjabloon voor rapport. Tijdens de stap **TSelecting the report template type** selecteert u achtereenvolgens **Other** → **Report on prohibited applications**.  
Wanneer u de wizard Nieuwe rapportsjabloon hebt voltooid, verschijnt de nieuwe rapportsjabloon in de tabel op het tabblad **Reports**.
5. Dubbelklik op het rapport om het te openen.

Het rapport wordt gemaakt. Het rapport wordt in een nieuw venster weergegeven.

## Regels van Programmacontrole testen

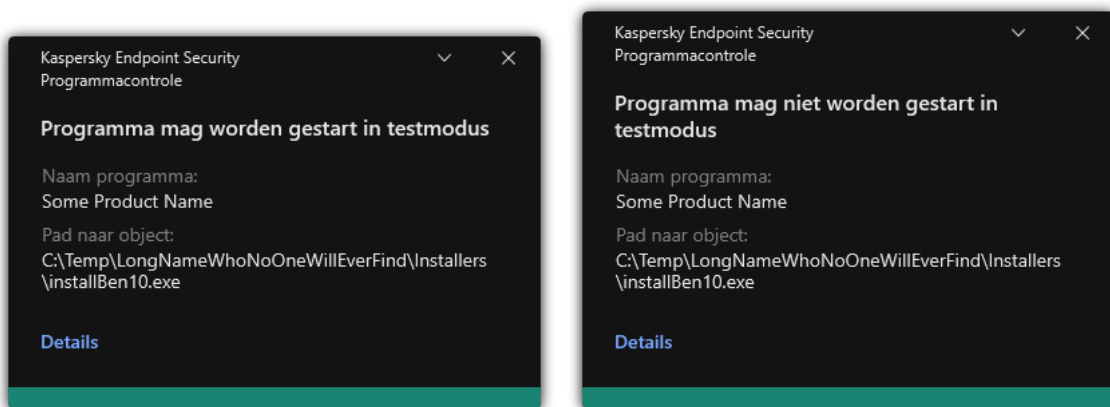
Als u ervoor wilt zorgen dat regel van Programmacontrole geen programma's blokkeren die u nodig hebt voor uw werk, wordt u aanbevolen om het testen van de regels van Programmacontrole in te schakelen en hun werking na de aanmaak van nieuwe regels te analyseren.

Voor een analyse van de werking van de regels van Programmacontrole moeten de resulterende gebeurtenissen van Programmacontrole die worden gerapporteerd aan Kaspersky Security Center worden onderzocht. Als de testen aangeven dat alle benodigde programma's voor het werk van de gebruiker kunnen worden gestart, betekent dit dat de juiste regels zijn aangemaakt. In het andere geval wordt u aanbevolen de instellingen van de aangemaakte regels bij te werken, extra regels aan te maken of de bestaande regels te verwijderen.

*Zo schakelt u het testen van de regels van Programmacontrole in of selecteert u een blokkerende actie voor Programmacontrole:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Klik op de knop **Geblokkeerde programma's** of **Toegestane programma's**.  
Hiermee wordt de lijst met regels van programmacontrole geopend.
4. Selecteer in het gedeelte **Status** de optie **Testen**.  
Deze status geeft aan dat Kaspersky Endpoint Security altijd de opstart van programma's toestaat waarop deze regel van toepassing is maar informatie over de opstart van zulke programma's in het rapport registreert.
5. Sla uw wijzigingen op.

Kaspersky Endpoint Security blokkeert geen programma's waarvan de opstart is verboden door het onderdeel Programmacontrole maar stuurt wel meldingen over de opstart ervan naar de Administration Server. U kunt ook [de weergave configureren van meldingen](#) over regeltesten op de computer van de gebruiker.



Meldingen programmacontrole in testmodus

## Bewaking van programma-activiteit

*Bewaking van programma-activiteit* is een tool ontworpen voor de realtime weergave van informatie over de activiteit van de computer van een gebruiker.

Voor het gebruik van de Bewaking van programma-activiteit moet u de onderdelen Programmacontrole en Host Intrusion Prevention installeren. Als deze componenten niet zijn geïnstalleerd, wordt de sectie Bewaking van programma-activiteit in de [hoofdvenster van het programma](#) is verborgen.

*De bewaking van programma-activiteit starten:*

Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **Bewaking van programma-activiteit**.

In dit venster wordt informatie over de activiteit van programma's op de computer van de gebruiker weergegeven op drie tabbladen:

- Het tabblad **Alle programma's** geeft informatie over alle programma's die op de computer geïnstalleerd zijn.
- Het tabblad **Gestart** geeft informatie over het verbruik van computerbronnen door elk programma in realtime. Vanaf dit tabblad kunt u ook doorgaan met het configureren van machtigingen voor een individuele toepassing.
- Het tabblad **Gestart bij opstart** geeft de lijst met programma's die worden gestart wanneer het besturingssysteem start.

Als u de informatie over de programma-activiteit wilt verbergen op de computer van de gebruiker, kunt u de toegang van de gebruiker tot Bewaking van programma-activiteit beperken.

[Bewaking van programma-activiteit verbergen in de programma-interface via Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
6. Gebruik het selectievakje **Bewaking van programma-activiteit verbergen** om de toegang tot de tool te verlenen of in te trekken.
7. Sla uw wijzigingen op.

### [Bewaking van programma-activiteit verbergen in de programma-interface via de Webconsole en Cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Interface**.
5. Gebruik het selectievakje **Hide Application Activity Monitor section** om de toegang tot de tool te verlenen of in te trekken.
6. Sla uw wijzigingen op.

## Regels voor het maken van naammaskers voor bestanden of mappen

Een *masker van een bestands- of mapnaam* is een voorstelling van de naam van een map of de naam en extensie van een bestand met normale tekens.

U kunt de volgende normale tekens gebruiken om het masker van een bestands- of mapnaam te maken:


- Het teken **\*** (sterretje), dat een willekeurig teken voorstelt (inclusief een lege set). Het masker `C:\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de `.txt`-extensie die zich in mappen en submappen op de C-schijf bevinden.
- Het teken **?** (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Voorbeeld` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

## Berichtsjablonen van Programmacontrole bewerken

Wanneer een gebruiker een programma probeert te starten dat door een regel van Programmacontrole 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. In het blok **Sjablonen van berichten over programmablokking** configureert u sjablonen voor berichten over programmacontrole:
  - **Bericht over blokkering** Sjabloon van het bericht dat wordt weergegeven bij de activering van een regel van Programmacontrole die de start van een programma blokkeert. De melding van een geblokkeerd programma wordt weergegeven in de onderstaande afbeelding.  
U kunt geen berichtsjablonen configureren voor programmacontrole in [testmodus](#). Programmacontrole in testmodus geeft vooraf ingestelde meldingen weer.
  - **Bericht aan beheerder** Sjabloon van het bericht dat een gebruiker naar de LAN-beheerder van het bedrijf kan sturen als de gebruiker denkt dat een programma per ongeluk is geblokkeerd. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: **Bericht over blokkering van programmastart aan beheerder**. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie **User requests**. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.
4. Sla uw wijzigingen op.



Melding van programmacontrole



# Best practices voor het implementeren van een lijst met toegestane programma's

Wanneer u de implementatie van een lijst met toegestane programma's plant, wordt u aanbevolen de volgende acties uit te voeren:

1. Maak de volgende soorten groepen:

- Gebruikersgroepen. Groepen gebruikers waarvoor u het gebruik van diverse programma's moet toestaan.
- Beheergroepen. Een of meerdere groepen van computers waarop Kaspersky Security Center de lijst met toegestane programma's zal toepassen. Het is noodzakelijk om meerdere groepen computers te maken als voor die groepen verschillende instellingen voor de allowlist worden gebruikt.

2. Maak een lijst met programma's die mogen worden gestart.

Voordat u een lijst maakt, wordt u aangeraden het volgende te doen:

a. Start de inventarisatietask.

Informatie over het maken, opnieuw configureren en opstarten van een inventarisatie vindt u in het onderdeel Taakbeheer.

b. Bekijk de [lijst met uitvoerbare bestanden](#).

## Allowlist-modus configureren voor programma's

Wanneer u de allowlist-modus configureert, wordt u aanbevolen de volgende acties uit te voeren:

1. Maak [programmacategorieën](#) met de programma's die mogen worden gestart.

U kunt een van de volgende methoden selecteren om programmacategorieën aan te maken:

- **Category with content added manually.** U kunt items handmatig toevoegen aan deze categorie door de volgende voorwaarden te gebruiken:
  - Metagegevens van bestanden. Kaspersky Security Center voegt alle uitvoerbare bestanden samen met de opgegeven metagegevens toe aan de programmacategorie.
  - Hash-code van bestanden. Kaspersky Security Center voegt alle uitvoerbare bestanden met de opgegeven hash toe aan de programmacategorie.

In het geval dat deze voorwaarde wordt gebruikt, kunnen updates niet automatisch worden geïnstalleerd omdat elke versie van een bestand een andere hash heeft.

- Certificaat van bestanden. Kaspersky Security Center voegt alle uitvoerbare bestanden met het opgegeven certificaat toe aan de programmacategorie.
- KL-categorie. Kaspersky Security Center voegt alle programma's uit de opgegeven KL-categorie toe aan de programmacategorie.

- Map van programma. Kaspersky Security Center voegt alle uitvoerbare bestanden in deze map toe aan de aangepaste programmacategorie.

Het gebruik van de voorwaarde 'Map van programma' is mogelijk onveilig omdat alle programma's uit de opgegeven map mogen worden gestart. U wordt aanbevolen om de programmacategorieën die de voorwaarde 'Map van programma' gebruiken alleen toe te passen op gebruikers waarvoor u de automatische installatie van updates wilt toestaan.

- **Category that includes executable files from a specific folder.** U kunt een map opgeven waarin de uitvoerbare bestanden zich bevinden die automatisch worden toegewezen aan de gemaakte programmacategorie.
- **Category that includes executable files from selected devices.** U kunt een computer opgeven waarvoor alle uitvoerbare bestanden automatisch worden toegewezen aan de gemaakte programmacategorie.

Wanneer deze methode voor het maken van programmacategorieën wordt gebruikt, ontvangt Kaspersky Security Center informatie over programma's op de computer via de map [Uitvoerbare bestanden](#)

2. [Selecteer de allowlist-modus](#) voor het onderdeel Programmacontrole.

3. [Maak regels van Programmacontrole aan](#) met behulp van de gemaakte programmacategorieën.

De **Golden Image**-regel en de **Vertrouwde updaters**-regel zijn aanvankelijk gedefinieerd voor de Allowlist-modus. Deze Application Control-regels komen overeen met KL-categorieën. De KL-categorie 'Golden Image' bevat programma's die de normale werking van het besturingssysteem verzekeren. De KL-categorie 'Vertrouwde updaters' bevat updaters voor de meest bekende softwareleveranciers. U kunt deze regels niet verwijderen. De instellingen van deze regels kunnen niet worden bewerkt. Standaard is de **Golden Image**-regel ingeschakeld en is de **Vertrouwde updaters**-regel uitgeschakeld. Alle gebruikers mogen programma's starten die aan de activeringsvoorwaarden van deze regels voldoen.

4. Bepaal voor welke programma's u de automatische installatie van updates wilt toestaan.

U kunt de automatische installatie van updates toestaan op een van de volgende manieren:

- Geef een uitgebreide lijst met toegestane programma's op door de opstart van alle programma's uit een bepaalde KL-categorie toe te staan.
- Geef een uitgebreide lijst met toegestane programma's op door de opstart van alle programma's die zijn ondertekend met een certificaat toe te staan.

Om de opstart van alle programma's die ondertekend zijn met certificaten toe te staan, kunt u een categorie maken met een voorwaarde op basis van certificaten die alleen de parameter **Subject** met de waarde \* gebruikt.

- Selecteer voor de regel van Programmacontrole de parameter **Vertrouwde updaters**. Als dit selectievakje is ingeschakeld, zal Kaspersky Endpoint Security de programma's die zijn opgenomen in de regel beschouwen als vertrouwde updaters. De opstart van programma's die zijn geïnstalleerd of bijgewerkt door de programma's die zijn opgenomen in de regel wordt door Kaspersky Endpoint Security toegestaan als er geen Blokkeren-regels zijn toegepast op die programma's.

Wanneer de instellingen van Kaspersky Endpoint Security worden gemigreerd, wordt de lijst met uitvoerbare bestanden die wordt gemaakt door vertrouwde updaters ook gemigreerd.

- Maak een map en plaats hierin de uitvoerbare bestanden van programma's waarvoor de automatische installatie van updates is toegestaan. Maak dan een programmacategorie met de voorwaarde 'Programmamap' en geef het pad naar die map op. Maak vervolgens een Toestaan-regel en selecteer deze categorie.

Het gebruik van de voorwaarde 'Map van programma' is mogelijk onveilig omdat alle programma's uit de opgegeven map mogen worden gestart. U wordt aanbevolen om de programmacategorieën die de voorwaarde 'Map van programma' gebruiken alleen toe te passen op gebruikers waarvoor u de automatische installatie van updates wilt toestaan.

## De allowlist-modus testen

Als u ervoor wilt zorgen dat regel van Programmacontrole geen programma's blokkeren die u nodig hebt voor uw werk, wordt u aanbevolen om het testen van de regels van Programmacontrole in te schakelen en hun werking na de aanmaak van nieuwe regels te analyseren. Wanneer het testen is ingeschakeld, blokkeert Kaspersky Endpoint Security geen programma's waarvan de opstart verboden is door regels van Programmacontrole maar stuurt het wel meldingen over de opstart ervan naar de Administration Server.

Wanneer u de allowlist-modus test, wordt u aanbevolen de volgende acties uit te voeren:

1. Bepaal de testperiode (gaande van enkele dagen tot twee maanden).
2. Schakel [het testen van de regels van Programmacontrole](#) in.
3. Controleer de [gebeurtenissen die zich voordeden tijdens het testen van de werking van Programmacontrole](#) en [rapporten over geblokkeerde programma's in de testmodus](#) om de resultaten van de test te analyseren.
4. Op basis van de resultaten van de analyse maakt u wijzigingen aan de instellingen van de allowlist-modus.

In het bijzonder kunt u op basis van de testresultaten [uitvoerbare bestanden met betrekking tot gebeurtenissen aan een programmacategorie toevoegen](#).

## Ondersteuning voor allowlist-modus

Na de [selectie van een blokkerende actie voor Programmacontrole](#), wordt u aanbevolen de ondersteuning voor de allowlist-modus voort te zetten door het volgende te doen:

- [Onderzoek de gebeurtenissen die zich voordeden tijdens de werking van Programmacontrole](#) en [rapporten over geblokkeerde opstarten](#) om de efficiëntie van Programmacontrole te analyseren.
- Analyseer verzoeken voor toegang tot programma's die gebruikers hebben ingediend.
- Analyseer onbekende uitvoerbare bestanden door hun reputatie in [Kaspersky Security Network](#) te controleren.
- Voordat u updates voor het besturingssysteem of software installeert, installeert u eerst die updates voor een testgroep van computers om te controleren hoe ze worden verwerkt door de regels van Programmacontrole.
- Voeg de noodzakelijke programma's toe aan categorieën die in regels van Programmacontrole worden gebruikt.

## Netwerkpoorten bewaken

Tijdens de werking van Kaspersky Endpoint Security monitoren de onderdelen [Webcontrole](#), [Mail Threat Protection](#) en [Web Threat Protection](#) gegevensstromen die via specifieke protocollen en door specifieke open TCP- en UDP-poorten worden verstuurd en ontvangen op de computer van de gebruiker. Het onderdeel Mail Threat Protection analyseert bijvoorbeeld informatie die via SMTP wordt verstuurd en ontvangen, terwijl het onderdeel Web Threat Protection informatie analyseert die via HTTP en FTP wordt verstuurd en ontvangen.

Kaspersky Endpoint Security verdeelt TCP- en UDP-poorten van de computer van de gebruiker in verschillende groepen, afhankelijk van het mogelijke gevaar via deze poorten. Sommige netwerkpoorten zijn voorbehouden voor kwetsbare services. U wordt aanbevolen om deze poorten nauwlettend te bewaken omdat ze veel meer kans hebben om het doelwit van netwerkaanvallen te zijn. Als u niet-standardservices 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 bijzondere aandacht van de onderdelen Mail Threat Protection en Web Threat Protection tijdens het monitoren van het netwerkverkeer.


## Bewaking van alle netwerkpoorten inschakelen

*Zo schakelt u de bewaking van alle netwerkpoorten in:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Selecteer in het blok **Bewaakte poorten** **Alle netwerkpoorten bewaken**.
4. Sla uw wijzigingen op.

## Een lijst met bewaakte netwerkpoorten aanmaken

*Zo maakt u een lijst met bewaakte netwerkpoorten aan:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Selecteer in het blok **Bewaakte poorten** **Alleen geselecteerde netwerkpoorten bewaken**.
4. Klik op **Selecteren**.

Dit open 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. Gebruik de schakelaar in de kolom **Status** om netwerkpoortbewaking in of uit te schakelen.

6. Als een netwerkpoort niet in de lijst met netwerkpoorten wordt weergegeven, voegt u die toe door het volgende te doen:

- a. Klik op **Toevoegen**.
- b. Voer in het geopende venster het netwerkpoortnummer en een korte beschrijving in.
- c. Stel de status **Actief** of **Inactief** in voor de bewaking van de netwerkpoort.

7. Sla uw wijzigingen op.


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 dergelijke verbindingen te beschermen, schakelt u [bewaking van alle netwerkpoorten in](#) of [configureert u de controle over netwerkpoorten voor programma's die FTP-verbindingen 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.
3. Selecteer in het blok **Bewaakte poorten Alleen geselecteerde netwerkpoorten bewaken**.
4. Selecteer het selectievakje **Bewaak alle poorten voor de programma's die voorkomen op de lijst aanbevolen door Kaspersky**.

Als dit selectievakje is ingeschakeld, bewaakt Kaspersky Endpoint Security alle poorten voor de volgende programma's:

- Adobe Reader.
- Apple Application Support.
- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.

- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- Yandex Browser.

5. Schakel het selectievakje **Bewaak alle poorten voor de opgegeven programma's** in.

6. Klik op **Selecteren**.

Dit opent een lijst met programma's waarvoor Kaspersky Endpoint Security alle netwerkpoorten monitort.

7. Gebruik de schakelaar in de kolom **Status** om netwerkpoortbewaking in of uit te schakelen.

8. Als een programma niet is opgenomen in de lijst met programma's, voegt u het als volgt toe:

a. Klik op **Toevoegen**.

b. Voer in het geopende venster het pad naar het uitvoerbare bestand van de toepassing en een korte beschrijving in.

c. Stel de status **Actief** of **Inactief** in voor de bewaking van netwerkpoorten.

9. Sla uw wijzigingen op.

## Lijsten met bewaakte poorten exporteren en importeren

Kaspersky Endpoint Security gebruikt de volgende lijsten om netwerkpoorten te bewaken: lijst met netwerkpoorten en lijst met programma's waarvan de poorten worden bewaakt door Kaspersky Endpoint Security. U kunt lijsten met bewaakte poorten exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal poorten met dezelfde omschrijving toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijsten met bewaakte poorten of om de lijsten naar een andere server te migreren.

[Lijsten met bewaakte poorten exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
6. Selecteer in het blok **Bewaakte poorten Alleen geselecteerde netwerkpoorten bewaken**.
7. Klik op **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.

8. De lijst met uitzonderingen exporteren:
  - a. Selecteer in de lijst met netwerkpoorten de poorten die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen poort hebt geselecteerd, exporteert Kaspersky Endpoint Security alle poorten.
  - b. Klik op **Exporteren**.
  - c. Voer in het venster dat opent de naam in van het XML-bestand waarnaar u de lijst met netwerkpoorten wilt exporteren, en selecteer de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met netwerkpoorten naar het XML-bestand.
9. De lijst met programma's exporteren waarvan de poorten worden bewaakt door Kaspersky Endpoint Security:
  - a. Schakel het selectievakje **Bewaak alle poorten voor de opgegeven programma's** in.
  - b. Selecteer in de lijst met programma's de programma's die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen programma hebt geselecteerd, exporteert Kaspersky Endpoint Security alle programma's.
  - c. Klik op **Exporteren**.
  - d. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met programma's wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - e. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met programma's naar het XML-bestand.
10. De lijst met netwerkpoorten importeren:
  - a. Klik in de lijst met netwerkpoorten op de knop **Importeren**.

Selecteer in het geopende venster het XML-bestand waaruit u de lijst met netwerkpoorten wilt importeren.

b. Open het bestand.

Als de computer al een lijst met netwerkpoorten heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.

11. De lijst met programma's importeren waarvan de poorten worden bewaakt door Kaspersky Endpoint Security:

a. Klik in de lijst met programma's op de knop **Importeren**.

Selecteer in het venster dat opent het XML-bestand waaruit u de lijst met programma's wilt importeren.

b. Open het bestand.

Als de computer al een lijst met programma's heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.

12. Sla uw wijzigingen op.

[Lijsten met bewaakte poorten exporteren en importeren via de Webconsole en Cloudconsole](#) 



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Netwerkinstellingen**.
5. De lijst met uitzonderingen exporteren:
  - a. Selecteer in het blok **Monitored ports** **Monitor selected network ports only**.
  - b. Klik op de **selected N ports** link.  
Het venster **Network ports** wordt geopend. In het venster **Network ports** 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.
  - c. Selecteer in de lijst met netwerkpoorten de poorten die u wilt exporteren.
  - d. Klik op **Export**.
  - e. Voer in het venster dat opent de naam in van het XML-bestand waarnaar u de lijst met netwerkpoorten wilt exporteren, en selecteer de map waarin u dit bestand wilt opslaan.
  - f. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met netwerkpoorten naar het XML-bestand.
6. De lijst met programma's exporteren waarvan de poorten worden bewaakt door Kaspersky Endpoint Security:
  - a. Schakel in het blok **Monitored ports** het selectievakje **Monitor all ports for specified applications** in.
  - b. Klik op de **selected N applications** link.
  - c. Selecteer in de lijst met programma's de programma's die u wilt exporteren.
  - d. Klik op **Export**.
  - e. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met programma's wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - f. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met programma's naar het XML-bestand.
7. De lijst met netwerkpoorten importeren:
  - a. Klik in de lijst met netwerkpoorten op de knop **Import**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met netwerkpoorten wilt importeren.
  - b. Open het bestand.

Als de computer al een lijst met netwerkpoorten heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.

8. De lijst met programma's importeren waarvan de poorten worden bewaakt door Kaspersky Endpoint Security:

a. Klik in de lijst met programma's op de knop **Import**.

Selecteer in het venster dat opent het XML-bestand waaruit u de lijst met programma's wilt importeren.

b. Open het bestand.

Als de computer al een lijst met programma's heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.

9. Sla uw wijzigingen op.

# Wachtwoordbeveiliging

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. Met de wachtwoordbeveiliging kunt u de toegang van gebruikers tot Kaspersky Endpoint Security beperken overeenkomstig de machtigingen die u hen hebt verleend (bijvoorbeeld de machtiging om het programma te sluiten).

Als de gebruiker die de Windows-sessie (*sessiegebruiker*) heeft gestart is gemachtigd om de actie uit te voeren, vraagt Kaspersky Endpoint Security geen gebruikersnaam en wachtwoord of geen tijdelijk wachtwoord. De gebruiker krijgt toegang tot Kaspersky Endpoint Security overeenkomstig de verleende machtigingen.

Als een sessiegebruiker niet is gemachtigd om een actie uit te voeren, kan de gebruiker toegang tot het programma krijgen op de volgende manieren:

- Voer een gebruikersnaam en wachtwoord in.

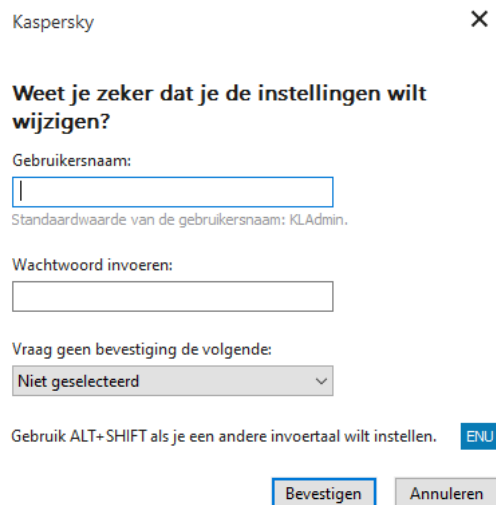
Deze methode is geschikt voor bewerkingen die u dagelijks uitvoert. Voor het uitvoeren van acties die zijn beveiligd met een wachtwoord moet u de accountgegevens voor de gebruiker met de vereiste machtiging invoeren. In dit geval moet de computer zich in dat domein bevinden. Als de computer zich niet in het domein bevindt, kunt u het KLAdmin-account gebruiken.

- Voer een tijdelijk wachtwoord in.

Deze methode is geschikt als u tijdelijke machtigingen voor het uitvoeren geblokkeerde acties (bijvoorbeeld om het programma te sluiten) wilt verlenen aan gebruikers buiten het bedrijfsnetwerk. Wanneer een tijdelijk wachtwoord verloopt of een sessie wordt beëindigd, herstelt Kaspersky Endpoint Security de eerdere waarden van de instellingen.

Als een gebruiker een actie probeert uit te voeren die met een wachtwoord is beveiligd, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om de gebruikersnaam en het wachtwoord of een tijdelijk wachtwoord in te voeren (zie onderstaande afbeelding).

In het wachtwoordinvoervenster kunt u alleen van taal wisselen door **ALT+SHIFT** in te drukken. Andere sneltoetscombinaties om van taal te wisselen werken niet, zelfs niet als deze zijn geconfigureerd in het besturingssysteem.



The screenshot shows a Kaspersky dialog box titled "Weet je zeker dat je de instellingen wilt wijzigen?". It contains two input fields: "Gebruikersnaam:" and "Wachtwoord invoeren:". Below the first field, it says "Standaardwaarde van de gebruikersnaam: KLAdmin.". There is a dropdown menu for "Vraag geen bevestiging de volgende:" with "Niet geselecteerd" selected. At the bottom, there is a note "Gebruik ALT+SHIFT als je een andere invoertaal wilt instellen." and a language selector "ENU". Two buttons, "Bevestigen" and "Annuleren", are at the bottom right.

Vraag van Kaspersky Endpoint Security om een wachtwoord voor de toegang in te voeren

## Gebruikersnaam en wachtwoord

Voor de toegang tot Kaspersky Endpoint Security voert u uw accountgegevens in die u binnen het domein gebruikt. De wachtwoordbeveiliging kunt u gebruiken voor de volgende accounts:

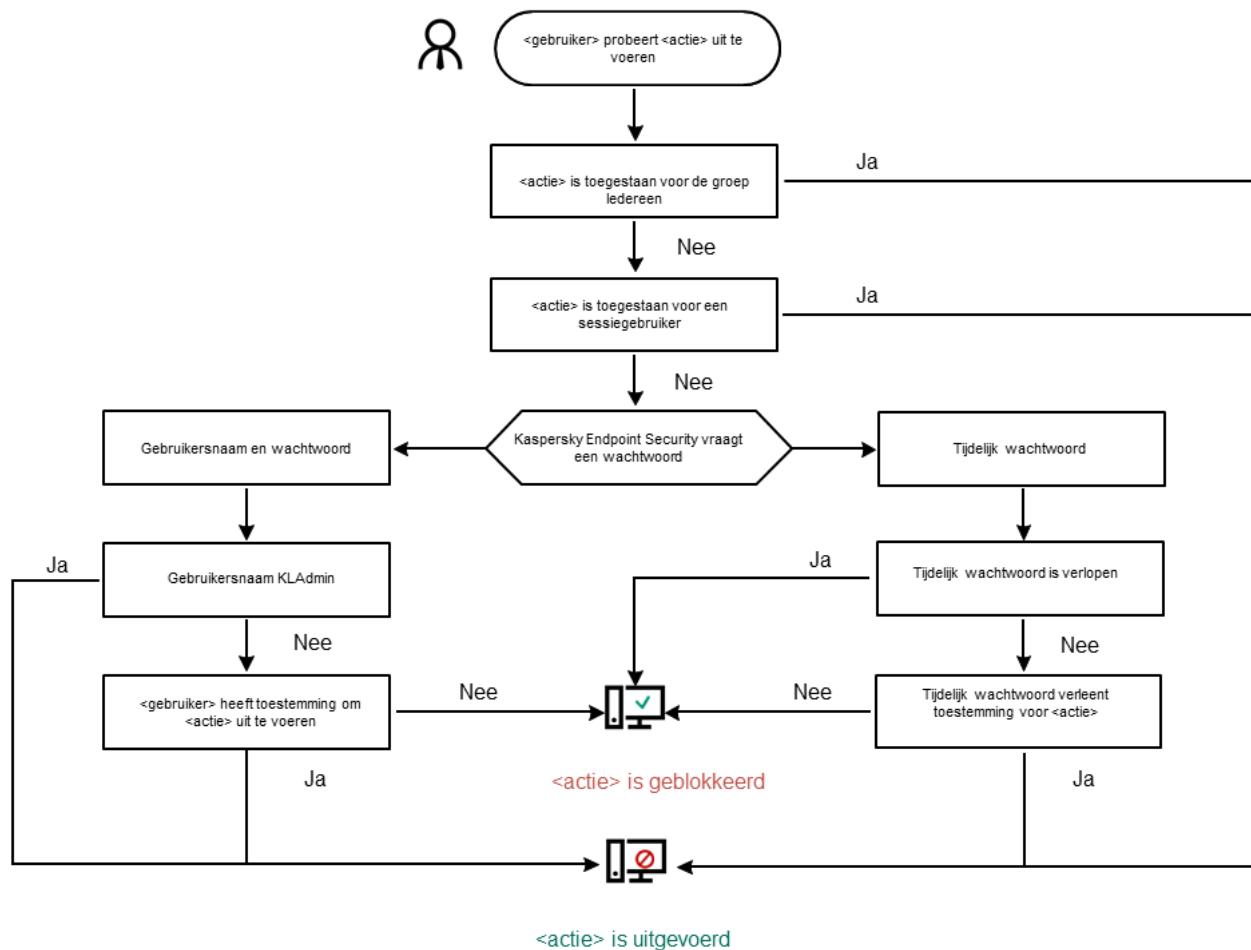
- **KLAdmin.** Een beheerdersaccount met onbeperkte toegang tot Kaspersky Endpoint Security. Het KLAdmin-account is gemachtigd om alle acties uit te voeren die met een wachtwoord zijn beveiligd. De machtigingen van het KLAdmin-account kunnen niet worden ingetrokken. Wanneer u de wachtwoordbeveiliging inschakelt, wordt u door Kaspersky Endpoint Security gevraagd of u een wachtwoord voor het KLAdmin-account wilt instellen.
- **De groep iedereen.** Een ingebouwde Windows-groep met alle gebruikers uit het bedrijfsnetwerk. Gebruikers in de groep iedereen hebben toegang tot het programma overeenkomstig de machtigingen die ze hebben.
- **Individuele gebruikers of groepen.** Gebruikersaccounts waarvoor u individuele machtigingen kunt configureren. Als een actie bijvoorbeeld is geblokkeerd voor de groep iedereen, kunt u deze actie toestaan voor een individuele gebruiker of groep.
- **Sessiegebruiker.** Account van de gebruiker die de Windows-sessie heeft gestart. U kunt wisselen van sessiegebruiker wanneer u een wachtwoord wordt gevraagd (het selectievakje **Save password for current session**). In dit geval beschouwt Kaspersky Endpoint Security de gebruiker waarvan de accountgegevens zijn ingevoerd als de sessiegebruiker in plaats van de gebruiker die de Windows-sessie heeft gestart.

## Tijdelijk wachtwoord

U kunt een tijdelijk wachtwoord gebruiken als u tijdelijke toegang tot Kaspersky Endpoint Security wilt verlenen aan een enkele computer buiten het bedrijfsnetwerk. De beheerder genereert een tijdelijk wachtwoord voor een enkele computer in de computereigenschappen in Kaspersky Security Center. De beheerder selecteert de acties die met het tijdelijke wachtwoord worden beveiligd en geeft op hoelang het tijdelijke wachtwoord geldig is.

## Algoritme voor werking van wachtwoordbeveiliging

Kaspersky Endpoint Security beslist of een actie met wachtwoordbeveiliging wordt toegestaan of geblokkeerd op basis van het volgende algoritme (zie onderstaande afbeelding).



Algoritme voor werking van wachtwoordbeveiliging

## Wachtwoordbeveiliging inschakelen

Met de wachtwoordbeveiliging kunt u de toegang van gebruikers tot Kaspersky Endpoint Security beperken overeenkomstig de machtigingen die u hen hebt verleend (bijvoorbeeld de machtiging om het programma te sluiten).

Zo schakelt u de wachtwoordbeveiliging in:

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
3. Gebruik de schakelaar **Wachtwoordbeveiliging** om de component in of uit te schakelen.
4. Geef het wachtwoord voor het KAdmin-account op en bevestig het.

Het KAdmin-account is gemachtigd om alle acties uit te voeren die met een wachtwoord zijn beveiligd.

Als een beleid is toegepast op een computer, kan de beheerder het wachtwoord voor het KAdmin-account opnieuw instellen in de beleidseigenschappen. Het is niet mogelijk om het wachtwoord te herstellen als de computer niet verbonden is met Kaspersky Security Center en u het wachtwoord voor het KAdmin-account vergeten bent.

5. Stel machtigingen voor alle gebruikers in het bedrijfsnetwerk in:

- a. Klik in de tabel account op de knop **Bewerken** om de lijst met machtigingen voor de groep ledereen te openen.

De *groep ledereen* is een ingebouwde Windows-groep met alle gebruikers uit het bedrijfsnetwerk.

- b. Schakel de selectievakjes in naast de acties die gebruikers mogen uitvoeren zonder het wachtwoord in te voeren.

Als een selectievakje is uitgeschakeld, kunnen de gebruikers de actie niet uitvoeren. Mocht bijvoorbeeld het selectievakje naast de machtiging **Programma afsluiten** uitgeschakeld zijn, dan kunt u het programma alleen afsluiten als u zich hebt aangemeld als KLAdmin, of als een [individuele gebruiker met de vereiste machtiging](#), of als u een [tijdelijk wachtwoord](#) invoert.

Bij machtigingen met wachtwoordbeveiliging moet u wel [rekening houden met enkele belangrijke aandachtspunten](#). Zorg dat aan alle voorwaarden voor de toegang tot Kaspersky Endpoint Security is voldaan.

## 6. Sla uw wijzigingen op.

Wanneer de wachtwoordbeveiliging is ingeschakeld, zal het programma de toegang van gebruikers tot Kaspersky Endpoint Security beperken volgens de machtigingen die aan de groep ledereen zijn verleend. Het uitvoeren van de acties die zijn geblokkeerd voor de groep ledereen is pas mogelijk als u het KLAdmin-account of [een ander account met de vereiste machtigingen](#) gebruikt of als u een [tijdelijk wachtwoord](#) invoert.

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.

Tijdens de wachtwoordcontrole kunt u het selectievakje **Onthoud wachtwoord voor deze sessie** inschakelen. In dit geval zal Kaspersky Endpoint Security geen wachtwoord vragen wanneer een gebruiker tijdens de sessie een andere actie probeert uit te voeren die met een wachtwoord is beveiligd.

## Machtigingen aan individuele gebruikers of groepen verlenen

U kunt toegang tot Kaspersky Endpoint Security verlenen aan individuele gebruikers of groepen. Als u het afsluiten van het programma bijvoorbeeld is geblokkeerd voor de groep ledereen, kunt u de machtiging **Programma afsluiten** aan een individuele gebruiker verlenen. In dat geval kunt u het programma alleen afsluiten als u bent aangemeld als die gebruiker of als KLAdmin.

U kunt alleen accountgegevens gebruiken om toegang te krijgen tot het programma als de computer zich in het domein bevindt. Als de computer zich niet in het domein bevindt, kunt u het KLAdmin-account of een [tijdelijk wachtwoord](#) gebruiken.

*Zo verleent u machtigingen aan individuele gebruikers of groepen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
3. Klik in de account-tabel op **Toevoegen**.
4. Klik in het venster op de knop **Gebruiker of groep selecteren**.

U ziet nu het standaard dialoogvenster 'Gebruikers of groepen selecteren'.

5. Selecteer een gebruiker of een groep in Active Directory en bevestig uw selectie.

6. Schakel in de lijst **Machtigingen** de selectievakjes in naast de acties die de geselecteerde gebruiker of groep mag uitvoeren zonder een wachtwoord in te voeren.

Als een selectievakje is uitgeschakeld, kunnen de gebruikers de actie niet uitvoeren. Mocht bijvoorbeeld het selectievakje naast de machtiging **Programma afsluiten** uitgeschakeld zijn, dan kunt u het programma alleen afsluiten als u zich hebt aangemeld als KLAdmin, of als een [individuele gebruiker met de vereiste machtiging](#), of als u een [tijdelijk wachtwoord](#) invoert.

Bij machtigingen met wachtwoordbeveiliging moet u wel [rekening houden met enkele belangrijke aandachtspunten](#). Zorg dat aan alle voorwaarden voor de toegang tot Kaspersky Endpoint Security is voldaan.

7. Sla uw wijzigingen op.

Als de toegang tot een programma is beperkt voor de groep iedereen, krijgen de gebruikers toegang tot Kaspersky Endpoint Security naargelang de machtigingen die hen zijn verleend.

## Een tijdelijk wachtwoord gebruiken om machtigingen te verlenen

U kunt een tijdelijk wachtwoord gebruiken als u tijdelijke toegang tot Kaspersky Endpoint Security wilt verlenen aan een enkele computer buiten het bedrijfsnetwerk. Dit is noodzakelijk opdat de gebruiker een geblokkeerde actie kan uitvoeren zonder de KLAdmin-accountgegevens. Voor het gebruik van een tijdelijk wachtwoord moet de computer worden toegevoegd aan Kaspersky Security Center.

[Zo staat u toe dat een gebruiker een geblokkeerde actie uitvoert met behulp van een tijdelijk wachtwoord via de beheerconsole \(MMC\)](#) <sup>2</sup>

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Dubbelklik om het venster met de eigenschappen van de computer te openen.
5. Selecteer het gedeelte **Programma's** in het venster met de eigenschappen van de computer.
6. Selecteer **Kaspersky Endpoint Security voor Windows** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.  
Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
7. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.
8. Klik in het venster **Tijdelijk wachtwoord** op de knop **instellingen**.
9. Het venster **Tijdelijk wachtwoord aanmaken** wordt geopend.
10. Geef in het veld **Verlooptdatum** op wanneer het tijdelijke wachtwoord verloopt.
11. Schakel in de tabel **Bereik tijdelijk wachtwoord** de selectievakjes in naast de acties die de gebruiker kan uitvoeren na het invoeren van het tijdelijke wachtwoord.
12. Klik op **Genereren**.  
Een venster met het tijdelijke wachtwoord wordt geopend (zie onderstaande afbeelding).
13. Kopieer het wachtwoord en geef het aan de gebruiker.

[Zo staat u toe dat een gebruiker een geblokkeerde actie uitvoert met behulp van een tijdelijk wachtwoord via de webconsole en cloudconsole](#) 



1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Klik op de naam van de computer waarop u een gebruiker een geblokkeerde actie wilt laten uitvoeren.
3. Selecteer het tabblad **Programma's**.
4. Klik op **Kaspersky Endpoint Security voor Windows**.  
U ziet nu de lokale programma-instellingen.
5. Selecteer het tabblad **Application settings**.
6. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
7. Klik in het blok **Wachtwoordbeveiliging** op de knop **Tijdelijk wachtwoord**.
8. Geef in het veld **Verloopdatum** op wanneer het tijdelijke wachtwoord verloopt.
9. Schakel in de tabel **Bereik tijdelijk wachtwoord** de selectievakjes in naast de acties die de gebruiker kan uitvoeren na het invoeren van het tijdelijke wachtwoord.
10. Klik op **Genereren**.  
Een venster met het tijdelijke wachtwoord wordt geopend.
11. Kopieer het wachtwoord en geef het aan de gebruiker.



### Toegang geweigerd

Het opgevraagde webadres kan niet worden weergegeven

[http://kl-test-page.avp.ru/new\\_ksn\\_samples/AVS\\_RISKWARE-KSN\\_BAD.exe](http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe)

**Reden:**


object is geïnfecteerd met [UDS:DangerousObject.Multi.Generic](#)

Bericht gemaakt op: 10/12/2020 7:39:53 PM

# Aandachtspunten bij machtigingen met wachtwoordbeveiliging

Bij machtigingen met wachtwoordbeveiliging moet u wel rekening houden met enkele belangrijke aandachtspunten en beperkingen.


## Programma-instellingen

Als een beleid is toegepast op de computer van een gebruiker, moet u ervoor zorgen dat alle vereiste instellingen in het beleid kunnen worden bewerkt (een open hangslot .


## Programma afsluiten

Er zijn geen aandachtspunten of beperkingen.

## Beschermingsonderdelen uitschakelen

- Het is niet mogelijk om de groep iedereen de machtiging te verlenen voor het uitschakelen van beschermingsonderdelen. Als u andere gebruikers dan KLAdmin wilt toestaan om Controleonderdelen uitschakelen, [voegt u in de instellingen van Wachtwoordbeveiliging een gebruiker of groep toe](#) die de machtiging **Beschermingsonderdelen uitschakelen** heeft.
- Als een beleid is toegepast op de computer van een gebruiker, moet u ervoor zorgen dat alle vereiste instellingen in het beleid kunnen worden bewerkt (een open hangslot .
- Voor het uitschakelen van beschermingsonderdelen in de programma-instellingen moet een gebruiker de machtiging **Programma-instellingen configureren** hebben.
- Voor het uitschakelen van beschermingsonderdelen vanuit het contextmenu (via de menuoptie **Bescherming pauzeren**) moet een gebruiker de machtiging **Beschermingsonderdelen uitschakelen** en **Controleonderdelen uitschakelen** hebben.

## Controleonderdelen uitschakelen

- Het is niet mogelijk om de groep iedereen de machtiging te verlenen om controleonderdelen uit te schakelen. Als u andere gebruikers dan KLAdmin wilt toestaan om Controleonderdelen uitschakelen, [voegt u in de instellingen van Wachtwoordbeveiliging een gebruiker of groep toe](#) die de machtiging **Controleonderdelen uitschakelen** heeft.
- Als een beleid is toegepast op de computer van een gebruiker, moet u ervoor zorgen dat alle vereiste instellingen in het beleid kunnen worden bewerkt (een open hangslot .
- Voor het uitschakelen van controleonderdelen in de programma-instellingen moet een gebruiker de machtiging **Programma-instellingen configureren** hebben.
- Voor het uitschakelen van controleonderdelen vanuit het contextmenu (via de menuoptie **Bescherming pauzeren**) moet een gebruiker de machtiging **Controleonderdelen uitschakelen** en **Beschermingsonderdelen uitschakelen** hebben.

## Kaspersky Security Center-beleid uitschakelen

U kunt de machtiging voor het uitschakelen van het Kaspersky Security Center-beleid niet verlenen aan de groep 'Iedereen'. Als u andere gebruikers dan KLAdmin wilt toestaan om het beleid uit te schakelen, [voegt u in de instellingen van Wachtwoordbeveiliging een gebruiker of groep toe](#) die de machtiging **Kaspersky Security Center-beleid uitschakelen** heeft.

## Licentie verwijderen

Er zijn geen aandachtspunten of beperkingen.

## Programma verwijderen/wijzigen/herstellen

Als u het verwijderen, wijzigen en herstellen van het programma voor de groep "Alle" hebt toegestaan, vraagt Kaspersky Endpoint Security niet om een wachtwoord wanneer de gebruiker deze bewerkingen probeert uit te voeren. Daarom kan elke gebruiker, inclusief gebruikers van buiten het domein de toepassing installeren, wijzigen of herstellen.

## Toegang tot gegevens op geëncrypte schijven herstellen

U kunt de toegang tot gegevens op geëncrypte schijven alleen herstellen als u bent aangemeld als KLAdmin. De toestemming voor de uitvoering van deze actie kan niet aan andere gebruikers worden verleend.

## Rapporten bekijken

Er zijn geen aandachtspunten of beperkingen.

## Terugzetten vanuit Back-up

Er zijn geen aandachtspunten of beperkingen.

## Het KLAdmin-wachtwoord resetten

Als u uw KLAdmin-accountwachtwoord bent vergeten, kunt u het wachtwoord opnieuw instellen in de beleidseigenschappen. U kunt het wachtwoord niet opnieuw instellen in de programma-interface.

U kunt met een wachtwoord beveiligde acties uitvoeren met behulp van een [tijdelijk wachtwoord](#). In dit geval hoeft u geen KLAdmin-inloggegevens in te voeren.

Het is niet mogelijk om het wachtwoord te herstellen als de computer niet verbonden is met Kaspersky Security Center en u het wachtwoord voor het KLAdmin-account vergeten bent.

[Het wachtwoord van het KLAdmin-account opnieuw instellen met behulp van de beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
6. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.
7. Dit opent een venster; schakel in dat venster het selectievakje **Wachtwoordbeveiliging** uit.
8. Sla uw wijzigingen op.
9. Schakel het selectievakje **Wachtwoordbeveiliging** opnieuw in.
10. Klik op **OK**.  
Hiermee wordt het venster voor het beheerderswachtwoord geopend.
11. Geef het wachtwoord voor het nieuwe KLAdmin-account op en bevestig het.
12. Sla uw wijzigingen op.

[Het wachtwoord van het KLAdmin-account opnieuw instellen in Webconsole en Cloudconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Programma's**.
4. Klik op **Kaspersky Endpoint Security voor Windows**.  
U ziet nu de lokale programma-instellingen.
5. Selecteer het tabblad **Application settings**.
6. Ga naar **Algemene instellingen** → **Interface** .
7. Zet onder **Wachtwoordbeveiliging** de schakelaar **Wachtwoordbeveiliging** uit.
8. Sla uw wijzigingen op.
9. Zet de schakelaar **Wachtwoordbeveiliging** opnieuw aan.
10. Geef het wachtwoord voor het nieuwe KLAdmin-account op en bevestig het.
11. Sla uw wijzigingen op.

Als gevolg hiervan wordt het wachtwoord van uw KLAdmin-account bijgewerkt nadat het beleid is toegepast.

## 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.

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. Een beheerder kan een gebruiker ook toestaan om zijn eigen lokale vertrouwde zone voor een specifieke computer te creëren. Op deze manier kunnen gebruikers hun eigen lokale lijsten met uitsluitingen en vertrouwde programma's maken naast de algemene vertrouwde zone in een beleid.

## Een scanuitzondering aanmaken

Een *scanuitzondering* is een reeks voorwaarden waaraan moet worden voldaan zodat een bepaald object niet door Kaspersky Endpoint Security wordt gescand op virussen en andere dreigingen.

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 dit soort programma's door indringers worden gebruikt als een hulpmiddel. Voor informatie over legitieme software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen, raadpleegt u de [website van de IT-encyclopedie van Kaspersky](#).<sup>[2]</sup>

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 IT-encyclopedie van Kaspersky toe aan de vertrouwde zone. Voorbeeld: u gebruikt vaak het Radmin-programma voor het externe beheer van computers. 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 IT-encyclopedie van Kaspersky voorkomt.

Als een programma dat informatie verzamelt en deze ter verwerking verstuurt op uw computer is geïnstalleerd, kan Kaspersky Endpoint Security dit programma classificeren als malware. 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:

- [Gedragsdetectie](#).
- [Exploit-preventie](#).
- [Host Intrusion Prevention](#).
- [File Threat Protection](#).
- [Web Threat Protection](#).
- [Mail Threat Protection](#).
- [Scantaken](#).

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.

[Een scanuitzondering maken in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Exclusions** in het beleidsvenster.
6. Klik in het venster **Scanuitzonderingen en vertrouwde programma's** op de knop **instellingen**.
7. Selecteer in het geopende venster het tabblad **Scanuitzonderingen**.  
Met een klik op deze koppeling opent u een venster waarin u een lijst met uitzonderingen vindt.
8. Schakel het selectievakje **Merge values when inheriting** in als u een geconsolideerde lijst met uitzonderingen voor alle computers in het bedrijf wilt maken. De lijsten met uitzonderingen in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Uitzonderingen van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Uitzonderingen van het bovenliggende beleid wijzigen of verwijderen is niet mogelijk.
9. Schakel het selectievakje **Allow use of local trusted applications** in als u wilt dat de gebruiker een lokale lijst met uitzonderingen kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met uitzonderingen maken naast de algemene lijst met uitzonderingen die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.  
Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met uitzonderingen die in het beleid is gegenereerd.
10. Klik op **Toevoegen**.
11. Zo stelt u in dat een bestand of een map niet moet worden gescand:
  - a. Schakel in het blok **Eigenschappen** het selectievakje **Bestand of map** in.
  - b. Klik op de link **Bestand of map selecteren** in het blok **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** 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.  
Gebruik maskers:
    - Het teken **\*** (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens **\** en **/** (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker **C:\\*\\*.txt** omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
    - Twee opeenvolgende sterretjes **\*\*** stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens **\** en **/** (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker **C:\Map\\*\*\\*.txt** omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in



de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker `C:\**\*.txt` is geen geldig masker.

- Het teken `?` (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Voorbeeld` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

d. Sla uw wijzigingen op.

12. Zo stelt u in dat objecten met een specifieke naam niet moeten worden gescand:

a. Schakel in het blok **Eigenschappen** het selectievakje **Objectnaam** in.

b. Klik op de koppeling **Voer objectnaam in** in het blok **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** om het venster **Objectnaam** te openen.

c. Voer de naam van het object in volgens de classificatie van de [encyclopedie van Kaspersky](#) (bijvoorbeeld `E-mailworm`, `Rootkit` of `RemoteAdmin`).

U kunt maskers gebruiken met het teken `?` (vervangt een willekeurig teken) en het teken `*` (vervangt een willekeurig aantal tekens). Als bijvoorbeeld het `Client *`-masker is opgegeven, sluit Kaspersky Endpoint Security `Client-IRC-`, `Client-P2P-` en `Client-SMTP-` objecten uit van scans.

d. Sla uw wijzigingen op.

13. Als u een afzonderlijk bestand van scans wilt uitsluiten:

a. Schakel in het blok **Eigenschappen** het selectievakje **Objecthash** in.

b. Klik op de object-hash-invoerlink om het **Object-hash**-venster te openen.

c. Voer de bestandshash in of selecteer het bestand door op de knop **Bladeren** te klikken.

Als het bestand is gewijzigd, wordt de bestandshash van het bestand ook gewijzigd. Als dit gebeurt, wordt het gewijzigde bestand niet toegevoegd aan uitsluitingen.

d. Sla uw wijzigingen op.

14. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

15. Geef de onderdelen van Kaspersky Endpoint Security op die de scanuitzondering moeten gebruiken:

a. Klik op **een** koppeling in het blok **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** 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. Sla uw wijzigingen op.

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.

16. U kunt het selectievakje gebruiken [om een uitsluiting](#) op elk moment te [stoppen](#).

17. Sla uw wijzigingen op.

[Een scanuitzondering maken in de webconsole en de cloudconsole](#) 


1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **General settings** → **Exclusions**.
5. Klik in het blok **Scan exclusions and trusted applications** op de koppeling **Scan exclusions**.
6. Schakel het selectievakje **Merge values when inheriting** in als u een geconsolideerde lijst met uitzonderingen voor alle computers in het bedrijf wilt maken. De lijsten met uitzonderingen in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Uitzonderingen van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Uitzonderingen van het bovenliggende beleid wijzigen of verwijderen is niet mogelijk.
7. Schakel het selectievakje **Allow use of local trusted applications** in als u wilt dat de gebruiker een lokale lijst met uitzonderingen kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met uitzonderingen maken naast de algemene lijst met uitzonderingen die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.  
  
Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met uitzonderingen die in het beleid is gegenereerd.
8. Klik op de knop **Add**.
9. Selecteer hoe u de uitzondering wil toevoegen: **File or folder**, **Object name** of **Object hash**.
10. Als u een bestand of map van scans wilt uitsluiten, selecteert u het bestand of de map door op de knop **Browse** te klikken.  
  
U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens \* en ? bij de invoer van een masker.
  - Het teken \* (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
  - Twee opeenvolgende sterretjes \*\* stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Map\\*\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker C:\\*\*\\*.txt is geen geldig masker.
  - Het teken ? (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
11. Als u een bepaald type object van scans wilt uitsluiten, voert u in het veld **Object name** de naam van het objecttype in volgens de classificatie van de [encyclopedie van Kaspersky](#) (bijvoorbeeld **Email-Worm**,

Rootkit of RemoteAdmin).

U kunt maskers gebruiken met het teken ? (vervangt een willekeurig teken) en het teken \* (vervangt een willekeurig aantal tekens). Als bijvoorbeeld het Client \*-masker is opgegeven, sluit Kaspersky Endpoint Security Client-IRC- , Client-P2P- en Client-SMTP- objecten uit van scans.

12. Als u een afzonderlijk bestand van scans wilt uitsluiten, voert u de bestandshash in het veld **Object hash** in. Als het bestand is gewijzigd, wordt de bestandshash van het bestand ook gewijzigd. Als dit gebeurt, wordt het gewijzigde bestand niet toegevoegd aan uitsluitingen.
13. Selecteer in het blok **Protection components** de componenten waarop u de scanuitzondering wilt toepassen.
14. Typ indien nodig in het veld **Comment** een korte opmerking over de scanuitzondering die u maakt.
15. U kunt de schakelaar gebruiken [om een uitzondering](#) op elk moment te [stoppen](#).
16. Sla uw wijzigingen op.

[Een scanuitzondering maken in de programma-interface](#) 

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.
4. Klik op **Toevoegen**.
5. Als u een bestand of map van scans wilt uitsluiten, selecteert u het bestand of de map door op de knop **Bladeren** te klikken.

U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens \* en ? bij de invoer van een masker.

- Het teken \* (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes \*\* stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Map\\*\*\\*.txt omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de Map, uitgezonderd de Map zelf. Het masker moet ten minste één genest niveau bevatten. Het masker C:\\*\*\\*.txt is geen geldig masker.
- Het teken ? (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens \ en / (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

6. Als u een bepaald type object van scans wilt uitsluiten, voert u in het veld **Object** de naam van het objecttype in volgens de classificatie van de [encyclopedie van Kaspersky](#) (bijvoorbeeld **Email-Worm**, **Rootkit** of **RemoteAdmin**).

U kunt maskers gebruiken met het teken ? (vervangt een willekeurig teken) en het teken \* (vervangt een willekeurig aantal tekens). Als bijvoorbeeld het Client \*-masker is opgegeven, sluit Kaspersky Endpoint Security Client-IRC-, Client-P2P- en Client-SMTP- objecten uit van scans.

7. Als u een afzonderlijk bestand van scans wilt uitsluiten, voert u de bestandshash in het veld **Objecthash** in. Als het bestand is gewijzigd, wordt de bestandshash van het bestand ook gewijzigd. Als dit gebeurt, wordt het gewijzigde bestand niet toegevoegd aan uitsluitingen.

8. Selecteer in het blok **Protection components** de componenten waarop u de scanuitzondering wilt toepassen.

9. Typ indien nodig in het veld **Comment** een korte opmerking over de scanuitzondering die u maakt.

10. Selecteer de status **Actief** voor de uitzondering.

U kunt de schakelaar gebruiken [om een uitzondering](#) op elk moment te [stoppen](#).

11. Sla uw wijzigingen op.

Paden naar bestanden in een willekeurige map:

- Het masker `*.exe` omvat alle paden naar bestanden met de EXE-extensie.
- Het masker `voorbeeld*` omvat alle paden naar bestanden met de naam VOORBEELD.

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\ inclusief submappen van C:\dir\.
- Het masker `C:\dir\` omvat alle paden naar bestanden in de map C:\dir\ inclusief submappen.
- 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.

## Een scanuitzondering inschakelen en uitschakelen



*Zo schakelt u een scanuitzondering in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

4. Selecteer de gewenste uitzondering in de lijst met scanuitzonderingen.
5. Gebruik de schakelaar naast een object om dit object op te nemen in het scanbereik of om het uit te sluiten.
6. Sla uw wijzigingen op.

## Soorten detecteerbare objecten selecteren

*Zo selecteert u soorten detecteerbare objecten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Schakel in het gedeelte **Soorten gedetecteerde objecten** de selectievakjes in naast de soorten objecten die Kaspersky Endpoint Security moet detecteren:
  - [Virussen en wormen](#) ;

**Subcategorie:** virussen en wormen (Virussen\_en\_Wormen)

**Veiligheidsrisico:** hoog

Klassieke virussen en wormen voeren acties uit die niet door de gebruiker zijn toegestaan. Ze kunnen kopieën van zichzelf maken die zichzelf kunnen repliceren.

### Klassiek virus

Wanneer een klassiek virus de computer binnendringt, infecteert het een bestand, wordt het actief, voert het schadelijke acties uit en voegt het kopieën van zichzelf toe aan andere bestanden.

Een klassiek virus vermenigvuldigt zich alleen in lokale bronnen van de computer; het kan zelf geen andere computers binnendringen. Het kan alleen op een andere computer terechtkomen als het een kopie van zichzelf toevoegt aan een bestand dat in een gedeelde map of op een geplaatste cd is opgeslagen of als de gebruiker een e-mailbericht met een geïnfecteerd bestand als bijlage doorstuurt.

Klassieke viruscode kan diverse delen van computers, besturingssystemen en programma's binnendringen. Afhankelijk van de omgeving worden virussen verdeeld in *bestandsvirussen*, *opstartvirussen*, *scriptvirussen* en *macrovirussen*.

Virussen kunnen bestanden infecteren door middel van diverse technieken. *Overschrijvende* virussen schrijven hun code over de licentie van het bestand dat wordt geïnfecteerd, waardoor de inhoud van het bestand wordt gewist. Het geïnfecteerde bestand werkt niet meer en kan niet worden hersteld. *Parasitaire* virussen wijzigen bestanden waardoor ze volledig of deels functioneel blijven. *Aanvullende virussen* wijzigen geen bestanden maar maken duplicaten. Wanneer een geïnfecteerd bestand wordt geopend, wordt een duplicaat ervan (wat eigenlijk een virus is) gemaakt. De volgende soorten virussen komen ook voor: *gekoppelde virussen*, *OBJ-virussen*, *LIB-virussen*, *broncodevirussen* en vele andere.

### Worm

Net als bij een klassiek virus wordt de code van een worm geactiveerd en voert deze schadelijke acties uit nadat deze een computer is binnengedrongen. Wormen hebben hun naam gekregen vanwege hun mogelijkheid om van de ene computer naar de andere te "kruipen" en kopieën via talrijke gegevenskanalen te verspreiden zonder toestemming van de gebruiker.

Wormen onderscheiden zich vooral van elkaar door de wijze waarop ze zich verspreiden. In de volgende tabel ziet u een overzicht van diverse soorten wormen die zijn geclassificeerd volgens de wijze waarop ze zich verspreiden.

Wijzen waarop wormen zich verspreiden

| Type       | Naam                   | Beschrijving   |
|------------|------------------------|--|
| E-mailworm | E-mailworm             | Deze verspreiden zich via e-mail.<br>Een geïnfecteerd e-mailbericht bevat een bijlage met een kopie van een worm of een koppeling naar een bestand dat is geüpload naar een website die mogelijk gehackt is of speciaal voor dat doel is gemaakt. Wanneer u de bijlage opent, wordt de worm geactiveerd. Wanneer u op de koppeling klikt en vervolgens het bestand downloadt en opent, begint de worm ook schadelijke acties uit te voeren. Daarna verspreidt de worm kopieën van zichzelf, zoekt die andere e-mailadressen en verstuurt die geïnfecteerde berichten ernaar. |
| IM-Worm    | Wormen voor IM-clients | Deze verspreiden zich via instant messengers.  |



|                 |                                   |  |
|-----------------|-----------------------------------|--|
|                 |                                   | Doorgaans gebruiken zulke wormen de lijst met contactpersonen van de gebruiker om berichten met een koppeling naar een bestand met een kopie van de worm op een website te versturen. Als de gebruiker het bestand downloadt en opent, wordt de worm geactiveerd.  |
| <b>IRC-Worm</b> | Online chatwormen                 | Deze verspreiden zich via Internet Relay Chats, servicesystemen waarmee mensen met elkaar kunnen communiceren in real time via het internet.<br><br>Deze wormen publiceren een bestand met een kopie van zichzelf of een kopie naar het bestand in een chat. Als de gebruiker het bestand downloadt en opent, wordt de worm geactiveerd.   |
| <b>Net-worm</b> | Netwerkwormen                     | Deze wormen verspreiden zich via computernetwerken.<br><br>In tegenstelling tot andere wormen kan een normale netwerkworm zich verspreiden zonder hulp van de gebruiker. De worm zoekt in het lokale netwerk naar computers die programma's met kwetsbaarheden bevatten. Hiertoe stuurt de worm een speciaal netwerkpakket (exploit) dat de wormcode of een deel ervan bevat. Als er een 'kwetsbare' computer in het netwerk is, ontvangt die computer zo'n netwerkpakket. Wanneer de worm de computer volledig is binnengedrongen, activeert die zichzelf.  |
| <b>P2P-worm</b> | Netwerkwormen voor bestandsdeling | Deze verspreiden zich via peer-to-peernetwerken voor bestandsdeling.<br><br>Om een P2P-netwerk te infiltreren, kopieert de worm zichzelf naar een map voor bestandsdeling die doorgaans op de computer van de gebruiker staat. Het P2P-netwerk toont informatie over dit bestand zodat de gebruiker het geïnfecteerde bestand in het netwerk kan "vinden", zoals andere bestanden, en het bestand vervolgens kan downloaden en openen.<br><br>Meer geavanceerde wormen emuleren het netwerkprotocol van een specifiek P2P-netwerk: ze geven positieve antwoorden op zoekopdrachten en bieden kopieën van zichzelf aan die de gebruiker dan kan downloaden.   |
| <b>Worm</b>     | Andere soorten wormen             | Enkele andere soorten wormen zijn: <ul style="list-style-type: none"> <li>• Wormen die kopieën van zichzelf verspreiden via netwerkbronnen. Met behulp van de functies van het besturingssysteem zoeken ze beschikbare netwerkmappen, maken ze verbinding met computers via het internet en proberen ze volledige toegang tot hun stations te krijgen. In tegenstelling tot de eerder beschreven wormen kunnen andere soorten wormen zichzelf niet activeren en moet de gebruiker een bestand met een kopie van de worm openen om de worm te activeren.</li> <li>• Wormen die een andere methode dan de methoden in de eerdere tabel gebruiken om zich te verspreiden (bijvoorbeeld wormen die zich verspreiden via mobiele telefoons).</li> </ul> |

- [Trojans \(inclusief ransomware\)](#)<sup>2</sup>:

## Subcategorie: Trojans

**Veiligheidsrisico:** hoog

In tegenstelling tot wormen en virussen kunnen Trojans zich niet zelf repliceren. Ze dringen bijvoorbeeld de computer binnen via e-mail of een browser wanneer de gebruiker een geïnfecteerde webpagina bezoekt. Trojans worden met de hulp van de gebruiker gestart. Net nadat ze zijn gestart, beginnen ze schadelijke acties uit te voeren.

Verschillende Trojans gedragen zich anders op geïnfecteerde computers. De belangrijkste functies van Trojans zijn het blokkeren, wijzigen of vernietigen van gegevens en het uitschakelen van computers of netwerken. Trojans kunnen ook bestanden ontvangen of versturen, bestanden uitvoeren, berichten op het scherm weergeven, webpagina's opvragen, programma's downloaden en installeren en de computer opnieuw opstarten.

Hackers gebruiken vaak "sets" van verschillende Trojans.

In de volgende tabel leest u hoe Trojans zich kunnen gedragen.

Gedrag van Trojans op een geïnfecteerde computer

| Type                  | Naam                       | Beschrijving  |
|-----------------------|----------------------------|---|
| <b>Trojan-ArcBomb</b> | Trojans – "archiefbommen"  | Tijdens het uitpakken worden deze archieven zo groot dat de werking van de computer wordt beïnvloed.<br><br>Als de gebruiker zo'n archief probeert uit te pakken, kan de computer vertragen of geblokkeerd raken. De harde schijf wordt gevuld met "lege" gegevens. "Archiefbommen" zijn in het bijzonder gevaarlijk voor bestands- en mailservers. Als de server een automatisch systeem voor de verwerking van inkomende gegevens gebruikt, kan de "archiefbom" de server laten crashen.  |
| <b>Backdoor</b>       | Trojans voor extern beheer | Deze worden beschouwd als de gevaarlijkste soort Trojan. Hun werking is vergelijkbaar met programma's voor extern beheer die op computers zijn geïnstalleerd.<br><br>Deze programma's installeren zichzelf ongemerkt op de computer, waardoor de indringer de computer op afstand kan beheren.  |
| <b>Trojan</b>         | Trojans                    | Deze omvatten de volgende schadelijke programma's: <ul style="list-style-type: none"><li>• <b>Klassieke Trojans.</b> Deze programma's voeren alleen de voornaamste functies van Trojans uit: gegevens blokkeren, wijzigen of vernietigen en computers of netwerken uitschakelen. In tegenstelling tot de andere soorten Trojans die in de tabel zijn beschreven, hebben ze geen geavanceerde functies.</li><li>• <b>Veelzijdige Trojans.</b> Deze programma's hebben geavanceerde functies die kenmerken zijn voor diverse soorten Trojans.</li></ul> |
| <b>Trojan-Ransom</b>  | Trojans voor losgeld       | Ze "gijzelen" de gegevens van de gebruiker, wijzigen of blokkeren ze of beïnvloeden de werking van de computer zodanig dat de gebruiker geen gegevens kan gebruiken. De indringer vraagt een geldsom aan de gebruiker in ruil voor een programma waarmee de werking van de computer en de   |

|                          |   |   |
|--------------------------|---|---|
|                          |   | toegang tot de gegevens op de computer kan worden hersteld.   |
| <b>Trojan-Clicker</b>    | Trojan clickers                           | <p>Deze openen webpagina's vanaf de computer van de gebruiker door zelf opdrachten naar een browser te sturen of door de opgegeven webadressen in de bestanden van het besturingssysteem te wijzigen.</p> <p>Met behulp van deze programma's voeren indringers netwerkaanvallen uit en verhogen ze bezoeken aan websites om zo het aantal weergaven van banners te verhogen.</p>  |
| <b>Trojan-Downloader</b> | Trojan downloaders                        | <p>Deze gaan naar de webpagina van de indringer, downloaden andere schadelijke programma's vanaf de webpagina en installeren de programma's op de computer van de gebruiker. Mogelijk bevatten ze de bestandsnaam van het schadelijke programma dat wordt gedownload of ontvangen ze die vanaf de bezochte webpagina.</p>   |
| <b>Trojan-Dropper</b>    | Trojan droppers                           | <p>Deze bevatten andere Trojans die ze op de harde schijf plaatsen en vervolgens installeren.</p> <p>Indringers kunnen programma's van het type Trojan Dropper gebruiken voor het volgende:</p> <ul style="list-style-type: none"> <li>• Een schadelijk programma ongemerkt installeren: programma's van het type Trojan Dropper geven geen berichten weer of geven valse berichten weer met meldingen over bijvoorbeeld een fout in een archief of een incompatibele versie van het besturingssysteem.</li> <li>• De detectie van een ander schadelijk programma voorkomen: niet alle antivirussoftware kan een schadelijk programma in een programma van het type Trojan Dropper detecteren.</li> </ul> |
| <b>Trojan-Notifier</b>   | Trojan notifiers                          | <p>Deze melden een indringer dat de geïnfecteerde computer toegankelijk is door informatie over de computer te versturen naar de indringer: IP-adres, nummer van geopende poort of e-mailadres. Ze maken verbinding met de indringer via e-mail of FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.</p> <p>Programma's van het type Trojan Notifier worden vaak gebruikt in sets die uit meerdere Trojans bestaan. Ze melden de indringer dat andere Trojans met succes zijn geïnstalleerd op de computer van de gebruiker.</p>   |
| <b>Trojan-Proxy</b>      | Trojan-proxy's                            | <p>Deze geven de indringer de mogelijkheid om webpagina's anoniem te bezoeken met de computer van de gebruiker. Ze worden vaak gebruikt voor het versturen van spam.</p>  |
| <b>Trojan-PSW</b>        | Software voor het stelen van wachtwoorden | <p>PSW is een soort Trojan die gebruikersaccounts steelt, zoals registratiegegevens van software. Deze Trojans vinden vertrouwelijke gegevens in systeembestanden en het register en versturen die naar de "aanvaller" per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.</p>   |

|                         |   |  |
|-------------------------|---|--|
|                         |   | Sommige van deze Trojans zijn afzonderlijk gecategoriseerd per type zoals in deze tabel is beschreven. Deze zijn Trojans die gegevens van bankrekeningen stelen (Trojan-Banker), gegevens van gebruikers van instant messengers (Trojan-IM), en gegevens van gebruikers van online games (Trojan-GameThief).   |
| <b>Trojan-Spy</b>       | Trojan-spionnen   | Deze bespioneren de gebruiker door informatie te verzamelen over de acties van de gebruiker terwijl die met de computer werkt. Ze kunnen de gegevens die de gebruiker invoert met het toetsenbord onderscheppen, schermafbeeldingen maken of lijsten met actieve programma's verzamelen. Nadat ze de informatie hebben ontvangen, versturen ze die naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Trojan-DDoS</b>      | Trojan-netwerkaanvallers  | Deze versturen een groot aantal verzoeken van de computer van de gebruiker naar een externe server. De server heeft onvoldoende bronnen om alle verzoeken te verwerken en stopt met werken (Denial of Service, of kortom DoS). Hackers infecteren vaak veel computers met deze programma's zodat ze de computers kunnen gebruiken om een enkele server tegelijk aan te vallen.<br><br>DoS-programma's voeren een aanval uit vanaf een enkele computer met het medeweten van de gebruiker. DDoS-programma's (Distributed DoS) voeren gedistribueerde aanvallen uit vanaf verschillende computers zonder dat de gebruiker van de geïnfecteerde computer dit opmerkt. |
| <b>Trojan-IM</b>        | Trojans die gegevens van gebruikers van Instant messengers stelen | Deze stelen accountnummers en wachtwoorden van gebruikers van instant messengers. Ze versturen de gegevens naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Rootkit</b>          | Rootkits  | Deze maskeren andere schadelijke programma's en hun activiteit waardoor de programma's langer in het besturingssysteem aanwezig blijven. Ze kunnen ook bestanden, processen in het geheugen van een geïnfecteerde computer of registersleutels verbergen die schadelijke programma's uitvoeren. De rootkits kunnen een gegevensoverdracht tussen programma's op de computer van de gebruiker en andere computers in het netwerk maskeren.  |
| <b>Trojan-SMS</b>       | Trojans in de vorm van sms-berichten                              | Deze infecteren mobiele telefoons door sms-berichten naar betalende telefoonnummers te versturen.  |
| <b>Trojan-GameThief</b> | Trojans die gegevens van gebruikers van online games stelen       | Deze stelen accountgegevens van gebruikers van online games, waarna ze de gegevens naar de indringer versturen per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Trojan-Banker</b>    | Trojans die gegevens van bankrekeningen stelen                    | Deze stelen gegevens van bankrekeningen of e-money-systeemgegevens en sturen die dan naar de hacker per e-mail, via FTP, met een bezoek aan de webpagina van de hacker of op een andere manier.  |
|                         |   |  |

|                          |                                       |   |
|--------------------------|---------------------------------------|---|
| <b>Trojan-Mailfinder</b> | Trojans die e-mailadressen verzamelen | Deze verzamelen e-mailadressen die op een computer zijn opgeslagen en versturen ze naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier. Indringers kunnen spam naar de verzamelde adressen versturen. |
|--------------------------|---------------------------------------|---|

- [Schadelijke tools](#) 

**Subcategorie:** schadelijke tools

**Veiligheidsrisico:** gemiddeld

In tegenstelling tot andere soorten malware voeren schadelijke tools hun acties niet direct na hun start uit. Ze kunnen veilig worden opgeslagen en gestart op de computer van de gebruiker. Indringers gebruiken vaak de functies van deze programma's om virussen, wormen en Trojans te maken, netwerkaanvallen op externe servers uit te voeren, computers te hacken of andere schadelijke acties uit te voeren.

Diverse functies van schadelijke tools zijn gegroepeerd op type en worden in de volgende tabel beschreven.

Functies van schadelijke tools

| Type                | Naam                 | Beschrijving  |
|---------------------|----------------------|---|
| <b>Constructeur</b> | Constructeurs        | Hiermee kunnen nieuwe virussen, wormen en Trojans worden gemaakt. Bepaalde constructeurs hebben een standaardinterface met vensters waarin de gebruiker kan kiezen welk type schadelijk programma moet worden gemaakt, hoe debuggers moeten worden tegengegaan, en andere functies.   |
| <b>Dos</b>          | Netwerkaanvallen     | Deze versturen een groot aantal verzoeken van de computer van de gebruiker naar een externe server. De server heeft onvoldoende bronnen om alle verzoeken te verwerken en stopt met werken (Denial of Service, of kortom DoS).  |
| <b>Exploit</b>      | Exploits             | <p>Een <i>exploit</i> is een reeks gegevens of een programmalicentie die kwetsbaarheden van het programma waarin deze wordt verwerkt gebruikt om een schadelijke actie op een computer uit te voeren. Een exploit kan bijvoorbeeld bestanden schrijven of lezen of "geïnfecteerde" webpagina's opvragen.</p> <p>Verschillende exploits gebruiken kwetsbaarheden in verschillende programma's of netwerkservices. Vermomd als een netwerkpakket wordt een exploit via het netwerk verstuurd naar heel veel computers, op zoek naar computers met kwetsbare netwerkservices. Een exploit in een DOC-bestand gebruikt de kwetsbaarheden van een teksteditor. Deze kan de acties beginnen uitvoeren die door de hacker vooraf zijn geprogrammeerd wanneer de gebruiker het geïnfecteerde bestand opent. Een exploit die is ingebed in een e-mailbericht zoekt naar kwetsbaarheden in een e-mailprogramma. Deze kan een schadelijke actie beginnen uitvoeren zodra de gebruiker het geïnfecteerde bericht in dit e-mailprogramma opent.</p> <p>Net-Worms verspreiden zich via netwerken door middel van exploits. Nuker exploits zijn netwerkpakketten die computers uitschakelen.</p> |
| <b>FileCryptor</b>  | Encryptors           | Deze encrypten andere schadelijke programma's om ze te verbergen voor het antivirusprogramma.   |
| <b>Flooder</b>      | Programma's voor het | Deze versturen een groot aantal berichten via netwerkkanalen. Dit type tools omvat bijvoorbeeld programma's die Internet Relay Chats besmetten.   |

|                      |  |   |
|----------------------|--|---|
|                      | besmetten van "netwerken"                                      | Tools van het type Flooder zijn geen programma's die kanalen "besmetten" die door e-mail, instant messengers en mobiele communicatiesystemen worden gebruikt. Deze programma's worden beschouwd als afzonderlijke types die in de tabel worden beschreven (Email-Flooder, IM-Flooder en SMS-Flooder).   |
| <b>HackTool</b>      | Tools om te hacken   | Deze maken het mogelijk om de computer waarop ze zijn geïnstalleerd te hacken of om een andere computer aan te vallen (bijvoorbeeld door nieuwe systeemaccounts toe te voegen zonder de toestemming van de gebruiker of door systeemlogboeken te wissen om sporen van hun aanwezigheid in het besturingssysteem te verbergen). Dit type tools omvat bepaalde sniffers die schadelijke functies hebben, zoals het onderscheppen van wachtwoorden. Sniffers zijn programma's waarmee netwerkverkeer kan worden bekeken. |
| <b>Hoax</b>          | Hoaxes   | Deze alarmeren de gebruiker met virusachtige berichten: ze kunnen "een virus detecteren" in een niet-geïnfecteerd bestand of de gebruiker melden dat de schijf is geformatteerd hoewel dit niet het geval is.   |
| <b>Spoofers</b>      | Tools voor vervalsing  | Deze versturen berichten en netwerkaanvragen met een vals adres van de zender. Indringers gebruiken tools van het type Spoofer om zich bijvoorbeeld voor te doen als de echte afzender van berichten.   |
| <b>VirTool</b>       | Tools die schadelijke programma's aanpassen                    | Deze kunnen worden gebruikt om malware aan te passen en ze te verbergen voor antivirusprogramma's.  |
| <b>Email-Flooder</b> | Programma's die e-mailadressen "besmetten"                     | Deze versturen een groot aantal berichten naar diverse e-mailadressen, waardoor ze "besmet raken". Een groot aantal inkomende berichten belet dat gebruikers de gewenste berichten in hun postvakken zien.  |
| <b>IM-Flooder</b>    | Programma's die het verkeer van instant messengers "besmetten" | Deze overspoelen gebruikers van instant messengers met berichten. Een groot aantal berichten belet dat gebruikers de gewenste inkomende berichten zien.   |
| <b>SMS-Flooder</b>   | Programma's die het verkeer van sms-berichten "besmetten"      | Deze versturen een groot aantal sms-berichten naar mobiele telefoons.   |

- [Adware](#) 

**Subcategorie:** software voor advertenties (Adware);

**Veiligheidsrisico:** gemiddeld

Adware toont advertenties aan de gebruiker. Adwareprogramma's tonen banners in de interfaces van andere programma's en verwijzen zoekopdrachten door naar webpagina's met advertenties. Sommige ervan verzamelen marketinginformatie over de gebruiker en versturen die naar de ontwikkelaar: deze informatie bevat mogelijk de namen van de websites die de gebruiker bezocht of de inhoud van de zoekopdrachten van de gebruiker. In tegenstelling tot programma's van het type Trojan-Spy stuurt adware deze informatie naar de ontwikkelaar met de toestemming van de gebruiker.

- [Automatische inbelprogramma's](#) 



**Subcategorie:** legitieme software die criminelen kunnen gebruiken om uw computer of persoonlijke gegevens te beschadigen.

**Veiligheidsrisico:** gemiddeld

De meeste van deze programma's zijn nuttig, waardoor veel gebruikers ze hebben. Deze programma's zijn onder andere IRC-clients, automatische inbelprogramma's, programma's om bestanden te downloaden, monitors voor de systeemactiviteit, hulpprogramma's voor wachtwoorden en internetserver voor FTP, HTTP en Telnet.

Als indringers echter toegang tot deze programma's krijgen of als ze die programma's op de computer van de gebruiker plaatsen, kunnen bepaalde functies van de programma's worden gebruikt om de beveiliging aan te tasten.

Deze programma's verschillen naargelang functie. De verschillende types worden in de onderstaande tabel beschreven.

| Type                | Naam                                      | Beschrijving   |
|---------------------|---|--|
| <b>Client-IRC</b>   | Online chatprogramma's                    | Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.   |
| <b>Inbeller</b>     | Automatische inbelprogramma's             | Deze kunnen verborgen verbindingen via een telefoonmodem tot stand brengen.  |
| <b>Downloader</b>   | Programma's voor downloads                | Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.   |
| <b>Monitor</b>      | Programma's voor monitoring               | Hiermee kan de activiteit op de computer waarop ze zijn geïnstalleerd worden gemonitord (zien welke programma's actief zijn en hoe ze gegevens met geïnstalleerde programma's op andere computers uitwisselen).  |
| <b>PSWTool</b>      | Programma's om wachtwoorden te herstellen | Hiermee kunnen wachtwoorden worden bekeken en vergeten wachtwoorden worden hersteld. Indringers plaatsen ze ongemerkt op computers van gebruikers met hetzelfde doel.  |
| <b>RemoteAdmin</b>  | Programma's voor extern beheer            | Deze worden veel gebruikt door systeembeheerders. Met deze programma's kan toegang tot de interface van een externe computer worden verkregen om die computer te monitoren en te beheren. Indringers plaatsen ze in het geheim op computers van gebruikers met hetzelfde doel: externe computers monitoren en beheren.<br><br>Legitieme programma's voor extern beheer verschillen van Trojans van het type Backdoor voor extern beheer. Trojans kunnen het besturingssysteem zelfstandig binnendringen en zichzelf installeren terwijl legitieme programma's dit niet kunnen. |
| <b>Server-FTP</b>   | FTP-servers                               | Deze werken als FTP-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via FTP.   |
| <b>Server-Proxy</b> | Proxyservers                              | Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.  |

|                      |   |  |
|----------------------|---|--|
| <b>Server-Telnet</b> | Telnet-servers                            | Deze werken als Telnet-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via Telnet.   |
| <b>Server-Web</b>    | Webservers                                | Deze werken als web servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.  |
| <b>RiskTool</b>      | Tools om op een lokale computer te werken | Deze geven de gebruiker extra opties wanneer die aan de computer van de gebruiker zelf zit. De gebruiker kan de tool gebruiken om bestanden of vensters van actieve programma's te verbergen en om actieve processen te beëindigen.                                    |
| <b>NetTool</b>       | Netwerkprogramma's                        | Deze geven de gebruiker extra opties tijdens het werken met andere computers in het netwerk. Met deze tools kunnen de computers opnieuw worden opgestart, kunnen open poorten worden gedetecteerd en kunnen geïnstalleerde programma's op de computers worden gestart. |
| <b>Client-P2P</b>    | P2P-netwerkprogramma's                    | Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.  |
| <b>Client-SMTP</b>   | SMTP-clients                              | Deze versturen e-mailberichten zonder medeweten van de gebruiker. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.  |
| <b>WebToolbar</b>    | Online werkbalken                         | Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.   |
| <b>FraudTool</b>     | Pseudoprogramma's                         | Deze doen zichzelf voor als andere programma's. Er zijn bijvoorbeeld pseudo-antivirusprogramma's die berichten over gevonden malware weergeven. In werkelijkheid vinden of desinfecteren deze programma's niets.   |

- [Detecteer andere software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen](#) 

**Subcategorie:** legitieme software die criminelen kunnen gebruiken om uw computer of persoonlijke gegevens te beschadigen.

**Veiligheidsrisico:** gemiddeld

De meeste van deze programma's zijn nuttig, waardoor veel gebruikers ze hebben. Deze programma's zijn onder andere IRC-clients, automatische inbelprogramma's, programma's om bestanden te downloaden, monitors voor de systeemactiviteit, hulpprogramma's voor wachtwoorden en internetserver voor FTP, HTTP en Telnet.

Als indringers echter toegang tot deze programma's krijgen of als ze die programma's op de computer van de gebruiker plaatsen, kunnen bepaalde functies van de programma's worden gebruikt om de beveiliging aan te tasten.

Deze programma's verschillen naargelang functie. De verschillende types worden in de onderstaande tabel beschreven.

| Type                | Naam                                      | Beschrijving   |
|---------------------|---|--|
| <b>Client-IRC</b>   | Online chatprogramma's                    | Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.   |
| <b>Inbeller</b>     | Automatische inbelprogramma's             | Deze kunnen verborgen verbindingen via een telefoonmodem tot stand brengen.  |
| <b>Downloader</b>   | Programma's voor downloads                | Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.   |
| <b>Monitor</b>      | Programma's voor monitoring               | Hiermee kan de activiteit op de computer waarop ze zijn geïnstalleerd worden gemonitord (zien welke programma's actief zijn en hoe ze gegevens met geïnstalleerde programma's op andere computers uitwisselen).  |
| <b>PSWTool</b>      | Programma's om wachtwoorden te herstellen | Hiermee kunnen wachtwoorden worden bekeken en vergeten wachtwoorden worden hersteld. Indringers plaatsen ze ongemerkt op computers van gebruikers met hetzelfde doel.  |
| <b>RemoteAdmin</b>  | Programma's voor extern beheer            | Deze worden veel gebruikt door systeembeheerders. Met deze programma's kan toegang tot de interface van een externe computer worden verkregen om die computer te monitoren en te beheren. Indringers plaatsen ze in het geheim op computers van gebruikers met hetzelfde doel: externe computers monitoren en beheren.<br><br>Legitieme programma's voor extern beheer verschillen van Trojans van het type Backdoor voor extern beheer. Trojans kunnen het besturingssysteem zelfstandig binnendringen en zichzelf installeren terwijl legitieme programma's dit niet kunnen. |
| <b>Server-FTP</b>   | FTP-servers                               | Deze werken als FTP-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via FTP.   |
| <b>Server-Proxy</b> | Proxyservers                              | Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.  |

|                      |   |  |
|----------------------|---|--|
| <b>Server-Telnet</b> | Telnet-servers                            | Deze werken als Telnet-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via Telnet.   |
| <b>Server-Web</b>    | Webservers                                | Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.   |
| <b>RiskTool</b>      | Tools om op een lokale computer te werken | Deze geven de gebruiker extra opties wanneer die aan de computer van de gebruiker zelf zit. De gebruiker kan de tool gebruiken om bestanden of vensters van actieve programma's te verbergen en om actieve processen te beëindigen.                                    |
| <b>NetTool</b>       | Netwerkprogramma's                        | Deze geven de gebruiker extra opties tijdens het werken met andere computers in het netwerk. Met deze tools kunnen de computers opnieuw worden opgestart, kunnen open poorten worden gedetecteerd en kunnen geïnstalleerde programma's op de computers worden gestart. |
| <b>Client-P2P</b>    | P2P-netwerkprogramma's                    | Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.  |
| <b>Client-SMTP</b>   | SMTP-clients                              | Deze versturen e-mailberichten zonder medeweten van de gebruiker. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.  |
| <b>WebToolbar</b>    | Online werkbalken                         | Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.   |
| <b>FraudTool</b>     | Pseudoprogramma's                         | Deze doen zichzelf voor als andere programma's. Er zijn bijvoorbeeld pseudo-antivirusprogramma's die berichten over gevonden malware weergeven. In werkelijkheid vinden of desinfecteren deze programma's niets.   |

- [Objecten die mogelijk zijn gecomprimeerd om schadelijke code te beschermen](#) [2];

Kaspersky Endpoint Security scant gecomprimeerde objecten en de decompressiemodule in SFX-archieven (zelfuitpakkende archieven).

Om gevaarlijke programma's te verbergen voor antivirusprogramma's, archiveren indringers ze met speciale compressieprogramma's of maken ze meermaals ingepakte bestanden aan.

Kaspersky-virusanalisten hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.

Als Kaspersky Endpoint Security een dergelijk compressieprogramma in een bestand detecteert, bevat het bestand wellicht een kwaadaardig programma of een programma dat criminelen kunnen gebruiken om schade aan uw computer of persoonlijke gegevens te berokkenen.

Kaspersky Endpoint Security onderscheidt de volgende soorten programma's:

- *Ingepakte bestanden die mogelijk schadelijk zijn* – gebruikt voor het comprimeren van malware, zoals virussen, wormen en Trojans.
- *Meermaals ingepakte bestanden* (gemiddeld veiligheidsrisico) – het object is drie keer gecomprimeerd door een of meerdere compressieprogramma's.

#### • [Meermaals ingepakte objecten](#)

Kaspersky Endpoint Security scant gecomprimeerde objecten en de decompressiemodule in SFX-archieven (zelfuitpakkende archieven).

Om gevaarlijke programma's te verbergen voor antivirusprogramma's, archiveren indringers ze met speciale compressieprogramma's of maken ze meermaals ingepakte bestanden aan.

Kaspersky-virusanalisten hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.

Als Kaspersky Endpoint Security een dergelijk compressieprogramma in een bestand detecteert, bevat het bestand wellicht een kwaadaardig programma of een programma dat criminelen kunnen gebruiken om schade aan uw computer of persoonlijke gegevens te berokkenen.

Kaspersky Endpoint Security onderscheidt de volgende soorten programma's:

- *Ingepakte bestanden die mogelijk schadelijk zijn* – gebruikt voor het comprimeren van malware, zoals virussen, wormen en Trojans.
- *Meermaals ingepakte bestanden* (gemiddeld veiligheidsrisico) – het object is drie keer gecomprimeerd door een of meerdere compressieprogramma's.

4. Sla uw wijzigingen op.

## De lijst met vertrouwde programma's bewerken

De *lijst met vertrouwde programma's* is een lijst met programma's waarvan de bestands- en netwerkactiviteit (inclusief schadelijke 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. Een programma dat toegevoegd is aan de lijst met vertrouwde programma's, wordt echter uitgesloten van scans door Kaspersky Endpoint Security.

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 programma toevoegen aan de vertrouwde lijst in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Algemene instellingen** → **Exclusions** in het beleidsvenster.
6. Klik in het venster **Scanuitzonderingen en vertrouwde programma's** op de knop **instellingen**.
7. Selecteer in het venster dat opent het tabblad **Vertrouwde programma's**.  
Dit opent een venster met een lijst met vertrouwde programma's.
8. Schakel het selectievakje **Waarden samenvoegen bij overname** in als u een geconsolideerde lijst met vertrouwde programma's wilt maken voor alle computers in het bedrijf. De lijsten met vertrouwde programma's in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Vertrouwde programma's van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Het wijzigen of verwijderen van vertrouwde programma's van het bovenliggende beleid is niet mogelijk.
9. Schakel het selectievakje **Gebruik van lokale vertrouwde programma's toestaan** in als u wilt dat de gebruiker een lokale lijst met vertrouwde programma's kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met vertrouwde programma's maken naast de algemene lijst met vertrouwde programma's die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.  
Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met vertrouwde programma's die in het beleid is gegenereerd.
10. Klik op **Toevoegen**.
11. Voer in het venster dat opent het pad in naar het uitvoerbare bestand van het vertrouwde programma. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.

Kaspersky Endpoint Security ondersteunt de omgevingsvariabele `%userprofile%` niet bij het genereren van een lijst met vertrouwde programma's op de Kaspersky Security Center-console. Om dit toe te passen op alle gebruikersaccounts, kunt u het teken `*` gebruiken (bijvoorbeeld, `C:\Users\*\Documents\File.exe`).

Telkens wanneer u een nieuwe omgevingsvariabele toevoegt, moet u het programma opnieuw starten.

12. Configureer de geavanceerde instellingen voor het vertrouwde programma (zie onderstaande tabel).
13. U kunt het selectievakje gebruiken [om een programma op elk gewenst moment uit te sluiten van de vertrouwde zone](#).
14. Sla uw wijzigingen op.

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Exclusions** .
5. Klik in het blok **Scan exclusions and trusted applications** op de koppeling **Trusted applications** .  
Dit opent een venster met een lijst met vertrouwde programma's.
6. Schakel het selectievakje **Waarden samenvoegen bij overname** in als u een geconsolideerde lijst met vertrouwde programma's wilt maken voor alle computers in het bedrijf. De lijsten met vertrouwde programma's in het bovenliggende en onderliggende beleid worden samengevoegd. De lijsten worden samengevoegd op voorwaarde dat samenvoegen van waarden bij overname is ingeschakeld. Vertrouwde programma's van het bovenliggende beleid worden in onderliggende beleidsregels weergegeven in een alleen-lezenweergave. Het wijzigen of verwijderen van vertrouwde programma's van het bovenliggende beleid is niet mogelijk.
7. Schakel het selectievakje **Gebruik van lokale vertrouwde programma's toestaan** in als u wilt dat de gebruiker een lokale lijst met vertrouwde programma's kan maken. Op deze manier kan een gebruiker zijn eigen lokale lijst met vertrouwde programma's maken naast de algemene lijst met vertrouwde programma's die in het beleid wordt gegenereerd. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.  
  
Als het selectievakje is uitgeschakeld, heeft de gebruiker alleen toegang tot de algemene lijst met vertrouwde programma's die in het beleid is gegenereerd.
8. Klik op **Toevoegen**.
9. Voer in het venster dat opent het pad in naar het uitvoerbare bestand van het vertrouwde programma.  
Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.  

Kaspersky Endpoint Security ondersteunt de omgevingsvariabele `%userprofile%` niet bij het genereren van een lijst met vertrouwde programma's op de Kaspersky Security Center-console. Om dit toe te passen op alle gebruikersaccounts, kunt u het teken `*` gebruiken (bijvoorbeeld, `C:\Users\*\Documents\File.exe`).

Telkens wanneer u een nieuwe omgevingsvariabele toevoegt, moet u het programma opnieuw starten.
10. Configureer de geavanceerde instellingen voor het vertrouwde programma (zie onderstaande tabel).
11. U kunt het selectievakje gebruiken [om een programma op elk gewenst moment uit te sluiten van de vertrouwde zone](#).
12. Sla uw wijzigingen op.



## Een programma vanuit de programma-interface toevoegen aan de vertrouwde lijst

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.
4. Klik in het geopende venster op de knop **Toevoegen**.
5. Selecteer het uitvoerbare bestand van het vertrouwde programma.

U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.

Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en converteert het pad in de lokale interface van het programma. Als u met andere woorden het bestandspad %userprofile%\Documents\File.exe opent, wordt een record C:\Users\Fred123\Documents\File.exe toegevoegd aan lokale interface van het programma voor gebruiker Fred123. Dienovereenkomstig negeert Kaspersky Endpoint Security het vertrouwde programma File.exe voor andere gebruikers. Om dit toe te passen op alle gebruikersaccounts, kunt u het teken \* gebruiken (bijvoorbeeld, C:\Users\\*\Documents\File.exe).

Telkens wanneer u een nieuwe omgevingsvariabele toevoegt, moet u het programma opnieuw starten.

6. Configureer de geavanceerde instellingen in het venster met eigenschappen van vertrouwde programma's (zie onderstaande tabel).
7. U kunt de schakelaar gebruiken [om op elk moment een programma uit de vertrouwde zone uit te sluiten](#).
8. Sla uw wijzigingen op.


Instellingen vertrouwde programma's

| Parameter   | Beschrijving   |
|---|--|
| <b>Scan geen bestanden geopend door de app</b>                        | Alle bestanden die door het programma worden geopend, worden uitgesloten van scans door Kaspersky Endpoint Security. Als u bijvoorbeeld programma's gebruikt om een backup van bestanden te maken, dan helpt deze functie het verbruik van bronnen door Kaspersky Endpoint Security te verminderen.  |
| <b>Bewaak de programma-activiteit niet</b>                            | Kaspersky Endpoint Security controleert de bestands- en netwerkactiviteit van het programma in het besturingssysteem niet. De programma/activiteit wordt gecontroleerd door de volgende componenten: <a href="#">Gedragdetectie</a> , <a href="#">Exploit-preventie</a> , <a href="#">Host Intrusion Prevention</a> , <a href="#">Remediation Engine</a> en <a href="#">Firewall</a> . |
| <b>Neem geen beperkingen van bovenliggend proces (programma) over</b> | De beperkingen die voor het bovenliggende proces zijn geconfigureerd, worden door Kaspersky Endpoint Security niet toegepast op een onderliggend proces. Het bovenliggende proces wordt gestart door een toepassing waarvoor <a href="#">programmamachtigingen</a> (Host Intrusion Prevention) en <a href="#">netwerkregels voor programma's</a> (Firewall) zijn geconfigureerd.       |

|  |   |
|--|---|
| <b>Bewaak de onderliggende programma-activiteit niet</b> | Kaspersky Endpoint Security bewaakt de bestands- of netwerkactiviteit van programma's die worden gestart door het programma niet.   |
| <b>Sta interactie met de programma-interface toe</b>     | <a href="#">Kaspersky Endpoint Security Self-Defense</a> blokkeert alle pogingen om services van programma's te beheren vanaf een externe computer. Als het selectievakje is ingeschakeld, mag het programma voor externe toegang de instellingen van Kaspersky Endpoint Security beheren via de interface van Kaspersky Endpoint Security. |
| <b>Blokkeer interactie met AMSI-bescherming niet</b>     | Kaspersky Endpoint Security controleert de verzoeken van het vertrouwde programma voor objecten die moeten worden gescand door de <a href="#">AMSI bescherming</a> niet.  |
| <b>Scan geen netwerkverkeer</b>                          | Netwerkverkeer dat wordt gestart door het programma, wordt uitgesloten van scans door Kaspersky Endpoint Security. U kunt alle verkeer of alleen versleuteld verkeer van scans uitsluiten. U kunt ook individuele IP-adressen en poortnummers uitsluiten van scans.   |
| <b>Opmerking</b>   | Indien nodig kunt u een korte opmerking plaatsen voor de vertrouwde toepassing. Opmerkingen helpen het zoeken en sorteren van vertrouwde applicaties te vereenvoudigen.   |
| <b>Status</b>  | Status van de vertrouwde applicatie: <ul style="list-style-type: none"> <li>• De status <b>Actief</b> betekent dat het programma in de vertrouwde zone zit.</li> <li>• <b>Inactief</b> status betekent dat de applicatie is uitgesloten van de vertrouwde zone.</li> </ul>  |

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.
4. Selecteer in de lijst met vertrouwde programma's het noodzakelijke vertrouwde programma.
5. Gebruik de schakelaar in de kolom **Status** om een vertrouwde toepassing in het scanbereik op te nemen of uit te sluiten.
6. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Selecteer in de vervolgkeuzelijst **Vertrouwde systeemcertificatenopslag** welke systeemopslag moet worden beschouwd als vertrouwd door Kaspersky Endpoint Security.
4. Sla uw wijzigingen op.

## Back-up beheren

*Back-up* bewaart back-ups van bestanden die tijdens de desinfectie zijn verwijderd of gewijzigd. Een *back-up* is een kopie van het bestand die is gemaakt voordat het bestand werd gedesinfecteerd of verwijderd. Back-ups van bestanden worden in een speciale indeling opgeslagen en zijn niet gevaarlijk.

Back-ups van bestanden worden opgeslagen in de map C:\ProgramData\Kaspersky Lab\KES\QB.

Gebruikers in de groep Beheerders hebben de benodigde machtigingen om deze map te openen. De gebruiker wiens account is gebruikt om Kaspersky Endpoint Security te installeren heeft beperkte toegangsrechten voor deze map.

Kaspersky Endpoint Security biedt de mogelijkheid niet om machtigingen voor de toegang tot back-ups van bestanden te configureren.


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 het bestand vanuit een back-up terugzetten in de originele map.

Als Kaspersky Endpoint Security werkt onder het beheer van Kaspersky Security Center, kunnen back-ups van bestanden worden verstuurd naar de Administration Server van Kaspersky Security Center. Voor meer informatie over het beheer van back-ups van bestanden in Kaspersky Security Center raadpleegt u het Help-systeem van Kaspersky Security Center.

## De maximale opslagduur voor bestanden in Back-up configureren

De standaard maximale opslagduur voor kopieën van bestanden in Back-up is 30 dagen. Na het verlopen van de maximale opslagduur verwijdert Kaspersky Endpoint Security de oudste bestanden in Back-up.

*Zo configureert u de maximale opslagduur voor bestanden in Back-up:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het venster met de programma-instellingen.
3. Als u de opslagperiode voor kopieën van bestanden in Back-up wilt beperken, selecteer dan **Bewaar objecten niet langer dan N days** in het blok **Back-up**. Voer de maximale opslagduur voor kopieën van bestanden in Back-up
4. Sla uw wijzigingen op.

## De maximale grootte van Back-up configureren

U kunt de maximale grootte van Back-up configureren. De grootte van Back-up is standaard onbeperkt. Wanneer de maximale grootte is bereikt, verwijdert Kaspersky Endpoint Security automatisch de oudste bestanden uit Back-up.

*Zo configureert u de maximale grootte van Back-up:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het venster met de programma-instellingen.
3. Als u de grootte van de back-up wilt beperken, selecteert u het selectievakje **Beperk de grootte van Back-up tot N MB** in het blok **Back-up**. Geef de maximale grootte van Back-up.
4. Sla uw wijzigingen op.

## Bestanden vanuit Back-up terugzetten

Als schadelijke code in een bestand wordt gevonden, blokkeert Kaspersky Endpoint Security het bestand, wijst het de status *Geïnfecteerd* eraan toe, 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.

Bestanden met de status *Wordt gedesinfecteerd bij herstart van computer* kunnen niet worden teruggezet. Start de computer opnieuw op en de status van het bestand zal wijzigen in *Gedesinfecteerd* of *Verwijderd*. U kunt ook het bestand uit de back-up terugzetten naar de oorspronkelijke map.

Bij de detectie van schadelijke 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).

De back-ups van bestanden worden als een tabel voorgesteld. Voor een back-up van een bestand wordt het pad naar de oorspronkelijke map van het bestand weergegeven. Het pad naar de oorspronkelijke map van het bestand bevat mogelijk persoonlijke gegevens.

Als meerdere bestanden met identieke namen en een verschillende inhoud uit dezelfde map worden verplaatst naar Back-up, kunt u alleen het bestand dat het laatst in Back-up is geplaatst terugzetten.

*Zo zet u bestanden vanuit Back-up terug:*

1. Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **Back-up**.
2. Hiermee opent u de lijst met bestanden in Back-up. Selecteer in die lijst de bestanden die u wilt terugzetten en klik op **Herstellen**.

Kaspersky Endpoint Security zet alle bestanden vanuit geselecteerde back-ups terug in hun oorspronkelijke mappen.

## Back-ups van bestanden uit Back-up verwijderen

Kaspersky Endpoint Security verwijdert automatisch back-ups van bestanden met een willekeurige status uit Back-up nadat de geconfigureerde opslagduur in de programma-instellingen is verstreken. U kunt een kopie van een bestand ook handmatig verwijderen uit Back-up.

*Zo verwijdert u back-ups van bestanden uit Back-up:*

1. Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **Back-up**.
2. Hiermee opent u de lijst met bestanden in Back-up. Selecteer in deze lijst de bestanden die u wilt verwijderen uit Back-up en klik op **Verwijderen**.

Kaspersky Endpoint Security verwijdert de geselecteerde back-ups van bestanden uit Back-up.

## Service voor meldingen

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.

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.
- Sorteert 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
3. In het blok **Meldingen**, klikt u op de knop **Instellingen voor 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.

Gebeurtenissen kunnen de volgende gebruikersgegevens bevatten:

- Paden naar bestanden die door Kaspersky Endpoint Security zijn gescand.
- Paden naar registersleutels die tijdens de werking van Kaspersky Endpoint Security zijn gewijzigd.
- Microsoft Windows-gebruikersnaam.
- Adressen van webpagina's die door de gebruiker zijn bezocht.

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 rapport** en **Opslaan in Windows-gebeurtenislogboek** in.

Gebeurtenissen met ingeschakelde selectievakjes in de kolom **Opslaan in lokaal rapport** worden weergegeven in de [programmalogboeken](#). Gebeurtenissen met ingeschakelde selectievakjes in de kolom **Opslaan in Windows-gebeurtenislogboek** worden in Windows-logboeken in het gedeelte Programma opgeslagen.

6. Sla uw wijzigingen op.

## Weergave en levering van meldingen configureren

*Zo configureert u de weergave en de levering van meldingen:*

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

2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.

3. In het blok **Meldingen**, klikt u op de knop **Instellingen voor 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.

Gebeurtenissen kunnen de volgende gebruikersgegevens bevatten:

- Paden naar bestanden die door Kaspersky Endpoint Security zijn gescand.
- Paden naar registersleutels die tijdens de werking van Kaspersky Endpoint Security zijn gewijzigd.
- Microsoft Windows-gebruikersnaam.
- Adressen van webpagina's die door de gebruiker zijn bezocht.

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 relevante 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 relevante 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 **OK**.

8. Als u e-mailmeldingen hebt ingeschakeld, configureert u de instellingen voor e-mailbezorging:

a. Klik op **Instellingen voor e-mailmeldingen**.

b. Schakel het selectievakje **Meld gebeurtenissen** in om informatie te ontvangen over de gebeurtenissen van Kaspersky Endpoint Security geselecteerd in de kolom **Melden per e-mail**.



c. Geef de instellingen voor de levering van meldingen per e-mail op.


Kaspersky Endpoint Security ondersteunt alleen de basis SMTP-authenticatie. De programma-instellingen bieden geen optie om het gebruik van TLS te configureren. U kunt e-mailmeldingen configureren in de eigenschappen van Kaspersky Security Center Administration Server. Kaspersky Security Center ondersteunt het gebruik van TLS voor SMTP-server.

d. Klik op **OK**.

9. Sla uw wijzigingen op.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
3. Schakel in het blok **Toon status van het programma in het systeemvak** de selectievakjes naast de categorieën van gebeurtenissen in waarvoor u meldingen in het systeemvak van Microsoft Windows wilt zien.
4. Sla uw wijzigingen op.

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.

## Berichten tussen gebruikers en de beheerder

Dankzij de onderdelen [Programmacontrole](#), [Apparaatcontrole](#), [Webcontrole](#) en [Adaptieve controle op afwijkingen](#) kunnen netwerkgebruikers met computers waarop Kaspersky Endpoint Security is geïnstalleerd berichten naar de beheerder versturen.

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.
- Programmacontrole 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 [Programmacontrole](#) 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 het Kaspersky Security Center (zie onderstaande instructie). De velden van het bericht worden ingevuld met de waarden van de velden uit de gedefinieerde sjabloon in het Kaspersky Security Center-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 het 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 het 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 Security Center-beleid.

*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 **Events**.  
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 **Gebeurtenisselecties** de optie **Gebruikersaanvragen**.
4. Selecteer het bericht dat u naar de beheerder hebt verstuurd.
5. Klik op de knop **Venster met eigenschappen van gebeurtenis openen** rechts in de werkruimte van de Beheerconsole.


# Rapporten beheren

Informatie over de werking van elk Kaspersky Endpoint Security-onderdeel, de gebeurtenissen die zijn gerelateerd aan gegevensencryptie, de prestaties van elke scantaak, updatetaak, integriteitscontrole en de algemene werking van het programma wordt in rapporten vastgelegd.

Rapporten worden opgeslagen in de map C:\ProgramData\Kaspersky Lab\KES\Report.

Rapporten kunnen de volgende gebruikersgegevens bevatten:

- Paden naar bestanden die door Kaspersky Endpoint Security zijn gescand.
- Paden naar registersleutels die tijdens de werking van Kaspersky Endpoint Security zijn gewijzigd.
- Microsoft Windows-gebruikersnaam.
- Adressen van webpagina's die door de gebruiker zijn bezocht.


De gegevens in het rapport worden in tabelvorm gepresenteerd. Elke rij 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. Klik op de knop  naast de naam van de kolom om de extra kenmerken te bekijken. 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 **Systemaudit**. 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.
- Rapporten over de werking van Kaspersky Endpoint Security-onderdelen.
- Rapporten over Kaspersky Endpoint Security-taken.
- Het rapport **Gegevensencryptie**. Bevat informatie over gebeurtenissen die zich tijdens de encryptie en decryptie van gegevens voordoen.

In rapporten kunnen gebeurtenissen het volgende belang hebben:


 **Informatieve berichten**. Referentie-gebeurtenissen die normaal gesproken geen belangrijke informatie bevatten.

 **Waarschuwingen**. Gebeurtenissen die uw aandacht vereisen omdat ze belangrijke situaties in de werking van Kaspersky Endpoint Security weerspiegelen.

 **Kritieke gebeurtenissen**. 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.
- Sorteert de lijst met gebeurtenissen op elke kolom in het rapport.
- Toon en verberg gebeurtenissen die met het gebeurtenissenfilter zijn gegroepeerd, met de knop .
- 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](#).

Als Kaspersky Endpoint Security wordt uitgevoerd onder beheer van Kaspersky Security Center, kan informatie over gebeurtenissen worden doorgestuurd naar de Kaspersky Security Center Administration Server (raadpleeg de [Help van Kaspersky Security Center](#) voor meer informatie).

## Rapporten bekijken

Als een gebruiker rapporten kan bekijken, kan de gebruiker ook alle gebeurtenissen in de rapporten bekijken.

*Zo bekijkt u rapporten:*

1. Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **Rapporten**.
2. Selecteer in de lijst met componenten en taken een component of taak.  
Rechts in het venster ziet u een rapport met een lijst met gebeurtenissen die zich voordeden tijdens de werking van het geselecteerde onderdeel of de geselecteerde taak van Kaspersky Endpoint Security. U kunt gebeurtenissen in het rapport sorteren op de waarden in de cellen van een van de kolommen.
3. Om gedetailleerde informatie over een gebeurtenis te zien, selecteert u de gebeurtenis in het rapport.

Een blok met de samenvatting van de gebeurtenis wordt onder in het venster weergegeven.

## Maximale opslagduur voor rapporten configureren

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.


*Zo wijzigt u de maximale opslagduur voor rapporten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het venster met de programma-instellingen.
3. Als u de opslagduur van rapporten wilt beperken, schakelt u in het blok **Bewaar rapporten niet langer dan** het selectievakje **Bewaar rapporten niet langer dan Rapporten N dagen** in. Definieer de maximale opslagduur voor rapporten.
4. Sla uw wijzigingen op.

## Maximale grootte van het rapportbestand configureren

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.

*Zo configureert u de maximale grootte van het rapportbestand:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het venster met de programma-instellingen.
3. Schakel in het blok **Rapporten** het selectievakje **Beperk grootte van rapportbestand tot N MB** in als u de grootte van een rapportbestand wilt beperken. Definieer de maximale grootte van het rapportbestand.
4. Sla uw wijzigingen op.

## Een rapport als een bestand opslaan

De gebruiker is persoonlijk verantwoordelijk voor het veilig houden van informatie dat vanuit een rapport is opgeslagen in een bestand, en in het bijzonder voor de controle en beperking van de toegang tot deze informatie.

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. Ga naar het gedeelte **Bewaking** in het hoofdvenster van het programma en klik op de tegel **Rapporten**.
2. U ziet nu een venster waarin u het onderdeel of de taak moet selecteren.  
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.
3. 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

4. Klik in de rechterbovenhoek van het venster op de knop **Rapport opslaan**.
5. Geef in het geopende venster de doelmap voor het rapportbestand op.
6. Voer de naam van het rapportbestand in.
7. Selecteer het benodigde rapportbestandsformaat: TXT of CSV.
8. Sla uw wijzigingen op.

## Rapporten wissen

*Zo verwijdert u informatie uit rapporten:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het venster met de programma-instellingen.
3. In het blok **Rapporten**, klikt u op de knop **Wissen**.
4. Als [Wachtwoordbescherming is ingeschakeld](#), kan Kaspersky Endpoint Security u vragen om de inloggegevens van uw gebruikersaccount. Het programma vraagt accountgegevens als de gebruiker niet over de vereiste machtiging beschikt.

Kaspersky Endpoint Security verwijdert alle rapporten voor alle programmaonderdelen en taken.

# Zelfbescherming van Kaspersky Endpoint Security

Zelfbescherming voorkomt dat andere programma's acties verrichten die de werking van Kaspersky Endpoint Security kunnen verstoren en, bijvoorbeeld, Kaspersky Endpoint Security van de computer verwijderen. De set beschikbare zelfbeschermingstechnologieën voor Kaspersky Endpoint Security hangt af van het feit of het besturingssysteem 32-bits of 64-bit is (zie onderstaande tabel).


Zelfbeschermingstechnologieën van Kaspersky Endpoint Security

| Technologie  | Beschrijving  | x86 computer | x64 computer                  |
|--|---|--------------|-------------------------------|
| <b>Zelfbeschermingsmechanisme.</b>                   | De technologie blokkeert de toegang tot de volgende programmacomponenten: <ul style="list-style-type: none"><li>• bestanden in de Kaspersky Endpoint Security-installatiemap en andere bestanden van het programma;</li><li>• registersleutels met records die bij het programma horen;</li><li>• processen die het programma uitvoert.</li></ul>   | ✓            | ✓                             |
| <b>AM-PPL (Antimalware Protected Process Light).</b> | De technologie beschermt Kaspersky Endpoint Security-processen tegen schadelijke acties. Voor meer informatie over AM-PPL-technologie gaat u naar de <a href="#">website van Microsoft</a> .<br><br><div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019.</div> | ✓            | ✓                             |
| <b>Verdedigingsmechanisme voor extern beheer.</b>    | Deze technologie voorkomt dat programma's voor extern beheer (bijvoorbeeld TeamViewer of RemotelyAnywhere) toegang krijgen tot Kaspersky Endpoint Security.   | ✓            | –<br>(behalve voor Windows 7) |

## Zelfbescherming inschakelen en uitschakelen

Het mechanisme Zelfbescherming van Kaspersky Endpoint Security is standaard ingeschakeld.

*Zo schakelt u Zelfbescherming in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik het selectievakje **Schakel Zelfbescherming in** om het zelfbeschermingsmechanisme in of uit te schakelen.

#### 4. Sla uw wijzigingen op.

## Ondersteuning voor AM-PPL inschakelen en uitschakelen

Kaspersky Endpoint Security ondersteunt Antimalware Protected Process Light-technologie (hierna 'AM-PPL' genoemd) van Microsoft. AM-PPL beschermt Kaspersky Endpoint Security-processen tegen schadelijke acties (bijvoorbeeld de beëindiging van het programma). Dankzij AM-PPL worden alleen vertrouwde processen uitgevoerd. Kaspersky Endpoint Security-processen zijn ondertekend in overeenstemming met de Windows-beveiligingsvereisten en zijn dus vertrouwd. Voor meer informatie over AM-PPL-technologie gaat u naar de [website van Microsoft](#). De AM-PPL-technologie is standaard ingeschakeld.

Kaspersky Endpoint Security heeft ook ingebouwde mechanismen om processen van programma's te beschermen. Met AM-PPL-ondersteuning kunt u functies voor procesbeveiliging delegeren aan het besturingssysteem. Zo werkt het programma sneller en verbruikt het minder computerbronnen.

AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019.

*Zo schakelt u de AM-PPL-technologie in of uit:*

#### 1. [Schakel het Zelfbescherming-mechanisme van het programma uit.](#)

Het Zelfbescherming-mechanisme voorkomt de wijziging en verwijdering van programmaprocessen in het computergeheugen, inclusief de wijziging van de AM-PPL-status.

2. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.

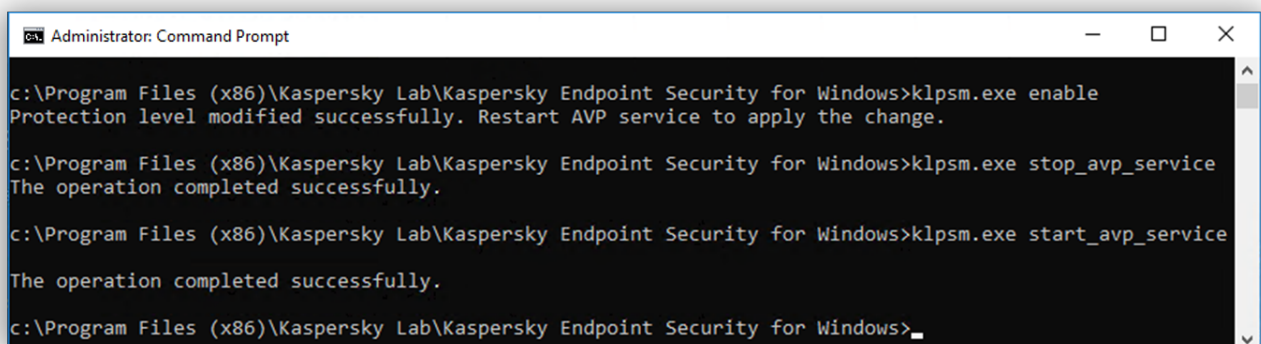
3. Ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

4. Typ het volgende op de opdrachtregel:

- `klpsm.exe enable` – schakel de ondersteuning voor AM-PPL-technologie in (zie onderstaande afbeelding).
- `klpsm.exe disable` – schakel de ondersteuning voor AM-PPL-technologie uit.

5. Herstart Kaspersky Endpoint Security.

#### 6. [Hervat het Zelfbescherming-mechanisme van het programma.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```




## Bescherming tegen extern beheer in- en uitschakelen

De bescherming tegen extern beheer voorkomt dat programma's voor extern beheer (bijvoorbeeld TeamViewer of RemotelyAnywhere) toegang krijgen tot Kaspersky Endpoint Security. Deze technologie bevat de volgende functies voor de bescherming tegen extern beheer:

- Bescherming tegen wijziging van de instellingen van Kaspersky Endpoint Security.
- Bescherming van de Kaspersky Endpoint Security-services (zoals de avp-service).
- Bescherming van programmaprocessen.

Bescherming tegen extern beheer is alleen beschikbaar voor computers met 32-bits besturingssystemen, uitgezonderd Windows 7. Voor Windows 7 is de technologie beschikbaar voor 32-bits en 64-bits besturingssystemen.

*Bescherming tegen extern beheer in- of uitschakelen:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik het selectievakje **Beheer van Kaspersky Endpoint Security-instellingen toestaan via programma's voor extern beheer** om de bescherming tegen extern beheer in of uit te schakelen.

Als het selectievakje is ingeschakeld, kunt u programma's voor extern beheer gebruiken om Kaspersky Endpoint Security te configureren en om de services en processen ervan te beheren.

Als het selectievakje is uitgeschakeld, voorkomt de bescherming tegen extern beheer dat programma's voor extern beheer toegang krijgen tot Kaspersky Endpoint Security. U kunt de configuratie van Kaspersky Endpoint Security met specifieke programma's voor extern beheer toestaan. Hiervoor moet u [het programma voor extern beheer toevoegen aan de lijst Vertrouwd](#). In dit geval zal de bescherming tegen extern beheer wel nog steeds voorkomen dat het programma voor extern beheer toegang krijgt tot de services en processen van Kaspersky Endpoint Security.

4. Gebruik het **Schakel extern beheer van services in** om de bescherming van Kaspersky Endpoint Security-services tegen extern beheer in of uit te schakelen.

Schakel de bescherming van Kaspersky Endpoint Security-services tegen extern beheer uit om het programma via de opdrachtregel af te sluiten.


5. Sla uw wijzigingen op.

Als gevolg hiervan voorkomt Kaspersky Endpoint Security dat de muisaanwijzer in het programmavenster raakt wanneer de bescherming tegen extern beheer is ingeschakeld. Wanneer een externe gebruiker probeert een service af te sluiten, verschijnt een systeemvenster met een foutmelding.

## 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Dreigingen en uitzonderingen** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven** .
4. Klik in het geopende venster op de knop **Toevoegen**.
5. Selecteer het uitvoerbare bestand van de toepassing voor beheer op afstand.  
U kunt het pad ook handmatig invoeren. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de \* en ?-tekens bij het invoeren van een masker.
6. Selecteer het selectievakje **Bewaak de programma-activiteit niet**.
7. Sla uw wijzigingen op.

# Prestaties van Kaspersky Endpoint Security en compatibiliteit met andere programma's

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;
- De taak Volledige Scan;
- De taak Kritieke Gebiedenscan;
- De taak Aangepaste Scan;
- De taak 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 verbruik van computerbronnen door Kaspersky Endpoint Security bij het scannen van de computer kan de belasting van de CPU en de subsystemen van de harde schijf verhogen en 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 bronnen aan andere programma's afstaan.

## Geavanceerde desinfectietechnologie gebruiken

De schadelijke programma's van vandaag kunnen de laagste niveaus van een besturingssysteem binnendringen, waardoor ze vrijwel onmogelijk te elimineren zijn. Na de detectie van schadelijke activiteit in het besturingssysteem voert Kaspersky Endpoint Security een uitgebreide desinfectieprocedure uit die een speciale geavanceerde desinfectietechnologie gebruikt. De *geavanceerde desinfectietechnologie* dient om schadelijke 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 dreiging 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 servers ziet de gebruiker geen vraag voor opnieuw opstarten van de computer wegens de specifieke eigenschappen van Kaspersky Endpoint Security. 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 server te desinfecteren, schakelt u de actieve desinfectietechnologie voor servers in en start u een *Virusscan* als groepstaak op een tijdstip dat de gebruikers van de bestandsserver goed uitkomt.

## Energiebesparingsmodus inschakelen of uitschakelen

*Zo inschakelt u de energiebesparingsmodus in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik in het blok **Prestaties** het selectievakje **Geplande taken uitstellen bij werking op accustroom** om de energiebesparingsmodus in of uit 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;
- De taak Volledige Scan;
- De taak Kritieke Gebiedenscan;
- De taak Aangepaste Scan;
- De taak Integriteitscontrole.

4. Sla uw wijzigingen op.

## Afstaan van bronnen aan andere programma's inschakelen of uitschakelen

Het verbruik van computerbronnen door Kaspersky Endpoint Security bij het scannen van de computer kan de belasting van de CPU en de subsystemen van de harde schijf verhogen. Dit kan andere programma's vertragen. Om de prestaties te optimaliseren, biedt Kaspersky Endpoint Security een *modus voor het overbrengen van bronnen naar andere programma's*. In deze modus kan het besturingssysteem de prioriteit van de scantaakthreads van Kaspersky Endpoint Security verlagen als de CPU-belasting hoog is. Hierdoor kunnen de bronnen van het besturingssysteem opnieuw worden gedistribueerd naar andere programma's. Scantaken krijgen dus minder CPU-tijd. Als gevolg hiervan zal Kaspersky Endpoint Security er langer over doen om de computer te scannen. Standaard is het programma geconfigureerd om bronnen aan andere programma's af te staan.

*Zo schakelt u het afstaan van bronnen aan andere programma's in of uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik in het blok **Prestaties** het selectievakje **Bronnen aan andere programma's geven** om het toewijzen van bronnen aan andere programma's in of uit te schakelen.
4. Sla uw wijzigingen op.

## Best practices voor het optimaliseren van de prestaties van Kaspersky Endpoint Security

Wanneer u Kaspersky Endpoint Security for Windows inzet, kunt u de volgende aanbevelingen gebruiken om de computerbeveiliging te configureren en de prestaties te optimaliseren.

### Algemeen

Configureer de algemene instellingen van het programma in overeenstemming met de volgende aanbevelingen:

1. [Upgrade Kaspersky Endpoint Security naar de nieuwste versie.](#)

In nieuwere versies van het programma zijn fouten verholpen, de stabiliteit verbeterd en zijn de prestaties geoptimaliseerd.

2. Schakel beveiligingscomponenten in met standaardinstellingen.

Standaardinstellingen worden als optimaal beschouwd. Deze instellingen worden aanbevolen door Kaspersky-experts. Standaardinstellingen bieden aanbevolen beschermingsniveau en optimaal gebruik van bronnen. Indien nodig kunt u [de standaard programma-instellingen herstellen](#).

3. Functies voor optimalisatie van programmaprestaties inschakelen.

Het programma heeft prestatie-optimalisatiefuncties: [energiebesparende modus](#) en [toekennen van middelen aan andere programma's](#). Zorg ervoor dat deze opties ingeschakeld zijn.

### Virusscan op werkstations

Het inschakelen van [Achtergrondscan](#) wordt aanbevolen voor virusscan van werkstations. Een *achtergrondscan* is een scanmodus van Kaspersky Endpoint Security waarin geen meldingen aan de gebruiker worden weergegeven. De achtergrondscan vereist minder computerbronnen dan andere scans (zoals een volledige scan). In deze modus scant Kaspersky Endpoint Security opstartobjecten, opstartsectoren, het systeemgeheugen en de systeempartitie. Achtergrondscaninstellingen worden als optimaal beschouwd. Deze instellingen worden aanbevolen door Kaspersky-experts. Voor het uitvoeren van een virusscan van de computer kunt u dus alleen de achtergrondscanmodus gebruiken zonder andere scantaken te gebruiken.

Als scannen op de achtergrond niet aan uw behoeften voldoet, configureert u de *Virusscantaak* in overeenstemming met de volgende aanbevelingen:

### 1. [Configureer het optimale computerscanschema.](#)

U kunt de taak zo configureren dat deze wordt uitgevoerd wanneer de computer onder minimale belasting werkt. U kunt de taak bijvoorbeeld zo configureren dat deze 's nachts of in het weekend wordt uitgevoerd.

Als gebruikers hun computer aan het eind van de dag uitschakelen, kunt u de scantaak als volgt configureren:

- Wake-on-LAN inschakelen. Met de Wake on LAN-functie kan de computer op afstand worden aangezet door een speciaal signaal via het lokale netwerk te sturen. Als u deze functie wilt gebruiken, moet u de Wake on LAN-instellingen in de BIOS-instellingen inschakelen. U kunt de computer ook automatisch laten uitschakelen nadat de scan is voltooid.
- Schakel de functie "Gemiste taken uitvoeren" uit. Kaspersky Endpoint Security slaat gemiste taken over wanneer de gebruiker de computer aanzet. Het uitvoeren van taken nadat de computer is ingeschakeld, kan de gebruiker hinderen, omdat de scan veel vermogen vereist van de computer.

Als u geen optimaal scanschema kunt configureren, stelt u in dat taken alleen worden uitgevoerd wanneer de computer niet actief is. Kaspersky Endpoint Security start de scantaak als de computer vergrendeld wordt of als de schermbeveiliging is ingeschakeld. Als u de uitvoering van de taak hebt onderbroken door de computer bijvoorbeeld te ontgrendelen, zet Kaspersky Endpoint Security de taak automatisch verder vanaf het punt waar deze werd onderbroken.

### 2. [Een scanbereik definiëren.](#)

Selecteer de volgende objecten om te scannen:

- Kernelgeheugen;
- Actieve processen en opstartobjecten;
- Opstartsectoren;
- Stuurprogramma systeem (%systemdrive%).

### 3. [Schakel iSwift- en iChecker-technologieën in.](#)

- iSwift-technologie.

Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.

- iChecker-technologie.

Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).

U kunt de iSwift- en iChecker-technologieën alleen inschakelen in de Beheerconsole (MMC) en Kaspersky Endpoint Security-interface. U kunt deze technologieën niet inschakelen in Kaspersky Security Center Webconsole.

#### 4. [Schakel het scannen van wachtwoordbeveiligde archieven uit.](#)

Als het scannen van wachtwoordbeveiligde archieven ingeschakeld is, wordt er een wachtwoordprompt weergegeven voordat het archief wordt gescand. Omdat het wordt aanbevolen om de taak buiten kantooruren in te plannen, kan de gebruiker het wachtwoord niet invoeren. U kunt [wachtwoordbeveiligde archieven handmatig scannen](#).

## Virusscan op servers

Configureer de *virusscantaak* in overeenstemming met de volgende aanbevelingen:

#### 1. [Configureer het optimale computerscanschema.](#)

U kunt de taak zo configureren dat deze wordt uitgevoerd wanneer de computer onder minimale belasting werkt. U kunt de taak bijvoorbeeld zo configureren dat deze 's nachts of in het weekend wordt uitgevoerd.

#### 2. [Schakel iSwift- en iChecker-technologieën in.](#)

- iSwift-technologie.

Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.

- iChecker-technologie.

Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).

U kunt de iSwift- en iChecker-technologieën alleen inschakelen in de Beheerconsole (MMC) en Kaspersky Endpoint Security-interface. U kunt deze technologieën niet inschakelen in Kaspersky Security Center Webconsole.

#### 3. [Schakel het scannen van wachtwoordbeveiligde archieven uit.](#)

Als het scannen van wachtwoordbeveiligde archieven ingeschakeld is, wordt er een wachtwoordprompt weergegeven voordat het archief wordt gescand. Omdat het wordt aanbevolen om de taak buiten kantooruren in te plannen, kan de gebruiker het wachtwoord niet invoeren. U kunt [wachtwoordbeveiligde archieven handmatig scannen](#).

## Kaspersky Security Network

Voor een efficiëntere bescherming van uw computer gebruikt Kaspersky Endpoint Security gegevens die het van gebruikers over de hele wereld ontvangt. Kaspersky Security Network is ontworpen om deze 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 dreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. Als u deelneemt aan Kaspersky Security Network, ontvangt Kaspersky Endpoint Security van de KSN-services informatie over de categorie en reputatie van gescande bestanden, alsook informatie over de reputatie van gescande webadressen.

Bewerk de instellingen van Kaspersky Security Network in overeenstemming met de volgende aanbevelingen:

### 1. [Uitgebreide KSN-modus inschakelen](#)

De *uitgebreide KSN-modus* is een modus waarin Kaspersky Endpoint Security [aanvullende gegevens](#) naar Kaspersky verstuurt.

### 2. Privaat KSN configureren.

*Privaat KSN* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang verkrijgen tot reputatiedatabases van Kaspersky Security Network en tot andere statistische gegevens zonder gegevens naar KSN te versturen vanaf hun eigen computers.

### 3. [Cloudmodus inschakelen](#).

*Cloudmodus* verwijst naar de modus waarin Kaspersky Endpoint Security een beperkte versie van de antivirusdatabases gebruikt. Kaspersky Security Network ondersteunt de werking van het programma wanneer een beperkte versie van de antivirusdatabases worden gebruikt. Met de beperkte versie van de antivirusdatabases verbruikt u ongeveer de helft van het RAM van de computer dat anders met de normale databases zou worden gebruikt. Als u niet deelneemt aan Kaspersky Security Network of als de cloudmodus is uitgeschakeld, downloadt Kaspersky Endpoint Security de volledige versie van de antivirusdatabases vanaf de Kaspersky-servers.



# 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. Kaspersky Endpoint Security gebruikt het AES-encryptiealgoritme (Advanced Encryption Standard).

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 licentiesleutel, 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 encryptiefunctie of zonder toegang tot de encryptiefunctie behoudt het bestand hierdoor een niet-geëncrypte toestand.

Kaspersky Endpoint Security beschikt over de volgende aspecten voor gegevensbescherming:

- **File Level Encryption op lokale schijven van de computer.** 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 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.
- **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 encryptiefunctie.

- **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 pakketten 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.
- **Full Disk Encryption.** 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 Full Disk Encryption-regel opgeven en een lijst met harde schijven maken die niet moeten worden geëncrypt. Kaspersky Endpoint Security voert de Full Disk Encryption sector per sector uit nadat het Kaspersky Security Center-beleid is toegepast. Het programma encrypt alle logische partities van harde schijven tegelijkertijd.

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 [Authenticatie-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 aangesloten op de computer worden ingevoerd of moeten de gebruikersnaam en het wachtwoord van de Authenticatie-agent-account worden ingevoerd. Dit account is door de lokale netwerkbeheerder aangemaakt met taken voor het [beheer van accounts voor Authenticatie-agenten](#). Dit account is gebaseerd op een Microsoft Windows-account waarmee een gebruiker zich bij het besturingssysteem aanmeldt. U kunt ook [Enmalige aanmelding \(SSO\)-technologie gebruiken](#), waarmee u zich automatisch bij het besturingssysteem kunt aanmelden met de gebruikersnaam en het wachtwoord van de account voor authenticatie-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 voor Authenticatie-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 Help van Kaspersky Security Center.

De toegang tot geëncrypte harde schijven is alleen mogelijk vanaf computers waarop Kaspersky Endpoint Security met Full Disk Encryption-functie 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 beschermd zijn, 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. Als bestanden dus worden geschreven naar een nieuw apparaat en het apparaat wordt regelmatig geëncrypt met de functie **Alleen gebruikte schijfruimte encrypten**, zullen na enige tijd alle sectoren geëncrypt 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 objecten om de een of andere reden door een andere beheerserver werd beheerd, kunt u op een van de volgende manieren toegang krijgen tot de geëncrypte gegevens:

- Beheerservers in dezelfde hiërarchie:
  - U hoeft niets te doen. De gebruiker behoudt toegang tot de geëncrypte objecten. Encryptiesleutels worden verstuurd naar alle Administration Servers.
- Gescheiden beheerservers:
  - Toegang tot geëncrypte objecten vragen aan de LAN-beheerder;
  - 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.

Als er geen toegang is tot geëncrypte gegevens, volg dan de speciale instructies voor het werken met geëncrypte gegevens ([Toegang tot geëncrypte bestanden herstellen](#), [Werken met geëncrypte apparaten als er geen toegang toe is](#)).

## Beperkingen van de encryptiefunctionaliteit

Gegevensencryptie heeft de volgende beperkingen:

- Het programma maakt tijdens de encryptie servicebestanden aan. Ongeveer 0,5% 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.
- U kunt alle onderdelen voor gegevensversleuteling beheren in de Kaspersky Security Center-beheerconsole en in de Kaspersky Security Center-webconsole. In de Kaspersky Security Center-cloudconsole kunt u alleen BitLocker beheren.
- Gegevensencryptie is alleen beschikbaar wanneer Kaspersky Endpoint Security met het Kaspersky Security Center-beheersysteem of de Cloudconsole van Kaspersky Security Center (alleen BitLocker) wordt gebruikt. Gegevensencryptie met Kaspersky Endpoint Security in de offline modus is niet mogelijk omdat Kaspersky Endpoint Security encryptiesleutels in Kaspersky Security Center opslaat.
- Als Kaspersky Endpoint Security is geïnstalleerd op een computer met [Microsoft Windows voor servers](#), is alleen Full Disk Encryption met de technologie BitLocker-stationsversleuteling beschikbaar. Als Kaspersky

Endpoint Security is geïnstalleerd op een computer met Windows voor werkstations, is de functionaliteit voor gegevensencryptie volledig beschikbaar.

Full Disk Encryption met Kaspersky Disk Encryption-technologie is niet beschikbaar voor harde schijven die niet aan de hardware- en softwarevereisten voldoen.

De compatibiliteit tussen Full Disk Encryption van Kaspersky Endpoint Security en Kaspersky Anti-Virus voor UEFI wordt niet ondersteund. Kaspersky Anti-Virus voor UEFI wordt gestart voordat het besturingssysteem wordt geladen. Wanneer u Full Disk Encryption gebruikt, detecteert het programma dat er geen besturingssysteem op de computer is geïnstalleerd. Hierdoor zal Kaspersky Anti-Virus voor UEFI niet werken. File Level Encryption (FLE) heeft geen invloed op de werking van Kaspersky Anti-Virus voor UEFI.

Kaspersky Endpoint Security ondersteunt de volgende configuraties:

- HDD-, SSD- en USB-stations.

Kaspersky Disk Encryption (FDE) -technologie ondersteunt het werken met SSD terwijl de prestaties en levensduur van SSD-schijven behouden blijven.

- Schijven verbonden via bus: SCSI, ATA, IEEE1394, USB, RAID, SAS, SATA, NVME.
- Niet-verwijderbare schijven aangesloten via SD- of MMC-bus.
- Schijven met sectoren van 512 bytes.
- Schijven met sectoren van 4096 bytes die 512 bytes emuleren.
- Schijven met de volgende soort partities: GPT, MBR en VBR (verwijderbare schijven).
- Ingebouwde software van de UEFI 64 en Legacy BIOS-standaard.
- Ingebouwde software van de UEFI-standaard met Secure Boot-ondersteuning.

*Secure Boot* is een technologie ontworpen om digitale handtekeningen voor UEFI-laderprogramma's en stuurprogramma's te verifiëren. Secure Boot blokkeert het opstarten van UEFI-toepassingen en stuurprogramma's die niet zijn ondertekend of ondertekend door onbekende uitgevers. Kaspersky Disk Encryption (FDE) ondersteunt Secure Boot volledig. Authenticatie-agent is ondertekend door een Microsoft Windows UEFI Driver Publisher-certificaat.

Op sommige apparaten (bijvoorbeeld Microsoft Surface Pro en Microsoft Surface Pro 2) is mogelijk standaard een verouderde lijst met verificatiecertificaten voor digitale handtekeningen geïnstalleerd. Voordat u de schijf encrypt, moet u de lijst met certificaten bijwerken.

- Embedded software van de UEFI-standaard met Fast Boot-ondersteuning.

*Fast Boot* is een technologie waarmee de computer sneller opstart. Wanneer Fast Boot-technologie is ingeschakeld, laadt de computer normaal alleen de minimale set UEFI-stuurprogramma's die nodig zijn om het besturingssysteem te starten. Wanneer de Fast Boot-technologie is ingeschakeld, werken USB-toetsenborden, muizen, USB-tokens, touchpads en touchscreens mogelijk niet terwijl Authentication Agent actief is.

Om Kaspersky Disk Encryption (FDE) te gebruiken, wordt aanbevolen om de Fast Boot-technologie uit te schakelen. U kunt het [FDE-testprogramma](#) gebruiken om de werking van Kaspersky Disk Encryption (FDE) te testen.

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.
- Het systeem heeft Intel® Rapid Start Technology en schijven met een sluimerstandpartitie zelfs als Intel® Rapid Start Technology is uitgeschakeld.
- Schijven in MBR-indeling met meer dan 10 uitgebreide partities.
- Het systeem heeft een wisselbestand op een niet-systeemstation.
- Systeem met meerdere opstartmogelijkheden dankzij verschillende geïnstalleerde besturingssystemen.
- Dynamische partities (alleen primaire partities worden ondersteund).
- Schijven met minder dan 0,5% vrije, niet-gefragmenteerde schijfruimte.
- Schijven met een sectorgrootte verschillend van 512 bytes of 4096 bytes die 512 bytes emuleren.
- Hybride stations.
- Het systeem heeft laders van derden.
- Schijven met gecomprimeerde NTFS-mappen.
- Kaspersky Disk Encryption (FDE)-technologie is niet compatibel met andere technologieën voor volledige schijfencryptie (zoals BitLocker, McAfee Drive Encryption en WinMagic SecureDoc).
- Kaspersky Disk Encryption (FDE)-technologie is niet compatibel met ExpressCache-technologie.
- Het maken, verwijderen en wijzigen van partities op een geëncrypte schijf wordt niet ondersteund. U kunt gegevens verliezen.
- Het formatteren van het bestandssysteem wordt niet ondersteund. U kunt gegevens verliezen.  
 Als u een schijf moet formatteren die is geëncrypt met Kaspersky Disk Encryption (FDE)-technologie, dan formatteert u de schijf op een computer die geen Kaspersky Endpoint Security voor Windows heeft en gebruikt u alleen full disk encryption.  
 Een geëncrypte schijf die is geformatteerd met de optie voor snel formatteren, kan ten onrechte worden geïdentificeerd als geëncrypt de volgende keer dat deze wordt aangesloten op een computer waarop Kaspersky Endpoint Security voor Windows is geïnstalleerd. Gebruikersgegevens zijn niet beschikbaar.
- Authenticatie-agent ondersteunt niet meer dan 100 accounts.
- Single Sign-On-technologie is niet compatibel met andere technologieën van externe ontwikkelaars.
- Kaspersky Disk Encryption (FDE)-technologie wordt niet ondersteund op de volgende modellen apparaten:
  - Dell Latitude E6410 (UEFI-modus)
  - HP Compaq nc8430 (oudere BIOS-modus)
  - Lenovo Think Center 8811 (oudere BIOS-modus)
- Authenticatie-agent ondersteunt het werken met USB-tokens niet wanneer Legacy USB Support is ingeschakeld. Alleen authenticatie met wachtwoord is mogelijk op de computer.

- Bij het encrypten van een schijf in de Legacy BIOS-modus, wordt u geadviseerd om Legacy USB-ondersteuning in te schakelen op de volgende modellen apparaten:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 microtower pc
  - Lenovo G550
  - Lenovo ThinkPad L530
  - Lenovo ThinkPad T510
  - Lenovo ThinkPad W540
  - Lenovo ThinkPad X121e
  - Lenovo ThinkPad X200s (74665YG)
  - Samsung R530
  - Toshiba Satellite A350

- Toshiba Satellite U400 100
- MSI 760GM-E51 (moederbord)

## Lengte van de encryptiesleutel wijzigen (AES56 / AES256)

Kaspersky Endpoint Security gebruikt het AES-encryptiealgoritme (Advanced Encryption Standard). Kaspersky Endpoint Security ondersteunt het AES-encryptiealgoritme met een effectieve sleutellengte van 256 of 56-bits. Het algoritme voor gegevensencryptie hangt af van de AES-encryptiebibliotheek die bij het distributiepakket wordt meegeleverd: *sterke encryptie (AES256)* of *normale encryptie (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.

Het wijzigen van de lengte van de encryptiesleutel is alleen beschikbaar voor Kaspersky Endpoint Security 11.2.0 of hoger.

Het wijzigen van de lengte van de encryptiesleutel bestaat uit de volgende stappen:

1. Decrypt objecten die Kaspersky Endpoint Security heeft geëncrypt voordat u de lengte van de encryptiesleutel begint te wijzigen:
  - a. [Decrypt harde schijven](#).
  - b. [Decrypt bestanden op lokale schijven](#).
  - c. [Decrypt verwisselbare schijven](#).

Na de wijziging van de lengte van de encryptiesleutel zijn eerder geëncrypte objecten niet meer beschikbaar.

2. [Verwijder Kaspersky Endpoint Security](#).
3. [Installeer Kaspersky Endpoint Security](#) met het Kaspersky Endpoint Security-distributiepakket dat een andere encryptiebibliotheek bevat.

U kunt ook de lengte van de encryptiesleutel wijzigen door het programma te upgraden. De sleutellengte kan alleen met een programma-upgrade worden gewijzigd als aan de volgende voorwaarden wordt voldaan:

- Kaspersky Endpoint Security versie 10 Service Pack 2 of hoger is op de computer geïnstalleerd.
- De onderdelen voor gegevensencryptie (File Level Encryption, Full Disk Encryption) zijn niet op de computer geïnstalleerd.

Standaard maken de onderdelen voor gegevensencryptie geen deel uit van Kaspersky Endpoint Security. Het onderdeel Beheer van BitLocker beïnvloedt de wijziging in de lengte van de encryptiesleutel niet.

Als u de lengte van de encryptiesleutel wilt wijzigen, start u het bestand kes\_win.msi of setup\_kes.exe uit het distributiepakket met de noodzakelijke encryptiebibliotheek. U kunt het programma ook op afstand upgraden met behulp van het installatiepakket.



De lengte van de encryptiesleutel kan niet worden gewijzigd met het distributiekpakket van dezelfde versie van het programma dat op uw computer is geïnstalleerd zonder het programma eerst te verwijderen.

## Kaspersky Disk Encryption

Kaspersky Disk Encryption is alleen beschikbaar voor computers met een Windows-besturingssysteem voor werkstations. Voor computers met een Windows-besturingssysteem voor servers gebruikt u BitLocker-stationsversleutelingstechnologie.

Kaspersky Endpoint Security ondersteunt Full Disk Encryption in FAT32-, NTFS- en exFat-bestandssystemen.

Voordat het programma de Full Disk Encryption 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 Authenticatie-agent of 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 Full Disk Encryption nadat het besturingssysteem is geladen en het programma is gestart. Als de harde schijf van het systeem niet compatibel is met Authenticatie-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 Full Disk Encryption 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 Authenticatie-agent en de BitLocker-encryptieonderdelen. Hiertoe typt u vóór de Full Disk Encryption `avp pbatestreset` op de opdrachtregel. Als het besturingssysteem niet wordt geladen nadat de harde schijf van het systeem is gecontroleerd op compatibiliteit met Authenticatie-agent, [moet u de resterende objecten en gegevens na de test van Authenticatie-agent verwijderen](#) met behulp van de Herstelvoorziening. Daarna start u Kaspersky Endpoint Security en voert u de opdracht `avp pbatestreset` opnieuw uit.

Wanneer de Full Disk Encryption 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 Full Disk Encryption, wordt Authenticatie-agent vóór de volgende opstart van het besturingssysteem geladen. Kaspersky Endpoint Security hervat de Full Disk Encryption na de geslaagde authenticatie in Authenticatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de sluimerstand gaat tijdens de Full Disk Encryption, wordt Authenticatie-agent geladen wanneer het besturingssysteem uit de sluimerstand wordt gehaald. Kaspersky Endpoint Security hervat de Full Disk Encryption na de geslaagde authenticatie in Authenticatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de slaapstand gaat tijdens de Full Disk Encryption, hervat Kaspersky Endpoint Security de Full Disk Encryption wanneer het besturingssysteem uit de slaapstand wordt gehaald zonder de Authenticatie-agent te laden.

De gebruikersauthenticatie in Authenticatie-agent kan op twee manieren worden uitgevoerd:



- Typ de naam en het wachtwoord van het account in Authenticatie-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.

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.

Authenticatie-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 Authenticatie-agent als deze indeling is toegevoegd in de taal- en regio-instellingen van het besturingssysteem en beschikbaar is in het welkomstscherf van Microsoft Windows.

Als de naam van het account voor Authenticatie-agent tekens bevat die niet met de beschikbare toetsenbordindelingen van Authenticatie-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 Authenticatie-agent zijn hersteld](#).

## Speciale kenmerken van SSD-schijfencryptie

Het programma ondersteunt de encryptie van SSD-schijven, hybride SSHD-schijven en schijven met de Intel Smart Response-functie. Geen programma ondersteunt geen encryptie van schijven met de Intel Rapid Start-functie. Schakel de Intel Rapid Start-functie uit voordat u een dergelijke schijf gaat encrypten.

Encryptie van SSD-schijven heeft de volgende speciale kenmerken:

- Als een SSD-schijf nieuw is en geen vertrouwelijke gegevens bevat, [schakel dan encryptie van alleen gebruikte ruimte in](#). Hierdoor kunt u de relevante schijfsectoren overschrijven.
- Als een SSD-schijf in gebruik is en vertrouwelijke gegevens bevat, selecteert u een van de volgende opties:
  - Veeg de SSD-schijf volledig schoon (Secure Erase), installeer het besturingssysteem en [voer de encryptie van de SSD-schijf uit terwijl de optie om alleen gebruikte ruimte te encrypten is ingeschakeld](#).
  - Voer encryptie van de SSD-schijf uit terwijl de optie om alleen gebruikte ruimte te encrypten is uitgeschakeld.

Voor de encryptie van een SSD-schijf is 5-10 GB vrije ruimte vereist. De vereisten voor vrije ruimte voor het opslaan van beheergegevens van encryptie staan in de onderstaande tabel.

Vereisten voor vrije ruimte voor het opslaan van beheergegevens van encryptie

| SSD-schijfgrootte (GB) | Vrije ruimte op primaire partitie van SSD-schijf (MB) | Vrije ruimte op secundaire partitie van SSD-schijf (MB) |
|------------------------|---|---|
| 128                    | 250   | 64  |
| 256                    | 250   | 640   |
| 512                    | 300   | 128   |

## Kaspersky Disk Encryption starten

Voordat u de Full Disk Encryption start, wordt u aanbevolen te controleren of de computer niet geïnfecteerd is. U kunt dit doen door een Volledige Scan of Kritieke Gebiedenscan te starten. Een Full Disk Encryption uitvoeren op een computer die is geïnfecteerd met een rootkit kan de computer onklaar maken.

Voordat u schijfversleuteling start, moet u de instellingen van Authenticatie-agent-accounts controleren. De Authenticatie-agent is nodig om te werken met schijven die zijn beveiligd met Kaspersky Disk Encryption-technologie (FDE). Voordat het besturingssysteem wordt geladen, moet de gebruiker de authenticatie bij de agent voltooien. Met Kaspersky Endpoint Security kunt u automatisch accounts voor Authenticatie-agent maken voordat u een schijf van encryptie voorziet. U kunt het automatisch maken van accounts voor Authenticatie-agenten inschakelen in de beleidsinstellingen voor Full Disk Encryption (zie de onderstaande instructies). U kunt ook [Single Sign-On-technologie \(SSO\) gebruiken](#).

Met Kaspersky Endpoint Security kunt u automatisch Authenticatie-agent maken voor de volgende gebruikersgroepen.

- **Alle accounts op de computer.** All accounts op de computer die op enig moment actief zijn geweest.
- **Alle domeinaccounts op de computer.** Alle accounts op de computer die behoren tot een bepaald domein en die op enig moment actief zijn geweest.

- **Alle lokale accounts op de computer.** Alle lokale accounts op de computer die op enig moment actief zijn geweest.
- **Service-account met een eenmalig wachtwoord.** De service-account is nodig om toegang te krijgen tot de computer, bijvoorbeeld wanneer de gebruiker het wachtwoord vergeet. U kunt de service-account ook gebruiken als reserve-account. U moet de naam invoeren van de service-account (standaard, ServiceAccount). Kaspersky Endpoint Security maakt automatisch een wachtwoord aan. U kunt het wachtwoord vinden in de [Kaspersky Security Center-console](#).
- **Lokale beheerder.** Kaspersky Endpoint Security maakt een authenticatie-agent-gebruikersaccount voor de lokale beheerder van de computer.
- **Computerbeheerder.** Kaspersky Endpoint Security maakt een authenticatie-agent-gebruikersaccount aan voor de account van de computerbeheerder. In Active Directory kunt u zien welke account de rol van computerbeheerder heeft in de eigenschappen van de computer. Standaard is de rol van computerbeheerder niet gedefinieerd, dat wil zeggen dat deze niet overeenkomt met een account.
- **Actief account.** Kaspersky Endpoint Security maakt automatisch een authenticatie-agent-account aan voor de account die actief is op het moment van schijfversleuteling.

De taak [Accounts voor Authenticatie-agent beheren](#) is ontworpen voor het configureren van instellingen voor gebruikersauthenticatie. U kunt deze taak gebruiken om nieuwe accounts toe te voegen, de instellingen van huidige accounts te wijzigen of accounts te verwijderen indien nodig. U kunt lokale taken voor afzonderlijke computers gebruiken, maar ook groepstaken voor computers uit afzonderlijke beheergroepen of een selectie van computers.

[Kaspersky Disk Encryption uitvoeren via de beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie Kaspersky Disk Encryption**.

Kaspersky Disk Encryption-technologie kan niet worden gebruikt als de computer harde schijven heeft die met BitLocker zijn geëncrypt.

7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven encrypten**.

Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie van alle harde schijven alleen het besturingssysteem laden dat u hebt gebruikt om het programma te installeren.

Als u wilt instellen dat enkele harde schijven niet moeten worden geëncrypt, [maakt u een lijst met die harde schijven aan](#).

8. Configureer geavanceerde Kaspersky Disk Encryption-opties (zie onderstaande tabel).
9. Sla uw wijzigingen op.

[Kaspersky Disk Encryption uitvoeren via de Webconsole en Cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Full Disk Encryption**.
5. Selecteer onder **Manage encryption Kaspersky Disk Encryption**.
6. Klik op de koppeling **Kaspersky Disk Encryption**.  
Dit opent het instellingenvenster van Kaspersky Disk Encryption.

Kaspersky Disk Encryption-technologie kan niet worden gebruikt als de computer harde schijven heeft die met BitLocker zijn geëncrypt.

7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven encrypten**.

Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om de encryptie uit te voeren.

Als u wilt instellen dat enkele harde schijven niet moeten worden geëncrypt, [maakt u een lijst met die harde schijven aan](#).

8. Configureer geavanceerde Kaspersky Disk Encryption-opties (zie onderstaande tabel).
9. Sla uw wijzigingen op.

U kunt de tool Versleutelingsmonitor gebruiken om het proces voor schijfversleuteling of decryptie op de computer van een gebruiker te regelen. U kunt de tool Versleutelingsmonitor uitvoeren vanuit het [hoofdvenster van het programma](#).

Als de harde schijven van het systeem zijn geëncrypt, wordt Authenticatie-agent geladen vóór de opstart van het besturingssysteem. Gebruik Authenticatie-agent voor de authenticatie 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 authenticatie wordt het besturingssysteem geladen. Het authenticatieproces wordt herhaald telkens als het besturingssysteem opnieuw wordt gestart.

Onderdeelinstellingen van Kaspersky Disk Encryption

| Parameter  | Beschrijving   |
|--|--|
| <b>Accounts voor Authenticatie-agent automatisch maken voor gebruikers tijdens encryptie</b> | Als dit selectievakje is ingeschakeld, maakt het programma Authenticatie-agent-accounts op basis van de lijst met Windows-gebruikersaccounts op de computer. Kaspersky Endpoint Security gebruikt standaard alle lokale en domeinaccounts waarmee de gebruiker zich de afgelopen 30 dagen heeft aangemeld bij het besturingssysteem. |

|  |  |
|--|--|
| <p><b>Accounts in Authenticatie-agent automatisch aanmaken voor alle gebruikers van deze computer bij aanmelding</b></p> | <p>Als dit selectievakje is ingeschakeld, zoekt het programma informatie over Windows-gebruikersaccounts op de computer voordat Authenticatie-agent wordt gestart. Als Kaspersky Endpoint Security een Windows-gebruikersaccount detecteert die geen Authenticatie-agent-account heeft, maakt het programma een nieuw account aan voor toegang tot geëncrypte schijven. Het nieuwe Authenticatie-agent-account heeft de volgende standaardinstellingen: alleen met wachtwoord beveiligde aanmelding en wachtwoordwijziging bij eerste authenticatie. Daarom hoeft u niet <a href="#">handmatig Authenticatie-agent-accounts</a> toe te voegen met de taak <i>Authenticatie-agent-accounts beheren</i> voor computers met reeds versleutelde stations.</p>  |
| <p><b>Ingevoerde gebruikersnaam in Authenticatie-agent opslaan</b></p>   | <p>Als het selectievakje is ingeschakeld, slaat het programma de naam van het account in Authenticatie-agent op. U hoeft de accountnaam niet in te voeren de volgende keer dat u in Authenticatie-agent de Authenticatie met hetzelfde account probeert te voltooien.</p>  |
| <p><b>Alleen gebruikte schijfruimte encrypten (snellere encryptie)</b></p>   | <p>Dit selectievakje schakelt de optie in of uit waarmee u het encryptiegebied beperkt tot de gebruikte sectoren van de harde schijf. Via deze beperking kunt u de encryptie verkorten.</p> <div data-bbox="400 779 1493 969" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>De in- of uitschakeling van de functie <b>Encrypt used disk space only (Windows 8 and later versions)</b> na het starten van de encryptie wijzigt deze instelling niet tenzij de harde schijven zijn gedecrypt. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.</p> </div> <p>Als het selectievakje is ingeschakeld, worden alleen delen van de harde schijf die door bestanden worden ingenomen geëncrypt. Kaspersky Endpoint Security encrypt automatisch nieuwe gegevens wanneer die worden toegevoegd.</p> <p>Als het selectievakje is uitgeschakeld, wordt de gehele harde schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden.</p> <div data-bbox="400 1238 1493 1464" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Deze optie wordt aanbevolen voor nieuwe harde schijven waarvan de gegevens niet zijn gewijzigd of verwijderd. Als u een encryptie toepast op een harde schijf die al wordt gebruikt, wordt u aanbevolen de gehele harde schijf te encrypten. Op deze manier zijn alle gegevens beschermd, zelfs verwijderde gegevens die mogelijk kunnen worden hersteld.</p> </div> <p>Dit selectievakje is standaard uitgeschakeld.</p> |
| <p><b>Ondersteuning voor verouderde USB-apparaten gebruiken (niet aanbevolen)</b></p>                                    | <p>Dit selectievakje schakelt de functie Ondersteuning voor verouderde USB-apparaten in of uit. <i>Ondersteuning voor verouderde USB-apparaten</i> is een BIOS/UEFI-functie waarmee u USB-apparaten (zoals een beveiligingstoken) kunt gebruiken tijdens de opstart van de computer voordat het besturingssysteem wordt gestart (BIOS-modus). Ondersteuning voor verouderde USB-apparaten is niet van invloed op de ondersteuning voor USB-apparaten nadat het besturingssysteem is gestart.</p> <p>Als het selectievakje is ingeschakeld, wordt de ondersteuning voor USB-apparaten tijdens de initiële opstart van de computer ingeschakeld.</p> <div data-bbox="400 1921 1493 2148" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f8d7da;"> <p>Wanneer de functie Ondersteuning voor verouderde USB-apparaten is ingeschakeld, biedt de Authenticatie-agent in de BIOS-modus geen ondersteuning voor het werken met tokens via USB. U wordt aanbevolen deze optie alleen te gebruiken als er een probleem met de compatibiliteit van de hardware is en voor computers waarop het probleem is opgetreden.</p> </div>  |

## 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 **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie 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.

7. Zo voegt u harde schijven toe aan de lijst met harde schijven die niet moeten worden geëncrypt:
  - a. Klik op **Toevoegen**.
  - b. Dit opent een venster; in dat venster kunt u de instellingen **Apparaatnaam**, **Computernaam**, **Schijftype**, **Kaspersky Disk Encryption** bewerken.
  - 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.

8. Sla uw wijzigingen op.

## Een lijst met harde schijven die niet moeten worden geëncrypt exporteren en importeren:

U kunt de lijst met uitzonderingen voor de encryptie van harde schijven exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal uitzonderingen van hetzelfde type toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijst met uitzonderingen of om de uitzonderingen naar een andere server te migreren.

### [Een lijst met uitzonderingen voor de encryptie van harde schijven exporteren en importeren in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie 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.
7. De lijst met uitzonderingen exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen uitzonderingen hebt geselecteerd, exporteert Kaspersky Endpoint Security alle uitzonderingen.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
8. De lijst met regels importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
9. Sla uw wijzigingen op.

### [Een lijst met uitzonderingen voor de encryptie van harde schijven exporteren en importeren in de Webconsole](#)



1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Full Disk Encryption**.
5. Selecteer de technologie **Kaspersky Disk Encryption** en volg de link om de instellingen te configureren.  
De encryptie-instellingen worden geopend.
6. Klik op de link **Exclusions**.
7. De lijst met regels exporteren:
  - a. Selecteer de uitzonderingen die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde uitzonderingen wilt exporteren of de volledige lijst met uitzonderingen wilt exporteren.
  - d. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met uitzonderingen wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - e. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de volledige lijst met uitzonderingen naar het XML-bestand.
8. De lijst met regels importeren:
  - a. Klik op **Importeren**.
  - b. Selecteer in het geopende venster het XML-bestand waaruit u de lijst met uitzonderingen wilt importeren.
  - c. Open het bestand.  
Als de computer al een lijst met uitzonderingen heeft, zal Kaspersky Endpoint Security u vragen de bestaande lijst te verwijderen of er nieuwe items aan toe te voegen vanuit het XML-bestand.
9. Sla uw wijzigingen op.

## Eenmalige aanmelding (SSO) inschakelen

Met Single Sign-On (SSO)-technologie kunt u automatisch aanmelden op het besturingssysteem met de inloggegevens van de authenticatie-agent.

Bij gebruik van Single Sign-on-technologie negeert de Authenticatie-agent de vereisten voor wachtwoordsterkte gespecificeerd in Kaspersky Security Center. U kunt de vereisten voor wachtwoordsterkte instellen in de instellingen van het besturingssysteem.

De Single Sign-On-technologie (SSO) is niet compatibel met andere providers van accountgegevens.

### [Het gebruik van Single Sign-On-technologie inschakelen in de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het venster Beleid **Data Encryption** → **Algemene encryptie-instellingen**.
6. In het blok **Wachtwoordinstellingen**, klikt u op de knop **Instellingen**.
7. Schakel in het geopende venster op het tabblad **Authenticatie-agent** het selectievakje **Eenmalige aanmelding (SSO) gebruiken** in.
8. Sla uw wijzigingen op.

Als gevolg hiervan hoeft de gebruiker de authenticatieprocedure slechts één keer met de agent te voltooien. De authenticatieprocedure is niet vereist om het besturingssysteem te laden. Het besturingssysteem wordt automatisch geladen.

### [Single Sign-On inschakelen in de webconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Full Disk Encryption**.
5. Selecteer de technologie **Kaspersky Disk Encryption** en volg de link om de instellingen te configureren.  
De encryptie-instellingen worden geopend.
6. Schakel in het blok **Password settings** het selectievakje **Use Single Sign-On (SSO) technology** in.
7. Sla uw wijzigingen op.

Als gevolg hiervan hoeft de gebruiker de authenticatieprocedure slechts één keer met de agent te voltooien. De authenticatieprocedure is niet vereist om het besturingssysteem te laden. Het besturingssysteem wordt automatisch geladen.

Single Sign-On werkt alleen als het Windows-accountwachtwoord en het wachtwoord voor de account van de authenticatie-agent overeenkomen. Als de wachtwoorden niet overeenkomen, moet de gebruiker de authenticatieprocedure twee keer uitvoeren: in de interface van de authenticatie-agent en voordat het besturingssysteem wordt geladen. Daarna zal Kaspersky Endpoint Security het wachtwoord van het Authenticatieagent-account vervangen door het wachtwoord van het Windows-account.

## Accounts voor Authenticatie-agent beheren

De Authenticatie-agent is nodig om te werken met schijven die zijn beveiligd met Kaspersky Disk Encryption-technologie (FDE). Voordat het besturingssysteem wordt geladen, moet de gebruiker de authenticatie bij de agent voltooien. De taak *Accounts voor Authenticatie-agent beheren* is ontworpen voor het configureren van instellingen voor gebruikersauthenticatie. U kunt lokale taken voor afzonderlijke computers gebruiken, maar ook groepstaken voor computers uit afzonderlijke beheergroepen of een selectie van computers.

U kunt geen schema configureren voor het starten van de taak *Accounts voor Authenticatie-agent beheren*. U kunt ook niet een taak geforceerd laten stoppen.

[De taak voor het beheren van accounts voor Authenticatie-agent maken in de Beheerconsole \(MMC\)](#) 

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

### Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)** → **Accounts voor Authenticatie-agent beheren**.

### Stap 2: Een opdracht voor het beheren van een account voor Authenticatie-agent selecteren

Genereer een lijst met opdrachten voor het beheren van een account voor Authenticatie-agent. Met beheeropdrachten kunt u accounts voor Authenticatie-agent toevoegen, wijzigen en verwijderen (zie onderstaande instructies). Alleen gebruikers met een account voor Authenticatie-agent kunnen de authenticatieprocedure voltooien, het besturingssysteem laden en toegang krijgen tot de geëncrypte schijf.

### Stap 3: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

### Stap 4. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Administrator-accounts* .

### Stap 5. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Dit betekent dat de nieuwe gebruiker, nadat de taak is uitgevoerd wanneer de computer de volgende keer wordt opgestart, de authenticatieprocedure kan voltooien, het besturingssysteem kan laden en toegang kan krijgen tot de geëncrypte schijf.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Accounts voor Authenticatie-agent beheren**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Administrator-accounts*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

## Stap 2: Accounts voor Authenticatie-agent beheren

Genereer een lijst met opdrachten voor het beheren van een account voor Authenticatie-agent. Met beheeropdrachten kunt u accounts voor Authenticatie-agent toevoegen, wijzigen en verwijderen (zie onderstaande instructies). Alleen gebruikers met een account voor Authenticatie-agent kunnen de authenticatieprocedure voltooien, het besturingssysteem laden en toegang krijgen tot de geëncrypte schijf.

## Stap 3. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. U ziet een nieuwe taak in de lijst met taken.

Start een taak door het selectievakje naast de taak in te schakelen en op de knop **Starten** te klikken.

Dit betekent dat de nieuwe gebruiker, nadat de taak is uitgevoerd wanneer de computer de volgende keer wordt opgestart, de authenticatieprocedure kan voltooien, het besturingssysteem kan laden en toegang kan krijgen tot de geëncrypte schijf.

Wanneer u een account voor Authenticatie-agent wilt toevoegen, moet u een speciale opdracht toevoegen aan de taak *accounts voor Authenticatie-agent beheren*. Het is handig om een groepstaak te gebruiken om bijvoorbeeld een beheerdersaccount aan alle computers toe te voegen.

Met Kaspersky Endpoint Security kunt u automatisch accounts voor Authenticatie-agent maken voordat u een schijf van encryptie voorziet. U kunt het automatisch maken van accounts voor Authenticatie-agent inschakelen in de [beleidsinstellingen voor Full Disk Encryption](#). U kunt ook [Single Sign-On-technologie \(SSO\) gebruiken](#).

[Een account voor Authenticatie-agent toevoegen via de Beheerconsole \(MMC\)](#) 

1. Open de eigenschappen van de taak *Accounts voor Authenticatie-agent beheren*.
2. Selecteer in de taakeigenschappen het gedeelte **Instellingen**.
3. Klik op **Toevoegen** → **Opdracht voor toevoegen van account**.
4. Geef in het geopende venster in het veld **Windows-account** de naam op van het Microsoft Windows-account dat wordt gebruikt om het account voor Authenticatie-agent te maken.
5. Als u de Windows-accountnaam handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om de accountbeveiligings-ID (SID) te definiëren.  
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.

Het definiëren van een Windows-accountbeveiligings-ID is nodig om te controleren of de Windows-accountnaam correct is ingevoerd. Als het Windows-account niet bestaat op de computer of in het vertrouwde domein, eindigt de taak *Accounts voor Authenticatie-agent beheren* met een fout.

6. Schakel het selectievakje **Bestaand account vervangen** in als u een eerder gemaakt account met dezelfde naam in Authenticatie-agent wilt vervangen door het nieuwe account.

Deze stap is beschikbaar als u een opdracht voor het aanmaken van een account voor Authenticatie-agent toevoegt aan de eigenschappen van een groepstaak voor het beheer van accounts voor Authenticatie-agent. Deze stap is niet beschikbaar als u een opdracht voor het aanmaken van een account voor Authenticatie-agent toevoegt aan de eigenschappen van de lokale taak *Accounts voor Authenticatie-agent beheren*.

7. Typ in het veld **Gebruikersnaam** de naam van het account voor Authenticatie-agent dat tijdens de authenticatie voor de toegang tot geëncrypte harde schijven moet worden ingevoerd.
8. Schakel het selectievakje **Authenticatie met wachtwoord toestaan** in als u wilt dat het programma de gebruiker vraagt om het wachtwoord voor het account voor Authenticatie-agent in te voeren tijdens de authenticatie voor de toegang tot geëncrypte harde schijven. Stel een wachtwoord in voor het account voor Authenticatie-agent. Indien nodig kunt u na de eerste authenticatie een nieuw wachtwoord aanvragen bij de gebruiker.
9. Schakel het selectievakje **Authenticatie 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 authenticatie voor de toegang tot geëncrypte harde schijven. Selecteer een certificaatbestand voor authenticatie met een smartcard of token.
10. Typ indien nodig in het veld **Beschrijving van opdracht** de gegevens van het account voor Authenticatie-agent dat u nodig hebt voor het beheer van de opdracht.
11. In het blok **Toegang tot authenticatie in Authenticatie-agent**, configureert u de toegang tot authenticatie in Authentication Agent voor de gebruiker die het account gebruikt dat is opgegeven in de opdracht.
12. Sla uw wijzigingen op.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de taak **Accounts voor Authenticatie-agent beheren** van Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Klik in de lijst met accounts voor Authenticatie-agent op de knop **Add**.

Hiermee start u de wizard Accounts voor Authenticatie-agent beheren.

5. Selecteer het opdrachttype **Add**.

6. Selecteer een gebruikersaccount. U kunt een account selecteren in de lijst met domeinaccounts of de accountnaam handmatig invoeren. Ga naar de volgende stap.

Kaspersky Endpoint Security bepaalt de accountbeveiligings-ID (SID). Dit is nodig om het account te verifiëren. Als u de gebruikersnaam verkeerd hebt ingevoerd, eindigt Kaspersky Endpoint Security de taak met een fout.

7. Configureer de accountinstellingen van de Authenticatie-agent.

- **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security scant bestaande accounts op de computer. Als de gebruikersbeveiligings-ID op de computer en in de taak overeenkomen, wijzigt Kaspersky Endpoint Security de gebruikersaccountinstellingen wijzigen in overeenstemming met de taak.
- **User name.** De standaard gebruikersnaam van de het account voor de Authenticatie-agent komt overeen met de domeinnaam van de gebruiker.
- **Allow password-based authentication.** Stel een wachtwoord in voor het account voor Authenticatie-agent. Indien nodig kunt u na de eerste authenticatie een nieuw wachtwoord aanvragen bij de gebruiker. Hierdoor heeft elke gebruiker zijn eigen unieke wachtwoord. U kunt ook vereisten voor wachtwoordsterkte instellen voor het account voor de Authenticatie-agent in het beleid.
- **Allow certificate-based authentication.** Selecteer een certificaatbestand voor authenticatie met een smartcard of token. Dit zorgt ervoor dat de gebruiker het wachtwoord voor de smartcard of het token moet invoeren.
- **Account access to encrypted data.** Configureer gebruikerstoegang tot de geëncrypte schijf. U kunt bijvoorbeeld gebruikersauthenticatie tijdelijk uitschakelen in plaats van het account voor de Authenticatie-agent te verwijderen.
- **Comment.** Voer indien nodig een accountbeschrijving in.

8. Sla uw wijzigingen op.

9. Start een taak door het selectievakje naast de taak aan te vinken en op de knop **Starten** te klikken.

Dit betekent dat de nieuwe gebruiker, nadat de taak is uitgevoerd wanneer de computer de volgende keer wordt opgestart, de authenticatieprocedure kan voltooien, het besturingssysteem kan laden en toegang kan krijgen tot de geëncrypte schijf.

Wanneer u het wachtwoord en andere instellingen van het account voor de Authenticatie-agent wilt wijzigen, moet u een speciale opdracht toevoegen aan de taak *Accounts voor Authenticatie-agent beheren*. Het is bijvoorbeeld handig om een groepstaak te gebruiken om het tokencertificaat van de beheerder op alle computers te vervangen.

[Het account voor Authenticatie-agent wijzigen via de Beheerconsole \(MMC\)](#) 



1. Open de eigenschappen van de taak *Accounts voor Authenticatie-agent beheren*.
2. Selecteer in de taakeigenschappen het gedeelte **Instellingen**.
3. Klik op **Toevoegen** → **Opdracht voor bewerken van account**.
4. Geef in het geopende venster in het veld **Windows-account** de naam op van het Microsoft Windows-gebruikersaccount dat u wilt wijzigen.
5. Als u de Windows-accountnaam handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om de accountbeveiligings-ID (SID) te definiëren.  
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.

Het definiëren van een Windows-accountbeveiligings-ID is nodig om te controleren of de Windows-accountnaam correct is ingevoerd. Als het Windows-account niet bestaat op de computer of in het vertrouwde domein, eindigt de taak *Accounts voor Authenticatie-agent beheren* met een fout.

6. Schakel het selectievakje **Gebruikersnaam wijzigen** in en voer een nieuwe naam voor het account voor Authenticatie-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 voor Authenticatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.
7. Schakel het selectievakje **Instellingen voor authenticatie met wachtwoord wijzigen** in om de instellingen voor de authenticatie met een wachtwoord te kunnen bewerken.
8. Schakel het selectievakje **Authenticatie met wachtwoord toestaan** in als u wilt dat het programma de gebruiker vraagt om het wachtwoord voor het account voor Authenticatie-agent in te voeren tijdens de authenticatie voor de toegang tot geëncrypte harde schijven. Stel een wachtwoord in voor het account voor Authenticatie-agent.
9. Schakel het selectievakje **Regel voor wijziging van wachtwoord bij authenticatie in Authenticatie-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 voor Authenticatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.
10. Geef de waarde voor de wijziging van wachtwoorden bij de authenticatie in Authenticatie-agent op.
11. Schakel het selectievakje **Instellingen voor authenticatie met certificaat wijzigen** in om de instellingen voor de authenticatie met het elektronische token- of smartcardcertificaat te kunnen bewerken.
12. Schakel het selectievakje **Authenticatie 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 authenticatie voor de toegang tot geëncrypte harde schijven. Selecteer een certificaatbestand voor authenticatie met een smartcard of token.
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 voor Authenticatie-agent die zijn gemaakt op basis van het Microsoft Windows-account met de opgegeven naam in het veld **Windows-account**.
14. Schakel het selectievakje **Toegangsregel voor authenticatie in Authenticatie-agent bewerken** in als u wilt dat Kaspersky Endpoint Security de regel voor de toegang van gebruikers tot het authenticatievenster in

Authenticatie-agent wijzigt in de eronder opgegeven waarde voor alle accounts voor Authenticatie-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 authenticatievenster in Authenticatie-agent op.

16. Sla uw wijzigingen op.

[Het account voor Authenticatie-agent wijzigen via de Webconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de taak **Accounts voor Authenticatie-agent beheren** van Kaspersky Endpoint Security.  
U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Klik in de lijst met accounts voor Authenticatie-agent op de knop **Add**.  
Hiermee start u de wizard Accounts voor Authenticatie-agent beheren.
5. Selecteer het opdrachttype **Change**.
6. Selecteer een gebruikersaccount. U kunt een account selecteren in de lijst met domeinaccounts of de accountnaam handmatig invoeren. Ga naar de volgende stap.  
Kaspersky Endpoint Security bepaalt de accountbeveiligings-ID (SID). Dit is nodig om het account te verifiëren. Als u de gebruikersnaam verkeerd hebt ingevoerd, eindigt Kaspersky Endpoint Security de taak met een fout.
7. Schakel de selectievakjes in naast de instellingen die u wilt bewerken.
8. Configureer de accountinstellingen van de Authenticatie-agent.
  - **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security scant bestaande accounts op de computer. Als de gebruikersbeveiligings-ID op de computer en in de taak overeenkomen, wijzigt Kaspersky Endpoint Security de gebruikersaccountinstellingen wijzigen in overeenstemming met de taak.
  - **User name.** De standaard gebruikersnaam van de het account voor de Authenticatie-agent komt overeen met de domeinnaam van de gebruiker.
  - **Allow password-based authentication.** Stel een wachtwoord in voor het account voor Authenticatie-agent. Indien nodig kunt u na de eerste authenticatie een nieuw wachtwoord aanvragen bij de gebruiker. Hierdoor heeft elke gebruiker zijn eigen unieke wachtwoord. U kunt ook vereisten voor wachtwoordsterkte instellen voor het account voor de Authenticatie-agent in het beleid.
  - **Allow certificate-based authentication.** Selecteer een certificaatbestand voor authenticatie met een smartcard of token. Dit zorgt ervoor dat de gebruiker het wachtwoord voor de smartcard of het token moet invoeren.
  - **Account access to encrypted data.** Configureer gebruikerstoegang tot de geëncrypte schijf. U kunt bijvoorbeeld gebruikersauthenticatie tijdelijk uitschakelen in plaats van het account voor de Authenticatie-agent te verwijderen.
  - **Comment.** Voer indien nodig een accountbeschrijving in.
9. Sla uw wijzigingen op.
10. Start een taak door het selectievakje naast de taak aan te vinken en op de knop **Starten** te klikken.

Wanneer u een account voor Authenticatie-agent wilt verwijderen, moet u een speciale opdracht toevoegen aan de taak *accounts voor Authenticatie-agent beheren*. Het is bijvoorbeeld handig om een groepstaak te gebruiken om het account van een vertrokken werknemer te verwijderen.

## [Een account voor Authenticatie-agent verwijderen via de Beheerconsole \(MMC\)](#)

1. Open de eigenschappen van de taak *Accounts voor Authenticatie-agent beheren*.
2. Selecteer in de taakeigenschappen het gedeelte **Instellingen**.
3. Klik op **Toevoegen** → **Opdracht voor verwijderen van account**.
4. Geef in het geopende venster in het veld **Windows-account** de naam op van het Microsoft Windows-gebruikersaccount dat is gebruikt om het account voor Authenticatie-agent te maken dat u nu wilt verwijderen.
5. Als u de Windows-accountnaam handmatig hebt ingevoerd, klikt u op de knop **Toestaan** om de accountbeveiligings-ID (SID) te definiëren.  
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.

Het definiëren van een Windows-accountbeveiligings-ID is nodig om te controleren of de Windows-accountnaam correct is ingevoerd. Als het Windows-account niet bestaat op de computer of in het vertrouwde domein, eindigt de taak *Accounts voor Authenticatie-agent beheren* met een fout.

6. Sla uw wijzigingen op.

## [Een account voor Authenticatie-agent verwijderen via de Webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de taak **Accounts voor Authenticatie-agent beheren** van Kaspersky Endpoint Security.  
U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Klik in de lijst met accounts voor Authenticatie-agent op de knop **Add**.  
Hiermee start u de wizard Accounts voor Authenticatie-agent beheren.
5. Selecteer het opdrachttype **Delete**.
6. Selecteer een gebruikersaccount. U kunt een account selecteren in de lijst met domeinaccounts of de accountnaam handmatig invoeren.
7. Sla uw wijzigingen op.
8. Start een taak door het selectievakje naast de taak aan te vinken en op de knop **Starten** te klikken.  
  
Als gevolg hiervan zal de gebruiker nadat de taak is voltooid, de authenticatieprocedure niet kunnen voltooien en het besturingssysteem niet kunnen laden de volgende keer dat de computer wordt opgestart. Kaspersky Endpoint Security weigert toegang tot geëncrypte gegevens.

Wanneer u de lijst wilt zien van gebruikers die de authenticatie met de Agent kunnen voltooien en het besturingssysteem kunnen laden, moet u naar de eigenschappen van de beheerde computer gaan.

### [De lijst met accounts voor Authenticatie-agent bekijken via de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Dubbelklik om het venster met de eigenschappen van de computer te openen.
5. Selecteer het gedeelte **Taken** in het venster met computereigenschappen.
6. Selecteer in de takenlijst **Authenticatie-agent-accounts beheren** en open de taakeigenschappen door te dubbelklikken.
7. Selecteer in de taakeigenschappen het gedeelte **Instellingen**.

U hebt hierdoor toegang tot een lijst met accounts voor Authenticatie-agents op deze computer. Alleen gebruikers in die lijst kunnen authenticatie voltooien met de Agent en het besturingssysteem laden.

### [Een lijst met accounts voor Authenticatie-agent bekijken via de Webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Klik op de naam van de computer waarop u de lijst met accounts voor Authenticatie-agent wilt bekijken.
3. Selecteer het tabblad **Taken** in de computereigenschappen.
4. Selecteer in de lijst met taken **Accounts voor Authenticatie-agent beheren**.
5. Selecteer het tabblad **Programma-instellingen** in de taakeigenschappen.

U hebt hierdoor toegang tot een lijst met accounts voor Authenticatie-agents op deze computer. Alleen gebruikers in die lijst kunnen authenticatie voltooien met de Agent en het besturingssysteem laden.

## Een token en een smartcard met Authenticatie-agent gebruiken

Een token of een smartcard kan voor de authenticatie tijdens de toegang tot geëncrypte harde schijven worden gebruikt. Om dit te doen, moet u het elektronische certificaatbestand van een token of smartcard toevoegen aan de taak *Accounts voor Authenticatie-agent beheren*.

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.

Kaspersky Endpoint Security ondersteunt de volgende tokens, smartcardlezers en smartcards:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Om een elektronisch token- of smartcardcertificaat toe te voegen aan de opdracht voor het maken van een account voor Authenticatie-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.
- Het certificaat bevat een RSA-sleutel met een minimale lengte van 1024 bits.

Als het elektronische certificaat van het token of de smartcard niet aan deze vereisten voldoet, kunt u het certificaatbestand niet laden in de opdracht voor het maken van een Authentication Agent-account.

De parameter `KeyUsage` van het certificaat moet de waarde `keyEncipherment` of `dataEncipherment` hebben. De parameter `KeyUsage` bepaalt het doel van het certificaat. Als de parameter een andere waarde heeft, zal Kaspersky Security Center het certificaatbestand downloaden, maar een waarschuwing weergeven.

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 Authenticatie-agent. Vervolgens moet de gebruiker de procedure voor het [krijgen van toegang tot geëncrypte apparaten of het terugzetten van gegevens op geëncrypte apparaten](#) voltooien.

## 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 **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de technologie waarmee de harde schijven zijn geëncrypt.
7. Doe een van de volgende acties:
  - 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.

8. Sla uw wijzigingen op.

U kunt de tool Versleutelingsmonitor gebruiken om het proces voor schijfversleuteling of decryptie op de computer van een gebruiker te regelen. U kunt de tool Versleutelingsmonitor uitvoeren vanuit het [hoofdvenster van het programma](#).

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 Authenticatie-agent vóór de volgende opstart van het besturingssysteem geladen. Kaspersky Endpoint Security hervat de decryptie van de harde schijf na de geslaagde authenticatie in Authenticatie-agent en de opstart van het besturingssysteem.

Als het besturingssysteem in de sluimerstand gaat wanneer harde schijven worden gecrypteerd, worden ze geëncrypt met de technologie Kaspersky Disk Encryption, wordt Authenticatie-agent geladen wanneer het besturingssysteem uit de sluimerstand wordt gehaald. Kaspersky Endpoint Security hervat de decryptie van de harde schijf na de geslaagde authenticatie in Authenticatie-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 Authenticatie-agent te laden.

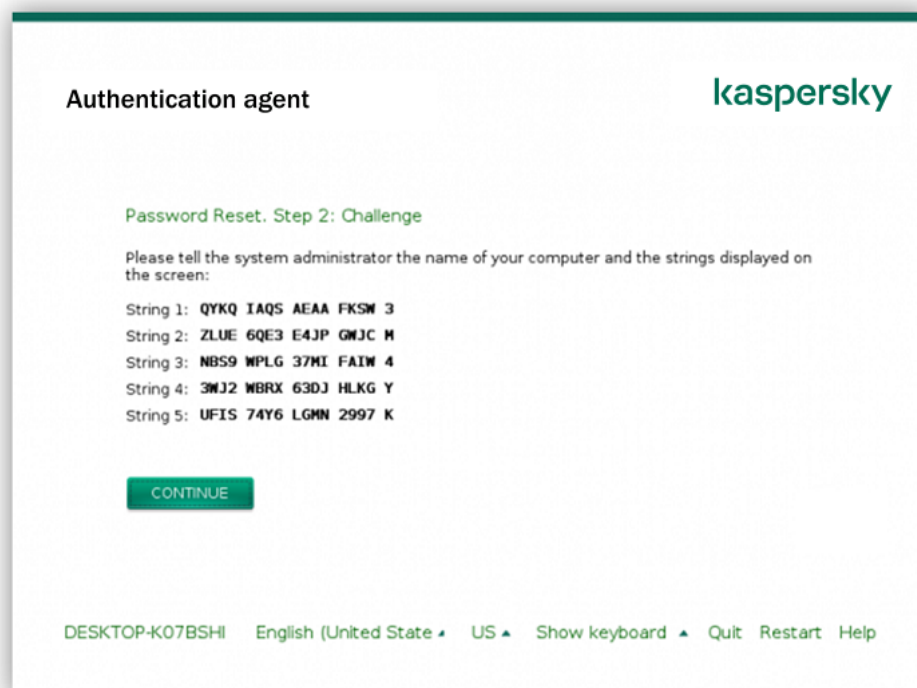
## Toegang herstellen tot een schijf beschermd met de Kaspersky Disk Encryption-technologie

Als een gebruiker het wachtwoord is vergeten voor toegang tot een harde schijf beschermd met de Kaspersky Disk Encryption-technologie, moet u de herstelprocedure starten (Request-Response). U kunt ook het [service-account](#) gebruiken om toegang te krijgen tot de harde schijf als deze functie ingeschakeld is in de instellingen voor schijfversleuteling.

### Toegang tot de harde schijf van het systeem herstellen

Het herstellen van de toegang tot een harde schijf van een systeem beschermd met de Kaspersky Disk Encryption-technologie bestaat uit de volgende stappen:

1. De gebruiker meldt de verzoekblokken aan de beheerder (zie onderstaande figuur).
2. De beheerder voert de verzoekblokken in Kaspersky Security Center in, ontvangt de antwoordblokken en meldt de antwoordblokken aan de gebruiker.
3. De gebruiker voert de antwoordblokken in de Authentication Agent-interface in en krijgt toegang tot de harde schijf.





Om de herstelprocedure te starten, moet de gebruiker op de knop **Wachtwoord vergeten?** klikken in de interface van Authenticatie-agent.

### [Antwoordblokken verkrijgen voor een systeemschijf beschermd met de Kaspersky Disk Encryption-technologie in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster het tabblad **Authenticatie-agent**.
7. Selecteer in het blok **Huidig encryptiealgoritme** het type van het encryptiealgoritme: **AES56** of **AES256**.  
Het algoritme voor gegevensencryptie hangt af van de AES-encryptiebibliotheek die bij het distributiepakket wordt meegeleverd: *sterke encryptie (AES256)* of *normale encryptie (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.
8. Selecteer in de vervolgkeuzelijst **Account** de naam van het gemaakte account voor Authenticatie-agent voor de gebruiker die het herstel van de toegang tot de schijf heeft aangevraagd.
9. Selecteer in de vervolgkeuzelijst **Harde schijf** de geëncrypte harde schijf waarvoor u de toegang wilt herstellen.
10. Voer in het blok **Gebruikersaanvraag** de blokken van de aanvraag in die de gebruiker geeft.

De inhoud van de blokken van het antwoord op het verzoek van de gebruiker voor het herstel van de gebruikersnaam en het wachtwoord van een account voor Authenticatie-agent wordt in het veld **Toegangssleutel** weergegeven. Breng de inhoud van de antwoordblokken over naar de gebruiker.

### [Antwoordblokken verkrijgen voor een systeemschijf beschermd met de Kaspersky Disk Encryption-technologie in de webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de schijf wilt herstellen.
3. Klik op de knop **Grant access to the device in offline mode**.
4. Selecteer in het geopende venster het gedeelte **Authenticatie-agent**.
5. Selecteer in de vervolgkeuzelijst **Account** de naam van het gemaakte account voor Authenticatie-agent voor de gebruiker die het herstel van de naam en het wachtwoord van het account voor Authenticatie-agent heeft gevraagd.
6. Voer de verzoekblokken in die door de gebruiker zijn overgebracht.

De inhoud van de blokken van het antwoord op de gebruikersaanvraag voor het herstel van de gebruikersnaam en het wachtwoord van een account van de Authenticatie-agent wordt onderaan het venster weergegeven. Breng de inhoud van de antwoordblokken over naar de gebruiker.

Na het voltooien van de herstelprocedure, zal de authenticatie-agent de gebruiker vragen het wachtwoord te wijzigen.

## Toegang herstellen tot een niet-systeem harde schijf

Het herstellen van de toegang tot een niet-systeem harde schijf beschermd met de Kaspersky Disk Encryption-technologie bestaat uit de volgende stappen:

1. De gebruiker stuurt een bestand met toegangsaanvraag naar de beheerder.
2. De beheerder voegt het bestand met toegangsaanvraag toe aan Kaspersky Security Center, maakt een bestand met toegangssleutel aan en stuurt het naar de gebruiker.
3. De gebruiker voegt het toegangssleutelbestand toe aan Kaspersky Endpoint Security en krijgt toegang tot de harde schijf.

Om de herstelprocedure te starten, moet de gebruiker proberen toegang te krijgen tot een harde schijf. Als gevolg hiervan zal Kaspersky Endpoint Security een bestand van de toegangsaanvraag maken (een bestand met de extensie KESDC), dat de gebruiker bijvoorbeeld per e-mail naar de beheerder moet sturen.

[Een toegangssleutelbestand verkrijgen voor een geëncrypte niet-systeem harde schijf in de beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster het tabblad **Gegevensencryptie**.
7. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.
8. Geef in het venster voor het selecteren van een bestand met verzoektoegang het pad op naar het bestand dat van de gebruiker is ontvangen.

U ziet informatie over het verzoek van de gebruiker. Kaspersky Security Center genereert een sleutelbestand. E-mail het gegenereerde bestand met de sleutel voor toegang tot de geëncrypte gegevens naar de gebruiker. Of sla het toegangsbestand op en gebruik een beschikbare methode om het bestand over te dragen.

### [Een bestand met een toegangssleutel voor een geëncrypte niet-systeem harde schijf verkrijgen in de webconsole](#)



1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
  2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.
  3. Klik op de knop **Grant access to the device in offline mode**.
  4. Selecteer het gedeelte **Gegevensencryptie**.
  5. Klik op de knop **Select file** en selecteer het bestand van de toegangs aanvraag dat u van de gebruiker hebt ontvangen (een bestand met de extensie KESDC).

De webconsole geeft informatie over de aanvraag weer. Dit omvat de naam van de computer waarop de gebruiker toegang tot het bestand vraagt.
  6. Klik op de knop **Sleutel opslaan** en selecteer een map om het bestand met de toegangssleutel voor de geëncrypte gegevens op te slaan (een bestand met de extensie KESDR).
- Als gevolg hiervan kunt u de gegevenstoegangssleutel verkrijgen, die u aan de gebruiker moet overdragen.

## Aanmelden met het service-account van de authenticatie-agent

Met Kaspersky Endpoint Security kunt u een Authenticatie-agent service-account maken voordat u een [schijf versleutelt](#). De service-account is nodig om toegang te krijgen tot de computer, bijvoorbeeld wanneer de gebruiker het wachtwoord vergeet. U kunt de service-account ook gebruiken als reserve-account. Om een account toe te voegen, selecteert u een service-account in [de instellingen voor schijfversleuteling](#) en voert u de naam van de gebruikersaccount in (standaard ServiceAccount). Om te authentifieren met behulp van de agent, hebt u een eenmalig wachtwoord nodig.

### [Het eenmalige wachtwoord achterhalen in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Dubbelklik om het venster met de eigenschappen van de computer te openen.
5. Selecteer het gedeelte **Taken** in het venster met computereigenschappen.
6. Selecteer in de takenlijst **Authenticatie-agent-accounts beheren** en open de taakeigenschappen door te dubbelklikken.
7. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
8. Selecteer in de lijst met accounts de serviceaccount van de authenticatie-agent (bijvoorbeeld WIN10-USER\ServiceAccount).
9. Selecteer in de vervolgkeuzelijst **Actie, Account weergeven**.
10. Selecteer in accounteigenschappen het selectievakje **Origineel wachtwoord tonen**.
11. Kopieer het eenmalige wachtwoord voor het inloggen met de service-account.

### [Het eenmalige wachtwoord in de webconsole achterhalen](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Klik op de naam van de computer waarop u de lijst met accounts voor Authenticatie-agent wilt bekijken.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Taken** in de computereigenschappen.
4. Selecteer in de lijst met taken **Accounts voor Authenticatie-agent beheren**.
5. Selecteer het tabblad **Programma-instellingen** in de taakeigenschappen.
6. Selecteer in de lijst met accounts de serviceaccount van de authenticatie-agent (bijvoorbeeld WIN10-USER\ServiceAccount).
7. Selecteer in accounteigenschappen het selectievakje **Origineel wachtwoord tonen**.
8. Kopieer het eenmalige wachtwoord voor het inloggen met de service-account.

Kaspersky Endpoint Security werkt het wachtwoord automatisch bij elke keer dat een gebruiker zich met de service-account authenticaceert. Nadat u zich heeft geauthenticeerd met behulp van de agent, moet u het wachtwoord van het Windows-account invoeren. Wanneer u zich aanmeldt met het service-account, kunt u de SSO-technologie niet gebruiken.

## Besturingssysteem updaten

Er zijn een aantal bijzondere aandachtspunten waarmee u rekening moet houden wanneer u het besturingssysteem updatet van een computer die met Full Disk Encryption (FDE) beveiligd is. Update het besturingssysteem als volgt: update eerst het besturingssysteem op een computer, update dan het besturingssysteem op een klein aantal computers en update vervolgens het besturingssysteem op alle andere computers in het netwerk.

Als u Kaspersky Disk Encryption-technologie gebruikt, wordt Authenticatie-agent geladen voordat het besturingssysteem wordt gestart. Met Authenticatie-agent kan de gebruiker zich aanmelden bij het systeem en toegang tot geëncrypte schijven krijgen. Daarna wordt het besturingssysteem geladen.

Als u het besturingssysteem begint te updaten op een computer die is beveiligd met Kaspersky Disk Encryption-technologie, wordt Authenticatie-agent verwijderd door de wizard Besturingssysteem updaten. Hierdoor raakt de computer vergrendeld omdat het laadprogramma van het besturingssysteem geen toegang tot de geëncrypte schijf krijgt.

Voor informatie over het veilig update van het besturingssysteem raadpleegt u de [Knowledge Base van de Technische Support](#).

Automatisch updaten van het besturingssysteem is mogelijk onder de volgende voorwaarden:

1. Het besturingssysteem wordt geüpdatet via WSUS (Windows Server Update Services).
2. Windows 10 versie 1607 (RS1) of hoger is op de computer geïnstalleerd.
3. Kaspersky Endpoint Security versie 11.2.0 of hoger is op de computer geïnstalleerd.

Als aan alle voorwaarden is voldaan, kunt u het besturingssysteem op de gebruikelijke manier updaten.

Als u Kaspersky Disk Encryption-technologie (FDE) gebruikt en Kaspersky Endpoint Security voor Windows versie 11.1.0 of 11.1.1 op de computer is geïnstalleerd, hoeft u de harde schijven niet te decrypten om Windows 10 te updaten.

Om het besturingssysteem te updaten, moet u het volgende doen:

1. Kopieer voordat u het systeem bijwerkt de stuurprogramma's met de naam cm\_km.inf, cm\_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf en klfdefsf.sys naar een lokale map. Bijvoorbeeld naar C:\fde\_drivers.
2. Voer de installatie van de systeemupdate uit met de switch `/ReflectDrivers` en specificeer de map met de opgeslagen stuurprogramma's:  
`setup.exe /ReflectDrivers C:\fde_drivers`

Als u BitLocker-technologie voor stationsversleuteling gebruikt, hoeft u de harde schijven niet te decrypten om Windows 10 te updaten. Voor meer informatie over BitLocker gaat u naar de [website van Microsoft](#).

## Fouten na updaten van encryptiefunctiefunctionaliteit verhelpen

Full Disk Encryption wordt bijgewerkt wanneer een oudere versie van het programma wordt bijgewerkt naar Kaspersky Endpoint Security voor Windows 11.9.0.

Bij de start van het updateproces voor de functionaliteit Full Disk Encryption kunnen de volgende fouten optreden:

- De update kan niet worden geïnitieerd.
- Apparaat is niet compatibel met Authenticatie-agent.

*Zo verhelpt u fouten die optreden wanneer u het updateproces voor Full Disk Encryption in de nieuwe programmaversie start:*

1. [Decrypt harde schijven](#).
2. [Encrypt harde schijven](#) opnieuw.

Tijdens het updaten van de functionaliteit Full Disk Encryption kunnen de volgende fouten optreden:

- De update kan niet worden voltooid.
- Het terugdraaien van de Full Disk Encryption-upgrade wordt met een fout voltooid.

*Als u fouten wilt verhelpen die zich voordoen tijdens het updateproces van de functionaliteit Full Disk Encryption,*

[herstelt u de toegang tot geëncrypte apparaten met behulp van de Herstelvoorziening](#).

## Het tracingniveau voor Authenticatie-agent selecteren

Het programma registreert in het tracebestand service-informatie over de werking van Authenticatie-agent en informatie over de bewerkingen van de gebruiker met Authenticatie-agent.

*Zo selecteert u het tracingniveau voor Authenticatie-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 Authenticatie-agent aan te roepen.

2. Selecteer het tracingniveau in het venster met de instellingen van Authenticatie-agent:

- **Disable debug logging (default).** Als deze optie is geselecteerd, registreert het programma in het tracebestand geen informatie over gebeurtenissen van Authenticatie-agent.
- **Enable debug logging.** Als deze optie is geselecteerd, registreert het programma in het tracebestand informatie over de werking van Authenticatie-agent en de bewerkingen die de gebruiker met Authenticatie-agent heeft uitgevoerd.
- **Enable verbose logging.** Als deze optie is geselecteerd, registreert het programma in het tracebestand gedetailleerde informatie over de werking van Authenticatie-agent en de bewerkingen die de gebruiker met Authenticatie-agent heeft uitgevoerd.

Met deze optie worden meer details geregistreerd in vergelijking met de optie **Enable debug logging**. De registratie van meer details kan de opstart van Authenticatie-agent en het besturingssysteem vertragen.

- **Enable debug logging and select serial port.** Als deze optie is geselecteerd, registreert het programma in het tracebestand informatie over de werking van Authenticatie-agent en de bewerkingen die de gebruiker met Authenticatie-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 Authenticatie-agent vanaf de andere computer worden onderzocht.
- **Enable verbose debug logging and select serial port.** Als deze optie is geselecteerd, registreert het programma in het tracebestand gedetailleerde informatie over de werking van Authenticatie-agent en de bewerkingen die de gebruiker met Authenticatie-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 **Enable debug logging and select serial port**. De registratie van meer details kan de opstart van Authenticatie-agent en het besturingssysteem vertragen.

De gegevens worden in het tracebestand van Authenticatie-agent geregistreerd als de computer geëncrypte harde schijven heeft of tijdens een Full Disk Encryption.

Het tracebestand van Authenticatie-agent wordt niet naar Kaspersky verstuurd, in tegenstelling tot andere tracebestanden van het programma. U kunt indien nodig het tracebestand van Authenticatie-agent handmatig versturen naar Kaspersky voor analyse.

## Helpteksten van Authenticatie-agent bewerken

Alvorens Help-berichten van Authenticatie-agent te bewerken, moet u de lijst met ondersteunde tekens in een preboot-omgeving bekijken (zie hieronder).

*Zo bewerkt u Help-berichten van Authenticatie-agent:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.

4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

5. Selecteer in het venster Beleid **Gegevensencryptie** → **Algemene encryptie-instellingen**.

6. In het blok **Sjablonen**, klikt u op de knop **Help**.

7. Doe in het venster dat opent het volgende:

- Selecteer het tabblad **Authenticatie** voor de bewerking van de weergegeven Help-tekst in het venster van Authenticatie-agent tijdens de invoer van de accountgegevens.
- Selecteer het tabblad **Wachtwoord wijzigen** voor de bewerking van de weergegeven Help-tekst in het venster van Authenticatie-agent wanneer het wachtwoord van het account voor Authenticatie-agent wordt gewijzigd.
- Selecteer het tabblad **Wachtwoord herstellen** voor de bewerking van de weergegeven Help-tekst in het venster van Authenticatie-agent wanneer het wachtwoord van het account voor Authenticatie-agent wordt hersteld.

8. Bewerk de Help-berichten.

Als u de originele tekst wilt herstellen, klikt u op de knop **Standaard**.

U kunt een Help-tekst van 16 regels of minder invoeren. De maximale lengte van een regel is 64 tekens.

9. Sla uw wijzigingen op.

## Beperkte ondersteuning voor tekens in Help-berichten van Authenticatie-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)
- Munteenheden (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 aanbevolen zulke tekens niet te gebruiken in Help-berichten van Authenticatie-agent.

## Verwijderen van overgebleven objecten en gegevens na het testen van de werking van Authenticatie-agent

Als Kaspersky Endpoint Security objecten en gegevens vindt die na de test van Authenticatie-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 Authenticatie-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 Authenticatie-agent is getest.

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

- Met het Kaspersky Security Center-beleid.
- [Met de Restore Utility](#).

*Zo gebruikt u een Kaspersky Security Center-beleid om objecten en gegevens te verwijderen die na de geteste werking van Authenticatie-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.

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

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

## Beheer van BitLocker

*BitLocker* is een encryptietechnologie die is ingebouwd in Windows-besturingssystemen. Met Kaspersky Endpoint Security kunt u BitLocker beheren. BitLocker zorgt voor de encryptie van logische volumes. BitLocker kan niet worden gebruikt voor de encryptie van verwisselbare schijven. Voor meer informatie over BitLocker raadpleegt u de [Microsoft-documentatie](#).

BitLocker biedt veilige opslag van toegangssleutels met behulp van een vertrouwde platformmodule. Een *Trusted Platform Module (TPM)* is een microchip die ontwikkeld is om basisfuncties voor beveiliging te leveren (bijvoorbeeld de opslag van encryptiesleutels). Een Trusted Platform Module wordt meestal op het moederbord van de computer geïnstalleerd en werkt via de hardwarebus samen met alle andere systeemonderdelen. Het gebruik van TPM is de veiligste manier om BitLocker-toegangssleutels op te slaan, aangezien TPM pre-opstartverificatie van de systeemintegriteit biedt. U kunt nog steeds schijven encrypten op een computer zonder een TPM. In dat geval wordt de toegangssleutel geëncrypt met een wachtwoord. BitLocker gebruikt de volgende authenticatiemethoden:

- TPM.
- TPM en pincode.
- Wachtwoord.

Na het encrypten van een schijf, maakt BitLocker een hoofdsleutel aan. Kaspersky Endpoint Security stuurt de hoofdsleutel naar Kaspersky Security Center zodat u [de toegang tot de schijf kunt herstellen](#), bijvoorbeeld als een gebruiker het wachtwoord is vergeten.

Als een gebruiker een schijf van encryptie voorziet met BitLocker, stuurt Kaspersky Endpoint Security [informatie over schijfencryptie naar Kaspersky Security Center](#). Kaspersky Endpoint Security stuurt de hoofdsleutel echter niet naar Kaspersky Security Center. Hierdoor is het niet mogelijk om de toegang tot de schijf te herstellen met Kaspersky Security Center. Om te zorgen dat BitLocker correct werkt met Kaspersky Security Center, moet u [de schijf decrypten](#) en [de schijf opnieuw encrypten](#) met een beleid. U kunt een schijf lokaal decrypten of een beleid gebruiken.

Na het encrypten van de harde schijf van het systeem, moet de gebruiker BitLocker-verificatie doorlopen om het besturingssysteem op te starten. Na de authenticatieprocedure kunnen gebruikers met BitLocker inloggen. BitLocker ondersteunt geen technologie voor eenmalige aanmelding (SSO).

Als u Windows-groepsbeleid gebruikt, schakelt u BitLocker-beheer uit in de beleidsinstellingen. De beleidsinstellingen van Windows kunnen in strijd zijn met de beleidsinstellingen van Kaspersky Endpoint Security. Bij het encrypten van een schijf kunnen er fouten optreden.

## BitLocker-stationsversleuteling starten

Voordat u de Full Disk Encryption start, wordt u aanbevolen te controleren of de computer niet geïnfecteerd is. U kunt dit doen door een Volledige Scan of Kritieke Gebiedenscan te starten. Een Full Disk Encryption uitvoeren op een computer die is geïnfecteerd met een rootkit kan de computer onklaar maken.

Als u BitLocker-stationsversleuteling wilt gebruiken op computers met Windows-besturingssystemen voor servers, moet u mogelijk het onderdeel BitLocker-stationsversleuteling installeren. Installeer het onderdeel met behulp van de tools van het besturingssysteem (Wizard Rollen en onderdelen toevoegen). Raadpleeg de [Microsoft-documentatie](#) voor meer informatie over het installeren van BitLocker-stationsversleuteling.

[BitLocker-stationsversleuteling uitvoeren via de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie BitLocker-stationsversleuteling**.
7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven encrypten**.

Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om de encryptie uit te voeren.

8. Configureer geavanceerde BitLocker-stationsversleutelingsopties (zie onderstaande tabel).
9. Sla uw wijzigingen op.

#### **BitLocker-stationsversleuteling uitvoeren via de Webconsole en Cloudconsole**

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Full Disk Encryption**.
5. Selecteer in het blok **Manage encryption BitLocker Drive Encryption**.
6. Klik op de koppeling **BitLocker Drive Encryption**.  
Dit opent het instellingenvenster van Bitlocker-stationsversleuteling.
7. Selecteer in de vervolgkeuzelijst **Encryption mode** de optie **Encrypt all hard drives**.

Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om de encryptie uit te voeren.

8. Configureer geavanceerde BitLocker-stationsversleutelingsopties (zie onderstaande tabel).
9. Sla uw wijzigingen op.

U kunt de tool Versleutelingsmonitor gebruiken om het proces voor schijfversleuteling of decryptie op de computer van een gebruiker te regelen. U kunt de tool Versleutelingsmonitor uitvoeren vanuit het [hoofdvenster van het programma](#).

Nadat het beleid is toegepast, geeft de app de volgende query's weer, afhankelijk van de verificatie-instellingen:

- Alleen TPM. Geen gebruikersinvoer vereist. De schijf wordt versleuteld wanneer de computer opnieuw wordt opgestart.
- TPM + pincode/wachtwoord. Als een TPM-module beschikbaar is, ziet u een venster waarin een pincode wordt gevraagd. Als geen TPM-modules beschikbaar is, ziet u een venster waarin een wachtwoord voor de preboot-authenticatie wordt gevraagd.
- Alleen wachtwoord. U ziet een venster waarin een wachtwoord voor de preboot-authenticatie wordt gevraagd.

Als de modus voor compatibiliteit met FIPS (Federal Information Processing Standard) is ingeschakeld voor het besturingssysteem van de computer, ziet de gebruiker in Windows 8 en lager een venster met de vraag om een opslagapparaat aan te sluiten waarop het bestand met de herstelsleutel kan worden opgeslagen. U kunt meerdere herstel-licentiebestanden op één opslagapparaat opslaan.

Nadat u een wachtwoord of pincode hebt ingesteld, vraagt BitLocker u om uw computer opnieuw op te starten om de encryptie te voltooien. Vervolgens moet de gebruiker de BitLocker-verificatieprocedure doorlopen. Na de authenticatieprocedure moet de gebruiker inloggen op het systeem. Nadat het besturingssysteem is geladen, voltooit BitLocker de encryptie.

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 opslagapparaat of verloren is gegaan).

Instellingen component BitLocker-stationsversleuteling

| Parameter  | Beschrijving  |
|--|---|
| <b>Enable use of BitLocker authentication requiring pre-boot keyboard input on tablets</b> | <p>Dit selectievakje schakelt het gebruik van een authenticatie met gegevensinvoer vóór de opstart in of uit, zelfs als het platform niet geschikt is voor invoer tijdens de opstart (bijvoorbeeld met toetsenborden op aanraakschermen van tablets).</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Het touchscreen van tabletcomputers is niet beschikbaar in de preboot-omgeving. Om de BitLocker-authenticatie op tabletcomputers te voltooien, moet de gebruiker bijvoorbeeld een USB-toetsenbord aansluiten.</p> </div> <p>Als het selectievakje is ingeschakeld, is het gebruik van een authenticatie met invoer vóór de opstart toegestaan. U wordt aanbevolen deze instelling alleen te gebruiken voor apparaten die beschikken over alternatieve middelen voor gegevensinvoer vóór de opstart, zoals een USB-toetsenbord naast schermtoetsenborden.</p> <p>Als het selectievakje is uitgeschakeld, is BitLocker-stationsversleuteling niet mogelijk op tablets.</p> |
| <b>Use hardware encryption (Windows 8 and later versions)</b>                              | <p>Als het selectievakje is ingeschakeld, past het programma een hardware-encryptie toe. Hiermee kunt u sneller encrypten en gebruikt u minder computerbronnen.</p>   |
| <b>Encrypt used disk space only (Windows 8 and later versions)</b>                         | <p>Dit selectievakje schakelt de optie in of uit waarmee u het encryptiegebied beperkt tot de gebruikte sectoren van de harde schijf. Via deze beperking kunt u de encryptie verkorten.</p>   |

De in- of uitschakeling van de functie **Encrypt used disk space only (Windows 8 and later versions)** na het starten van de encryptie wijzigt deze instelling niet tenzij de harde schijven zijn gedecrypt. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.

Als het selectievakje is ingeschakeld, worden alleen delen van de harde schijf die door bestanden worden ingenomen geëncrypt. Kaspersky Endpoint Security encrypt automatisch nieuwe gegevens wanneer die worden toegevoegd.

Als het selectievakje is uitgeschakeld, wordt de gehele harde schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden.

Deze optie wordt aanbevolen voor nieuwe harde schijven waarvan de gegevens niet zijn gewijzigd of verwijderd. Als u een encryptie toepast op een harde schijf die al wordt gebruikt, wordt u aanbevolen de gehele harde schijf te encrypten. Op deze manier zijn alle gegevens beschermd, zelfs verwijderde gegevens die mogelijk kunnen worden hersteld.

Dit selectievakje is standaard uitgeschakeld.

## Authentication settings

### Use password (Windows 8 and later versions)

Als deze optie is geselecteerd, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om een wachtwoord in te voeren als die toegang tot een geëncrypte schijf probeert te krijgen.

Deze optie kan worden geselecteerd als geen Trusted Platform Module (TPM) wordt gebruikt.

### Use Trusted Platform Module (TPM)

Als deze optie is geselecteerd, gebruikt BitLocker een Trusted Platform Module (TPM).

Een *Trusted Platform Module (TPM)* is een microchip die ontwikkeld is 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.

Voor computers met Windows 7 of Windows Server 2008 R2 is alleen encryptie met een TPM-module beschikbaar. Als geen TPM-module is geïnstalleerd, is BitLocker-encryptie niet mogelijk. Het gebruik van een wachtwoord op deze computers wordt niet ondersteund.

Een apparaat met een Trusted Platform Module kan encryptiesleutels aanmaken die alleen met het apparaat kunnen worden gedecrypt. Een Trusted Platform Module encrypt encryptiesleutels met een eigen rootopslagsleutel. De rootopslagsleutel wordt in de Trusted Platform Module opgeslagen. Dit biedt meer bescherming tegen pogingen om de encryptiesleutels te hacken.

Deze actie is standaard geselecteerd.

U kunt een extra beveiligingslaag instellen voor toegang tot de encryptiesleutel en de sleutel coderen met een wachtwoord of een pincode:

- **Use PIN for TPM.** Als dit selectievakje geselecteerd is, dan kan een gebruiker een pincode gebruiken om toegang tot een encryptiesleutel te krijgen die in een Trusted Platform Module (TPM) is opgeslagen. Als dit selectievakje is uitgeschakeld, mogen gebruikers geen pincodes gebruiken. Om toegang te krijgen tot de encryptiesleutel, moet een gebruiker het wachtwoord invoeren.

U kunt de gebruiker toestaan om een geavanceerde pincode te gebruiken. Met *Geavanceerde pincode* kunt u naast cijfers ook andere tekens gebruiken: hoofdletters en kleine letters, speciale tekens en spaties.

- **Use Trusted Platform Module (TPM); if it is unavailable - use password.** Als het selectievakje is ingeschakeld, kan de gebruiker een wachtwoord gebruiken om toegang tot encryptiesleutels te krijgen wanneer geen Trusted Platform Module (TPM) beschikbaar is.

Als het selectievakje is uitgeschakeld en de TPM niet beschikbaar is, zal de volledige schijfencryptie niet starten.

## Een harde schijf die wordt beschermd door BitLocker decrypten

Gebruikers kunnen een schijf decrypten met behulp van het besturingssysteem (de functie *BitLocker uitschakelen*). Daarna vraagt Kaspersky Endpoint Security de gebruiker om de schijf opnieuw te encrypten. Kaspersky Endpoint Security vraagt om de schijf te encrypten, tenzij u schijfdecryptie in het beleid inschakelt.

### [Een door BitLocker beveiligde harde schijf decrypten via de Beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Full Disk Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptietechnologie BitLocker-stationsversleuteling**.
7. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven decrypten**.
8. Sla uw wijzigingen op.

### [Een met BitLocker versleutelde harde schijf decrypten via de webconsole en de cloudconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Full Disk Encryption**.
5. Selecteer de technologie **BitLocker Drive Encryption** en volg de link om de instellingen te configureren.  
De encryptie-instellingen worden geopend.
6. Selecteer in de vervolgkeuzelijst **Encryption mode** de optie **Decrypt all hard drives**.
7. Klik op **OK**.

U kunt de tool Versleutelingsmonitor gebruiken om het proces voor schijfversleuteling of decryptie op de computer van een gebruiker te regelen. U kunt de tool Versleutelingsmonitor uitvoeren vanuit het [hoofdvenster van het programma](#).

## Toegang tot een met BitLocker beschermde schijf herstellen

Als een gebruiker het wachtwoord is vergeten voor toegang tot een harde schijf geëncrypt door BitLocker, moet u de herstelprocedure starten (Request-Response).

Als het besturingssysteem van de computer de Federal Information Processing Standard (FIPS)-compatibiliteitsmodus ingeschakeld heeft, wordt in Windows 8 en later het herstelsleutelbestand opgeslagen op de verwisselbare schijf voorafgaand aan encryptie. Om toegang tot de schijf te herstellen, plaatst u de verwisselbare schijf en volgt u de instructies op het scherm.

Het herstellen van de toegang tot een harde schijf die met BitLocker is geëncrypt, bestaat uit de volgende stappen:

1. De gebruiker vertelt de beheerder de ID van de herstelsleutel (zie onderstaande afbeelding).
2. De beheerder verifieert de ID van de herstelsleutel in de computereigenschappen in Kaspersky Security Center. De ID die de gebruiker heeft opgegeven, moet overeenkomen met de ID die wordt weergegeven in de computereigenschappen.
3. Als de ID's van de herstelsleutel overeenkomen, geeft de beheerder de gebruiker de herstelsleutel of stuurt hij een herstelsleutelbestand.

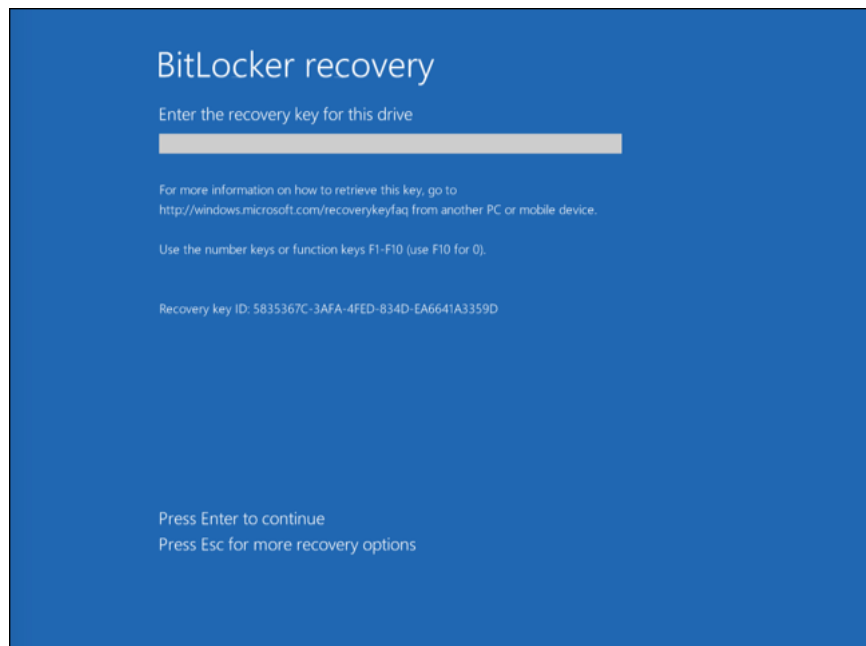
Een herstelsleutelbestand wordt gebruikt voor computers met de volgende besturingssystemen:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;

- Windows Server 2012.

Voor alle andere besturingssystemen wordt een herstelsleutel gebruikt.

4. De gebruiker voert de herstelsleutel in en krijgt toegang tot de harde schijf.



Toegang herstellen tot een harde schijf geëncrypt met BitLocker

## Toegang tot een systeemstation herstellen

Om de herstelprocedure te starten, moet de gebruiker op de **Esc**-toets drukken tijdens de authenticatiefase vóór het opstarten.

[De herstelsleutel bekijken voor een systeemstation geëncrypt met BitLocker in de beheerconsole \(MMC\)](#) 



1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster 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.

Als gevolg krijgt u toegang tot de herstelsleutel of het bestand van de herstelsleutel, dat moet worden overgedragen aan de gebruiker.

## [De herstelsleutel voor een met BitLocker versleuteld systeemstation in de Webconsole en Cloudconsole bekijken](#)



1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de schijf wilt herstellen.
3. Klik op de knop **Grant access to the device in offline mode**.
4. Selecteer in het geopende venster het gedeelte **Bitlocker**.
5. Controleer de ID van de herstelsleutel. De ID die door de gebruiker wordt verstrekt, moet overeenkomen met de ID die wordt weergegeven in de computerinstellingen.

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.

6. Klik op de knop **Receive key**.

Als gevolg krijgt u toegang tot de herstelsleutel of het bestand van de herstelsleutel, dat moet worden overgedragen aan de gebruiker.

Nadat het besturingssysteem is geladen, vraagt Kaspersky Endpoint Security de gebruiker om het wachtwoord of de pincode te wijzigen. Nadat u een nieuw wachtwoord of nieuwe pincode hebt ingesteld, maakt BitLocker een nieuwe hoofdsleutel aan en stuurt de sleutel naar Kaspersky Security Center. Als gevolg worden de herstelsleutel en het herstelsleutelbestand bijgewerkt. Als de gebruiker het wachtwoord niet heeft gewijzigd, kunt u de oude herstelsleutel gebruiken de volgende keer dat het besturingssysteem wordt geladen.

Windows 7-computers staan het wijzigen van het wachtwoord of de pincode niet toe. Na het invoeren van de herstelsleutel en het laden van het besturingssysteem, vraagt Kaspersky Endpoint Security de gebruiker om het wachtwoord of de pincode te wijzigen. Het is dus onmogelijk om een nieuw wachtwoord of een pincode in te stellen. Dit probleem komt voort vanuit de specifieke kenmerken van het besturingssysteem. Om door te gaan, moet u de harde schijf opnieuw encrypten.

## Toegang herstellen tot een niet-systeemstation

Om de herstelprocedure te starten, moet de gebruiker op de link **Wachtwoord vergeten** klikken in het venster dat toegang geeft tot de schijf. Nadat de gebruiker toegang heeft gekregen tot de geëncrypte schijf, kan de gebruiker automatische ontgrendeling van de schijf inschakelen tijdens Windows-authenticatie in de BitLocker-instellingen.

### [De herstelsleutel bekijken voor een niet-systeemstation geëncrypt met BitLocker in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Extra** → **Data encryption and protection** → **Encrypted drives**.
3. Selecteer in de werkruijnte het geëncrypte apparaat waarvoor u een bestand met een toegangscode wilt aanmaken en klik vervolgens in het contextmenu van het apparaat op **Krijg toegang tot het apparaat in Kaspersky Endpoint Security voor Windows**.
4. 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.

5. Stuur de gebruiker de sleutel die in het veld **Herstelsleutel** is vermeld.

### [De herstelsleutel voor een met BitLocker versleuteld niet-systeemstation in de Webconsole en Cloudconsole bekijken](#)

1. Selecteer in het hoofdvenster van de Webconsole **Operations** → **Data encryption and protection** → **Encrypted Drives**.

2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de schijf wilt herstellen.

3. Klik op de knop **Grant access to the device in offline mode**.

Dit start de wizard voor het verlenen van toegang tot een apparaat.

4. Volg de instructies van de wizard om toegang te verlenen tot een apparaat:

a. Selecteer de beheerplug-in **Kaspersky Endpoint Security voor Windows**

b. Controleer de ID van de herstelsleutel. De ID die door de gebruiker wordt verstrekt, moet overeenkomen met de ID die wordt weergegeven in de computerinstellingen.

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.

c. Klik op de knop **Receive key**.

Als gevolg krijgt u toegang tot de herstelsleutel of het bestand van de herstelsleutel, dat moet worden overgedragen aan de gebruiker.

## BitLocker-bescherming pauzeren om software te updaten

Er zijn een aantal speciale overwegingen voor het bijwerken van het besturingssysteem, installeren van updatepakketten voor het besturingssysteem of het bijwerken van andere software met BitLocker-beveiliging ingeschakeld. Na de installatie van updates moet de computer mogelijk meermaals opnieuw worden opgestart. De gebruiker moet dan na elke herstart de BitLocker-authenticatie voltooien. Om ervoor te zorgen dat updates correct worden geïnstalleerd, kunt u BitLocker-authenticatie tijdelijk uitschakelen. In dit geval blijft het station versleuteld en heeft de gebruiker toegang tot gegevens na inloggen op het systeem. Om BitLocker-authenticatie te beheren, kunt u de taak *BitLocker Protection Management* gebruiken. U kunt deze taak gebruiken om het aantal herstarts van de computer op te geven waarvoor geen BitLocker-authenticatie is vereist. Op deze manier, nadat updates zijn geïnstalleerd en de taak *BitLocker Protection Management* is voltooid, wordt BitLocker-authenticatie automatisch ingeschakeld. U kunt BitLocker-authenticatie op elk moment inschakelen.

[BitLocker-beveiliging pauzeren met behulp van de beheerconsole \(MMC\)](#) 

1. Ga in de beheerconsole naar de map **Administration Server** → **Taken** .

De lijst met taken wordt geopend.

2. Klik op de knop **Nieuwe taak**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows (11.9.0)** → **BitLocker Protection Management**.

## Stap 2. BitLocker Protection Management

BitLocker-authenticatie configureren Selecteer om BitLocker-authenticatie te pauzeren **Overslaan van BitLocker-authenticatie tijdelijk toestaan** en voer het aantal herstarts in zonder BitLocker-authenticatie (1 tot 15 keer). Voer indien nodig een vervaldatum en -tijd in voor de taak. Op het opgegeven tijdstip wordt de taak automatisch uitgeschakeld en moet de gebruiker BitLocker-verificatie voltooien wanneer de computer opnieuw wordt opgestart.

## Stap 3: De apparaten selecteren waaraan de taak zal worden toegewezen

Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

- Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
- Selecteer computers die door Administration Server zijn gevonden in het netwerk: *niet-toegewezen apparaten*. De specifieke apparaten kunnen apparaten in beheergroepen of niet-toegewezen apparaten zijn.
- Geef de adressen van apparaten handmatig op of importeer de adressen vanuit een lijst. U kunt NetBIOS-namen, IP-adressen en IP-subnetten van apparaten opgeven waaraan u de taak wilt toewijzen.

## Stap 4. Taaknaam definiëren

Voer de naam van de taak in, bijvoorbeeld *Updaten naar Windows 10*.

## Stap 5. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Taak uitvoeren nadat de wizard is voltooid** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

[BitLocker-bescherming pauzeren met Webconsole](#) 

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart. Volg de instructies van de wizard.

## Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

2. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **BitLocker Protection Management**.

3. Typ in het veld **Taaknaam** een korte omschrijving, zoals *Updaten naar Windows 10*.

4. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

## Stap 2. BitLocker Protection Management

BitLocker-authenticatie configureren Selecteer om BitLocker-authenticatie te pauzeren **Overslaan van BitLocker-authenticatie tijdelijk toestaan** en voer het aantal herstarts in zonder BitLocker-authenticatie (1 tot 15 keer). Voer indien nodig een vervaldatum en -tijd in voor de taak. Op het opgegeven tijdstip wordt de taak automatisch uitgeschakeld en moet de gebruiker BitLocker-verificatie voltooien wanneer de computer opnieuw wordt opgestart.

## Stap 3. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. U ziet een nieuwe taak in de lijst met taken.

Start een taak door het selectievakje naast de taak in te schakelen en op de knop **Starten** te klikken.

Als resultaat vraagt BitLocker de gebruiker niet om authenticatie wanneer de taak wordt uitgevoerd, na de volgende herstart van de computer. Na elke herstart van de computer zonder BitLocker-authenticatie, genereert Kaspersky Endpoint Security een overeenkomstige gebeurtenis en registreert het aantal resterende herstarts. Kaspersky Endpoint Security stuurt de gebeurtenis vervolgens naar Kaspersky Security Center voor controle door de beheerder. U kunt ook het aantal resterende herstarts vinden in de computereigenschappen in de Kaspersky Security Center-console.

Wanneer het opgegeven aantal herstarts of de vervaltijd van de taak is bereikt, wordt BitLocker-authenticatie automatisch ingeschakeld. Om toegang te krijgen tot gegevens, moet de gebruiker BitLocker-authenticatie voltooien.

Op computers met Windows 7 kan BitLocker de herstarts van de computer niet tellen. Het tellen van herstarts op computers met Windows 7 wordt afgehandeld door Kaspersky Endpoint Security. Om BitLocker-authenticatie na elke herstart automatisch in te schakelen, moet Kaspersky Endpoint Security dus worden gestart.

Als u BitLocker-authenticatie van tevoren wilt inschakelen, opent u de taakeigenschappen van *BitLocker Protection Management* en selecteert u **Authenticatie telkens vóór opstarten vragen**.

## File Level Encryption op lokale schijven van de computer

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

Bestandsencryptie heeft de volgende speciale kenmerken:

- 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.
- Kaspersky Endpoint Security encrypt geen bestanden die het besturingssysteem en geïnstalleerde programma's kunnen beschadigen als ze worden gewijzigd. De volgende bestanden en mappen met alle geneste mappen staan bijvoorbeeld op de lijst met encryptie-uitzonderingen:
  - %WINDIR%;
  - %PROGRAMFILES% en %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 bestandsencryptie.

## Bestanden op schijven van een lokale computer encrypten

Kaspersky Endpoint Security versleutelt geen bestanden die zich in OneDrive-cloudopslag of in andere mappen met OneDrive als naam bevinden. Kaspersky Endpoint Security blokkeert ook het kopiëren van versleutelde bestanden naar OneDrive-mappen als die bestanden niet worden toegevoegd aan de [decryptieregel](#).

*Zo encrypt u bestanden op lokale schijven:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.

6. Selecteer in de vervolgkeuzelijst **Encryptiemodus Volgens regels**.

7. 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.

- **Documenten**. Bestanden in de standaardmap *Documenten* van het besturingssysteem, en de submappen ervan.
- **Favorieten**. Bestanden in de standaardmap *Favorieten* van het besturingssysteem en de submappen ervan.
- **Bureaublad**. Bestanden in de standaardmap *Bureaublad* van het besturingssysteem, en de submappen ervan.
- **Tijdelijke bestanden**. Tijdelijke bestanden voor de werking van op de computer geïnstalleerde programma's. Microsoft Office-programma's maken bijvoorbeeld tijdelijke bestanden aan die back-ups van documenten bevatten.
- **Outlook-bestanden**. Bestanden voor de werking van het e-mailprogramma Outlook: gegevensbestanden (PST), offline gegevensbestanden (OST), offline adresboekbestanden (OAB) en persoonlijk-adresboekbestanden (PAB).

b. Selecteer de optie **Aangepaste map** om een handmatig ingevoerd pad naar een map toe te voegen aan een encryptieregel.

Houd u bij het toevoegen van een mappad aan de volgende regels:

- Gebruik een omgevingsvariabele (bijvoorbeeld %FOLDER%\UserFolder\). U kunt een omgevingsvariabele slechts één keer gebruiken en alleen aan het begin van het pad.
- Gebruik geen relatieve paden.
- Gebruik de tekens \* en ? niet.
- Gebruik geen UNC-paden.
- Gebruik ; of , als scheidingsteken.

c. Selecteer de optie **Bestanden op extensie** om individuele bestandsextensies aan een encryptieregel toe te voegen. Kaspersky Endpoint Security encrypt bestanden met de opgegeven extensies op alle lokale schijven van de computer.

d. Selecteer de optie **Bestanden op groepen van extensies** om groepen van bestandsextensies aan een encryptieregel toe te voegen (bijvoorbeeld, *Microsoft Office-documenten*). Kaspersky Endpoint Security encrypt bestanden met extensies uit de groepen van extensies op alle lokale schijven van de computer.

8. Sla uw wijzigingen op.

Zodra het beleid is toegepast, encrypt Kaspersky Endpoint Security de bestanden die in de encryptieregel zijn opgenomen en niet in de [decryptieregel](#) zijn opgenomen.

Bestandsencryptie heeft de volgende speciale kenmerken:

- Als hetzelfde bestand wordt toegevoegd aan zowel een encryptieregel als een decryptieregel, voert Kaspersky Endpoint Security de volgende acties uit:
  - Als het bestand niet is geëncrypt, dan encrypt Kaspersky Endpoint Security dit bestand niet.
  - Als het bestand is geëncrypt, dan decrypt Kaspersky Endpoint Security dit bestand.
- Kaspersky Endpoint Security blijft nieuwe bestanden encrypten als deze bestanden voldoen aan de criteria van de encryptieregel. Als u bijvoorbeeld de eigenschappen van een niet-geëncrypt bestand (pad of extensie) wijzigt, voldoet het bestand aan de criteria van de encryptieregel. Kaspersky Endpoint Security encrypt dit bestand.
- 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.
- Kaspersky Endpoint Security encrypt geopende bestanden pas nadat ze zijn gesloten.
- 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.
- Als u een bestand decrypt en naar een andere lokale map kopieert die niet is opgenomen in de decryptieregel, dan kan een kopie van het bestand worden geëncrypt. Maak een decryptieregel voor de doelmap om te voorkomen dat het gekopieerde bestand wordt geëncrypt.

## 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 **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruiimte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptiemodus Volgens regels**.

Toegangsregels worden alleen in de modus **Volgens regels** toegepast. Als u na het toepassen van de toegangsregels in de modus **Volgens regels** overschakelt naar de modus **Ongewijzigd laten**, dan negeert Kaspersky Endpoint Security alle toegangsregels. Alle programma's hebben dan toegang tot alle geëncrypte bestanden.

7. Selecteer rechts in het venster het tabblad **Regels voor programma's**.
8. 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**.
  - 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 blok **Groep**.



b. Klik op de knop **Vernieuwen**.

c. In de tabel ziet u programma's die aan de toegepaste filters voldoen.

d. Schakel in de kolom **Programma** de selectievakjes naast de programma's in waarvoor u toegangsregels voor geëncrypte bestanden wilt maken.

e. Selecteer in de vervolgkeuzelijst **Regel voor programma's** de regel die de toegang van programma's tot geëncrypte bestanden zal bepalen.

f. 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.

De details van een toegangsregel voor geëncrypte bestanden voor programma's ziet u in de tabel op het tabblad **Regels voor programma's**.

9. Als u programma's handmatig wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Aangepaste programma's**.

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.

De details van een toegangsregel voor geëncrypte bestanden voor programma's ziet u in de tabel op het tabblad **Regels voor programma's**.

10. Sla uw wijzigingen op.

## 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 **Managed devices** 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 **Policies**.

4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptiemodus Volgens regels**.

Encryptieregels worden alleen in de modus **Volgens regels** toegepast. Als u na het toepassen van de encryptieregels in de modus **Volgens regels** overschakelt naar de modus **Ongewijzigd laten**, negeert Kaspersky Endpoint Security alle encryptieregels. Bestanden die eerder werden geëncrypt blijven geëncrypt.

7. Selecteer rechts in het venster het tabblad **Regels voor programma's**.
8. 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**.
  - 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 blok **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 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.

Informatie over de encryptieregel voor bestanden die door de geselecteerde programma's zijn gemaakt of gewijzigd, ziet u in de tabel op het tabblad **Regels voor programma's**.

9. Als u programma's handmatig wilt selecteren, klikt u op de knop **Toevoegen** en selecteert u in de vervolgkeuzelijst de optie **Aangepaste programma's**.
  - 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 Alle gemaakte bestanden encrypten**.

Informatie over de encryptieregel voor bestanden die door de geselecteerde programma's zijn gemaakt of gewijzigd, ziet u in de tabel op het tabblad **Regels voor programma's**.

10. Sla uw wijzigingen op.

## Een decryptieregel genereren

*Zo genereert u een decryptieregel:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptiemodus Volgens regels**.
7. 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.
  - b. Selecteer de optie **Aangepaste map** om een handmatig ingevoerd pad naar een map toe te voegen aan een decryptieregel.
  - 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.
  - d. Selecteer de optie **Bestanden op groepen van extensies** om groepen van bestandsextensies aan een decryptieregel toe te voegen (bijvoorbeeld *Microsoft Office-documenten*). Kaspersky Endpoint Security encrypt geen bestanden met extensies uit de groepen van extensies op alle lokale schijven van de computer.
8. Sla uw wijzigingen op.

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 **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.

6. Selecteer rechts in het venster het tabblad **Encryptie**.

7. 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**.

Bestanden en mappen die worden verwijderd uit de encryptielijst worden automatisch toegevoegd aan de decryptielijst.

8. [Maak een decryptielijst voor bestanden](#).

9. Sla uw wijzigingen op.

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

U kunt uw gegevens beschermen bij het verzenden van bestanden naar gebruikers buiten het bedrijfsnetwerk, door geëncrypte pakketten te gebruiken. Geëncrypte pakketten kunnen handig zijn voor het overbrengen van grote bestanden op verwisselbare schijven, aangezien e-mailclients beperkingen voor de bestandsgrootte hebben.

Voordat geëncrypte pakketten worden gemaakt, vraagt Kaspersky Endpoint Security de gebruiker om een wachtwoord. Voor een betrouwbare bescherming van de gegevens kunt u de Controle van wachtwoordsterkte inschakelen en de vereisten voor wachtwoordsterkte specificeren. Dit voorkomt dat gebruikers korte en eenvoudige wachtwoorden gebruiken, bijvoorbeeld 1234.

### [Controle van wachtwoordsterkte inschakelen bij het maken van geëncrypte archieven in de Beheerconsole \(MMC\)](#)



1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het venster Beleid **Data Encryption** → **Algemene encryptie-instellingen**.
6. In het blok **Wachtwoordinstellingen**, klikt u op de knop **Instellingen**.
7. Selecteer in het geopende venster het tabblad **Netwerkregels**.
8. Configureer instellingen voor wachtwoordcomplexiteit bij het maken van geëncrypte pakketten.


1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **File Level Encryption**.
5. In het blok **Wachtwoordinstellingen voor geëncrypt pakket**, configureert u de criteria voor wachtwoordsterkte vereist bij het maken van versleutelde pakketten.

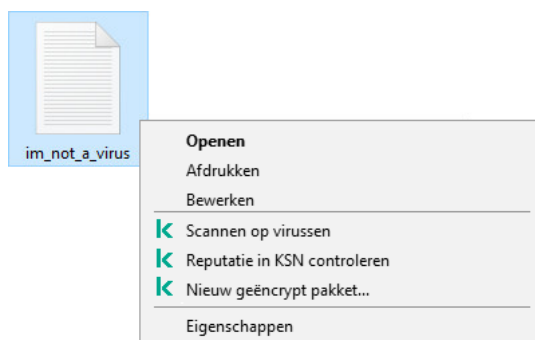
U kunt geëncrypte pakketten maken op computers waarop Kaspersky Endpoint Security is geïnstalleerd en waarop File Level Encryption beschikbaar is.

Wanneer u een bestand toevoegt aan het geëncrypte pakket waarvan de inhoud zich in de OneDrive-cloudopslag bevindt, downloadt Kaspersky Endpoint Security de inhoud van de bestanden en voert het de encryptie uit.

*Zo maakt u een geëncrypt pakket aan:*

1. Selecteer in een bestandsbeheerder de bestanden of mappen die u aan het geëncrypte pakket wilt toevoegen. Klik rechts om het contextmenu ervan te openen.
2. Selecteer in het contextmenu de optie **Nieuw geëncrypt pakket** (zie onderstaande afbeelding).
3. Selecteer in het geopende venster een locatie op een verwisselbare schijf om het geëncrypte pakket op te slaan, specificeer de pakketnaam en klik op de knop **Opslaan**.
4. Geef in het geopende venster het wachtwoord op en bevestig het.  
Het wachtwoord moet voldoen aan de complexiteitscriteria die in het beleid zijn gespecificeerd.
5. Klik op de knop **Maken**.

Het aanmaken van het geëncrypte pakket wordt gestart. Kaspersky Endpoint Security comprimeert geen bestanden wanneer het een geëncrypt pakket aanmaakt. Wanneer het proces is voltooid, wordt een zelfuitpakkend, met een wachtwoord beveiligd, geëncrypt pakket (een uitvoerbaar bestand met de extensie .exe)  gemaakt in de geselecteerde bestemmingsmap.



Een geëncrypt pakket maken

Wanneer u toegang wilt krijgen tot bestanden in een geëncrypt pakket, dubbelklikt u erop om de wizard Uitpakken te starten en voert u het wachtwoord in. Als u uw wachtwoord bent vergeten of kwijtgeraakt, is het niet mogelijk om het te herstellen en toegang te krijgen tot de bestanden in het geëncrypte pakket. U kunt het geëncrypte pakket opnieuw maken.

## Toegang tot geëncrypte gegevens herstellen

Wanneer bestanden zijn gecodeerd, ontvangt Kaspersky Endpoint Security een encryptiesleutel die nodig is voor directe toegang tot de geëncrypte bestanden. 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 toegangssleutel 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 toegangssleutels 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.

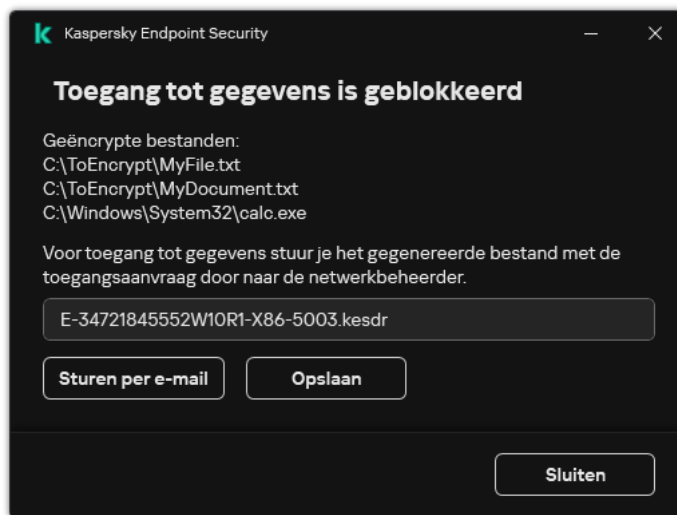
De gebruiker kan werken met geëncrypte bestanden onder de volgende omstandigheden:

- 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.

Om toegang te krijgen tot geëncrypte bestanden, moet de gebruiker de herstelprocedure starten (Request-Response).

Het herstellen van toegang tot geëncrypte bestanden bestaat uit de volgende stappen:

1. De gebruiker stuurt een bestand met een toegangsaanvraag naar de beheerder (zie onderstaande afbeelding).
2. De beheerder voegt het bestand met toegangsaanvraag toe aan Kaspersky Security Center, maakt een bestand met toegangssleutel aan en stuurt het naar de gebruiker.
3. De gebruiker voegt het toegangssleutelbestand toe aan Kaspersky Endpoint Security en krijgt toegang tot de bestanden.



Toegang tot geëncrypte gegevens herstellen

Om de herstelprocedure te starten, moet de gebruiker proberen toegang te krijgen tot een bestand. Als gevolg hiervan zal Kaspersky Endpoint Security een bestand van de toegangs aanvraag maken (een bestand met de extensie KESDC), dat de gebruiker bijvoorbeeld per e-mail naar de beheerder moet sturen.

Kaspersky Endpoint Security genereert een bestand van de toegangs aanvraag voor toegang tot alle geëncrypte bestanden die zijn opgeslagen op de schijf van de computer (lokale schijf of verwisselbare schijf).

### [Een bestand met toegangssleutel voor geëncrypte bestanden verkrijgen in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster het tabblad **Gegevensencryptie**.
7. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.
8. Geef in het venster voor het selecteren van een bestand met verzoektoegang het pad op naar het bestand dat van de gebruiker is ontvangen.

U ziet informatie over het verzoek van de gebruiker. Kaspersky Security Center genereert een sleutelbestand. E-mail het gegenereerde bestand met de sleutel voor toegang tot de geëncrypte gegevens naar de gebruiker. Of sla het toegangsbestand op en gebruik een beschikbare methode om het bestand over te dragen.

### [Hoe een bestand met toegangssleutel voor geëncrypte bestanden verkrijgt in de webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.
3. Klik op de knop **Grant access to the device in offline mode**.
4. Selecteer het gedeelte **Gegevensencryptie**.
5. Klik op de knop **Select file** en selecteer het bestand van de toegangs aanvraag dat u van de gebruiker hebt ontvangen (een bestand met de extensie KESDC).  
De webconsole geeft informatie over de aanvraag weer. Dit omvat de naam van de computer waarop de gebruiker toegang tot het bestand vraagt.
6. Klik op de knop **Sleutel opslaan** en selecteer een map om het bestand met de toegangssleutel voor de geëncrypte gegevens op te slaan (een bestand met de extensie KESDR).

Als gevolg hiervan kunt u de gegevenstoegangssleutel verkrijgen, die u aan de gebruiker moet overdragen.

Na ontvangst van het bestand met toegangssleutel voor geëncrypte bestanden, moet de gebruiker het bestand uitvoeren door erop te dubbelklikken. Als gevolg hiervan verleent Kaspersky Endpoint Security toegang tot alle geëncrypte bestanden die op de schijf zijn opgeslagen. Om toegang tot geëncrypte bestanden op andere schijven te krijgen, moet u een afzonderlijke toegangssleutel voor elke verwisselbare schijf krijgen.

## 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 wanneer de gegevens werden geëncrypt.

De toegang tot de geëncrypte gegevens wordt verleend onder dezelfde voorwaarden die vóór de fout in het besturingssysteem van toepassing waren.

## 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 **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer in het venster Beleid **Gegevensencryptie** → **Algemene encryptie-instellingen**.
6. Klik in het blok **Sjablonen** op de knop **Sjablonen**.
7. Doe in het venster dat opent het volgende:
  - Als u de sjabloon van het bericht van de gebruiker wilt bewerken, selecteert u het tabblad **Bericht van gebruiker**. Het venster **Toegang tot gegevens is geblokkeerd** wordt geopend wanneer de gebruiker toegang tot een geëncrypt bestand probeert te krijgen wanneer er geen beschikbare sleutel op de computer is voor toegang tot geëncrypte bestanden. Met een klik op de knop **Versturen per e-mail** in het venster **Toegang tot gegevens is geblokkeerd** wordt automatisch een bericht 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 u op de knop **Versturen per e-mail** in het venster **Aanvraag voor toegang tot geëncrypte bestanden** klikt en wordt naar de gebruiker verstuurd nadat de toegang tot geëncrypte bestanden heeft gekregen.
8. Bewerk de sjablonen van de berichten.
9. Sla uw wijzigingen op.

## Encryptie van verwisselbare schijven

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

Kaspersky Endpoint Security ondersteunt de encryptie van bestanden in FAT32- en NTFS-bestandssystemen. Als een verwisselbare schijf met een niet-ondersteund bestandssysteem is aangesloten op de computer, wordt de encryptietaak voor deze verwisselbare schijf beëindigd met een fout en wijst Kaspersky Endpoint Security de alleen-lezenstatus toe aan de verwisselbare schijf.

Om gegevens op verwisselbare schijven te beschermen, kunt u de volgende soorten encryptie gebruiken:

- Full Disk Encryption (FDE)

Encryptie van de volledige verwisselbare schijf, inclusief het bestandssysteem.

Het is niet mogelijk om toegang te krijgen tot geëncrypte gegevens buiten het bedrijfsnetwerk. Het is ook onmogelijk om toegang te krijgen tot geëncrypte gegevens binnen het bedrijfsnetwerk als de computer niet is verbonden met Kaspersky Security Center (bijvoorbeeld op een gastcomputer).

- File Level Encryption (FLE).

Encryptie van alleen bestanden op een verwisselbare schijf. Het bestandssysteem blijft ongewijzigd.

Encryptie van bestanden op verwisselbare schijven biedt de mogelijkheid om toegang te krijgen tot gegevens buiten het bedrijfsnetwerk met behulp van een speciale modus met de naam *portable modus*.

Tijdens de encryptie maakt Kaspersky Endpoint Security een hoofdsleutel aan. Kaspersky Endpoint Security slaat de hoofdsleutel op in de volgende opslagplaatsen:

- Kaspersky Security Center.  
De hoofdsleutel is geëncrypt met de geheime sleutel van de gebruiker.
- Gebruikerscomputer.  
De hoofdsleutel is gecodeerd met de openbare sleutel van Kaspersky Security Center.

Nadat de encryptie is voltooid, zijn de gegevens op de verwisselbare schijf toegankelijk binnen het bedrijfsnetwerk alsof ze zich op een gewone niet geëncrypte verwisselbare schijf bevinden.

## Toegang tot geëncrypte gegevens

Wanneer een verwisselbare schijf met geëncrypte gegevens is aangesloten, voert Kaspersky Endpoint Security de volgende acties uit:

1. Controleert op een hoofdsleutel in de lokale opslag op de computer van de gebruiker.  
Als de hoofdsleutel wordt gevonden, krijgt de gebruiker toegang tot de gegevens op de verwisselbare schijf.  
Als de hoofdsleutel niet wordt gevonden, voert Kaspersky Endpoint Security de volgende acties uit:
  - a. Stuurt een verzoek naar Kaspersky Security Center.  
Na ontvangst van het verzoek stuurt Kaspersky Security Center een antwoord met de hoofdsleutel.
  - b. Kaspersky Endpoint Security slaat de hoofdsleutel op in de lokale opslag op de computer van de gebruiker voor daaropvolgende bewerkingen met de geëncrypte verwisselbare schijf.
2. Decrypt de gegevens.

## Speciale functies voor encryptie van verwisselbare schijf

Encryptie van verwisselbare schijven heeft de volgende speciale functies:

- Het beleid met vooraf geconfigureerde instellingen voor de encryptie van verwisselbare schijven is opgesteld voor een specifieke groep beheerde computers. Daarom is het resultaat van de toepassing van het geconfigureerde Kaspersky Security Center-beleid voor de encryptie of decryptie van verwisselbare schijven afhankelijk van de computer waarop de verwisselbare schijf is aangesloten.
- Kaspersky Endpoint Security encrypt of decrypt geen alleen-lezenbestanden die op verwisselbare schijven zijn opgeslagen.
- 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

## Encryptie van verwisselbare schijven starten

U kunt een beleid gebruiken om een verwisselbaar station te decrypten. Een beleid met gedefinieerde instellingen voor encryptie van verwijderbare schijven wordt gegenereerd voor een specifieke beheergroep. Daarom hangt het resultaat van de decryptie van gegevens op verwisselbare schijven af van de computer waarop de verwisselbare schijven zijn aangesloten.

Kaspersky Endpoint Security ondersteunt encryptie in FAT32- en NTFS-bestandssystemen. Als een verwisselbare schijf met een niet-ondersteund bestandssysteem is aangesloten op de computer, wordt de encryptie van de verwisselbare schijf beëindigd met een fout en wijst Kaspersky Endpoint Security alleen-lezentoegang aan de verwisselbare schijf toe.

*Zo encrypt u verwisselbare schijven:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** in de structuur van de Beheerconsole de map met de naam van de beheergroep waartoe de relevante clientcomputers behoren.
3. Selecteer in de werkruijnte het tabblad **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Encryption of removable drives** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de standaardactie die Kaspersky Endpoint Security moet uitvoeren op verwisselbare schijven:
  - **Gehele verwisselbare schijf encrypten** (FDE). Kaspersky Endpoint Security encrypt de inhoud van een verwisselbare schijf sector per sector. Daarom encrypt het programma niet alleen de bestanden op de verwisselbare schijf maar ook de bestandssystemen ervan, en zelfs de bestandsnamen en mapstructuren.
  - **Alle bestanden encrypten** (FLE). Kaspersky Endpoint Security encrypt alle bestanden die op verwisselbare schijven zijn opgeslagen. Het programma encrypt geen bestandssystemen van verwisselbare schijven, noch namen van bestanden of mapstructuren.
  - **Alleen nieuwe bestanden encrypten** (FLE). Kaspersky Endpoint Security encrypt alleen bestanden die aan verwisselbare schijven zijn toegevoegd of die op verwisselbare schijven waren opgeslagen en zijn gewijzigd nadat het Kaspersky Security Center-beleid voor het laatst is toegepast.

Kaspersky Endpoint Security encrypt geen verwisselbare schijven die al waren geëncrypt.

7. Als u de [portable modus](#) voor de encryptie van verwisselbare schijven wilt gebruiken, schakelt u het selectievakje **Portable modus** in.

De *portable modus* is een modus voor bestandsencryptie (FLE) op verwisselbare schijven die u de mogelijkheid biedt om toegang tot gegevens te verkrijgen wanneer u niet verbonden bent met het bedrijfsnetwerk. Dankzij de portable modus kunt u ook werken met geëncrypte gegevens op computers waarop Kaspersky Endpoint Security niet is geïnstalleerd.

8. Als u een nieuwe verwisselbare schijf wilt encrypten, wordt u aanbevolen het selectievakje **Alleen gebruikte schijfruimte encrypten** in te schakelen. Wanneer het selectievakje is uitgeschakeld, encrypt Kaspersky Endpoint Security alle bestanden, inclusief de restjes van verwijderde of gewijzigde bestanden.

9. [Definieer encryptieregels](#) als u encryptie voor afzonderlijke verwisselbare schijven wilt configureren.

10. Schakel het selectievakje **Encryptie van verwisselbare schijven in offline modus toestaan** in als u Full Disk Encryption van verwisselbare schijven in de offline modus wilt gebruiken.

*Offline encryptiemodus* is de encryptie van verwisselbare schijven (FDE) als er geen verbinding met Kaspersky Security Center is. Tijdens de encryptie slaat Kaspersky Endpoint Security de hoofdsleutel alleen op de computer van de gebruiker op. Kaspersky Endpoint Security verstuurt tijdens de volgende synchronisatie de hoofdsleutel naar Kaspersky Security Center.

Als de computer waarop de hoofdsleutel is opgeslagen beschadigd is geraakt en de gegevens zijn niet naar Kaspersky Security Center verstuurd, is het niet mogelijk om toegang tot de verwisselbare schijf te krijgen.

Als het selectievakje **Encryptie van verwisselbare schijven in offline modus toestaan** is uitgeschakeld en er is ook geen verbinding met Kaspersky Security Center, dan kan de verwisselbare schijf niet worden geëncrypt.

11. Sla uw wijzigingen op.

Wanneer het beleid is toegepast en de gebruiker een verwisselbare schijf aansluit, of als er al een verwisselbare schijf is aangesloten, zal de gebruiker door Kaspersky Endpoint Security worden gevraagd om de encryptie te bevestigen (zie onderstaande afbeelding).

Met het programma kunt u dan de volgende acties uitvoeren:

- Als de gebruiker het encryptieverzoek bevestigt, encrypt Kaspersky Endpoint Security de gegevens.
- Als de gebruiker het encryptieverzoek weigert, laat Kaspersky Endpoint Security de gegevens ongewijzigd en wijst het alleen-lezentoegang aan deze verwisselbare schijf toe.
- Als de gebruiker niet reageert op het encryptieverzoek, laat Kaspersky Endpoint Security de gegevens ongewijzigd en wijst het alleen-lezentoegang aan deze verwisselbare schijf toe. Het programma zal opnieuw om bevestiging vragen wanneer een beleid wordt toegepast of de volgende keer dat deze verwisselbare schijf wordt 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. De gegevensencryptie gaat verder de volgende keer dat de verwisselbare schijf wordt aangesloten op deze computer.

Als de encryptie van een verwisselbare schijf is mislukt, bekijkt u het rapport **Gegevensencryptie** in de interface van Kaspersky Endpoint Security. De toegang tot bestanden kan worden geblokkeerd door een ander programma. Probeer in dat geval de verwisselbare schijf los te koppelen van de computer en opnieuw aan te sluiten.



Verzoek voor encryptie van verwisselbare schijf

## 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 **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Encryption of removable drives** in het beleidsvenster.
6. Klik 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**.
  - 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**.
7. 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.
8. 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](#).

9. 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.

10. 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 de eerder aangemaakte encryptieregel voor de verwisselbare schijf wordt vervangen door de nieuwe regel, selecteert u **Vernieuwen**.

11. Sla uw wijzigingen op.

De toegevoegde encryptieregels voor verwisselbare schijven worden toegepast op verwisselbare schijven die zijn aangesloten op computers in de organisatie.

## Een lijst met encryptieregels voor verwisselbare schijven exporteren en importeren

U kunt de lijst met encryptieregels voor verwisselbare schijven exporteren naar een XML-bestand. Vervolgens kunt u het bestand wijzigen om bijvoorbeeld een groot aantal regels toe te voegen voor hetzelfde type verwisselbare schijven. U kunt ook de export/import-functie gebruiken om een back-up te maken van de lijst met encryptieregels voor verwisselbare schijven of om de regels naar een andere server te migreren.

[Een lijst met encryptieregels voor verwisselbare schijven exporteren en importeren in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Encryption of removable drives** in het beleidsvenster.
6. De lijst met encryptieregels voor verwisselbare schijven exporteren:
  - a. Selecteer de regels die u wilt exporteren. Gebruik de **CTRL**- of **SHIFT**-toets om meerdere poorten te selecteren.  
Als u geen regel hebt geselecteerd, exporteert Kaspersky Endpoint Security alle regels.
  - b. Klik op de link **Exporteren**.
  - c. Geef in het geopende venster de naam van het XML-bestand op waarnaar u de lijst met regels wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.
7. De lijst met encryptieregels voor verwisselbare schijven importeren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

[Een lijst met encryptieregels voor verwisselbare schijven exporteren en importeren in de Webconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Encryption of removable drives**.
5. Klik in het blok **Encryption rules for selected devices** op de koppeling **Encryption rules**.  
Hierdoor wordt de lijst met encryptieregels voor verwisselbare schijven geopend.
6. De lijst met encryptieregels voor verwisselbare schijven exporteren:
  - a. Selecteer de regels die u wilt exporteren.
  - b. Klik op **Export**.
  - c. Bevestig dat u alleen de geselecteerde regels wilt exporteren of de volledige lijst wilt exporteren.
  - d. Sla het bestand op.  
Kaspersky Endpoint Security exporteert de lijst met regels naar een XML-bestand in de standaard downloadmap.
7. De lijst met regels importeren:
  - a. Klik op de link **Importeren**.  
Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
  - b. Open het bestand.  
Als de computer al een lijst met regels heeft, vraagt Kaspersky Endpoint Security u de bestaande lijst te verwijderen of nieuwe items eraan toe te voegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

## Portable modus voor toegang tot geëncrypte bestanden op verwisselbare schijven

De *portable modus* is een modus voor bestandsencryptie (FLE) op verwisselbare schijven die u de mogelijkheid biedt om toegang tot gegevens te verkrijgen wanneer u niet verbonden bent met het bedrijfsnetwerk. Dankzij de portable modus kunt u ook werken met geëncrypte gegevens op computers waarop Kaspersky Endpoint Security niet is geïnstalleerd.

De portable modus is gemakkelijk te gebruiken in de volgende gevallen:

- Er is geen verbinding tussen de computer en de Kaspersky Security Center Administration Server.
- De infrastructuur is veranderd met de wijziging van de Kaspersky Security Center Administration Server.



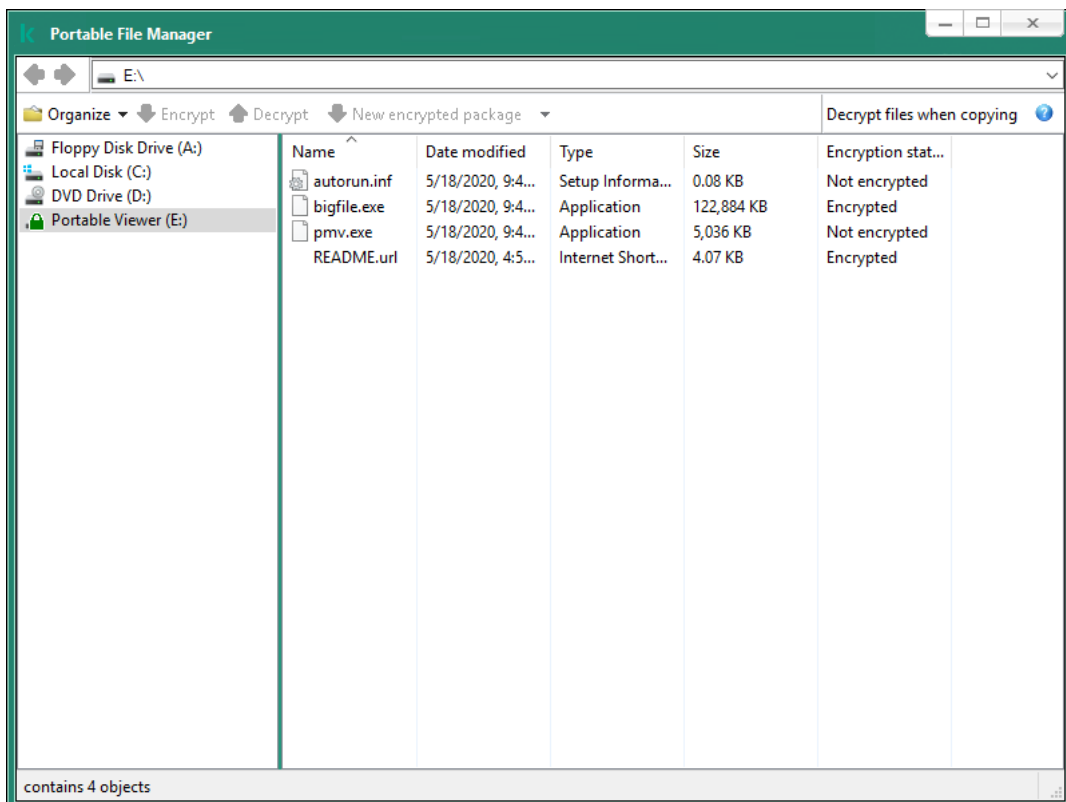
- Kaspersky Endpoint Security is niet op de computer geïnstalleerd.

## Portable bestandsbeheer

Om in portable modus te werken, installeert Kaspersky Endpoint Security een speciale encryptiemodule genaamd *Portable bestandsbeheer* op een verwisselbare schijf. De Portable File Manager biedt een interface voor het werken met geëncrypte gegevens als Kaspersky Endpoint Security niet op de computer is geïnstalleerd (zie onderstaande afbeelding). Als Kaspersky Endpoint Security op uw computer is geïnstalleerd, kunt u met geëncrypte verwisselbare schijven werken met uw gebruikelijke bestandsverkenners (bijvoorbeeld Verkenner).

Portable bestandsbeheer slaat een sleutel op om bestanden te encrypten op een verwisselbare schijf. De sleutel is geëncrypt met het gebruikerswachtwoord. De gebruiker stelt een wachtwoord in voordat bestanden op een verwisselbaar station worden geëncrypt.

Portable bestandsbeheer start automatisch wanneer een verwisselbare schijf wordt aangesloten op een computer waarop Kaspersky Endpoint Security niet is geïnstalleerd. Als het automatisch opstarten van programma's op de computer is uitgeschakeld, start dan handmatig het portable bestandsbeheer. Om dit te doen, voert u het bestand met de naam pmv.exe uit dat is opgeslagen op de verwisselbare schijf.



Portable bestandsbeheer

Ondersteuning voor draagbare modus voor het werken met geëncrypte bestanden

[Ondersteuning voor portable modus inschakelen voor het werken met geëncrypte bestanden op verwisselbare schijven in de beheerconsole \(MMC\)](#)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Encryption of removable drives** in het beleidsvenster.
6. Selecteer in de vervolgkeuzelijst **Encryptiemodus voor geselecteerde apparaten** de optie **Alle bestanden encrypten** of **Alleen nieuwe bestanden encrypten**.

De portable modus is alleen beschikbaar met File Level Encryption (FLE). Het is niet mogelijk om ondersteuning voor portable modus in te schakelen voor Full Disk Encryption (FDE).

7. Schakel het selectievakje **Portable modus** in.
8. [Voeg](#) indien nodig [encryptieregels toe voor individuele verwisselbare schijven](#).
9. Sla uw wijzigingen op.
10. Sluit de verwisselbare schijf aan op de computer nadat u het beleid hebt 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. Sla uw wijzigingen op.

Kaspersky Endpoint Security encrypt bestanden op de verwisselbare schijf. Het portable bestandsbeheer (voor het werken met geëncrypte bestanden) wordt ook toegevoegd aan de verwisselbare schijf. Als er al geëncrypte bestanden op de verwisselbare schijf staan, zal Kaspersky Endpoint Security deze opnieuw encrypten met zijn eigen sleutel. Hierdoor heeft de gebruiker toegang tot alle bestanden op de verwisselbare schijf in draagbare modus.

[Ondersteuning voor portable modus inschakelen voor het werken met geëncrypte bestanden op verwisselbare schijven in de webconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Data Encryption** → **Encryption of removable drives**.
5. Selecteer in het blok **Encryptie beheren** **Alle bestanden encrypten** of **Alleen nieuwe bestanden encrypten**.

De portable modus is alleen beschikbaar met File Level Encryption (FLE). Het is niet mogelijk om ondersteuning voor portable modus in te schakelen voor Full Disk Encryption (FDE).

6. Schakel het selectievakje **Portable modus** in.
7. Voeg indien nodig [encryptieregels toe voor individuele verwisselbare schijven](#).
8. Sla uw wijzigingen op.
9. Sluit de verwisselbare schijf aan op de computer nadat u het beleid hebt toegepast.
10. Bevestig de encryptie van de verwisselbare schijf.  
U ziet nu een venster waarin u een wachtwoord voor Portable bestandsbeheer kunt aanmaken.
11. Geef een wachtwoord op dat sterk genoeg is en bevestig het.
12. Sla uw wijzigingen op.

Kaspersky Endpoint Security encrypt bestanden op de verwisselbare schijf. Het portable bestandsbeheer (voor het werken met geëncrypte bestanden) wordt ook toegevoegd aan de verwisselbare schijf. Als er al geëncrypte bestanden op de verwisselbare schijf staan, zal Kaspersky Endpoint Security deze opnieuw encrypten met zijn eigen sleutel. Hierdoor heeft de gebruiker toegang tot alle bestanden op de verwisselbare schijf in draagbare modus.

## Geëncrypte bestanden op een verwisselbare schijf openen

Na het encrypten van bestanden op een verwisselbare schijf met ondersteuning voor portable modus, zijn de volgende methoden voor bestandstoegang beschikbaar:

- Als Kaspersky Endpoint Security niet op de computer is geïnstalleerd, zal portable bestandsbeheer u vragen om een wachtwoord in te voeren. Elke keer dat u de computer opnieuw opstart of de verwisselbare schijf opnieuw aansluit, moet u het wachtwoord invoeren.
- Als de computer zich buiten het bedrijfsnetwerk bevindt en Kaspersky Endpoint Security is geïnstalleerd op de computer, dan vraagt het programma u om het wachtwoord in te voeren of stuurt het de beheerder een verzoek om toegang tot de bestanden. Nadat Kaspersky Endpoint Security toegang heeft gekregen tot bestanden op een verwisselbare schijf, slaat het de geheime sleutel op in de sleutelopslag van de computer. Op deze manier krijgt u in de toekomst toegang tot bestanden zonder een wachtwoord in te voeren of de beheerder te vragen.

- Als de computer zich in het bedrijfsnetwerk bevindt en Kaspersky Endpoint Security op de computer is geïnstalleerd, krijgt u toegang tot het apparaat zonder een wachtwoord in te voeren. Kaspersky Endpoint Security ontvangt de geheime sleutel van de Kaspersky Security Center Administration Server waarmee de computer is verbonden.

## Het wachtwoord herstellen om in portable modus te werken

Als u het wachtwoord voor het werken in portable modus bent vergeten, moet u de verwisselbare schijf aansluiten op een computer waarop Kaspersky Endpoint Security is geïnstalleerd in het bedrijfsnetwerk. U krijgt toegang tot de bestanden omdat de geheime sleutel is opgeslagen in de sleutelopslag van de computer of op de Administration Server. Decrypt en encrypt bestanden opnieuw met een nieuw wachtwoord.

## Kenmerken van de portable modus bij het aansluiten van een verwisselbare schijf op een computer vanaf een ander netwerk

Als de computer zich buiten het bedrijfsnetwerk bevindt en Kaspersky Endpoint Security op de computer is geïnstalleerd, dan kunt u de bestanden op de volgende manieren openen:

- **Toegang met een wachtwoord**

Nadat u het wachtwoord hebt ingevoerd, kunt u bestanden op de verwisselbare schijf openen, wijzigen en opslaan (*transparante toegang*). Kaspersky Endpoint Security kan een alleen-lezen toegangsrecht instellen voor een verwisselbare schijf als de volgende parameters zijn geconfigureerd in de beleidsinstellingen voor encryptie van verwisselbare schijven:

- De ondersteuning voor de portable modus is uitgeschakeld.
- De modus **Alle bestanden encrypten** of **Alleen nieuwe bestanden encrypten** is geselecteerd.

In alle andere gevallen krijgt u volledige toegang tot de verwisselbare schijf (lees- en schrijfmachtiging). U kunt dan bestanden toevoegen en verwijderen.

U kunt de toegangsmachtigingen voor de verwisselbare schijf zelfs wijzigen wanneer de verwisselbare schijf is aangesloten op de computer. Als de toegangsmachtigingen voor de verwisselbare schijf worden gewijzigd, blokkeert Kaspersky Endpoint Security de toegang tot de bestanden en wordt u gevraagd het wachtwoord opnieuw in te voeren.

Na het invoeren van het wachtwoord kunt u de instellingen van het encryptiebeleid voor de verwisselbare schijf niet toepassen. In dit geval kunt u de bestanden op de verwisselbare schijf niet decrypten of opnieuw encrypten.

- **Vraag de beheerder om toegang tot de bestanden**

Als u het wachtwoord voor het werken in portable modus bent vergeten, dan vraagt u de beheerder om toegang tot bestanden. Als u toegang tot de bestanden wilt, moet u een bestand met een toegangsaanvraag versturen naar de beheerder. Dit bestand heeft de extensie .kesdc. De gebruiker kan het bestand met de toegangsaanvraag bijvoorbeeld versturen per e-mail. De beheerder stuurt een geëncrypt gegevenstoegangsbestand (een bestand met de KESDR-extensie).

Nadat u de procedure van aanvraag en antwoord voor wachtwoordherstel hebt voltooid, ontvangt u transparante toegang tot de bestanden op de verwisselbare schijf en volledige toegang tot de verwisselbare schijf (lees- en schrijfmachtiging).

U kunt een encryptiebeleid op de verwisselbare schijf toepassen en bijvoorbeeld bestanden decrypten. Na het herstellen van het wachtwoord of wanneer het beleid is geüpdatet, wordt u door Kaspersky Endpoint Security gevraagd om de wijzigingen te bevestigen.

[Een geëncrypt gegevenstoegangsbestand verkrijgen in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Devices**.
4. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
6. Selecteer in het geopende venster het tabblad **Gegevensencryptie**.
7. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.
8. Geef in het venster voor het selecteren van een bestand met verzoektoegang het pad op naar het bestand dat van de gebruiker is ontvangen.

U ziet informatie over het verzoek van de gebruiker. Kaspersky Security Center genereert een sleutelbestand. E-mail het gegenereerde bestand met de sleutel voor toegang tot de geëncrypte gegevens naar de gebruiker. Of sla het toegangsbestand op en gebruik een beschikbare methode om het bestand over te dragen.

#### [Een geëncrypt gegevenstoegangsbestand verkrijgen in de webconsole](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.
3. Klik op de knop **Grant access to the device in offline mode**.
4. Selecteer het gedeelte **Gegevensencryptie**.
5. Klik op de knop **Select file** en selecteer het bestand van de toegangsaanvraag dat u van de gebruiker hebt ontvangen (een bestand met de extensie KESDC).  
De webconsole geeft informatie over de aanvraag weer. Dit omvat de naam van de computer waarop de gebruiker toegang tot het bestand vraagt.
6. Klik op de knop **Sleutel opslaan** en selecteer een map om het bestand met de toegangssleutel voor de geëncrypte gegevens op te slaan (een bestand met de extensie KESDR).

Als gevolg hiervan kunt u de gegevenstoegangssleutel verkrijgen, die u aan de gebruiker moet overdragen.

## Decryptie van verwisselbare schijven

U kunt een beleid gebruiken om een verwisselbaar station te decrypten. Een beleid met gedefinieerde instellingen voor encryptie van verwijderbare schijven wordt gegenereerd voor een specifieke beheergroep. Daarom hangt het resultaat van de decryptie van gegevens op verwisselbare schijven af van de computer waarop de verwisselbare schijven zijn aangesloten.

*Zo decrypt u verwisselbare schijven:*

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Data Encryption** → **Encryption of removable drives** in het beleidsvenster.
6. Als u alle geëncrypte bestanden op verwisselbare schijven wilt decrypten, selecteert u in de vervolgkeuzelijst **Encryptiemodus** de optie **Gehele verwisselbare schijf decrypten**.
7. 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.
  - c. Klik in het contextmenu van de knop **Een regel instellen** op de optie **Gehele verwisselbare schijf decrypten**.
8. Sla uw wijzigingen op.

Als een gebruiker een verwisselbare schijf aansluit of al heeft aangesloten, dan decrypt Kaspersky Endpoint Security de verwisselbare schijf. Het programma waarschuwt de gebruiker dat de decryptie enige tijd kan duren. 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. De gegevensdecryptie gaat verder de volgende keer dat de verwisselbare schijf wordt aangesloten op deze computer.

Als het decrypten van een verwisselbare schijf mislukt is, bekijkt u het rapport **Gegevensencryptie** in de interface van Kaspersky Endpoint Security. De toegang tot bestanden kan worden geblokkeerd door een ander programma. Probeer in dat geval de verwisselbare schijf los te koppelen van de computer en opnieuw aan te sluiten.

## Details van gegevensencryptie bekijken

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:

- *Encryptiebeleid niet gedefinieerd.* Er is geen Kaspersky Security Center-encryptiebeleid gedefinieerd voor de computer.
- *Beleid wordt toegepast.* 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 gegevensencryptie 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.

## 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 **Managed devices** 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 **Devices**.
4. Schuif op het tabblad **Apparaten** in de werkruimte de schuifbalk helemaal naar rechts.
5. Als de kolom **Encryptiestatus** niet wordt weergegeven:
  - a. Klik rechts om het contextmenu van de tabelkop te openen.
  - b. Selecteer in de vervolgkeuzelijst **Weergeven** van het contextmenu de optie **Kolommen toevoegen/verwijderen**.
  - c. Selecteer in het geopende venster het tabblad **Encryptiestatus**.
  - d. Klik op **OK**.

In de kolom **Encryptiestatus** ziet u de encryptiestatus van de gegevens op de computers uit de geselecteerde beheergroep. Deze status is gebaseerd op informatie over bestandsencryptie op lokale schijven van de computer en over Full Disk Encryption.

## Encryptiestatistieken bekijken op dashboards van Kaspersky Security Center

*De encryptiestatus op de dashboards van Kaspersky Security Center bekijken:*

1. Open de Beheerconsole van Kaspersky Security Center.

2. Selecteer in de consolestructuur het knooppunt **Administration Server**.
3. Selecteer het tabblad **Statistics** 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 **Statistics** op de knop **Customize view**.
  - b. Klik in het venster op de knop **Toevoegen**.
  - c. Dit opent een venster. Voer in dat venster de naam van de pagina in in het gedeelte **General**.
  - d. Klik in het gedeelte **Information panels** op de knop **Add**.
  - e. Selecteer in het venster dat opent in de groep **Protection status** de optie **Encryption of devices**.
  - f. Klik op **OK**.
  - g. Bewerk indien nodig de instellingen van het detailvenster. Gebruik hiervoor **View** en **Devices**.
  - h. Klik op **OK**.
  - i. Herhaal stappen d tot en met h van de instructies en selecteer de optie **Encryption of removable drives** in het gedeelte **Protection status**.  
Het toegevoegde detailpaneel verschijnt in de lijst **Information panels**.
  - j. Klik op **OK**.  
De naam van de pagina met de informatievensters die tijdens de vorige stappen zijn gemaakt verschijnt in de lijst **Pages**.
  - k. Klik op de knop **Close**.
5. Open op het tabblad **Statistics** 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 **Managed devices** 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 **Devices**.
4. Selecteer de naam van de computer in de lijst en klik rechts om het contextmenu te openen.
5. Selecteer in het contextmenu van de computer de optie **Properties**. Selecteer in het geopende venster het gedeelte **Bescherming**.



6. Klik op de link **Gegevensencryptiefouten bekijken** om het venster **Gegevensencryptiefouten** 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 **Data encryption errors**.

## 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 **Reports**.
3. Klik op de knop **New report template**.  
De wizard Nieuwe rapportsjabloon wordt gestart.
4. Volg de instructies van de wizard Sjabloon voor rapport. In het venster **Selecting the report template type** selecteert u in het gedeelte **Other** een van de volgende opties:

- **Report on encryption status of managed devices.**
- **Report on encryption status of mass storage devices.**
- **Report on file encryption errors.**
- **Report on blockage of access to encrypted files.**

Wanneer u de wizard Nieuwe rapportsjabloon hebt voltooid, verschijnt de nieuwe rapportsjabloon in de tabel op het tabblad **Reports**.

5. Selecteer de rapportsjabloon die tijdens de vorige stappen van de instructies zijn aangemaakt.
6. Selecteer in het contextmenu van de sjabloon de optie **Show report**.

Het rapport wordt gemaakt. Het rapport wordt in een nieuw venster weergegeven.

## 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 toegangssleutel 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 toegangssleutel aan te maken (dit bestand heeft een KESDR-extensie) en stuurt het naar de gebruiker.
3. De gebruiker past de toegangssleutel 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 toegangssleutel 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 Restore Utility om een bestand met een toegangsaanvraag aan te maken (dit bestand heeft een FDERTC-extensie) en stuurt het naar de LAN-beheerder van het bedrijf.
2. De beheerder gebruikt de beheerconsole van Kaspersky Security Center om een bestand met een toegangssleutel aan te maken (dit bestand heeft een FDERTR-extensie) en stuurt het naar de gebruiker.
3. De gebruiker past de toegangssleutel toe.

Om gegevens op geëncrypte harde schijven van het systeem te herstellen, kan de gebruiker ook de accountgegevens voor Authenticatie-agent opgeven in de Herstelvoorziening. Als de metagegevens van het account voor Authenticatie-agent beschadigd zijn, moet de gebruiker de herstelprocedure voltooien met het bestand met de toegangsaanvraag.

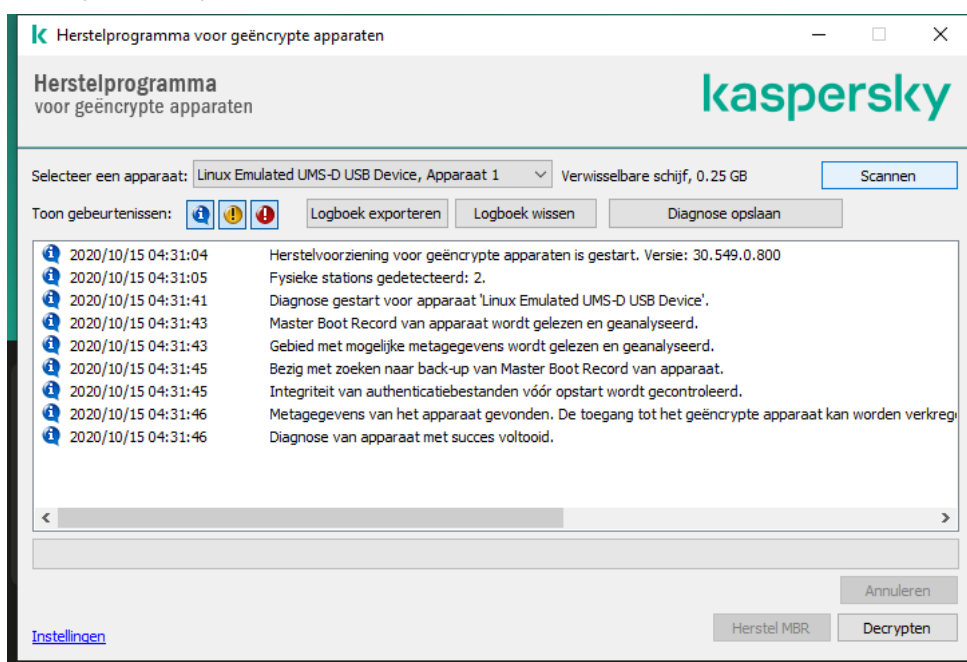
Voordat u gegevens op geëncrypte apparaten herstelt, wordt u aanbevolen het Kaspersky Security Center-beleid te annuleren of de encryptie in de Kaspersky Security Center-beleidsinstellingen uit te schakelen op de computer waarop de procedure zal worden uitgevoerd. Hiermee voorkomt u dat het apparaat opnieuw wordt geëncrypt.

## Gegevens herstellen met behulp van de FDERT Restore Utility

Als de harde schijf defect raakt, is het bestandssysteem mogelijk beschadigd. Als dit het geval is, zijn gegevens beschermd door Kaspersky Disk Encryption-technologie niet beschikbaar. U kunt de gegevens decrypten en naar een nieuwe schijf kopiëren.

Gegevensherstel op een schijf beschermd door Kaspersky Disk Encryption-technologie bestaat uit de volgende stappen:


1. Maak een zelfstandige herstelvoorziening (restore utility) (zie onderstaande afbeelding).
2. Sluit een schijf aan op een computer waarop geen Kaspersky Endpoint Security-encryptiecomponenten zijn geïnstalleerd.
3. Voer de Restore Utility uit en voer een diagnose van de harde schijf uit.
4. Toegang tot gegevens op de schijf. Voer hiervoor de inloggegevens van de authenticatie-agent in of start de herstelprocedure (Request-Response).



FDERT Restore Utility

## Een zelfstandige herstelvoorziening maken

*Zo maakt u het uitvoerbare bestand van Herstelvoorziening aan:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Klik in het venster op de knop **Geëncrypt apparaat herstellen**.  
De herstelvoorziening voor geëncrypte apparaten wordt gestart.
3. Klik op de knop **Maak standalone herstelvoorziening** in het venster van Herstelvoorziening.
4. Sla de zelfstandige herstelvoorziening op in het computergeheugen.

Als gevolg hiervan wordt het uitvoerbare bestand van de herstelvoorziening (fdert.exe) opgeslagen in de opgegeven map. Kopieer de herstelvoorziening naar een computer die geen encryptiecomponenten van Kaspersky Endpoint Security heeft. Hiermee voorkomt u dat de schijf opnieuw wordt geëncrypt.

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.

## Gegevens herstellen op een harde schijf

*Zo herstelt u de toegang tot geëncrypte bestanden met de Herstelvoorziening:*

1. Voer het bestand met de naam fdert.exe uit, het uitvoerbare bestand van de Restore Utility. Dit bestand wordt door Kaspersky Endpoint Security aangemaakt.
2. Selecteer in het venster Herstelvoorziening het geëncrypte 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 encryptiefunctie 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 encryptiefunctie van Kaspersky Endpoint Security, wordt u door de Herstelvoorziening gevraagd om het apparaat te decrypten.

4. Als u diagnosegegevens wilt importeren, klikt u op de knop **Diagnose opslaan**.  
Het hulpprogramma slaat een archief op met bestanden met diagnosegegevens.
5. Klik op de knop **Herstel MBR** 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 verkregen.
6. Klik op de knop **Ontgrendelen** of **Decrypten** naargelang de resultaten van de diagnose.
7. Om gegevens met behulp van een Authenticatie-agent-account herstellen, selecteert u de optie **Instellingen van account voor Authenticatie-agent gebruiken** en voer de gegevens van de Authenticatie-agent in.  
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 voor Authenticatie-agent verloren zijn geraakt, moet u een toegangssleutel vragen aan de netwerkbeheerder van het bedrijf om de gegevens op een geëncrypt apparaat te herstellen.
8. Doe het volgende om de herstelprocedure te starten:
  - a. Selecteer de optie **Toegangssleutel voor apparaat handmatig opgeven**.
  - b. Klik op de knop **Toegangssleutel ontvangen** en sla het bestand van de toegangs aanvraag op in het computergeheugen (een bestand met de extensie FDERTC).
  - c. Stuur het bestand met de toegangs aanvraag naar de netwerkbeheerder van het bedrijf.

Sluit het venster **Toegangssleutel voor apparaat ontvangen** pas als u de toegangssleutel hebt ontvangen. Wanneer dit venster opnieuw wordt geopend, kunt u de toegangssleutel die eerder is aangemaakt door de beheerder niet toepassen.

d. Ontvang het toegangsbestand (een bestand met de extensie FDERTR) dat is gemaakt en naar u is verzonden door de LAN-beheerder en sla het op (zie onderstaande instructies).

e. Download het toegangsbestand in het venster **Toegangssleutel voor apparaat ontvangen**.

9. Als u een apparaat decrypt, moet u aanvullende decryptie-instellingen configureren:

- 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 geeft u de grenzen van het te decrypten gebied op.
- 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 **Decrypten naar een schijfkopie** uit.
  - Als u de gedecrypte gegevens gescheiden wilt houden van de originele geëncrypte gegevens, schakelt u het selectievakje **Decrypten naar een schijfkopie** in en gebruikt u de knop **Bladeren** om het pad op te geven waar u het VHD-bestand wilt opslaan.

10. Klik op **OK**.

Het apparaat start de ontgrendeling of de decryptie.

[Een geëncrypt gegevenstoegangsbestand maken in de Beheerconsole \(MMC\)](#) 

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Extra** → **Data encryption and protection** → **Encrypted drives**.
3. Selecteer in de werkruimte het geëncrypte apparaat waarvoor u een bestand met een toegangscode wilt aanmaken en klik vervolgens in het contextmenu van het apparaat op **Krijg toegang tot het apparaat in Kaspersky Endpoint Security voor Windows**.

Als u niet zeker weet voor welke computer het bestand met de toegangsaanvraag is gegenereerd, selecteert u in de structuur van de Beheerconsole achtereenvolgens **Extra** → **Gegevensencryptie en -bescherming** en klikt u in de werkruimte op de koppeling **Krijg encryptiesleutel voor apparaat in Kaspersky Endpoint Security voor Windows**.

4. Selecteer in het geopende venster het te gebruiken encryptie-algoritme: **AES256** of **AES56**.  
Het algoritme voor gegevensencryptie hangt af van de AES-encryptiebibliotheek die bij het distributiepakket wordt meegeleverd: *sterke encryptie (AES256)* of *normale encryptie (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.
5. Klik op **Bladeren** om een venster te openen en selecteer in dit venster het pad naar het aanvraagbestand met de fdertc-extensie die u hebt gekregen van de gebruiker.
6. Klik op de knop **Openen**.

U ziet informatie over het verzoek van de gebruiker. Kaspersky Security Center genereert een sleutelbestand. E-mail het gegenereerde bestand met de sleutel voor toegang tot de geëncrypte gegevens naar de gebruiker. Of sla het toegangsbestand op en gebruik een beschikbare methode om het bestand over te dragen.

[Hoe u een bestand voor toegang tot geëncrypte gegevens maakt in de webconsole](#) 

1. Selecteer in het hoofdvenster van de Webconsole **Operations** → **Data encryption and protection** → **Encrypted Drives**.

2. Schakel het selectievakje in naast de naam van de computer waarvoor u gegevens wil herstellen.

3. Klik op de knop **Grant access to the device in offline mode**.

Dit start de wizard voor het verlenen van toegang tot een apparaat.

4. Volg de instructies van de wizard om toegang te verlenen tot een apparaat:

a. Selecteer de beheerplug-in **Kaspersky Endpoint Security voor Windows**

b. Selecteer het coderingsalgoritme dat u wilt gebruiken: **AES256** of **AES56**.

Het algoritme voor gegevensencryptie hangt af van de AES-encryptiebibliotheek die bij het distributiepakket wordt meegeleverd: *sterke encryptie (AES256)* of *normale encryptie (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.

c. Klik op de knop **Bestand selecteren** en selecteer het bestand van de toegangs aanvraag dat u van de gebruiker hebt ontvangen (een bestand met de extensie FDERTC).

d. Klik op de knop **Save key** en selecteer een map om het bestand met de toegangssleutel voor de geëncrypte gegevens op te slaan (een bestand met de extensie FDERTR).

Als gevolg hiervan kunt u de gegevenstoegangssleutel verkrijgen, die u aan de gebruiker moet overdragen.

## 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](#)).

## Detection and Response-oplossingen

Kaspersky Endpoint Security ondersteunt detectie- en responsoplossingen met behulp van een ingebouwde agent. Om Detection and Response te gebruiken, moet u integratie met deze oplossingen inschakelen bij het installeren van het programma. De ingebouwde agent ondersteunt:

- Kaspersky Managed Detection and Response (MDR);
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum);
- Kaspersky Endpoint Detection and Response Expert (EDR Expert);
- Kaspersky Sandbox 2.0.

U kunt Kaspersky Endpoint Security met Detection and Response-oplossing in verschillende configuraties gebruiken, bijvoorbeeld [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

Kaspersky Endpoint Agent ondersteunt Detection and Response-oplossingen die de ingebouwde Kaspersky Endpoint Security niet ondersteunt (bijvoorbeeld Kaspersky Sandbox 1.0).

In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiekpakket niet langer deel uit van de Kaspersky Endpoint Security-distributiek. U moet het Kaspersky Endpoint Agent-distributiekpakket afzonderlijk downloaden.

## Kaspersky Endpoint Agent beheren

*Kaspersky Endpoint Agent* ondersteunt de interactie tussen het programma en andere Kaspersky-oplossingen voor het detecteren van geavanceerde dreigingen (bijv. Kaspersky Sandbox). Kaspersky-oplossingen zijn compatibel met specifieke versies van Kaspersky Endpoint Agent.

Om Kaspersky Endpoint Agent te gebruiken als onderdeel van Kaspersky-oplossingen, moet u die oplossingen activeren met een bijbehorende licentiecode.

Raadpleeg de Helpgids van het relevante product voor volledige informatie over de Kaspersky Endpoint Agent voor Windows opgenomen in de softwareoplossing die u gebruikt, en voor volledige informatie over de zelfstandige oplossing.

- *Help van Kaspersky Anti Targeted Attack Platform*
- *Help van Kaspersky Sandbox*
- *Help van Kaspersky Endpoint Detection and Response Optimum*
- *Help van Kaspersky Managed Detection and Response*

In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiekpakket niet langer deel uit van de Kaspersky Endpoint Security-distributiek. U moet het Kaspersky Endpoint Agent-distributiekpakket afzonderlijk downloaden.



| Kaspersky Endpoint Security voor Windows | Kaspersky Endpoint Agent beheren |
|--|----------------------------------|
| 11.8.0                                   | 3.11.0.216.mr1                   |
| 11.7.0                                   | 3,11                             |
| 11.6.0                                   | 3,10                             |
| 11.5.0                                   | 3,9                              |
| 11.4.0                                   | 3,9                              |
| 11.3.0                                   | 3,9                              |
| 11.2.0                                   | 3,9                              |

## Migratie van beleid en taken voor Kaspersky Endpoint Agent

Kaspersky Endpoint Security 11.7.0 heeft nu een wizard voor de migratie van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security. U kunt beleids- en taakinstellingen migreren voor de volgende oplossingen:

- Kaspersky Sandbox;
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum);
- Kaspersky Managed Detection and Response (MDR).

U wordt aanbevolen eerst Kaspersky Endpoint Agent naar Kaspersky Endpoint Security te migreren op een enkele computer en vervolgens op een groep computers. Daarna voltooit u de migratie op alle computers van het bedrijf.

*Zo migreert u beleids- en taakinstellingen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security:*

Selecteer **Bewerkingen** → **Migratie vanaf Kaspersky Endpoint Agent** in het hoofdvenster van de Webconsole.

De wizard Beleids- en taakmigratie wordt gestart. Volg de instructies van de wizard.

### Stap 1. Beleidsmigratie

De migratiewizard maakt een nieuw beleid die de instellingen van het Kaspersky Endpoint Security-beleid en het Kaspersky Endpoint Agent-beleid samenvoegt. In de beleidslijst selecteert u het Kaspersky Endpoint Agent-beleid waarvan u de instellingen wilt samenvoegen met het Kaspersky Endpoint Security-beleid. Klik op een Kaspersky Endpoint Agent-beleid om het Kaspersky Endpoint Security-beleid te selecteren waarmee u de instellingen wilt samenvoegen. Zorg dat u telkens het juiste beleid hebt geselecteerd en ga naar de volgende stap.

### Stap 2. Taakmigratie

De Migratiewizard maakt nieuwe taken voor Kaspersky Endpoint Security voor Windows. In de takenlijst selecteert u de Kaspersky Endpoint Agent-taken die u wilt maken voor het Kaspersky Endpoint Security-beleid. De Wizard ondersteunt taken voor Kaspersky Endpoint Detection and Response en Kaspersky Sandbox. Ga naar de volgende stap.

## Stap 3. Voltooiing van wizard

Verlaat de wizard verlaten. De wizard:

- Maakt een nieuw Kaspersky Endpoint Security-beleid.

Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint samen. Het beleid krijgt de naam <Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>. Het nieuwe beleid heeft de status *Inactief*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactief* en activeer het nieuwe samengevoegde beleid.

Controleer na de migratie van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security voor Windows of in het nieuwe beleid [de functionaliteit voor gegevensoverdracht naar de Administration Server](#) (gegevens van quarantainebestanden en de bedreigingsontwikkelingsketen) is ingesteld. Parameterwaarden voor gegevensoverdracht worden niet gemigreerd vanuit een Kaspersky Endpoint Agent-beleid.

- Maakt nieuwe Kaspersky Endpoint Security-taken.

Nieuwe taken zijn kopieën van Kaspersky Endpoint Agent-taken voor de oplossing Kaspersky Endpoint Detection and Response. De taken van Kaspersky Endpoint Agent worden door de wizard niet gewijzigd.

## De [KES+KEA]-configuratie migreren naar [KES+built-in agent]

Kaspersky Endpoint Security 11.7.0 heeft nu ingebouwde agents voor de oplossingen Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) en Kaspersky Sandbox 2.0. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met deze oplossingen te werken. Wanneer u Kaspersky Endpoint Security upgradet naar versie 11.7.0, blijven de EDR Optimum- en Kaspersky Sandbox-oplossingen werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd.

In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiepakket niet langer deel uit van de Kaspersky Endpoint Security-distributiekit. U moet het Kaspersky Endpoint Agent-distributiepakket afzonderlijk downloaden.

Het migreren van de configuratie [KES+KEA] naar [KES+ingebouwde agent] omvat de volgende stappen:

### 1 Kaspersky Security Center upgraden

Upgrade alle onderdelen van Kaspersky Security Center naar versie 13.2, inclusief de Administration Agent, op Webconsole en computers van gebruikers.

### 2 De webplug-in voor Kaspersky Endpoint Security upgraden

Upgrade in Kaspersky Security Center Web Console de Kaspersky Endpoint Security-webplug-in naar versie 11.7.0. Voor het beheren van EDR Optimum- en Kaspersky Sandbox-onderdelen moet u Webconsole gebruiken.

### 3 Het beleid en de taken migreren

Gebruik de [wizard voor beleids- en taakmigratie voor Kaspersky Endpoint Agent](#) om instellingen van Kaspersky Endpoint Agent te migreren naar Kaspersky Endpoint Security voor Windows.

Hierdoor wordt een nieuw Kaspersky Endpoint Security-beleid gemaakt. Het nieuwe beleid heeft de status *Inactief*. Om het beleid toe te passen, opent u de beleidseigenschappen, accepteert u de Kaspersky Security Network-verklaring en stelt u de status in op *Actief*.

#### 4 Licentiefunctionaliteit

Als u een algemene Kaspersky Endpoint Detection and Response Optimum- of Kaspersky Optimum Security-licentie gebruikt om Kaspersky Endpoint Security voor Windows en Kaspersky Endpoint Agent te activeren, wordt de EDR Optimum-functionaliteit automatisch geactiveerd na het upgraden van het programma naar versie 11.7.0. U hoeft verder niets te doen.

Als u een afzonderlijke add-on-licentie voor Kaspersky Endpoint Detection and Response Optimum gebruikt om EDR Optimum-functionaliteit te activeren, moet de EDR Optimum-sleutel toegevoegd zijn aan de Kaspersky Security Center-repository en [de functie voor automatische distributie van licentiesleutels ingeschakeld zijn](#). Nadat u het programma hebt geüpgraded naar versie 11.7.0, wordt de EDR Optimum-functionaliteit automatisch geactiveerd.

Als u een Kaspersky Endpoint Detection and Response Optimum- of Kaspersky Optimum Security-licentie gebruikt om Kaspersky Endpoint Agent te activeren, en een andere licentie om Kaspersky Endpoint Security voor Windows te activeren, moet u de sleutel van Kaspersky Endpoint Security voor Windows vervangen door de algemene Endpoint Detection and Response Optimum- of Kaspersky Optimum Security-sleutel. U kunt dan de sleutel vervangen met de taak [Sleutel toevoegen](#).

U hoeft de Kaspersky Sandbox-functionaliteit niet te activeren. Kaspersky Sandbox-functionaliteit is onmiddellijk beschikbaar na het upgraden en activeren van Kaspersky Endpoint Security voor Windows.

#### 5 Het Kaspersky Endpoint Security-programma upgraden

Voor het upgraden van het programma en het migreren van EDR Optimum- en Kaspersky Sandbox-functionaliteit, wordt een [installatietaak op afstand](#) aanbevolen.

Als u het programma wilt upgraden met behulp van een installatietaak op afstand, moet u de volgende instellingen bewerken:

- Selecteer de onderdelen Endpoint Detection and Response Optimum of Kaspersky Sandbox in de instellingen van het installatiepakket.
- Sluit het onderdeel Kaspersky Endpoint Agent uit in de instellingen van het installatiepakket.

U kunt het programma ook upgraden met behulp van de volgende methoden:

- Kaspersky-updateservice gebruiken (Seamless Update – SMU).
- Lokaal, met behulp van de Installatiewizard.

In dit geval moet u de configuratie van Kaspersky Endpoint Agent controleren die op de computer is geïnstalleerd. Als de geïnstalleerde Kaspersky Endpoint Agent het onderdeel Endpoint Detection and Response Expert (KATA EDR) bevat, verwijdert u het onderdeel voordat u een upgrade van het programma uitvoert. Als u het onderdeel Endpoint Detection and Response Expert (KATA EDR) niet kunt verwijderen, slaat Kaspersky Endpoint Security de onderdelen EDR Optimum en Kaspersky Sandbox over bij het upgraden van het programma. U kunt de onderdelen installeren met behulp van de taak [Programmaonderdelen wijzigen](#) na het upgraden van het programma.

Kaspersky Endpoint Security ondersteunt het automatisch selecteren van onderdelen bij het upgraden van het programma op een computer waarop het programma Kaspersky Endpoint Agent is geïnstalleerd. De automatische selectie van onderdelen hangt af van de machtigingen van het gebruikersaccount dat het programma opwaardeert.

Als u Kaspersky Endpoint Security upgradet met behulp van het EXE- of MSI-bestand onder de systeemaccount (SYSTEM), krijgt Kaspersky Endpoint Security toegang tot actieve licenties van Kaspersky-oplossingen. Als op de computer bijvoorbeeld Kaspersky Endpoint Agent is geïnstalleerd en de EDR Optimum-oplossing is geactiveerd, configureert het Kaspersky Endpoint Security-installatieprogramma automatisch de set onderdelen en selecteert het EDR Optimum-onderdeel. Hierdoor schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd. Het uitvoeren van het MSI-installatieprogramma onder de systeemaccount (SYSTEM) wordt meestal uitgevoerd bij het upgraden via de Kaspersky-updateservice (SMU) of bij het implementeren van een installatiepakket via Kaspersky Security Center.

Als u Kaspersky Endpoint Security upgradet met behulp van een MSI-bestand onder een gebruikersaccount zonder privileges, dan heeft Kaspersky Endpoint Security toegang tekort tot actieve licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security als volgt automatisch onderdelen op basis van de Kaspersky Endpoint Agent-configuratie:

- Als het onderdeel Endpoint Detection and Response Expert (KATA EDR) is geïnstalleerd, selecteert Kaspersky Endpoint Security het onderdeel Endpoint Agent. Kaspersky Endpoint Security selecteert alleen het onderdeel Endpoint Agent, zelfs als Kaspersky Endpoint Agent andere onderdelen geïnstalleerd heeft, bijvoorbeeld de [KATA EDR+KSB]-configuratie.
- Als het onderdeel Kaspersky Sandbox, EDR Optimum, of de configuratie [Kaspersky Sandbox+EDR Optimum] is geselecteerd, dan selecteert Kaspersky Endpoint Security de relevante onderdelen. Hierdoor schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

## 6 Computer herstarten

Start uw computer opnieuw op om de upgrade van het programma met de ingebouwde agent te voltooien. Bij het upgraden van het programma verwijdert het installatieprogramma Kaspersky Endpoint Agent voordat de computer opnieuw wordt heropgestart. Nadat de computer opnieuw is opgestart, voegt het installatieprogramma de ingebouwde agent toe. Dit betekent dat Kaspersky Endpoint Security de functies van EDR en Kaspersky Sandbox pas uitvoert nadat de computer opnieuw is heropgestart.

## 7 De status van Kaspersky Endpoint Detection and Response Optimum en Kaspersky Sandbox controleren

Als de computer na de upgrade de status *Kritiek* heeft in de Kaspersky Security Center-console:

- Zorg ervoor dat op de computer Administration Agent 13.2 is geïnstalleerd.
- Controleer de werkingsstatus van de onderdelen EDR Optimum en Kaspersky Sandbox in het *statusrapport van de programmaonderdelen*. Als een onderdeel de status *Niet geïnstalleerd* heeft, installeert u de onderdelen met behulp van de taak [Programmaonderdelen wijzigen](#).
- Zorg ervoor dat u akkoord gaat met de Kaspersky Security Network-verklaring in het nieuwe beleid van Kaspersky Endpoint Security voor Windows.

Verifieer via het *statusrapport van de programmaonderdelen* dat de EDR Optimum-functionaliteit is geactiveerd. Als een onderdeel de status *Niet gedekt door licentie* heeft, zorg er dan voor dat [de functie voor automatische distributie van licentiesleutels van EDR Optimum is ingeschakeld](#).

## Het programma upgraden als onderdeel van KATA EDR

Als Kaspersky Endpoint Agent is geïnstalleerd voor integratie met Kaspersky Anti Targeted Attack Platform (het onderdeel Endpoint Detection and Response Expert (KATA EDR)), kunt u Kaspersky Endpoint Security voor Windows op een van de volgende manieren upgraden:

- Een taak voor een externe installatie gebruiken  
Hiervoor moet u de volgende instellingen wijzigen:

- Sluit de onderdelen Endpoint Detection and Response Optimum en Kaspersky Sandbox uit in de instellingen van het installatiepakket.
- Selecteer het onderdeel Kaspersky Endpoint Agent in de instellingen van het installatiepakket. Als Kaspersky Endpoint Agent al op de computer is geïnstalleerd, wordt het programma geüpgraded naar versie 3.11.
- De Kaspersky-updateservice (SMU) gebruiken.  
Om dit te doen, moet u de programma-upgrade bevestigen. Kaspersky Endpoint Security sluit Endpoint Detection and Response Optimum en Kaspersky Sandbox uit van de installatie. Upgraden van Kaspersky Endpoint Agent wordt niet ondersteund. U kunt Kaspersky Endpoint Agent handmatig upgraden.
- Lokaal, met behulp van de Installatiewizard.  
Kaspersky Endpoint Security sluit Endpoint Detection and Response Optimum en Kaspersky Sandbox uit van de installatie. Als Kaspersky Endpoint Agent al op de computer is geïnstalleerd, wordt het programma geüpgraded naar versie 3.11.

## Beheerde detectie en respons



Kaspersky Endpoint Security 11.6.0 heeft een ingebouwde agent voor de Managed Detection and Response-oplossing. De *Kaspersky Managed Detection and Response (MDR)*-oplossing detecteert en analyseert automatisch beveiligingsincidenten in uw bedrijf. Hiertoe gebruikt MDR telemetriegegevens van eindpunten en machine learning. MDR stuurt incidentgegevens naar Kaspersky-experts. De experts kunnen vervolgens het incident verwerken en bijvoorbeeld een nieuwe vermelding toevoegen aan de antivirusdatabases. Of de experts kunnen aanbevelingen geven voor de verwerking van het incident en bijvoorbeeld voorstellen om de computer te isoleren van het netwerk. Voor gedetailleerde informatie over de werking van de oplossing raadpleegt u de [Help van Kaspersky Managed Detection and Response](#).

## Integratie met MDR

Om integratie met Kaspersky Managed Detection and Response in te stellen, moet u de component Managed Detection and Response inschakelen en Kaspersky Endpoint Security configureren.

U moet de volgende componenten inschakelen zodat Beheerde detectie en respons kan werken.

- [Kaspersky Security Network \(uitgebreide modus\)](#).
- [Gedragsdetectie](#).

Het inschakelen van deze componenten is niet optioneel. Anders kan Kaspersky Beheerde detectie en respons niet werken omdat het geen vereiste telemetriegegevens ontvangt.

Daarnaast kan Kaspersky Beheerde detectie en respons de ontvangen gegevens gebruiken van andere programmacomponenten. Het inschakelen van deze componenten is optioneel. Componenten die extra gegevens leveren omvatten:

- [Web Threat Protection](#).
- [Mail Threat Protection](#).

- [Firewall](#).

U moet ook een nieuwe beveiligde verbinding (een *achtergrondverbinding*) tot stand brengen opdat Kaspersky Managed Detection and Response kan werken met Administration Server via de Webconsole van Kaspersky Security Center. U wordt door Kaspersky Managed Detection and Response gevraagd om een achtergrondverbinding te maken wanneer u de oplossing implementeert. Zorg ervoor dat de achtergrondverbinding tot stand is gebracht. Voor informatie over de integratie van Kaspersky Security Center met andere Kaspersky-oplossingen raadpleegt u de [Help van Kaspersky Security Center](#).

Integratie met Kaspersky Beheerde detectie en respons bestaat uit de volgende stappen:

## 1 Privé Kaspersky Security Network configureren

Sla deze stap over als u Kaspersky Security Center Cloud Console gebruikt. Kaspersky Security Center Cloud Console configureert automatisch Lokaal Kaspersky Security Network bij het installeren van de MDR plug-in.

Privé KSN ondersteunt gegevensuitwisseling tussen computers en dedicated servers van Kaspersky Security Network, maar niet Global KSN.

Upload het Kaspersky Security Network-configuratiebestand in de Administration Server-eigenschappen. Het configuratiebestand van Kaspersky Security Network bevindt zich in het Ziparchief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Beheerde detectie en respons-console. Raadpleeg de [help van Kaspersky Security Center](#) voor meer informatie over de configuratie van de private Kaspersky Security Network-proxyserver. U kunt ook een Kaspersky Security Network-configuratiebestand uploaden naar de computer vanaf de opdrachtregel (zie onderstaande instructies).

### [Het privé Kaspersky Security Network configureren vanaf de opdrachtregel](#)

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.
2. Ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.
3. Voer de volgende opdracht uit:  
`avp.com KSN /private <bestandsnaam>`  
Waarbij <bestandsnaam> is de naam van het configuratiebestand met de Privaat KSN-instellingen (PKCS7- of PEM-bestandsindeling).

Voorbeeld:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Als gevolg hiervan zal Kaspersky Endpoint Security Privaat KSN gebruiken om de reputatie van bestanden, programma's en websites te bepalen. De beleidsinstellingen in het gedeelte **Kaspersky Security Network** geven de volgende bedrijfsstatus weer: *KSN-netwerk: Privé-KSN*.

U moet [de uitgebreide KSN-modus inschakelen](#) zodat Managed Detection and Response kan werken.

## 2 Kaspersky Managed Detection and Response-onderdeel inschakelen

Laad het BLOB-configuratiebestand in het Kaspersky Endpoint Security-beleid (zie onderstaande instructies). Het BLOB-bestand bevat de client-ID en informatie over de licentie voor Kaspersky Beheerde detectie en respons. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Beheerde detectie en respons-console. Raadpleeg de [Help van Kaspersky Managed Detection and Response](#) voor gedetailleerde informatie over een BLOB-bestand.

## Managed detectie en respons inschakelen in de beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Open in de map **Managed devices** 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 **Policies**.
4. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
5. Selecteer **Detection and Response** → **Managed Detection and Response** in het beleidsvenster.
6. Selecteer het selectievakje **Managed Detection and Response**.
7. Klik in het blok **Instellingen** op **Importeren** en selecteer het BLOB-bestand ontvangen in de Kaspersky Beheerde detectie en respons-console. Het bestand heeft de extensie P7.
8. Sla uw wijzigingen op.

## Managed Detection and Response activeren in de Webconsole en cloudconsole

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Managed Detection and Response**.
5. Zet de schakelaar **Managed Detection and Response** aan.
6. Klik op **Import** en selecteer het BLOB-bestand dat is verkregen in de Kaspersky Beheerde detectie en respons-console. Het bestand heeft de extensie P7.
7. Sla uw wijzigingen op.

## Managed Detection and Response activeren via de opdrachtregel

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.
2. Ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.
3. Voer de volgende opdracht uit:  
`avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>`

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de toestemming **Programma-instellingen configureren** hebben.



Kaspersky Endpoint Security controleert nu het BLOB-bestand. Verificatie van het BLOB-bestand omvat het controleren van de digitale handtekening en de geldigheidsduur van de licentie. Als het BLOB-bestand met succes is geverifieerd, zal Kaspersky Endpoint Security het bestand uploaden en naar de computer sturen tijdens de volgende synchronisatie met Kaspersky Security Center. Controleer de werkingsstatus van het onderdeel door het *statusrapport van de programmaonderdelen* te bekijken. U kunt de werkingsstatus van een onderdeel ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Managed Detection and Response** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

## Migratie van Kaspersky Endpoint Agent

Kaspersky Endpoint Security versie 11 en hoger ondersteunt de MDR-oplossing. Kaspersky Endpoint Security versies 11 – 11.5.0 verzendt alleen telemetriegegevens naar Kaspersky Beheerde detectie en respons om detectie van dreigingen mogelijk te maken. Kaspersky Endpoint Security versie 11.6.0 heeft alle functies van de ingebouwde agent (Kaspersky Endpoint Agent).

Als u Kaspersky Endpoint Security 11 - 11.5.0 gebruikt, moet u de databases updaten naar de nieuwste versie om te werken met de MDR-oplossing. U moet ook Kaspersky Endpoint Agent installeren.

Als u Kaspersky Endpoint Security 11.6.0 of hoger gebruikt, hoeft u Kaspersky Endpoint Agent niet te installeren om de MDR-oplossing te gebruiken.

Kaspersky Endpoint Agent migreren naar Kaspersky Endpoint Security voor Windows:

1. Configureer integratie met Kaspersky Managed Detection and Response in het Kaspersky Endpoint Security-beleid.
2. Schakel de component Beheerde detectie en respons in het Kaspersky Endpoint Agent-beleid uit.

Als het Kaspersky Endpoint Security-beleid ook van toepassing is op computers waarop Kaspersky Endpoint Security 11 - 11.5.0 niet is geïnstalleerd, moet u eerst een afzonderlijk Kaspersky Endpoint Agent-beleid voor die computers maken. Configureer in het nieuwe beleid de integratie met Kaspersky Beheerde detectie en respons.

## Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 heeft nu een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing (hierna ook 'EDR Optimum' genoemd). Kaspersky Endpoint Security 11.8.0 heeft nu een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Expert-oplossing (hierna ook 'EDR Expert' genoemd). *Kaspersky Endpoint Detection and Response Optimum* is een bereik van oplossingen die de IT-infrastructuur van het bedrijf beschermt tegen geavanceerde digitale dreigingen. De functionaliteit van de oplossingen combineert de automatische detectie van dreigingen met de respons op deze dreigingen om geavanceerde aanvallen te neutraliseren, zoals nieuwe exploits, ransomware, bestandsloze aanvallen en methoden met legitieme hulpprogramma's van het systeem. EDR Expert biedt meer bewaking van dreigingen en reactie-functionaliteit dan EDR Optimum. Voor details over de oplossingen, bekijk [Kaspersky Endpoint Detection and Response Optimum Help](#) en [Kaspersky Endpoint Detection and Response Expert Help](#).



Kaspersky Endpoint Detection and Response controleert en analyseert de ontwikkeling van dreigingen en geeft *beveiligingspersoneel* of *beheerders* informatie over de potentiële aanval die noodzakelijk is voor een tijdige reactie. Kaspersky Endpoint Detection and Response geeft detectiegegevens in een apart venster weer. *Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Detection and Response gebruikt de volgende tools voor informatie over dreigingen:

- De Kaspersky Security Network-cloudservice (hierna ook 'KSN' genoemd) die realtime toegang biedt tot informatie over de reputatie van bestanden, websites en software uit de Knowledge Base van Kaspersky. Het gebruik van gegevens uit Kaspersky Security Network zorgt niet alleen voor een snellere respons door Kaspersky-programma's bij dreigingen, maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. EDR Expert maakt gebruik van de Kaspersky Private Security Network (KPSN)-oplossing, die gegevens naar regionale servers stuurt zonder gegevens van apparaten naar het KSN te sturen.
- De integratie met de portal van de [Kaspersky Threat Intelligence Portal](#) dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- [Kaspersky Threats](#)-database.

## Integratie met Kaspersky Endpoint Detection and Response

Om te integreren met Kaspersky Endpoint Detection and Response, moet u het Endpoint Detection and Response Optimum (EDR Optimum)-onderdeel of het Endpoint Detection and Response Expert (EDR Expert)-onderdeel toevoegen en Kaspersky Endpoint Security configureren.

De onderdelen EDR Optimum en EDR Expert zijn niet compatibel.

Aan de volgende voorwaarden moet worden voldaan om Endpoint Detection and Response te laten werken:

- Kaspersky Security Center 13.2. In eerdere versies van Kaspersky Security Center is het onmogelijk om de Endpoint Detection and Response-functie te activeren.
- EDR Optimum kan worden beheerd in Kaspersky Security Center Web Console en Kaspersky Security Center Cloud Console. EDR Expert kan alleen worden beheerd met behulp van de Cloudconsole van Kaspersky Security Center. U kunt deze functionaliteit niet beheren met de Beheerconsole (MMC).
- Het programma is geactiveerd en de functionaliteit valt onder de licentie.
- Het onderdeel Endpoint Detection and Response is ingeschakeld.
- Programmaonderdelen waarvan Endpoint Detection and Response afhankelijk is, zijn ingeschakeld en operationeel. Endpoint Detection and Response is afhankelijk van de volgende onderdelen:
  - [File Threat Protection](#).
  - [Web Threat Protection](#).

- [Mail Threat Protection](#).
- [Exploit-preventie](#).
- [Gedragsdetectie](#).
- [Host Intrusion Prevention](#).
- [Remediation Engine](#).
- [Adaptieve controle op afwijkingen](#).

De integratie met Kaspersky Endpoint Detection and Response omvat de volgende stappen:

### 1 Endpoint Detection and Response-onderdelen installeren

U kunt het onderdeel EDR Optimum of EDR Expert selecteren tijdens de [installatie](#) of [upgrade](#) en kunt ook de taak [Programmaonderdelen wijzigen](#) gebruiken.

U moet uw computer opnieuw opstarten om de upgrade van het programma met de nieuwe componenten te voltooien.

### 2 Kaspersky Endpoint Detection and Response activeren

U kunt op de volgende manieren een licentie verkrijgen om Kaspersky Endpoint Detection and Response te gebruiken:

- Endpoint Detection and Response-functionaliteit is inbegrepen in de Kaspersky Endpoint Security for Windows-licentie.

De functie zal beschikbaar zijn onmiddellijk na de [activering van Kaspersky Endpoint Security voor Windows](#).

- Een afzonderlijke licentie kopen voor EDR Optimum of EDR Expert. (Kaspersky Endpoint Detection and Response add-on).

De functie is beschikbaar nadat u een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response hebt toegevoegd. Als resultaat worden er twee sleutels op de computer geïnstalleerd: een sleutel voor Kaspersky Endpoint Security en een sleutel voor Kaspersky Endpoint Detection and Response.

Licenties voor de zelfstandige Endpoint Detection and Response-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

Zorg ervoor dat de EDR Optimum of EDR Expert-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de [lokale interface van het programma](#).

### 3 Kaspersky Endpoint Detection and Response-onderdelen inschakelen

U kunt het onderdeel in- of uitschakelen in de beleidsinstellingen van Kaspersky Endpoint Security voor Windows.

[Het onderdeel Endpoint Detection and Response in- of uitschakelen in de webconsole en cloudconsole](#) 

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Endpoint Detection and Response**.
5. Zet de schakelaar **Endpoint Detection and Response** aan.
6. Sla uw wijzigingen op.

Het onderdeel Kaspersky Endpoint Detection and Response is ingeschakeld. Controleer de werkingsstatus van het onderdeel door het *statusrapport van de programmaonderdelen* te bekijken. U kunt de werkingsstatus van een onderdeel ook in [rapporten](#) bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Endpoint Detection and Response Optimum** of **Endpoint Detection and Response Expert** is toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

#### 4 Gegevensoverdracht naar Administration Server inschakelen

Om alle Endpoint Detection and Response-functies in te schakelen, moet gegevensoverdracht zijn ingeschakeld voor de volgende soorten gegevens:

- Gegevens over quarantainebestanden

De gegevens zijn nodig om via Webconsole en Cloud Console informatie te verkrijgen over bestanden die op een computer in quarantaine zijn geplaatst. U kunt bijvoorbeeld een bestand vanuit quarantaine downloaden voor analyse in Webconsole en Cloud Console.

- Gegevens van de bedreigingsontwikkelingsketen

De gegevens zijn nodig om via Webconsole en Cloud Console informatie te verkrijgen over bedreigingen die op een computer zijn gevonden. U kunt detectiedetails bekijken en maatregelen nemen in Webconsole en Cloud Console.

#### [Gegevensoverdracht naar de Administration Server inschakelen in Webconsole en Cloud Console](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Rapporten en Opslag**.
5. Controleer de volgende vakken in het blok **Data transfer to Administration Server**:
  - **About Quarantine files.**
  - **About a threat development chain.**
6. Sla uw wijzigingen op.

## Migratie van Kaspersky Endpoint Agent

Als u Kaspersky Endpoint Security 11.7.0 of nieuwer gebruikt met het onderdeel EDR Optimum (ingebouwde agent) geïnstalleerd, is de ondersteuning van integratie met Kaspersky Endpoint Detection and Response Optimum-oplossing direct beschikbaar na de installatie. Het EDR Optimum-onderdeel is niet compatibel met Kaspersky Endpoint Agent. Als Kaspersky Endpoint Agent op de computer is geïnstalleerd en Kaspersky Endpoint Security wordt bijgewerkt naar versie 11.7.0, dan blijft Kaspersky Endpoint Detection and Response Optimum werken met Kaspersky Endpoint Security. ([de \[KES+KEA\]-configuratie migreren naar \[KES+ingebouwde agent\]](#)). Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Om migratie van Kaspersky Endpoint naar Kaspersky Endpoint Security for Windows te voltooien, moet u beleid en taakinstellingen overdragen met de [Migratiewizard](#).

Als u Kaspersky Endpoint Security 11.4.0–11.6.0 gebruikt voor interoperabiliteit met Kaspersky Endpoint Detection and Response Optimum, bevat het programma ook Kaspersky Endpoint Agent. U kunt Kaspersky Endpoint Agent samen met Kaspersky Endpoint Security installeren.

In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiekpakket niet langer deel uit van de Kaspersky Endpoint Security-distributiek. U moet het Kaspersky Endpoint Agent-distributiekpakket afzonderlijk downloaden.

De Kaspersky Endpoint Detection and Response Expert-oplossing biedt geen ondersteuning voor interoperabiliteit met Kaspersky Endpoint Agent. De Kaspersky Endpoint Detection and Response Expert-oplossing maakt gebruik van Kaspersky Endpoint Security met ingebouwde agent (versie 11.8.0 en hoger).

Het EDR Optimum-onderdeel als onderdeel van Kaspersky Endpoint Security ondersteunt de interactie met de Kaspersky Endpoint Detection and Response Optimum 2.0-oplossing. De interactie met Kaspersky Endpoint Detection and Response Optimum versie 1.0 wordt niet ondersteund.

## Scannen op indicatoren van compromis (standaard taak).

Een *Indicator of Compromise (IOC)* is een set gegevens over een object of activiteit die wijst op onbevoegde toegang tot de computer (compromittering van gegevens). Vele mislukte aanmeldingen bij het systeem kunnen bijvoorbeeld een Indicator of Compromise zijn. Met de *IOC-scantaken* kunnen Indicators of Compromise op de computer worden gevonden en maatregelen als respons op deze dreiging worden genomen.

Kaspersky Endpoint Security zoekt Indicators of Compromise met behulp van *IOC-bestanden*. Dat zijn bestanden met de sets indicatoren die het programma zoekt om een detectie waar te nemen. IOC-bestanden moet voldoen aan de [OpenIOC-norm](#).

### Uitvoermodus van IOC-scantaak

Met Kaspersky Endpoint Detection and Response kunt u standaard IOC-scantaken creëren om gegevens te detecteren. De *standaard IOC-scantaak* is een groepstaak of lokale taak die handmatig is gemaakt en geconfigureerd in de Webconsole. De taken worden uitgevoerd met IOC-bestanden die door de gebruiker zijn voorbereid. Als u handmatig een indicator van een compromis wilt toevoegen, leest u de [vereisten voor IOC-bestanden](#).

Het bestand dat u kunt downloaden door op de onderstaande koppeling te klikken, bevat een tabel met de volledige lijst met IOC-voorwaarden van de OpenIOC-norm.

 [IOC TERMS.XLSX DOWNLOADEN](#)

Kaspersky Endpoint Security ondersteunt ook [alleenstaande IOC-scantaken](#) wanneer het programma gebruikt wordt als onderdeel van de oplossing [Kaspersky Sandbox](#).

## Zo maakt u een IOC-scantaak

U kunt *IOC Scantaken* handmatig maken:

- Details in waarschuwing (alleen voor EDR Optimum).

*Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

- Met de taakwizard.

U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

*Zo maakt u een IOC-scantaak:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

- a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

- b. Selecteer in de vervolgkeuzelijst **Task type** de optie **IOC Scan**.

- c. Typ in het veld **Task name** een korte omschrijving.

- d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Ga naar de volgende stap.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Ga naar de volgende stap.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

De systeemaccount (SYSTEM) heeft geen machtiging om de *IOC Scantaak* uit te voeren op netwerkstations. Als u de taak wilt starten voor een netwerkschijf, selecteert u het account van een gebruiker die toegang heeft tot die schijf.

Voor zelfstandige IOC-scantaken op netwerkstations moet u in de taakeigenschappen handmatig het gebruikersaccount selecteren dat toegang heeft tot dit station.

6. Verlaat de wizard verlaten.

U ziet een nieuwe taak in de lijst met taken.

7. Klik op de nieuwe taak.

U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Ga naar het gedeelte **IOC scan settings**.

10. Laad de IOC-bestanden om Indicators of Compromise te zoeken.

Nadat de IOC-bestanden zijn geladen, kunt u de lijst met indicatoren van de IOC-bestanden bekijken.

Het toevoegen of verwijderen van IOC-bestanden nadat de taak is uitgevoerd, wordt niet aanbevolen. Dit kan ertoe leiden dat de IOC-scanresultaten onjuist worden weergegeven voor eerdere uitvoeringen van de taak. Om indicatoren van compromis door nieuwe IOC-bestanden te zoeken, wordt aanbevolen om nieuwe taken toe te voegen.

11. Configureer acties bij de detectie van IOC's:

- **Isolate computer from the network.** Als deze optie is geselecteerd, isoleert Kaspersky Endpoint Security de computer van het netwerk zodat de dreiging zich niet kan verspreiden. U kunt in de [instellingen van het onderdeel Endpoint Detection and Response](#) de duur van de isolatie configureren.
- **Move copy to Quarantine, delete object.** Als deze optie is geselecteerd, verwijdert Kaspersky Endpoint Security het schadelijke object dat op de computer is gevonden. Voordat het object wordt verwijderd, maakt Kaspersky Endpoint Security een back-up voor het geval dat het object later moet worden teruggezet. Kaspersky Endpoint Security plaatst de back-up in Quarantaine.
- **Run scan of critical areas.** Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak [Kritieke Gebiedenscan](#). Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.

12. Ga naar het gedeelte **Advanced**.

13. Selecteer gegevenstypen (IOC-documenten) die als onderdeel van de taak moeten worden geanalyseerd.

Kaspersky Endpoint Security selecteert automatisch gegevenstypen (IOC-documenten) voor de *IOC-scantaak* overeenkomstig de inhoud van geladen IOC-bestanden. Gegevenstypen deselecteren wordt niet aanbevolen.

U kunt aanvullende scanbereiken voor de volgende gegevenstypen configureren:

- **Files - FileItem.** Stel een IOC-scanbereik op de computer in met vooraf ingestelde bereiken.

Kaspersky Endpoint Security scant standaard alleen op IOC's in belangrijke delen van de computer, zoals de map Downloads, het bureaublad, de map met tijdelijke besturingssysteembestanden, enz. U kunt het scanbereik ook handmatig toevoegen.

- **Windows event logs - EventLogItem.** Voer de periode in wanneer de gebeurtenissen zijn geregistreerd. U kunt ook selecteren welke Windows-gebeurtenislogboeken moeten worden gebruikt voor IOC-scannen. Standaard worden de volgende gebeurtenislogboeken geselecteerd: programmagebeurtenislogboek, systeemgebeurtenislogboek en beveiligingsgebeurtenislogboek.

Voor het gegevenstype **Windows registry - RegistryItem** scant Kaspersky Endpoint Security [een reeks registersleutels](#).

14. Selecteer het tabblad **Schema** in het venster met taakeigenschappen.

15. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

16. Sla uw wijzigingen op.

17. Schakel het selectievakje naast de taak in.

18. Klik op de knop **Run**.

Kaspersky Endpoint Security begint nu te zoeken naar Indicators of Compromise op de computer. U kunt de resultaten van de taak bekijken in de taakeigenschappen in het gedeelte **Results**. U kunt informatie over gedetecteerde Indicators of Compromise bekijken in de taakeigenschappen: **Programma-instellingen** → **IOC Scan Results**.

De resultaten van een IOC-scan worden 30 dagen bewaard. Na die tijd worden de oudste gegevens automatisch verwijderd door Kaspersky Endpoint Security.

## Bestand in Quarantaine plaatsen

Als reactie op een dreiging kunnen Kaspersky Endpoint Detection and Response Optimum *Plaats bestand in Quarantaine*-taken maken. Dit is nodig om de gevolgen van de dreiging te minimaliseren. *Quarantaine* is een speciale lokale opslagplaats op de computer. De gebruiker kan bestanden die de gebruiker gevaarlijk acht voor de computer in quarantaine plaatsen. Bestanden in quarantaine worden in een geëncrypte staat bewaard en vormen geen bedreiging voor de beveiliging van de computer. Kaspersky Endpoint Security gebruikt Quarantaine alleen met de oplossingen Kaspersky Sandbox en Kaspersky Endpoint Detection and Response. In alle andere gevallen plaatst Kaspersky Endpoint Security het relevante bestand in [Back-up](#). Voor meer informatie over het beheer van Quarantaine als onderdeel van de oplossingen raadpleegt u de [Kaspersky Sandbox Help](#), [Kaspersky Endpoint Detection and Response Optimum Help](#), en [Kaspersky Endpoint Detection and Response Expert Help](#).

U kunt op de volgende manieren *Plaats bestand in Quarantaine*-taken maken:

- Details in waarschuwing (alleen voor EDR Optimum).

*Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

- Met de taakwizard.

U moet het bestandspad of de hash (SHA256 of MD5) invoeren, of zowel het bestandspad als de bestandshash.

De taak *Plaats bestand in Quarantaine* heeft de volgende beperkingen:

1. Het bestand mag niet groter zijn dan 100 MB.
2. Essentiële systeemobjecten (SCO) kunnen niet in quarantaine worden gezet. SCO's zijn bestanden die het besturingssysteem en Kaspersky Endpoint Security voor Windows nodig hebben om te kunnen werken.
3. U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

*Zo maakt u een Plaats bestand in Quarantaine-taak:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de knop **Add**.  
De wizard Taak wordt gestart.
3. Configureer de taakinstellingen:
  - a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.
  - b. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Plaats bestand in Quarantaine**.
  - c. Typ in het veld **Task name** een korte omschrijving.
  - d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.
4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Klik op de knop **Next**.
5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op de knop **Next**.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Voltooi de wizard door op de knop **Finish** te klikken.  
U ziet een nieuwe taak in de lijst met taken.
7. Klik op de nieuwe taak.  
U ziet nu het venster met de taakeigenschappen.
8. Selecteer het tabblad **Application settings**.



9. Klik in de lijst met bestanden op **Toevoegen**.

De wizard voor het toevoegen van bestanden wordt gestart.

10. Om het bestand toe te voegen, moet u het volledige pad naar het bestand of zowel de bestandshash als het pad invoeren.

Als het bestand zich op een netwerkstation bevindt, voert u het bestandspad in dat begint met `\\` en niet de letter van het station. Bijvoorbeeld `\\server\shared_folder\file.exe`. Als de padnaam een letter van een netwerkschijf bevat, verschijnt mogelijk de foutmelding *Bestand niet gevonden*.

11. Selecteer het tabblad **Schema** in het venster met taakeigenschappen.

12. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

13. Klik op de knop **Save**.

14. Schakel het selectievakje naast de taak in.

15. Klik op de knop **Run**.

Kaspersky Endpoint Security verplaatst nu het bestand naar Quarantaine. Als het bestand is vergrendeld vanwege een ander proces, wordt de taak weergegeven als *Voltooid*. Het bestand wordt echter pas in quarantaine geplaatst nadat de computer opnieuw is opgestart. Controleer na het opnieuw opstarten van de computer of het bestand is verwijderd.

De taak *Plaats bestand in Quarantaine* wordt mogelijk afgebroken na de foutmelding *Toegang geweigerd* wanneer u probeert een bestand in quarantaine te plaatsen dat momenteel wordt uitgevoerd. [Maak een Proces beëindigd-taak](#) voor het bestand en probeer het opnieuw.

De taak *Plaats bestand in Quarantaine* wordt mogelijk afgebroken na de foutmelding *Onvoldoende ruimte in Quarantaine-opslag* wanneer u probeert een bestand in quarantaine te plaatsen dat te groot is. Maak de Quarantaine leeg of [maak de Quarantaine groter](#). Probeer het daarna opnieuw.

U kunt een bestand terugzetten vanuit Quarantaine of de Quarantaine leegmaken met Webconsole. U kunt bestanden lokaal op de computer terugzetten met de [opdrachtregel](#).

## Bestand ophalen

U kunt bestanden van computers van gebruikers ophalen. U kunt bijvoorbeeld een taak configureren voor het ophalen van een gebeurtenislogboek dat door een programma van derden is gemaakt. Om het bestand op te halen, moet u een speciale taak maken. Na het uitvoeren van de taak wordt het bestand opgeslagen in Quarantaine. Met Webconsole kunt u dit bestand vanuit Quarantaine downloaden naar uw computer. Het bestand blijft beschikbaar in de oorspronkelijke map van de computer van de gebruiker.

Het bestand mag niet groter zijn dan 100 MB.

U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

Zo maakt u een *Bestand ophalen*-taak:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Get file**.

c. Typ in het veld **Task name** een korte omschrijving.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Klik op de knop **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op de knop **Next**.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Voltooi de wizard door op de knop **Finish** te klikken.

U ziet een nieuwe taak in de lijst met taken.

7. Klik op de nieuwe taak.

U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Klik in de lijst met bestanden op **Toevoegen**.

De wizard voor het toevoegen van bestanden wordt gestart.

10. Om het bestand toe te voegen, moet u het volledige pad naar het bestand of zowel de bestandshash als het pad invoeren.

Als het bestand zich op een netwerkstation bevindt, voert u het bestandspad in dat begint met `\\` en niet de letter van het station. Bijvoorbeeld `\\server\shared_folder\file.exe`. Als de padnaam een letter van een netwerkschijf bevat, verschijnt mogelijk de foutmelding *Bestand niet gevonden*.

11. Selecteer het tabblad **Schema** in het venster met taakeigenschappen.

12. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

13. Klik op de knop **Save**.

14. Schakel het selectievakje naast de taak in.

15. Klik op de knop **Run**.

Kaspersky Endpoint Security maakt een kopie van het bestand en verplaatst deze kopie naar Quarantaine. Met Webconsole kunt u het bestand vanuit Quarantaine downloaden naar uw computer.

## Bestand verwijderen

Met de taak *Bestand verwijderen* kunt u op afstand bestanden verwijderen, bijvoorbeeld wanneer er sprake is van een dreiging.

De taak *Bestand wissen* heeft de volgende beperkingen:

- Essentiële systeemobjecten (System Critical Objects SCO) kunnen niet worden verwijderd. SCO's zijn bestanden die het besturingssysteem en Kaspersky Endpoint Security voor Windows nodig hebben om te kunnen werken.
- U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

Zo maakt u een *Bestand verwijderen*-taak:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Taaktype** de optie **Bestand verwijderen**.

c. Typ in het veld **Task name** een korte omschrijving.

d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Klik op de knop **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op de knop **Next**.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Voltooi de wizard door op de knop **Finish** te klikken.

U ziet een nieuwe taak in de lijst met taken.

7. Klik op de nieuwe taak.

U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Klik in de lijst met bestanden op **Toevoegen**.

De wizard voor het toevoegen van bestanden wordt gestart.

10. Om het bestand toe te voegen, moet u het volledige pad naar het bestand of zowel de bestandshash als het pad invoeren.

Als het bestand zich op een netwerkstation bevindt, voert u het bestandspad in dat begint met `\\` en niet de letter van het station. Bijvoorbeeld `\\server\shared_folder\file.exe`. Als de padnaam een letter van een netwerkschijf bevat, verschijnt mogelijk de foutmelding *Bestand niet gevonden*.

11. Selecteer het tabblad **Schema** in het venster met taakeigenschappen.

12. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

13. Klik op de knop **Save**.

14. Schakel het selectievakje naast de taak in.

15. Klik op de knop **Run**.

Kaspersky Endpoint Security verwijdert nu het bestand van de computer. Als het bestand is vergrendeld vanwege een ander proces, wordt de taak weergegeven als *Voltooid*. Het bestand wordt echter pas verwijderd nadat de computer opnieuw is opgestart. Controleer na het opnieuw opstarten van de computer of het bestand is verwijderd.

De taak *Bestand verwijderen* wordt mogelijk afgebroken na de foutmelding *Toegang geweigerd* wanneer u probeert een uitvoerbaar bestand te verwijderen dat momenteel wordt uitgevoerd. [Maak een Proces beëindigd-taak](#) voor het bestand en probeer het opnieuw.

## Proces starten

Met de taak *Proces starten* kunt u op afstand bestanden uitvoeren. U kunt bijvoorbeeld op afstand een hulpprogramma uitvoeren voor het maken van het configuratiebestand van de computer. Met de taak [Bestand ophalen](#) kunt u het gemaakte bestand ontvangen in de Webconsole van Kaspersky Security Center.

U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

Zo maakt u een *Proces starten*-taak:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.  
De lijst met taken wordt geopend.
2. Klik op de knop **Add**.  
De wizard Taak wordt gestart.
3. Configureer de taakinstellingen:
  - a. Selecteer in de vervolgkeuzelijst **Application Kaspersky Endpoint Security voor Windows (11.9.0)**.
  - b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Process start**.
  - c. Typ in het veld **Task name** een korte omschrijving.
  - d. Selecteer in het gedeelte **Selecteer apparaten waarvoor de taak wordt toegewezen** het bereik van de taak.
4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Klik op de knop **Next**.
5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op de knop **Next**.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Voltooi de wizard door op de knop **Finish** te klikken.  
U ziet een nieuwe taak in de lijst met taken.
7. Klik op de nieuwe taak.
8. U ziet nu het venster met de taakeigenschappen.
9. Selecteer het tabblad **Application settings**.
10. Voer de opdracht in voor het starten van een proces.  
Als u bijvoorbeeld een hulpprogramma wilt uitvoeren (*utility.exe*) waarmee de configuratie van een computer wordt opgeslagen in een bestand met de naam *conf.txt*, moet u de volgende waarden invoeren:
  - **Executable command** – *utility.exe*
  - **Command-line arguments** – */R conf.txt*
  - **Path to the working folder** – *C:\Users\admin\Diagnostic\*

Een andere optie is om in het veld **Executable command** het pad *C:\Users\admin\Diagnostic\utility.exe /R conf.txt* in te voeren. U kunt de overige instellingen dan achterwege laten.

11. Selecteer het tabblad **Schema** in het venster met taakeigenschappen.

12. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

13. Klik op de knop **Save**.

14. Schakel het selectievakje naast de taak in.

15. Klik op de knop **Run**.

Kaspersky Endpoint Security voert de opdracht nu in stille modus uit en start het proces. U kunt de resultaten van de taak bekijken in de taakeigenschappen in het gedeelte **Results**.

## Proces beëindigen

Met de taak *Proces beëindigd* kunt u op afstand processen beëindigen. U kunt bijvoorbeeld op afstand een hulpprogramma voor het testen van de snelheid van internet beëindigen met de [taak \*Proces starten\*](#).

Configureer het onderdeel [Preventie van uitvoering](#) als u het uitvoeren van een bestand wilt verhinderen. U kunt het uitvoeren van uitvoerbare bestanden, scripts en bestanden met een Office-indeling verhinderen.

De taak *Proces beëindigen* heeft de volgende beperkingen:

- Processen van essentieel systeemobjecten (System Critical Objects SCO) kunnen niet worden gestopt. SCO's zijn bestanden die het besturingssysteem en Kaspersky Endpoint Security voor Windows nodig hebben om te kunnen werken.
- U kunt de taak configureren voor EDR Optimum in Webconsole en Cloud Console. Taakinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

*Zo maakt u een *Proces beëindigd*-taak:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de knop **Add**.

De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows (11.9.0)**.

b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Process termination**.

c. Typ in het veld **Task name** een korte omschrijving.

d. Selecteer in het gedeelte **Select devices to which the task will be assigned** het bereik van de taak.

4. Selecteer apparaten naargelang de geselecteerde optie voor het bereik van de taak. Klik op de knop **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op de knop **Next**.

Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Voltooi de wizard door op de knop **Finish** te klikken.

U ziet een nieuwe taak in de lijst met taken.

7. Klik op de nieuwe taak.

U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Als u het proces wilt voltooien, moet u het bestand selecteren dat u wilt beëindigen. U kunt op een van de volgende manieren een bestand selecteren:

- Voer de volledige naam van het bestand in.
- Voer de hash van het bestand en het pad naar het bestand in.
- Voer de PID van het proces in (alleen voor lokale taken).

Als het bestand zich op een netwerkstation bevindt, voert u het bestandspad in dat begint met `\\` en niet de letter van het station. Bijvoorbeeld `\\server\shared_folder\file.exe`. Als de padnaam een letter van een netwerkschijf bevat, verschijnt mogelijk de foutmelding *Bestand niet gevonden*.

10. Selecteer het tabblad **Schedule** in het venster met taakeigenschappen.

11. Configureer het taakschema.

Wake-on-LAN is niet beschikbaar voor deze taak. Zorg ervoor dat de computer is ingeschakeld om de taak uit te voeren.

12. Klik op de knop **Save**.

13. Schakel het selectievakje naast de taak in.

14. Klik op de knop **Run**.

Kaspersky Endpoint Security beëindigt nu het proces op de computer. Als u bijvoorbeeld tijdens de uitvoering van een 'GAME'-programma het `game.exe`-proces beëindigt, wordt het programma afgesloten zonder dat gegevens worden opgeslagen. U kunt de resultaten van de taak bekijken in de taakeigenschappen in het gedeelte **Results**.

## Preventie van uitvoering

Preventie van uitvoering maakt het mogelijk om de uitvoering van uitvoerbare bestanden en scripts te beheren, evenals het openen van bestanden in Office-indeling. Op deze manier kunt u bijvoorbeeld voorkomen dat programma's worden uitgevoerd die u als onveilig beschouwt. Hierdoor kan de verspreiding van de dreiging worden gestopt. Preventie van uitvoering ondersteunt [een reeks office-bestandsextensies](#) en [een reeks scriptinterpreters](#).

## Regel preventie van uitvoering

Preventie van uitvoering beheert gebruikerstoegang tot bestanden met regels voor preventie van uitvoering. *Regels voor preventie van uitvoering* is een set criteria waarmee het programma rekening houdt bij het reageren op een objectuitvoering, bijvoorbeeld bij het blokkeren van objectuitvoering. Het programma identificeert bestanden aan de hand van hun paden of checksums berekend met behulp van MD5- en SHA256-hash-algoritmen.

U kunt regels instellen voor preventie van uitvoering:

- Details in waarschuwing (alleen voor EDR Optimum).

*Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

- Een groepsbeleid of lokale programma-instellingen gebruiken.

U moet het bestandspad of de hash (SHA256 of MD5) invoeren, of zowel het bestandspad als de bestandshash.

U kunt preventie van uitvoering ook lokaal beheren met behulp van de [opdrachtregel](#).

Het is niet aanbevolen om meer dan 5000 regels voor runpreventie te maken, omdat dit systeeminstabiliteit kan veroorzaken.

Preventieregels zijn niet van toepassing op bestanden op cd's of in ISO-images. Het programma blokkeert het uitvoeren of openen van deze bestanden niet.

## Regelmodi voor preventie van uitvoering

Het component voor preventie van uitvoering kan werken in twee modi:

- **Statistics only.**

In deze modus publiceert Kaspersky Endpoint Security een gebeurtenis over pogingen om uitvoerbare objecten uit te voeren of documenten te openen die voldoen aan de criteria van de regel voor preventie voor het Windows-gebeurtenislogboek en Kaspersky Security Center, maar blokkeert niet de poging om het object of document uit te voeren of te openen. Deze modus is standaard geselecteerd.

- **Actief.**

In deze modus blokkeert het programma de uitvoering van objecten of het openen van documenten die voldoen aan de criteria van regels voor preventie van uitvoering. Het programma publiceert ook een gebeurtenis over pogingen om objecten uit te voeren of documenten te openen naar het Windows-gebeurtenislogboek en het Kaspersky Security Center-gebeurtenislogboek.

## Preventie van uitvoering beheren



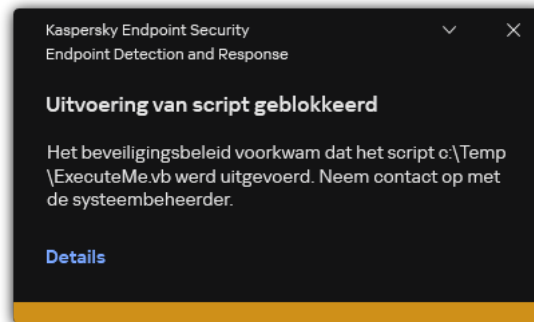
U kunt de instellingen van het onderdeel alleen configureren in de webconsole.

Om preventie van uitvoering in te schakelen:

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Endpoint Detection and Response**.
5. Gebruik de schakelaar **Execution prevention** om het onderdeel in of uit te schakelen.
6. Selecteer in het blok **Action on execution or opening of forbidden object** de uitvoermodus voor het onderdeel:
  - **Block and write to report.** In deze modus blokkeert het programma de uitvoering van objecten of het openen van documenten die voldoen aan de criteria van regels voor preventie van uitvoering. Het programma publiceert ook een gebeurtenis over pogingen om objecten uit te voeren of documenten te openen naar het Windows-gebeurtenislogboek en het Kaspersky Security Center-gebeurtenislogboek.
  - **Log events only.** In deze modus publiceert Kaspersky Endpoint Security een gebeurtenis over pogingen om uitvoerbare objecten uit te voeren of documenten te openen die voldoen aan de criteria van de regel voor preventie voor het Windows-gebeurtenislogboek en Kaspersky Security Center, maar blokkeert niet de poging om het object of document uit te voeren of te openen. Deze modus is standaard geselecteerd.
7. Maak een lijst met regels voor de preventie van uitvoering:
  - a. Klik op de knop **Add**.
  - b. Dit opent een venster. Voer in dit venster de naam van de regels voor preventie van uitvoering in (bijvoorbeeld *Programma A*).
  - c. In de vervolgkeuzelijst **Type** selecteert u het object dat u wil blokkeren: **Executable file, Script, Microsoft Office document**.  
Als u een verkeerd objecttype selecteert, blokkeert Kaspersky Endpoint Security het bestand of script niet.
  - d. Om het bestand toe te voegen, moet u de hash van het bestand (SHA256 of MD5), het volledige pad naar het bestand of zowel de hash als het pad invoeren.

Als het bestand zich op een netwerkstation bevindt, voert u het bestandspad in dat begint met `\\` en niet de letter van het station. Bijvoorbeeld `\\server\shared_folder\file.exe`. Als het bestandspad een netwerkstationletter bevat, blokkeert Kaspersky Endpoint Security het bestand of de script niet.
  - e. Klik op **OK**.
8. Sla uw wijzigingen op.

Als gevolg hiervan blokkeert Kaspersky Endpoint Security de uitvoering van objecten: het uitvoeren van uitvoerbare bestanden en scripts en het openen van bestanden in Office-indeling. U kunt echter bijvoorbeeld een scriptbestand in een teksteditor openen, zelfs als het uitvoeren van het script is verhinderd. Bij het blokkeren van de uitvoering van een object geeft Kaspersky Endpoint Security een standaardmelding weer (zie onderstaande afbeelding) als meldingen [ingeschakeld zijn in de programma-instellingen](#).



Melding preventie van uitvoering

## Computer isoleren van netwerk

Isolatie van computernetwerken maakt het automatisch isoleren van een computer van het netwerk mogelijk als reactie op de detectie van een indicator van compromis (IOC). – dit is de *automatische modus*. U kunt netwerkisolatie handmatig inschakelen terwijl je de gedetecteerde bedreiging onderzoekt. – dit is de *handmatige modus*.

Wanneer netwerkisolatie is ingeschakeld, verbreekt de applicatie alle actieve verbindingen en blokkeert alle nieuwe TCP/IP-netwerkverbindingen op de computer, uitgezonderd de volgende aansluitingen:

- Verbindingen die worden vermeld in uitzonderingen voor netwerkisolatie.
- Verbindingen gestart door Kaspersky Endpoint Security-services.
- Verbindingen gestart door de Kaspersky Security Center Netwerkagent.

U kunt de instellingen van het onderdeel alleen configureren in de webconsole.

### Automatische netwerkisolatie modus

U kunt netwerkisolatie zo configureren dat deze automatisch wordt ingeschakeld als reactie op een IOC-detectie. U kunt de automatische netwerkisolatie modus instellen met een groepsbeleid.

[Netwerkisolatie configureren zodat deze automatisch wordt ingeschakeld als reactie op een IOC-detectie.](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Klik op de taak **IOC Scan** van Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

Maak indien nodig de [IOC-scan](#)-taak aan.

3. Selecteer het tabblad **Application settings**.

4. Schakel in het blok **Action on IOC detection** de selectievakjes **Take response actions after an IOC is found** en **Isolate computer from the network** in.

5. Sla uw wijzigingen op.

Wanneer hierdoor een IOC wordt gedetecteerd, isoleert het programma de computer van het netwerk om te voorkomen dat de dreiging zich verspreidt.

U kunt netwerkisolatie zo configureren dat het automatisch wordt uitgeschakeld nadat een bepaalde tijd is verstreken. Standaard schakelt de toepassing netwerkisolatie uit nadat er 8 uur zijn verstreken vanaf het moment dat het werd ingeschakeld. U kunt netwerkisolatie ook handmatig uitschakelen (zie onderstaande instructies). Nadat netwerkisolatie is uitgeschakeld, kan de computer het netwerk zonder beperkingen gebruiken.

### [De vertraging configureren voor het uitschakelen van netwerkisolatie van een computer in automatische modus](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Policies & profiles**.

2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar **Detection and Response** → **Endpoint Detection and Response**.

5. Klik in het blok **Network isolation Configure computer unlock settings**.

6. Dit opent een venster: selecteer in dit venster het vakje **Automatically unlock isolated computer in N hours** en voer de vertraging in voor het automatisch uitschakelen van netwerkisolatie.

7. Sla uw wijzigingen op.

## Handmatige netwerkisolatie modus

U kunt netwerkisolatie handmatig in- en uitschakelen. U kunt de handmatige netwerkisolatie modus instellen met de computereigenschappen in de Kaspersky Security Center console.

U kunt netwerkisolatie inschakelen:

- Details in waarschuwing (alleen voor EDR Optimum).

*Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

- Met behulp van lokale programma-instellingen

### [Netwerkisolatie van een computer handmatig inschakelen](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Applications**.
4. Klik op **Kaspersky Endpoint Security for Windows**.  
U ziet nu de lokale programma-instellingen.
5. Selecteer het tabblad **Application settings**.
6. Ga naar **Detection and Response** → **Endpoint Detection and Response**.
7. Klik in het blok **Network isolation** **Isolate computer from the network**.

U kunt netwerkisolatie zo configureren dat het automatisch wordt uitgeschakeld nadat een bepaalde tijd is verstreken. Standaard schakelt de toepassing netwerkisolatie uit nadat er 8 uur zijn verstreken vanaf het moment dat het werd ingeschakeld. Nadat netwerkisolatie is uitgeschakeld, kan de computer het netwerk zonder beperkingen gebruiken.

### [De vertraging configureren voor het uitschakelen van netwerkisolatie van een computer in handmatige modus](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Tasks**.  
Dit toont de beschikbare taken op de computer.
4. Selecteer de taak **Network isolation**.
5. Selecteer het tabblad **Application settings**.
6. Dit opent een venster; kies in dit venster de vertraging voor het uitschakelen van netwerkisolatie.
7. Sla uw wijzigingen op.

### [Netwerkisolatie van een computer handmatig uitschakelen](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Applications**.
4. Klik op **Kaspersky Endpoint Security for Windows**.  
U ziet nu de lokale programma-instellingen.
5. Selecteer het tabblad **Application settings**.
6. Ga naar **Detection and Response** → **Endpoint Detection and Response**.
7. Klik in het blok **Network isolation Unblock computer isolated from the network**.

U kunt netwerkisolatie ook lokaal uitschakelen met de [opdrachtregel](#).

## Uitzonderingen netwerkisolatie

U kunt uitzonderingen netwerkisolatie configureren. Netwerkverbindingen die overeenkomen met de regels, worden niet geblokkeerd op de computer wanneer netwerkisolatie is ingeschakeld.

Om uitzonderingen van netwerkisolatie te configureren, kunt u een lijst gebruiken van *standaard netwerkprofielen*. Standaard omvatten uitzonderingen netwerkprofielen die regels bevatten die zorgen voor een ononderbroken werking van apparaten met de DNS/DHCP-server en DNS/DHCP-clientrollen. U kunt ook de instellingen van standaard netwerkprofielen wijzigen of uitzonderingen handmatig definiëren (zie onderstaande instructies).

Uitzonderingen die zijn opgegeven in beleidseigenschappen worden alleen toegepast als netwerkisolatie automatisch wordt ingeschakeld als reactie op een gedetecteerde dreiging. Uitzonderingen opgegeven in computereigenschappen worden alleen toegepast als netwerkisolatie handmatig is ingeschakeld in computereigenschappen in de Kaspersky Security Center-console of in alarmdetails.

Een actief beleid verhindert niet de toepassing van uitzonderingen van netwerkisolatie geconfigureerd in computereigenschappen, omdat deze parameters verschillende gebruiksscenario's hebben.

### [Uitzondering netwerkisolatie toevoegen in automatische modus](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Policies & profiles**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Endpoint Detection and Response**.
5. Klik in het blok **Network isolation exclusions Exclusions**.
6. Dit opent een venster. Klik in dit venster op **Add from profile** en selecteer standaard netwerkprofielen voor het configureren van uitzonderingen.  
Uitzonderingen voor netwerkisolatie van het profiel worden toegevoegd aan de lijst met uitzonderingen voor netwerkisolatie. U kunt de eigenschappen van netwerkverbindingen bekijken. Indien nodig kunt u de netwerkverbindinginstellingen wijzigen.
7. Voeg indien nodig handmatig een uitzondering voor netwerkisolatie toe. Klik hiervoor in het venster met de lijst met uitzonderingen op **Add** en bewerk de instellingen van netwerkverbindingen handmatig.
8. Sla uw wijzigingen op.

#### [Uitzondering netwerkisolatie toevoegen in handmatige modus](#)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Managed devices**.
2. Selecteer de computer waarvoor u lokale programma-instellingen wilt configureren.  
U ziet nu de computereigenschappen.
3. Selecteer het tabblad **Tasks**.  
Dit toont de beschikbare taken op de computer.
4. Selecteer de taak **Network isolation**.
5. Selecteer het tabblad **Application settings**.
6. Dit opent een venster; klik in dit venster op **Exclusions**.
7. Dit opent een venster. Klik in dit venster op **Add from profile** en selecteer standaard netwerkprofielen voor het configureren van uitzonderingen.  
Uitzonderingen voor netwerkisolatie van het profiel worden toegevoegd aan de lijst met uitzonderingen voor netwerkisolatie. U kunt de eigenschappen van netwerkverbindingen bekijken. Indien nodig kunt u de netwerkverbindinginstellingen wijzigen.
8. Voeg indien nodig handmatig een uitzondering voor netwerkisolatie toe. Klik hiervoor in het venster met de lijst met uitzonderingen op **Add** en bewerk de instellingen van netwerkverbindingen handmatig.
9. Sla uw wijzigingen op.

U kunt de lijst met uitzonderingen voor netwerkisolatie ook lokaal bekijken met de [opdrachtregel](#). In dit geval moet de computer geïsoleerd zijn.

## Appendix 1. Ondersteunde bestandsextensies voor Preventie van uitvoering

Kaspersky Endpoint Security ondersteunt de preventie van het openen van bestanden met een Office-indeling in bepaalde programma's. Informatie over ondersteunde bestandsextensies en programma's vindt u in de onderstaande tabel.

Ondersteunde bestandsextensies voor Preventie van uitvoering

| Programmanaam        | Uitvoerbaar bestand | Bestandsextensie   |
|----------------------|---------------------|--|
| Microsoft Word       | winword.exe         | rtf<br>doc<br>dot<br>docm<br>docx<br>dotx<br>dotm<br>docb                              |
| WordPad              | wordpad.exe         | docx<br>rtf  |
| Microsoft Excel      | excel.exe           | xls<br>xlt<br>xlm<br>xlsx<br>xlsm<br>xltx<br>xltn<br>xlsb<br>xla<br>xlam<br>xll<br>xlw |
| Microsoft PowerPoint | powerpnt.exe        | ppt<br>pot<br>pps<br>pptx<br>pptm<br>potx<br>potm<br>ppam<br>ppsx<br>ppsm              |

|                  |                   |              |
|------------------|-------------------|--------------|
|                  |                   | sldx<br>sldm |
| Adobe Acrobat    | acrord32.exe      | pdf          |
| Foxit PDF Reader | FoxitReader.exe   |              |
| STDU Viewer      | STDUViewerApp.exe |              |
| Microsoft Edge   | MicrosoftEdge.exe |              |
| Google Chrome    | chrome.exe        |              |
| Mozilla Firefox  | firefox.exe       |              |
| Yandex Browser   | browser.exe       |              |
| Tor Browser      | tor.exe           |              |

## Appendix 2. Ondersteunde script interpreters

De volgende script interpreters worden ondersteund door Preventie van uitvoering:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msixexec.exe
- perl.exe



- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacyelevated.exe
- wscript.exe
- wwaahost.exe

Preventie van uitvoering ondersteunt het werken met Java-applicaties in de Java Runtime-omgeving (java.exe en javaw.exe-processen).

## Appendix 3. IOC-scanbereik in het register (RegistryItem)

Wanneer u het gegevenstype RegistryItem toevoegt aan het IOC-scanbereik, scant Kaspersky Endpoint Security de volgende registersleutels:

HKEY\_CLASSES\_ROOT\htafile

HKEY\_CLASSES\_ROOT\batfile

HKEY\_CLASSES\_ROOT\exefile

HKEY\_CLASSES\_ROOT\comfile

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Class

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

HKEY\_LOCAL\_MACHINE\Software\Classes\piffile

HKEY\_LOCAL\_MACHINE\Software\Classes\htafile

HKEY\_LOCAL\_MACHINE\Software\Classes\exefile

HKEY\_LOCAL\_MACHINE\Software\Classes\comfile

HKEY\_LOCAL\_MACHINE\Software\Classes\CLSID

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebg

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

## Appendix 4. IOC-bestandsvereisten

Houd bij het maken van IOC-scantaken rekening met de volgende IOC-bestandsvereisten en -beperkingen:

- Het programma ondersteunt IOC-bestanden met de IOC- en XML-extensies in de open standaard OpenIOC versies 1.0 en 1.1 voor het beschrijven van indicatoren van compromis.
- Als u tijdens het maken van een [IOC Scan-taak](#) IOC-bestanden uploadt, waarvan sommige niet worden ondersteund, gebruikt het programma tijdens het uitvoeren van de taak alleen de ondersteunde IOC-bestanden. Als bij het maken van een *IOC-scantask* op de opdrachtregel blijkt dat alle IOC-bestanden die u uploadt niet worden ondersteund, kan de taak nog steeds worden uitgevoerd, maar worden er geen compromisindicatoren gedetecteerd. Het is niet mogelijk om niet-ondersteunde IOC-bestanden te uploaden met behulp van Webconsole of Cloud Console.
- Semantische fouten en niet-ondersteunde IOC-termen en -tags in IOC-bestanden zorgen er niet voor dat de taakuitvoering mislukt. In dergelijke secties van IOC-bestanden detecteert het programma geen overeenkomst.
- [De ID's van alle IOC files](#) gebruikt in een enkele IOC-scantask moeten uniek zijn. Als er IOC-bestanden zijn met dezelfde ID, kan dit van invloed zijn op de resultaten van de taakuitvoering.

- Een enkel IOC-bestand mag niet groter zijn dan 2 MB. Grotere bestanden beëindigen IOC-scantaken met een fout. De totale grootte van alle bestanden die worden toegevoegd aan de IOC collectie mag niet groter zijn dan 10 MB. Als de totale grootte van alle bestanden groter is dan 10 MB, moet u de collectie IOC's opsplitsen en meerdere *IOC Scan*-taken maken.
- Het wordt aanbevolen om één IOC-bestand per bedreiging te maken. Dit maakt het gemakkelijker om de resultaten van de IOC Scan-taak te analyseren.

Het bestand dat u kunt downloaden door op de onderstaande koppeling te klikken, bevat een tabel met de volledige lijst met IOC-voorwaarden van de OpenIOC-norm.

 [IOC TERMS.XLSX DOWNLOADEN](#)

Functies en beperkingen van de programma-ondersteuning voor de OpenIOC-standaard worden weergegeven in de volgende tabel.

Functies en beperkingen van de ondersteuning voor OpenIOC versie 1.0 en 1.1.

|  |  |
|--|--|
| Ondersteunde condities                       | <p>OpenIOC 1.0:</p> <p>is<br/>isnot (als uitzondering van de set)<br/>contains<br/>containsnot (als uitzondering van de set)</p> <p>OpenIOC 1.1:</p> <p>is<br/>contains<br/>starts-with<br/>ends-with<br/>matches<br/>greater-than<br/>less-than</p>   |
| Ondersteunde conditie-attributen             | <p>OpenIOC 1.1:</p> <p>preserve-case<br/>negate</p>  |
| Ondersteunde operators                       | <p>AND<br/>OR</p>  |
| Ondersteunde gegevenstypes                   | <p>"date": datum (toepasselijke condities: is, greater-than, less-than)</p> <p>"int": integer (toepasselijke condities: is, greater-than, less-than)</p> <p>"string": string (toepasselijke condities: is, contains, matches, starts-with, ends-with)</p> <p>"duration": duur in seconden (toepasselijke condities: is, greater-than, less-than)</p> |
| Kenmerken van interpretatie van gegevenstype | <p>De gegevenstypes "boolean string", "restricted string", "md5", "IP", "sha256" en "base64Binary" worden geïnterpreteerd als string.</p> <p>Het programma ondersteunt de interpretatie van de instelling Content voor de gegevenstypes int en date wanneer het is ingesteld in de vorm van intervallen:</p>   |

OpenIOC 1.0:  
Met de operator TO in het veld Content:  
<Content type="int">49600 TO 50700</Content>  
<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>  
<Content type="int">[154192 TO 154192]</Content>  
OpenIOC 1.1:  
Met de condities greater-than en less-than  
Met de operator TO in het veld Content  
Het programma ondersteunt interpretatie van de gegevenstypes date en duration als de indicators ingesteld zijn in het formaat ISO 8601, Zulu Time Zone, UTC.

## Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 heeft nu een ingebouwde agent voor integratie met de Kaspersky Sandbox-oplossing. *De Kaspersky Sandbox-oplossing* detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Kaspersky Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Kaspersky Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Kaspersky Sandbox-servers). Voor meer informatie over de oplossing gaat u naar de [Help van Kaspersky Sandbox](#).

De volgende configuraties zijn mogelijk voor de Kaspersky Sandbox-oplossing:

### Kaspersky Sandbox 2.0

Kaspersky Sandbox 2.0 ondersteunt de configuratie [KES+built-in agent].

Minimumvereisten:

- Kaspersky Endpoint Security 11.7.0 voor Windows of later.
- Kaspersky Endpoint Agent is niet vereist.
- Kaspersky Security Center 13.2.

### Kaspersky Sandbox 1.0

Kaspersky Sandbox 1.0 ondersteunt de [KES+KEA]-configuratie.

Minimumvereisten:

- Kaspersky Endpoint Security 11.2.0 - 11.6.0 voor Windows.
- Kaspersky Endpoint Agent 3.8.

U kunt Kaspersky Endpoint Agent installeren vanuit de Kaspersky Endpoint Security voor Windows-distributiekit.

- Kaspersky Security Center 11.

## Integratie met Kaspersky Sandbox

Het toevoegen van de Kaspersky Sandbox-component is vereist voor integratie met de Kaspersky Sandbox-component. U kunt het Kaspersky Sandbox-component selecteren tijdens: [installatie](#) of [upgrade](#), alsook tijdens het gebruik van de taak [Programmacomponenten veranderen](#).

Voor het gebruik van het onderdeel moet aan de volgende voorwaarden worden voldaan:

- Kaspersky Security Center 13.2. In eerdere versies van Kaspersky Security Center is het niet mogelijk om alleenstaande IOC-scantaken te maken als reactie op bedreigingen.
- Het onderdeel kan alleen worden beheerd met behulp van de webconsole. U kunt dit onderdeel niet beheren met de Beheerconsole (MMC).
- Het programma is geactiveerd en de functionaliteit valt onder de licentie.
- Gegevensoverdracht naar Administration Server inschakelen

Wilt u alle functies van Kaspersky Sandbox gebruiken, dan moet u ervoor zorgen dat overdracht van quarantainebestandsgegevens is ingeschakeld. De gegevens zijn nodig om via Webconsole informatie te verkrijgen over bestanden die op een computer in quarantaine zijn geplaatst. U kunt bijvoorbeeld een bestand vanuit quarantaine downloaden voor analyse in Webconsole.

### [Gegevensoverdracht naar de Administration Server inschakelen in Webconsole](#)

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Algemene instellingen** → **Rapporten en Opslag**.
5. Schakel in het blok **Data transfer to Administration Server** het selectievakje **About Quarantine files** in.
6. Sla uw wijzigingen op.

- Er is een achtergrondverbinding tot stand gebracht tussen Kaspersky Security Center Webconsole en Administration Server

Om Kaspersky Sandbox te laten werken met Administration Server via Kaspersky Security Center Webconsole, moet u een nieuwe beveiligde verbinding tot stand brengen, een *achtergrondverbinding*. Voor informatie over de integratie van Kaspersky Security Center met andere Kaspersky-oplossingen raadpleegt u de [Help van Kaspersky Security Center](#).

### [Een achtergrondverbinding tot stand brengen in Webconsole](#)

1. Selecteer in het hoofdvenster van de Webconsole **Console settings** → **Integration**.
2. Ga naar het gedeelte **Cross-service integration**.
3. Zet de schakelaar **Establish a background connection for cross-service integration** aan.
4. Sla uw wijzigingen op.

Als er geen achtergrondverbinding tussen Kaspersky Security Center Webconsole en Administration Server tot stand is gebracht, kunnen er geen zelfstandige IOC-scantaken worden gemaakt als onderdeel van Threat Response.

- Het onderdeel Kaspersky Sandbox wordt ingeschakeld.

U kunt de integratie met Kaspersky Sandbox in webconsole of lokaal in- of uitschakelen met de [opdrachtregel](#).

*De integratie met Kaspersky Sandbox in- of uitschakelen:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Kaspersky Sandbox**.
5. Gebruik de schakelaar **Integration with Kaspersky Sandbox** om het onderdeel in of uit te schakelen.
6. Sla uw wijzigingen op.

Het onderdeel Kaspersky Sandbox wordt hierdoor ingeschakeld. Controleer de werkingsstatus van het component door het *statusrapport van de programmaonderdelen* te bekijken. U kunt de werkingsstatus van een onderdeel ook in [rapporten](#) bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Kaspersky Sandbox** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

Kaspersky Endpoint Security slaat informatie op over de werking van het onderdeel Kaspersky Sandbox in een rapport. Het rapport bevat ook informatie over fouten. Als u een fout krijgt met een beschrijving die past bij de Foutcode: XXX indeling (bijvoorbeeld, 0xa67b01f4), neem dan contact op met de [Technische Support](#).

## Migratie van Kaspersky Endpoint Agent

Als u Kaspersky Endpoint Security 11.7.0 of nieuwer gebruikt met de Kaspersky Sandbox-component (ingebouwde agent) geïnstalleerd, is interoperabiliteit met de Kaspersky Sandbox-oplossing direct na installatie beschikbaar. Het component Kaspersky Sandbox is niet compatibel met Kaspersky Endpoint Agent. Als Kaspersky Endpoint Agent op de computer is geïnstalleerd en Kaspersky Endpoint Security wordt bijgewerkt naar versie 11.7.0, dan blijft Kaspersky Sandbox werken met Kaspersky Endpoint Security. ([de \[KES+KEA\]-configuratie migreren naar \[KES+ingebouwde agent\]](#)). Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Om migratie van Kaspersky Endpoint naar Kaspersky Endpoint Security for Windows te voltooien, moet u beleid en taakinstellingen overdragen met de [Migratiewizard](#).

Als u Kaspersky Endpoint Security 11.4.0–11.6.0 gebruikt voor interoperabiliteit met Kaspersky Sandbox, dan bevat het programma Kaspersky Endpoint Agent. U kunt Kaspersky Endpoint Agent samen met Kaspersky Endpoint Security installeren.

In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiepakket niet langer deel uit van de Kaspersky Endpoint Security-distributiekit. U moet het Kaspersky Endpoint Agent-distributiepakket afzonderlijk downloaden.

Het onderdeel Kaspersky Sandbox dat deel uitmaakt van Kaspersky Endpoint Security ondersteunt interoperabiliteit met Kaspersky Sandbox-oplossing 2.0. Kaspersky Sandbox-oplossing 1.0 wordt niet ondersteund.

## Een TLS-certificaat toevoegen

Om een vertrouwde verbinding met Kaspersky Sandbox-servers te configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat toevoegen aan Kaspersky Sandbox-servers en het Kaspersky Endpoint Security-beleid. Voor details over het voorbereiden van het certificaat en het toevoegen van het certificaat aan servers, raadpleegt u [Kaspersky Sandbox Help](#).

U kunt ook lokaal een TLS-certificaat aan de computer toevoegen met behulp van de [opdrachtregel](#).

*Een TLS-certificaat toevoegen in webconsole:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.

2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar **Detection and Response** → **Kaspersky Sandbox**.

5. Klik op de koppeling **Server connection settings**.

Dit opent het venster Kaspersky Sandbox-serververbindinginstellingen.

6. Klik in het blok **Server TLS certificate** op **Add** en selecteer het TLS-certificaatbestand.

Kaspersky Endpoint Security kan slechts één TLS-certificaat hebben voor een Kaspersky Sandbox-server. Als u al eerder een TLS-certificaat hebt toegevoegd, dan wordt dat certificaat ingetrokken. Alleen het laatst toegevoegde certificaat wordt gebruikt.

7. Configureer geavanceerde verbindinginstellingen voor Kaspersky Sandbox-servers:

- **Timeout.** Verbindingstime-out voor Kaspersky Sandbox-server. Nadat de geconfigureerde time-out is verstreken, stuurt Kaspersky Endpoint Security een verzoek naar de volgende server. U kunt de verbindingstime-out voor Kaspersky Sandbox verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder.
- **Kaspersky Sandbox request queue.** Grootte van de verzoekwachtrijmap. Wanneer een object op de computer wordt geopend (uitvoerbaar bestand gestart of document geopend, bijvoorbeeld in DOCX- of PDF-indeling), dan kan Kaspersky Endpoint Security het object ook verzenden om te worden gescand door

Kaspersky Sandbox. Als er meerdere verzoeken zijn, maakt Kaspersky Endpoint Security een verzoekwachtrij aan. Standaard is de grootte van de verzoekwachtrijmap beperkt tot 100 MB. Nadat de maximale grootte is bereikt, stopt Kaspersky Sandbox met het toevoegen van nieuwe verzoeken aan de wachtrij en stuurt het de bijbehorende gebeurtenis naar Kaspersky Security Center. U kunt de grootte van de verzoekwachtrijmap configureren, afhankelijk van uw serverconfiguratie.

8. Sla uw wijzigingen op.

Als resultaat controleert Kaspersky Endpoint Security het TLS-certificaat. Als het certificaat met succes is geverifieerd, zal Kaspersky Endpoint Security het bestand uploaden en naar de computer sturen tijdens de volgende synchronisatie met Kaspersky Security Center. Als u twee TLS-certificaten hebt toegevoegd, gebruikt Kaspersky Sandbox het nieuwste certificaat om een vertrouwde verbinding tot stand te brengen.

## Kaspersky Sandbox-servers toevoegen.

Om computers te verbinden met Kaspersky Sandbox-servers met virtuele afbeeldingen van besturingssystemen, moet u een serveradres en een poort invoeren. Raadpleeg voor details over het inzetten van virtuele afbeeldingen en het configureren van Kaspersky Sandbox-servers de [Kaspersky Sandbox](#) Help.

*Kaspersky Sandbox-servers toevoegen aan de webconsole:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Detection and Response** → **Kaspersky Sandbox**.
5. Klik in het blok **Kaspersky Sandbox servers** op **Toevoegen**.
6. Dit opent een venster; voer in het venster het Kaspersky Sandbox-serveradres (IPv4, IPv6, DNS) en de poort in.
7. Sla uw wijzigingen op.

## Scannen op indicatoren van compromis (stand-alone taak)

Een *Indicator of Compromise (IOC)* is een set gegevens over een object of activiteit die wijst op onbevoegde toegang tot de computer (compromittering van gegevens). Vele mislukte aanmeldingen bij het systeem kunnen bijvoorbeeld een Indicator of Compromise zijn. Met de *IOC-scantaken* kunnen Indicators of Compromise op de computer worden gevonden en maatregelen als respons op deze dreiging worden genomen.

Kaspersky Endpoint Security zoekt Indicators of Compromise met behulp van *IOC-bestanden*. Dat zijn bestanden met de sets indicatoren die het programma zoekt om een detectie waar te nemen. IOC-bestanden moet voldoen aan de [OpenIOC-norm](#). Kaspersky Endpoint Security genereert automatisch IOC-bestanden voor Kaspersky Sandbox.

Uitvoermodus van IOC-scantaak



Het programma maakt zelfstandige IOC-scantaken voor Kaspersky Sandbox. De *zelfstandige IOC-scant* is een groepstaak die automatisch is gemaakt als respons op een dreiging die door Kaspersky Sandbox is gedetecteerd. Kaspersky Endpoint Security genereert automatisch het IOC-bestand. Aangepaste IOC-bestanden worden niet ondersteund. Taken worden 30 dagen na de aanmaaktijd automatisch verwijderd. Voor meer informatie over zelfstandige IOC-scantaken raadpleegt u de [Help van Kaspersky Sandbox](#).

## Instellingen IOC-scant

Kaspersky Sandbox kan automatisch *IOC-scant* maken en uitvoeren bij het reageren op bedreigingen.

U kunt de instellingen alleen configureren in de webconsole.

U hebt Kaspersky Security Center 13.2 voor zelfstandige IOC-scantaken nodig opdat alle functies van Kaspersky Sandbox zouden werken.

*De instellingen van de IOC-scant wijzigen:*

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Devices** → **Tasks**.

De lijst met taken wordt geopend.

2. Selecteer de taak **IOC-scan** van Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar het gedeelte **IOC scan settings**.

5. Configureer acties bij de detectie van IOC's:

- **Move copy to Quarantine, delete object.** Als deze optie is geselecteerd, verwijdert Kaspersky Endpoint Security het schadelijke object dat op de computer is gevonden. Voordat het object wordt verwijderd, maakt Kaspersky Endpoint Security een back-up voor het geval dat het object later moet worden teruggezet. Kaspersky Endpoint Security plaatst de back-up in Quarantaine.
- **Run scan of critical areas.** Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak [Kritieke Gebiedenscan](#). Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.

6. Configureer de uitvoermodus van de IOC-scant met behulp van het selectievakje **Run only when the computer is idle**. Dit selectievakje schakelt de functie in of uit waarmee u de *IOC-scant* uitstelt als de computerbronnen beperkt zijn. Kaspersky Endpoint Security pauzeert de *IOC-scant* als de schermbeveiliging uitgeschakeld is en de computer ontgrendeld is.

Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.

7. Sla uw wijzigingen op.

U kunt de resultaten van de taak bekijken in de taakeigenschappen in het gedeelte **Results**. U kunt informatie over gedetecteerde Indicators of Compromise bekijken in de taakeigenschappen: **Programma-instellingen** → **IOC Scan Results**.

De resultaten van een IOC-scan worden 30 dagen bewaard. Na die tijd worden de oudste gegevens automatisch verwijderd door Kaspersky Endpoint Security.

## Server van Kaspersky Anti Targeted Attack Platform (KATA EDR)



Kaspersky Endpoint Security 11.9.0 voegt ondersteuning toe voor integratie met het onderdeel Kaspersky Endpoint Detection and Response dat deel uitmaakt van de Kaspersky Anti Targeted Attack Platform-oplossing. Kaspersky *Anti Targeted Attack Platform* is een oplossing voor de tijdige detectie van geavanceerde dreigingen, zoals doelgerichte aanvallen, geavanceerde aanhoudende dreigingen (Advanced Persistent Threats, APT), en zero-day-aanvallen en anderen. Kaspersky Anti Targeted Attack platform omvat twee functionele blokken: Kaspersky Targeted Attack (hierna ook wel 'KATA' genoemd) en Kaspersky Endpoint Detection and Response (hierna ook wel 'KEDR' genoemd). U kunt KEDR afzonderlijk aanschaffen. Voor informatie over de oplossing raadpleegt u de [Help van Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Endpoint Detection and Response gebruikt de volgende tools voor informatie over dreigingen:

- De Kaspersky Security Network-cloudservice (hierna ook 'KSN' genoemd) die realtime toegang biedt tot informatie over de reputatie van bestanden, websites en software uit de Knowledge Base van Kaspersky. Het gebruik van gegevens uit Kaspersky Security Network zorgt niet alleen voor een snellere respons door Kaspersky-programma's bij dreigingen, maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives.
- De integratie met de portal van de [Kaspersky Threat Intelligence Portal](#) dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- [Kaspersky Threats](#)-database.

### Werkingsprincipe van de oplossing

Het programma Kaspersky Endpoint Agent wordt op individuele computers op de IT-infrastructuur van het bedrijf geïnstalleerd en bewaakt continu processen, open netwerkverbindingen en bestanden die worden gewijzigd. Informatie over gebeurtenissen op de computer wordt verzonden naar de Kaspersky Anti Targeted Attack Platform-server.

Kaspersky Endpoint Agent kan worden geïntegreerd met Kaspersky Endpoint Security voor Windows. In dit geval verzendt Kaspersky Endpoint Agent ook informatie naar de Kaspersky Anti Targeted Attack Platform-server over dreigingen gevonden door Kaspersky Endpoint Security voor Windows, evenals informatie over verwerkingsresultaten voor deze dreigingen.

### Integratie met KATA EDR

Integratie met KATA EDR vereist het toevoegen van het onderdeel Kaspersky Anti Targeted Attack Platform (KATA EDR) en het installeren van Kaspersky Endpoint Agent. U kunt het KATA EDR-onderdeel selecteren tijdens: [installatie](#) of [upgrade](#), alsook tijdens het gebruik van de taak [Programmacomponenten veranderen](#).

Het KATA EDR-onderdeel is niet compatibel met de onderdelen EDR Optimum en EDR Expert.

In Kaspersky Endpoint Security 11.9.0 bevat de distributiekit niet langer het Kaspersky Endpoint Agent-distributiepakket. U kunt het Kaspersky Endpoint Agent-distributiepakket downloaden van de Kaspersky Anti Targeted Attack Platform-distributiekit.

KATA EDR gebruikt informatie van programma-onderdelen. De volgende onderdelen zorgen voor de werking van KATA EDR:

- [File Threat Protection](#).
- [Web Threat Protection](#).
- [Mail Threat Protection](#).
- [Exploit-preventie](#).
- [Gedragsdetectie](#).
- [Host Intrusion Prevention](#).
- [Remediation Engine](#).
- [Adaptieve controle op afwijkingen](#).

Zorg ervoor dat deze onderdelen ingeschakeld zijn en werken.

## Quarantaine beheren

*Quarantaine* is een speciale lokale opslagplaats op de computer. De gebruiker kan bestanden die de gebruiker gevaarlijk acht voor de computer in quarantaine plaatsen. Bestanden in quarantaine worden in een geëncrypte staat bewaard en vormen geen bedreiging voor de beveiliging van de computer. Kaspersky Endpoint Security gebruikt Quarantaine alleen met de oplossingen Kaspersky Sandbox en Kaspersky Endpoint Detection and Response. In alle andere gevallen plaatst Kaspersky Endpoint Security het relevante bestand in [Back-up](#). Voor meer informatie over het beheer van Quarantaine als onderdeel van de oplossingen raadpleegt u de [Kaspersky Sandbox Help](#), [Kaspersky Endpoint Detection and Response Optimum Help](#), en [Kaspersky Endpoint Detection and Response Expert Help](#).

Kaspersky Endpoint Security gebruikt het systeemaccount (SYSTEEM) om bestanden in quarantaine te plaatsen.

Quarantaine kan alleen via Webconsole worden geconfigureerd. U kunt ook Webconsole gebruiken om objecten in quarantaine te beheren (terugzetten, verwijderen, toevoegen, etc.). Lokaal, op de computer, kunt u alleen [het object herstellen met behulp van de opdrachtregel](#).

## De maximale quarantainegrootte configureren

Standaard is de grootte van de quarantaine beperkt tot 200 MB. Wanneer de maximale grootte is bereikt, verwijdert Kaspersky Endpoint Security automatisch de oudste bestanden uit quarantaine.

*Zo configureert u de maximale grootte van de quarantaine:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.  
U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar **Algemene instellingen** → **Rapporten en Opslag** .

5. Configureer de **Quarantine**grootte in het quarantaineblok:

- **Limit the size of Quarantine to N MB**. Maximale grootte van Quarantine in MB. U kunt de maximale grootte van Quarantine bijvoorbeeld instellen op 200 MB. Wanneer Quarantine dan de maximale grootte bereikt, stuurt Kaspersky Endpoint Security de desbetreffende gebeurtenis naar Kaspersky Security Center en publiceert het de gebeurtenis in het Windows-gebeurtenislogboek. Inmiddels stopt het programma nieuwe objecten in quarantaine plaatsen. U moet de quarantaine handmatig legen.
- **Notify when the Quarantine storage reaches N percent**. Drempelwaarde voor de Quarantine. U kunt de drempel van Quarantine bijvoorbeeld instellen op 50%. Wanneer Quarantine dan de drempel bereikt, stuurt Kaspersky Endpoint Security de desbetreffende gebeurtenis naar Kaspersky Security Center en publiceert het de gebeurtenis in het Windows-gebeurtenislogboek. Inmiddels blijft het programma nieuwe objecten in quarantaine plaatsen.

6. Sla uw wijzigingen op.

## Gegevens over in quarantaine geplaatste bestanden verzenden naar Kaspersky Security Center

Om acties uit te voeren met in quarantaine geplaatste objecten in webconsole, moet u het verzenden van in quarantaine geplaatste bestandsgegevens naar de Administration Server inschakelen. U kunt bijvoorbeeld een bestand vanuit quarantaine downloaden voor analyse in Webconsole. Het verzenden van gegevens in quarantainebestanden moet ingeschakeld zijn voor de werking van alle functionaliteit van [Kaspersky Sandbox](#) en [Kaspersky Endpoint Detection and Response](#).

*De overdracht van in quarantaine geplaatste bestandsgegevens naar Kaspersky Security Center inschakelen:*

1. Selecteer **Apparaten** → **Policies & Profiles** in het hoofdvenster van de webconsole.

2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.

4. Ga naar **Algemene instellingen** → **Rapporten en Opslag** .

5. Schakel in het blok **Data transfer to Administration Server** het selectievakje **About Quarantine files** in.

6. Sla uw wijzigingen op.

Als gevolg hiervan kunt u in webconsole de lijst met in quarantaine geplaatste bestanden op een computer bekijken (**Activiteiten** → **Opslag** → **Quarantine**). U kunt ook webconsole gebruiken om objecten in quarantaine te beheren (terugzetten, verwijderen, toevoegen, etc.).

# Kaspersky Security for Windows Server



Kaspersky Endpoint Security 11.8.0 ondersteunt de basisfunctionaliteit van de Kaspersky Security voor Windows Server (KWS)-oplossing. *Kaspersky Security voor Windows Server* beschermt servers met Microsoft Windows-besturingssystemen en op het netwerk aangesloten opslagplaatsen tegen virussen en andere computerbedreigingen waaraan servers en op het netwerk aangesloten opslagplaatsen worden blootgesteld tijdens het uitwisselen van bestanden. Voor gedetailleerde informatie over hoe de oplossing werkt, verwijzen wij u naar de: [help van Kaspersky Security for Windows Server](#). Vanaf Kaspersky Endpoint Security 11.8.0 kunt u migreren van KWS naar Kaspersky Endpoint Security voor Windows en dezelfde oplossing gebruiken voor het beschermen van werkstations en servers.

## KES installeren bovenop KWS

Kaspersky Endpoint Security (KES) ondersteunt de basisfunctionaliteit van de Kaspersky Security voor Windows Server (KWS)-programma. Vanaf Kaspersky Endpoint Security versie 11.8.0, kunt u KES gebruiken in plaats van KWS.

Voordat u KES installeert, moet u KWS verwijderen. U kunt de installatie van het programma op afstand ongedaan maken met de taak [Programma op afstand verwijderen](#) of [lokaal op de server](#). Na het verwijderen van KWS kan het nodig zijn om de server opnieuw op te starten. Als u Kaspersky Endpoint Security wilt installeren zonder de computer opnieuw op te starten, wordt u geadviseerd ervoor te zorgen dat Kaspersky Security for Windows Server volledig is verwijderd. Hieronder vindt u de lijst met bestanden en services om te controleren. Als het programma niet volledig is verwijderd, kunnen er serverstoringen optreden na de installatie van Kaspersky Endpoint Security. Het wordt ook aanbevolen om ervoor te zorgen dat het programma volledig is verwijderd als u het hulpprogramma kavremover heeft gebruikt. Het [hulpprogramma kavremover](#) biedt geen ondersteuning voor KWS.

Nadat u KWS heeft verwijderd, [installeert u Kaspersky Endpoint Security for Windows](#) met behulp van een beschikbare methode.

## De verwijdering van Kaspersky Security for Windows Server wordt gecontroleerd

Zorg ervoor dat Kaspersky Security for Windows Server volledig is verwijderd:

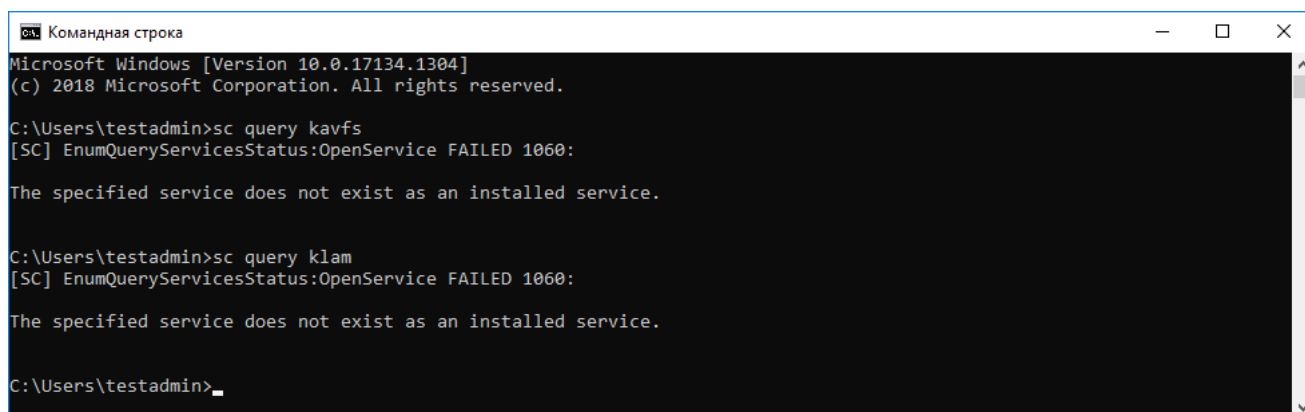
- De map %ProgramFiles%Kaspersky LabKaspersky Security for Windows Server\ bestaat niet.
- De volgende services worden niet uitgevoerd:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management Service (KAVFSGT)
  - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
  - Kaspersky Security Script Checker Service (KAVFSSCS)

U kunt de actieve services controleren in Taakbeheer of met de opdracht `sc query` (zie onderstaande afbeelding).

- De volgende stuurprogramma's zijn niet geïnstalleerd:

- klam.sys
- klft.sys
- kramdisk.sys
- klelaml.sys
- klftdev.sys
- klips.sys
- klids.sys
- klwtpee

U kunt de geïnstalleerde stuurprogramma's controleren in de map `C:\Windows\System32\drivers` of met behulp van de opdracht `sc query`. Als de service of het stuurprogramma ontbreekt, krijgt u het volgende antwoord:



```

Командная строка
Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\testadmin>sc query kavfs
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>sc query klam
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>

```

Controle van de verwijdering van services en stuurprogramma's van Kaspersky Security for Windows Server

Als er nog bestanden van programma's of stuurprogramma's op de server staan, verwijdert u deze handmatig. Als sommige services van Kaspersky Security for Windows Server nog actief zijn, stop (`sc stop`) en verwijder (`sc delete`) deze handmatig. Om het stuurprogramma `klam.sys` te stoppen, gebruikt u de opdracht `fltmc unload klam`.

## KES activeren met een KSWs-sleutel

Nadat u het programma hebt geïnstalleerd, kunt u Kaspersky Endpoint Security voor Windows (KES) activeren met een licentiecode van Kaspersky Security voor Windows Server (KSWs). Het activeringsproces na migratie is afhankelijk van de KSWs-activeringsmethode (zie onderstaande tabel).

Kaspersky Endpoint Security voor Windows activeren met een Kaspersky Security voor Windows Server-code

| Kaspersky Security voor Windows Server-activeringsmethode        | De code van Kaspersky Endpoint Security voor Windows migreren.   |
|--|--|
| Automatische distributie van de KSWs-licentiecode naar computers | Als automatische codedistributie is ingeschakeld in KSWs-licentiecode-eigenschappen, wordt KES automatisch geactiveerd met de KSWs-code. |
| De KSWs-code   | Als uw KSWs wordt geactiveerd met behulp van de taak, wordt de KSWs-   |

|   |   |
|---|---|
| wordt toegevoegd door een taak                                    | licentiecode verwijderd tijdens de migratie van KSWs. U moet het programma opnieuw activeren. U kunt bijvoorbeeld <a href="#">een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket</a> .   |
| De KSWs-sleutel wordt lokaal toegevoegd in de programma-interface | Als uw KSWs lokaal wordt geactiveerd met behulp van de Wizard programma-activering, wordt de KSWs-licentiecode verwijderd tijdens de migratie van KSWs. U moet het programma opnieuw activeren. U kunt bijvoorbeeld <a href="#">een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket</a> . |
| De KSWs-code wordt toegevoegd aan het installatiepakket           | Als uw KSWs is geactiveerd met de code uit het installatiepakket, wordt de KSWs-licentiecode verwijderd tijdens de migratie van KSWs. U moet het programma opnieuw activeren. U kunt bijvoorbeeld <a href="#">een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket</a> .                   |

## Het beheren van het programma op een Core Mode server

Een server in de Core Mode heeft geen GUI. Daarom kunt u het programma alleen op afstand beheren met behulp van de Kaspersky Security Center-console of lokaal op de opdrachtregel.

### De toepassing beheren met behulp van de Kaspersky Security Center-console

Het installeren van het programma met behulp van de Kaspersky Security Center-console verschilt niet van [een normale installatie](#). Bij het [aanmaken van een installatiepakket](#) kunt u een licentiecode toevoegen om het programma te activeren. U kunt een Kaspersky Endpoint Security for Windows-code of een Kaspersky Security for Windows Server-code gebruiken.

Op een Core Mode-server zijn de volgende programmaonderdelen niet beschikbaar: Web Threat Protection, Mail Threat Protection, Webcontrole, BadUSB Attack Prevention, File Level Encryption (FLE), Kaspersky Disk Encryption (FDE).

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. Het programma kan geen venster weergeven waarin de gebruiker wordt gevraagd de server opnieuw op te starten. U kunt leren over de noodzaak om de server opnieuw te starten vanuit rapporten in de Kaspersky Security Center-console.

Het beheren van het programma op de Core Mode-server verschilt niet van het beheren van een computer. U kunt beleid en taken gebruiken om het programma te configureren.

Het beheer van het programma op Core Mode-servers omvat de volgende speciale overwegingen:

- De Core Mode-server heeft geen GUI, daarom geeft Kaspersky Endpoint Security geen waarschuwing weer dat geavanceerde desinfectie nodig is. Voor de desinfectie van een dreiging moet u [de technologie Geavanceerde desinfectie inschakelen](#) in de programma-instellingen en [directe Geavanceerde desinfectie inschakelen](#) in de instellingen van de taak *Virusscan*. Vervolgens moet u de *virusscantaak* starten.
- BitLocker-stationsversleuteling is alleen beschikbaar met een Trusted Platform Module (TPM). Een pincode/wachtwoord kan niet worden gebruikt voor encryptie, omdat het programma het wachtwoordpromptvenster voor preboot-authenticatie niet kan weergeven. Als het besturingssysteem de compatibiliteitsmodus Federal Information Processing Standard (FIPS) heeft ingeschakeld, sluit dan een verwisselbare schijf aan om de encryptiesleutel op te slaan voordat u begint met het coderen van de schijf.

## Het programma vanaf de opdrachtregel beheren

Wanneer u geen GUI kunt gebruiken [beheer Kaspersky Endpoint Security dan vanuit de opdrachtregel](#).

Voer de volgende opdracht uit om het programma op een Core Mode-server te installeren:

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Voer de volgende opdracht uit om het programma te activeren:

```
avp.com license / <activatiecode of licentiebestand>
```

Voer de volgende opdracht uit om de status van het programmaprofiel te controleren:

```
avp.com status
```

Voor de volgende opdracht uit om de lijst met opdrachten voor programmabeheer te bekijken:

```
avp.com help
```



## Het programma vanaf de opdrachtregel beheren

U kunt Kaspersky Endpoint Security vanaf de opdrachtregel beheren. De lijst met opdrachten voor het beheer van het programma kunt u bekijken door de opdracht `HELP` uit te voeren. Als u de syntaxis van een specifieke opdracht wilt lezen, typt u `HELP <opdracht>`.

Speciale tekens in de opdracht moeten worden geëscaped. Als u de tekens `&`, `|`, `(`, `)`, `<`, `>`, `^` wilt escaperen, gebruikt u het teken `^` (voorbeeld: als u het teken `&` wilt gebruiken, typt u `^&`). Om het teken `%` te escaperen, dient u `%%` in te voeren.

## Het programma 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.

Open lees de Gebruiksrechtovereenkomst en het Privacybeleid voordat u het programma in de stille modus installeert. De Gebruiksrechtovereenkomst en het Privacybeleid worden bij het [distributiepakket van Kaspersky Endpoint Security](#) meegeleverd. U mag het programma pas installeren nadat u de voorwaarden van de Gebruiksrechtovereenkomst hebt doorgelezen en begrepen en ermee akkoord bent gegaan, als u begrijpt en aanvaardt dat uw gegevens worden verwerkt en verstuurd (inclusief naar andere landen) in overeenstemming met het Privacybeleid en nadat u het Privacybeleid hebt doorgelezen en begrepen. Als u niet akkoord gaat met de voorwaarden van de Gebruiksrechtovereenkomst en het Privacybeleid, moet u afzien van de installatie en het gebruik van Kaspersky Endpoint Security.

*Zo installeert u het programma of voert u een upgrade voor een oudere versie van het programma uit:*

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]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<gebruikersnaam>
/pKLPASSWD=<password> /pKLPASSWDAREA=<wachtwoordbereik>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<tracingniveau>] [/s]
```

of

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

Als gevolg hiervan wordt het programma op de computer geïnstalleerd. U kunt bevestigen dat het programma is geïnstalleerd en de programma-instellingen controleren door de opdracht `status`.

|  |  |  |
|--|--|--|
|  |  |  |
|--|--|--|

|                        |  |
|------------------------|--|
| EULA=1                 | <p>Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het <a href="#">distributiepakket van Kaspersky Endpoint Security</a>.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.</p> </div>   |
| PRIVACYPOLICY=1        | <p>Aanvaarding van het Privacybeleid. De tekst van het Privacybeleid wordt bij het <a href="#">distributiepakket van Kaspersky Endpoint Security</a> meegeleverd.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.</p> </div>  |
| KSN                    | <p>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:</p> <ul style="list-style-type: none"> <li>• 1 – Aanvaarding van de deelname aan KSN.</li> <li>• 0 – Weigering van de deelname aan KSN (standaardwaarde).</li> </ul> <p>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.</p> |
| ALLOWREBOOT=1          | <p>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.</p> <p>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.</p>   |
| SKIPPRODUCTCHECK=1     | <p>Controle op incompatibele software uitschakelen. De lijst met incompatibele software vindt u in het bestand incompatible.txt in het <a href="#">distributiepakket</a>. Als er geen waarde is ingesteld voor deze parameter en incompatibele software wordt gedetecteerd, dan wordt de installatie van Kaspersky Endpoint Security beëindigd.</p>  |
| SKIPPRODUCTUNINSTALL=1 | <p>Automatische verwijdering van gedetecteerde incompatibele software uitschakelen. Als er geen waarde is ingesteld voor deze parameter, dan probeert Kaspersky Endpoint Security incompatibele software te verwijderen.</p>   |

|              |   |
|--------------|---|
|              | <p>Automatische verwijdering van incompatibele software kan niet worden ingeschakeld wanneer Kaspersky Endpoint Security wordt geïnstalleerd met behulp van het msiexec-installatieprogramma. Gebruik setup_kes.exe om de automatische verwijdering van incompatibele software in te schakelen.</p>   |
| KLLOGIN      | <p>Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel <a href="#">Wachtwoordbeveiliging</a>). De gebruikersnaam wordt samen met de parameters KLPASSWD en KLPASSWDAREA ingesteld. De gebruikersnaam 'KLAdmin' wordt standaard gebruikt.</p>   |
| KLPASSWD     | <p>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).</p> <p>Als u wel een wachtwoord hebt opgegeven maar geen gebruikersnaam bij de parameter KLLOGIN, wordt de gebruikersnaam 'KLAdmin' standaard gebruikt.</p>  |
| KLPASSWDAREA | <p>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, vraagt Kaspersky Endpoint Security de accountgegevens van de gebruiker (de parameters KLLOGIN en KLPASSWD). Gebruik het teken ' ; ' om meerdere waarden op te geven. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• SET – voor het wijzigen van de programma-instellingen.</li> <li>• EXIT – voor het afsluiten van het programma.</li> <li>• DISPROTECT – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken.</li> <li>• DISPOLICY – voor het uitschakelen van het Kaspersky Security Center-beleid.</li> <li>• UNINST – voor het verwijderen van het programma op de computer.</li> <li>• DISCTRL – voor het uitschakelen van de controleonderdelen.</li> <li>• REMOVELIC – voor het verwijderen van de licentie.</li> <li>• REPORTS – voor het bekijken van rapporten.</li> </ul> |
| ENABLETRACES | <p>Programmatracing inschakelen of uitschakelen. Nadat Kaspersky Endpoint Security is gestart, worden de tracebestanden opgeslagen in de map %ProgramData%/Kaspersky Lab\KES\Traces. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – tracing is ingeschakeld.</li> <li>• 0 – tracing is uitgeschakeld (standaardwaarde).</li> </ul>   |
| TRACESLEVEL  | <p>Detailniveau van tracing. Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 100 (kritiek). Alleen berichten over onherstelbare fouten.</li> </ul>  |

|                     |  |
|---------------------|--|
|                     | <ul style="list-style-type: none"> <li>• <b>200</b> (hoog). Berichten over alle fouten, inclusief onherstelbare fouten.</li> <li>• <b>300</b> (diagnostisch). Berichten over alle fouten, alsook waarschuwingen.</li> <li>• <b>400</b> (belangrijk). Alle foutberichten, waarschuwingen en aanvullende informatie.</li> <li>• <b>500</b> (normaal). Berichten over alle fouten en waarschuwingen, alsook gedetailleerde informatie over de werking van het programma in de normale modus (standaard).</li> <li>• <b>600</b> (laag). Alle berichten.</li> </ul>   |
| AMPPL               | <p>Schakelt de bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie (Antimalware Protected Process Light) in of uit. Voor meer informatie over AM-PPL-technologie gaat u naar de <a href="#">website van Microsoft</a>.</p> <p>AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• <b>1</b> – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is ingeschakeld.</li> <li>• <b>0</b> – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is uitgeschakeld.</li> </ul> |
| RESTAPI             | <p>Het programma via de REST API beheren. Voor het beheer van het programma via de REST API moet u de gebruikersnaam opgeven (parameter RESTAPI_User).</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• <b>1</b> – Beheer via de REST API is toegestaan.</li> <li>• <b>0</b> – Beheer via de REST API is niet toegestaan (standaardwaarde).</li> </ul> <p>Voor het beheer van het programma via de REST API moet het beheer met beheersystemen toegestaan zijn. Hiervoor stelt u de parameter AdminKitConnector=1 in. Als u het programma via de REST API beheert, is het niet mogelijk om het programma via de beheersystemen van Kaspersky te beheren.</p>                         |
| RESTAPI_User        | <p>Gebruikersnaam van het Windows-domeinaccount dat wordt gebruikt voor het beheer van het programma via de REST API. Alleen deze gebruiker kan het programma via de REST API beheren. Voer de gebruikersnaam in de structuur &lt;DOMEIN&gt;\&lt;Gebruikersnaam&gt; in (bijvoorbeeld, RESTAPI_User=BEDRIJF\Beheerder). U kunt slechts één gebruiker kiezen die met de REST API mag werken.</p> <p>Een gebruikersnaam toevoegen is een vereiste voor het beheer van het programma via de REST API.</p>  |
| RESTAPI_Port        | <p>Poort die wordt gebruikt voor het beheer van het programma via de REST API. Poort 6782 wordt standaard gebruikt.</p>  |
| RESTAPI_Certificate | <p>Certificaat voor de identificatie van verzoeken (bijvoorbeeld RESTAPI_Certificate=C:\cert.pem). Voor de beveiligde interactie tussen Kaspersky Endpoint Security en de REST-client moet de identificatie</p>  |

|                   |   |
|-------------------|---|
|                   | van verzoeken worden geconfigureerd. Hiervoor moet u een certificaat installeren en vervolgens de payload van elk verzoek ondertekenen.   |
| ADMINKITCONNECTOR | <p>Programmabeheer met beheersystemen. Kaspersky Security Center is bijvoorbeeld een beheersysteem. Naast de Kaspersky-beheersystemen kunt u ook oplossingen van andere leveranciers gebruiken. Kaspersky Endpoint Security heeft hiervoor een API.</p> <p>Beschikbare waarden:</p> <ul style="list-style-type: none"> <li>• 1 – Programmabeheer met behulp van beheersystemen is toegestaan (standaardwaarde).</li> <li>• 0 – Programmabeheer is alleen via de lokale interface toegestaan.</li> </ul> |

**Voorbeeld:**

```

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1

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

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

```

Na de installatie van Kaspersky Endpoint Security wordt de evaluatielicentie geactiveerd, tenzij u een activeringscode 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 het programma activeren met een commerciële licentie via de [wizard Programma-activering](#) of een [speciale opdracht](#).

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](#) – Instellingen voor de werking 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 file](#). 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. U kunt het bestand setup.reg ook in een andere map plaatsen. Als u dit doet, moet u het pad naar het bestand aangeven met de volgende installatieopdracht voor het programma: SETUPREG=<path to the setup.reg file>.

## Programma activeren

*Om het programma vanaf de opdrachtregel te activeren,*

typt u de volgende opdracht op de opdrachtregel:

```
avp.com license /add <activeringscode of licentiebestand> [/login=<gebruikersnaam> /password=<wachtwoord>]
```

U moet de gegevens van het gebruikersaccount invoeren (/login=<gebruikersnaam> /password=<wachtwoord>) als [Wachtwoordbeveiliging is ingeschakeld](#).

## Programma verwijderen

U kunt Kaspersky Endpoint Security op de volgende manieren verwijderen via de opdrachtregel:

- In de interactieve modus via de Installatiewizard van het programma.
- In de stille modus. Nadat de verwijdering in de stille modus is gestart, is uw assistentie tijdens de verwijdering niet meer vereist. Gebruik de switchparameters /s en /qn om het programma in de stille modus te verwijderen.

*Zo verwijdert u het programma in de stille modus:*

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:

- Als de verwijdering niet [beveiligd is met een wachtwoord](#):

```
setup_kes.exe /s /x
```

of

```
msiexec.exe /x <GUID> /qn
```

<GUID> is de unieke ID van het programma. U kunt de GUID van het programma achterhalen door de volgende opdracht te gebruiken:

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber.
```

- Als de verwijdering [beveiligd is met een wachtwoord](#):

```
setup_kes.exe /pKLLLOGIN=<gebruikersnaam> /pKLPASSWD=<wachtwoord> /s /x
```

of

```
msiexec.exe /x <GUID> KLLLOGIN=<gebruikersnaam> KLPASSWD=<wachtwoord> /qn
```

Voorbeeld:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

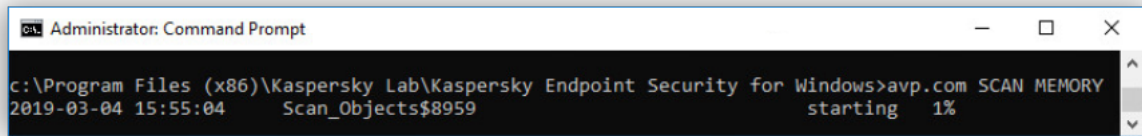
## AVP-opdrachten

*Zo beheert u Kaspersky Endpoint Security vanaf de opdrachtregel:*

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

```
avp.com <opdracht> [opties]
```

Kaspersky Endpoint Security zal nu de opdracht uitvoeren (zie onderstaande afbeelding).



Het programma vanaf de opdrachtregel beheren

## SCAN. Virusscan

Start de virusscantaak.

### Syntaxis van opdracht

```
SCAN [<scanbereik>] [<actie bij detectie van een dreiging>] [<bestandstypen>]
[<scanuitzonderingen>] [/R[A]:<rapportbestand>] [<scantechnologieën>] [/C:<bestand met
instellingen van virusscan>]
```

| Scanbereik             |  |
|------------------------|--|
| <te scannen bestanden> | <p>Een lijst met bestanden en mappen, gescheiden door spaties. Lange paden moeten tussen aanhalingstekens staan. Korte paden (MS-DOS-structuur) moet niet tussen aanhalingstekens staan. Bijvoorbeeld:</p> <ul style="list-style-type: none"> <li>• "C:\Program Files (x86)\Voorbeeldmap" – lang pad.</li> <li>• C:\PROGRA~2\EXAMPL~1 – kort pad.</li> </ul>                     |
| /ALL                   | <p>Start de taak <i>Volledige Scan</i>. Kaspersky Endpoint Security scant de volgende objecten:</p> <ul style="list-style-type: none"> <li>• Kernelgeheugen;</li> <li>• Objecten die bij de opstart van het besturingssysteem worden geladen</li> <li>• Opstartsectoren;</li> <li>• Back-up van het besturingssysteem</li> <li>• Alle harde en verwisselbare schijven</li> </ul> |

|                            |   |
|----------------------------|---|
| /MEMORY                    | Scan het kernelgeheugen   |
| /STARTUP                   | Scan de objecten die bij de opstart van het besturingssysteem worden geladen  |
| /MAIL                      | Scan de Outlook-mailbox   |
| /REMDRIVES                 | Scan verwisselbare schijven.  |
| /FIXDRIVES                 | Scan harde schijven.  |
| /NETDRIVES                 | Scan netwerkschijven.   |
| /QUARANTINE                | Scan de bestanden in Back-up van Kaspersky Endpoint Security.   |
| /@:<br><bestandslijst.lst> | <p>Scan de bestanden en mappen uit een lijst. Elk bestand in de lijst moet in een nieuwe rij staan. Lange paden moeten tussen aanhalingstekens staan. Korte paden (MS-DOS-structuur) moet niet tussen aanhalingstekens staan. Bijvoorbeeld:</p> <ul style="list-style-type: none"> <li>• "C:\Program Files (x86)\Voorbeeldmap" – lang pad.</li> <li>• C:\PROGRA~2\EXAMPL~1 – kort pad.</li> </ul> |

| Actie bij detectie van een dreiging |   |
|-------------------------------------|---|
| /i0                                 | Melden. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security de informatie over geïnfecteerde bestanden toe aan de lijst met actieve dreigingen wanneer deze bestanden worden gedetecteerd.  |
| /i1                                 | Desinfecteren of blokkeren als desinfectie mislukt. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen. |
| /i2                                 | Desinfecteren of verwijderen als desinfectie mislukt. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.<br><br>Deze actie is standaard geselecteerd.                 |
| /i3                                 | Gedetecteerde geïnfecteerde bestanden verwijderen. Als de desinfectie mislukt, worden de geïnfecteerde bestanden verwijderd. Ook samengestelde bestanden (bijvoorbeeld archieven) worden verwijderd als het geïnfecteerde bestand niet kan worden gedesinfecteerd of verwijderd.  |
| /i4                                 | Geïnfecteerde bestanden verwijderen. Ook samengestelde bestanden (bijvoorbeeld archieven) worden verwijderd als het geïnfecteerde bestand niet kan worden verwijderd.   |

| Bestandstypes |  |
|---------------|--|
| /fe           | Bestanden gescand op extensie. Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.                      |
| /fi           | Bestanden gescand op indeling. Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand |



|     |   |
|-----|---|
|     | geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.   |
| /fa | Alle bestanden. Als deze instelling is ingeschakeld, worden alle bestanden gecontroleerd door Kaspersky Endpoint Security, zonder uitzondering (alle indelingen en extensies). Dit is de standaardinstelling. |

| Scanuitzonderingen      |  |
|-------------------------|--|
| -e:a                    | Archieven met de indeling RAR, ARJ, ZIP, CAB, LHA, JAR en ICE worden niet gescand.   |
| -e:b                    | E-maildatabases, inkomende en uitgaande e-mails worden niet gescand.   |
| -e:<br><bestandsmasker> | Bestanden die overeenkomen met het bestandsmasker worden niet gescand. Bijvoorbeeld: <ul style="list-style-type: none"> <li>Het masker *.exe omvat alle paden naar bestanden met de EXE-extensie.</li> <li>Het masker voorbeeld* omvat alle paden naar bestanden met de naam VOORBEELD.</li> </ul> |
| -e:<seconden>           | Bestanden waarvan de scan langer duurt dan de opgegeven tijdslimiet (in seconden) worden niet gescand.   |
| -es:<megabyte>          | Bestanden die groter zijn dan de opgegeven grootte (in megabyte) worden niet gescand.  |

| Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen) |  |
|--|--|
| /R:<rapportbestand>  | Sla alleen kritieke gebeurtenissen in het rapportbestand op. |
| /RA:<rapportbestand>   | Sla alle gebeurtenissen in een rapportbestand op.            |

| Scantechnologieën |  |
|-------------------|--|
| /iChecker=on off  | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR). |
| /iSwift=on off    | Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.   |

| Geavanceerde instellingen |  |
|---------------------------|--|
|                           |  |

|   |   |
|---|---|
| /C:<bestand met instellingen van virusscan> | Bestand met instellingen van de virusscantaak. Het bestand moet handmatig worden aangemaakt en in de TXT-indeling worden opgeslagen. Het bestand kan de volgende inhoud hebben: [<scanbereik>] [<actie bij detectie van een dreiging>] [<bestandstypen>] [<scanuitzonderingen>] [/R[A]:<rapportbestand>] [<scantechnologieën>]. |
|---|---|

**Voorbeeld:**

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

## UPDATE. Databases en softwaremodules van het programma bijwerken

Start de taak *Update*.

### Syntaxis van opdracht

```
UPDATE [local] ["<updatebron>"] [/R[A]:<rapportbestand>] [/C:<bestand met update-instellingen >]
```

| Instellingen van updatetaak |   |
|-----------------------------|---|
| lokaal                      | <p>Start van de <i>updatetaak</i> die na de installatie van het programma automatisch is gemaakt. U kunt de instellingen van de <i>updatetaak</i> wijzigen in de lokale programma-interface of in de console van Kaspersky Security Center. Als deze instelling niet is geconfigureerd, start Kaspersky Endpoint Security de <i>updatetaak</i> met de standaardinstellingen of met de instellingen die in de opdracht zijn opgegeven. U kunt de instellingen van de updatetaak als volgt configureren:</p> <ul style="list-style-type: none"> <li>• UPDATE start de taak <i>Updaten</i> met de standaardinstellingen: de updatebron is Kaspersky-updateservers, het account is Systeem en andere standaardinstellingen.</li> <li>• lokaal UPDATEN start de taak <i>Updaten</i> die automatisch werd aangemaakt na installatie (voorgedefinieerde taak).</li> <li>• UPDATE &lt;update-instellingen&gt; start de taak <i>Updaten</i> met handmatig gedefinieerde instellingen (zie hieronder).</li> </ul> |

| Updatebron     |  |
|----------------|--|
| "<updatebron>" | Adres van een HTTP- of FTP-server of van een gedeelde map met het updatepakket. U kunt maar één updatebron opgeven. Als de updatebron niet is opgegeven, gebruikt Kaspersky Endpoint Security de standaardbron: Kaspersky-updateservers. |

| Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen) |  |
|--|--|
| /R:<rapportbestand>  | Sla alleen kritieke gebeurtenissen in het rapportbestand op. |
| /RA:<rapportbestand>   | Sla alle gebeurtenissen in een                               |

|                                      |   |
|--------------------------------------|---|
| <b>Geavanceerde instellingen</b>     |   |
| /C:<bestand met update-instellingen> | Bestand met de instellingen van de taak <i>Update</i> . Het bestand moet handmatig worden aangemaakt en in de TXT-indeling worden opgeslagen. Het bestand kan de volgende inhoud hebben: ["<updatebron>"] [/R[A]:<rapportbestand>]. |

**Voorbeeld:**

```
avp.com UPDATE lokaal
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

## ROLLBACK. Laatste update terugdraaien

Draai de meest recente update van de antivirusdatabases terug. Zo kunt u indien nodig de databases en de programmamodules terugdraaien naar hun vorige versie wanneer de nieuwe databaseversie bijvoorbeeld een ongeldige definitie bevat waardoor Kaspersky Endpoint Security een veilig programma blokkeert.

**Syntaxis van opdracht**

```
ROLLBACK [/R[A]:<rapportbestand>]
```

|   |  |
|---|--|
| <b>Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen)</b> |  |
| /R:<rapportbestand>   | Sla alleen kritieke gebeurtenissen in het rapportbestand op. |
| /RA:<rapportbestand>  | Sla alle gebeurtenissen in een rapportbestand op.            |

**Voorbeeld:**

```
avp.com ROLLBACK /RA:rollback.txt
```

## TRACES. Tracing

Schakel tracing in of uit. [Tracebestanden](#) worden opslagen op de computer zolang het programma actief is en worden permanent verwijderd wanneer het programma wordt verwijderd. Tracebestanden, behalve tracebestanden van Authenticatie-agent, worden opgeslagen in de map %ProgramData%\Kaspersky Lab\KES\Traces. Standaard is tracing uitgeschakeld.

**Syntaxis van opdracht**

```
TRACES on|off [<tracingniveau>] [<geavanceerde instellingen>]
```

|                      |  |
|----------------------|--|
| <b>Tracingniveau</b> |  |
|----------------------|--|

<tracingniveau>

Detailniveau van tracing. Beschikbare waarden:

- **100** (kritiek). Alleen berichten over onherstelbare fouten.
- **200** (hoog). Berichten over alle fouten, inclusief onherstelbare fouten.
- **300** (diagnostisch). Berichten over alle fouten, alsook waarschuwingen.
- **400** (belangrijk). Alle foutberichten, waarschuwingen en aanvullende informatie.
- **500** (normaal). Berichten over alle fouten en waarschuwingen, alsook gedetailleerde informatie over de werking van het programma in de normale modus (standaard).
- **600** (laag). Alle berichten.

| Geavanceerde instellingen |   |
|---------------------------|---|
| all                       | Start een opdracht met de parameters <code>dbg</code> , <code>file</code> en <code>mem</code> .   |
| dbg                       | Gebruik de functie <code>OutputDebugString</code> en sla het tracebestand op. De functie <code>OutputDebugString</code> verstuurt een tekenreeks naar het foutopsporingsprogramma die op het scherm moet worden weergegeven. Voor meer informatie gaat u naar de <a href="#">MSDN-website</a> . |
| file                      | Sla één tracebestand op (geen maximale grootte).  |
| rot                       | Sla traces op als een beperkt aantal bestanden met een beperkte grootte en overschrijf de oudere bestanden wanneer de maximale grootte wordt bereikt.   |
| mem                       | Sla traces in dumpbestanden op.   |

Voorbeelden:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

## START. Start het profiel

Start het profiel (bijvoorbeeld om databases te updaten of om een beschermingsonderdeel in te schakelen).

Syntaxis van opdracht

```
START <profiel> [/R[A]:<rapportbestand>]
```

|                |  |
|----------------|--|
| <b>Profiel</b> |  |
| <profiel>      | Naam van profiel. Een <i>Profiel</i> is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare <a href="#">profielen</a> bekijken door de opdracht <code>HELP START</code> uit te voeren. |

|   |  |
|---|--|
| <b>Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen)</b> |  |
| /R:<rapportbestand>   | Sla alleen kritieke gebeurtenissen in het rapportbestand op. |
| /RA:<rapportbestand>  | Sla alle gebeurtenissen in een rapportbestand op.            |

Voorbeeld:

avp.com START Scan\_Objects

## STOP. Een profiel stoppen

Stop het profiel (bijvoorbeeld: stop de scans, stop de scan van verwisselbare schijven of schakel een beschermingsonderdeel uit).

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtigingen **Beschermingsonderdelen uitschakelen** en **Controleonderdelen uitschakelen** hebben.

### Syntaxis van opdracht

```
STOP <profiel> /login=<gebruikersnaam> /password=<wachtwoord>
```

|                |   |
|----------------|---|
| <b>Profiel</b> |   |
| <profiel>      | Naam van profiel. Een <i>Profiel</i> is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare <a href="#">profielen</a> bekijken door de opdracht <code>HELP STOP</code> uit te voeren. |

|   |   |
|---|---|
| <b>Authenticatie</b>                              |   |
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

## STATUS. Profielstatus

Toon statusinformatie voor [programmaprofielen](#) (bijvoorbeeld `actief` of `voltooid`). U kunt de lijst met beschikbare profielen bekijken door de opdracht `HELP STATUS` uit te voeren.

Kaspersky Endpoint Security toont ook informatie over de status van serviceprofielen. Informatie over de status van serviceprofielen is mogelijk vereist wanneer u contact opneemt met de Technische Support van Kaspersky.

#### Syntaxis van opdracht

```
avp.com STATUS [<profiel>]
```

Als u de opdracht invoert zonder profiel, geeft Kaspersky Endpoint Security de status weer voor alle profielen van het programma.

## STATISTICS. Statistieken over werking van profiel

Bekijk statistieken over een [programmaprofiel](#) (bijvoorbeeld de scanduur of het aantal gedetecteerde dreigingen.) U kunt de lijst met beschikbare profielen bekijken door de opdracht `HELP STATISTICS` uit te voeren.

#### Syntaxis van opdracht

```
STATISTICS <profiel>
```

## RESTORE. Bestanden vanuit Back-up terugzetten

U kunt een bestand terugzetten vanuit Back-up naar de oorspronkelijke map. Als er al een bestand met dezelfde naam bestaat op het opgegeven pad, zal het programma om bevestiging vragen om het bestand te vervangen. Het bestand dat wordt teruggezet behoudt tijdens het kopiëren de originele naam.

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtiging **Terugzetten vanuit Back-up** hebben.

*Back-up* bewaart back-ups van bestanden die tijdens de desinfectie zijn verwijderd of gewijzigd. Een *back-up* is een kopie van het bestand die is gemaakt voordat het bestand werd gedesinfecteerd of verwijderd. Back-ups van bestanden worden in een speciale indeling opgeslagen en zijn niet gevaarlijk.

Back-ups van bestanden worden opgeslagen in de map `C:\ProgramData\Kaspersky Lab\KES\QB`.

Gebruikers in de groep Beheerders hebben de benodigde machtigingen om deze map te openen. De gebruiker wiens account is gebruikt om Kaspersky Endpoint Security te installeren heeft beperkte toegangsrechten voor deze map.

Kaspersky Endpoint Security biedt de mogelijkheid niet om machtigingen voor de toegang tot back-ups van bestanden te configureren.

#### Syntaxis van opdracht

```
RESTORE [/REPLACE] <bestandsnaam> /login=<gebruikersnaam> /password=<wachtwoord>
```

|                                  |   |
|----------------------------------|---|
| <b>Geavanceerde instellingen</b> |   |
| /REPLACE                         | Overschrijf een bestaand bestand.             |
| <bestandsnaam>                   | De naam van het bestand dat wordt teruggezet. |

|   |  |
|---|--|
| <b>Authenticatie</b>                              |  |
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gebuikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

Voorbeeld:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

## EXPORT. Programma-instellingen exporteren

Exporteer instellingen van Kaspersky Endpoint Security naar een bestand. Het bestand wordt geschreven naar de map C:\Windows\SysWOW64.

### Syntaxis van opdracht

```
EXPORT <profiel> <bestandsnaam>
```

|                |  |
|----------------|--|
| <b>Profiel</b> |  |
| <profiel>      | Naam van profiel. Een <i>Profiel</i> is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare <a href="#">profielen</a> bekijken door de opdracht <code>HELP EXPORT</code> uit te voeren . |

|                              |   |
|------------------------------|---|
| <b>Te exporteren bestand</b> |   |
| <bestandsnaam>               | De naam van het bestand waarnaar de programma-instellingen worden geëxporteerd. U kunt de instellingen van Kaspersky Endpoint Security exporteren naar een DAT- of CFG-configuratiebestand, een TXT-tekstbestand of een XML-document. |

Voorbeelden:

- avp.com EXPORT ids ids\_config.dat
- avp.com EXPORT fm fm\_config.txt

## IMPORT. Programma-instellingen importeren

Importeer instellingen voor Kaspersky Endpoint Security vanuit een bestand dat is aangemaakt met de opdracht `EXPORT`.

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtiging **Programma-instellingen configureren** hebben.

#### Syntaxis van opdracht

```
IMPORT <bestandsnaam> /login=<gebruikersnaam> /password=<wachtwoord>
```

| Te importeren bestand |   |
|-----------------------|---|
| <bestandsnaam>        | De naam van het bestand waaruit de programma-instellingen worden geïmporteerd. U kunt instellingen van Kaspersky Endpoint Security importeren vanuit een DAT- of CFG-configuratiebestand, een TXT-tekstbestand of een XML-document. |

| Authenticatie                                     |   |
|---|---|
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

#### Voorbeeld:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

## ADDKEY. Een licentiebestand toepassen

Pas het licentiebestand toe om Kaspersky Endpoint Security te activeren. Als het programma al is geactiveerd, wordt de licentie toegevoegd als een reservelicentie.

#### Syntaxis van opdracht

```
ADDKEY <bestandsnaam> /login=<gebruikersnaam> /password=<wachtwoord>
```

| Licentiebestand |                           |
|-----------------|---------------------------|
| <bestandsnaam>  | Naam van licentiebestand. |

| Authenticatie                                     |   |
|---|---|
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gegevens van gebruikersaccount. Deze gebruikersgegevens moeten alleen worden ingevoerd als <a href="#">Wachtwoordbeveiliging</a> is ingeschakeld. |

#### Voorbeeld:

```
avp.com ADDKEY file.key
```

## LICENSE. Licentiebeheer



Voer bewerkingen uit met de licentiecodes van Kaspersky Endpoint Security of met de codes van EDR Optimum of EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

Voor het uitvoeren van deze opdracht en het verwijderen van een licentiecode [moet Wachtwoordbeveiliging zijn ingeschakeld](#). De gebruiker moet de machtiging **Code verwijderen** hebben.

#### Syntaxis van opdracht

```
avp.com LICENSE <bewerking> [/login=<gebruikersnaam> /password=<wachtwoord>]
```

| Bewerking   |   |
|---|---|
| /ADD <bestandsnaam>                                     | Pas het licentiebestand toe om Kaspersky Endpoint Security te activeren. Als het programma al is geactiveerd, wordt de licentie toegevoegd als een reservelicentie.                                 |
| /ADD <activeringscode>                                  | Activeer Kaspersky Endpoint Security met een activeringscode. Als het programma al is geactiveerd, wordt de licentie toegevoegd als een reservelicentie.  |
| /REFRESH  | Werk de status bij van het Kaspersky Endpoint Security-beleid. Als gevolg hiervan ontvangt het programma actuele licentiestatusgegevens van Kaspersky-activeringsservers.                           |
| /REFRESH EDR  | Werk de status bij van de add-on-licentie van Kaspersky Endpoint Detection and Response. Als gevolg hiervan ontvangt het programma actuele licentiestatusgegevens van Kaspersky-activeringsservers. |
| /DEL /login=<gebruikersnaam> /password=<wachtwoord>     | Verwijder de licentiesleutel van het programma. De reservelicentie wordt ook verwijderd.  |
| /DEL EDR /login=<gebruikersnaam> /password=<wachtwoord> | Verwijder de licentiecode van de add-on Kaspersky Endpoint Detection and Response. De reservelicentie wordt ook verwijderd.   |

| Authenticatie                                  |   |
|--|---|
| /login=<gebruikersnaam> /password=<wachtwoord> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

#### Voorbeeld:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL EDR /login=KLAdmin /password=!Password1

## RENEW. Een licentie aanschaffen

Hiermee opent u de Kaspersky-website om een licentie te kopen of te verlengen.

## PBATESTRESET. Reset de resultaten van de schijfcontrole voordat u de schijf encrypt

Stel de resultaten van de compatibiliteitscontrole voor Full Disk Encryption (FDE) opnieuw in, inclusief de technologieën Kaspersky Disk Encryption en BitLocker-schijfencryptie.

Alvorens Full Disk Encryption te starten, voert het programma een aantal controles uit om na te gaan of de computer kan worden geëncrypt. Als de computer Full Disk Encryption niet ondersteunt, registreert Kaspersky Endpoint Security informatie over de incompatibiliteit in het logboek. De volgende keer dat u de computer probeert te encrypten, voert het programma deze controle niet uit en wordt u gewaarschuwd dat de encryptie niet kan worden uitgevoerd. Als de hardwareconfiguratie van de computer is gewijzigd, moeten de vastgelegde resultaten van de eerdere compatibiliteitscontrole opnieuw worden ingesteld om de harde schijf van de computer weer te controleren op compatibiliteit met Kaspersky Disk Encryption en BitLocker-encryptietechnologie.

## EXIT. Programma afsluiten

Hiermee sluit u Kaspersky Endpoint Security af. Het programma wordt dan uit het RAM van de computer gehaald.

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtiging **Programma afsluiten** hebben.

### Syntaxis van opdracht

```
EXIT /login=<gebruikersnaam> /password=<wachtwoord>
```

## EXITPOLICY. Beleid uitschakelen

Hiermee schakelt u een Kaspersky Security Center-beleid op de computer uit. Alle Kaspersky Endpoint Security-instellingen kunnen worden geconfigureerd, inclusief instellingen met een gesloten hangslot in het beleid (🔒).

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtiging **Kaspersky Security Center-beleid uitschakelen** hebben.

### Syntaxis van opdracht

```
EXITPOLICY /login=<gebruikersnaam> /password=<wachtwoord>
```

## STARTPOLICY. Beleid inschakelen

Hiermee schakelt u een Kaspersky Security Center-beleid op de computer in. De programma-instellingen worden geconfigureerd volgens het beleid.

## DISABLE. Bescherming uitschakelen

Hiermee schakelt u File Threat Protection uit op een computer met een verlopen licentie voor Kaspersky Endpoint Security. Deze opdracht kan niet worden uitgevoerd op een computer met een niet-geactiveerd programma of met een geldige licentie voor het programma.

## SPYWARE. Detectie van spyware

Hiermee schakelt u de detectie van spyware in of uit. De detectie van spyware is standaard ingeschakeld.

### Syntaxis van opdracht

```
SPYWARE on|off
```

## KSN. Wereldwijde/privaat KSN-overgang

Een Kaspersky Security Network-oplossing selecteren om de reputatie van bestanden of websites te bepalen. Kaspersky Endpoint Security ondersteunt de volgende infrastructurele KSN-oplossingen:

- *Wereldwijd KSN* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky Security Network en sturen Kaspersky informatie over objecten die op hun computers worden gedetecteerd. Dankzij deze informatie worden de objecten dan verder onderzocht door Kaspersky-analisten en worden ze toegevoegd aan de Kaspersky Security Network-databases die reputatie-informatie en statistische gegevens bevatten.
- *Privaat KSN* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang verkrijgen tot reputatiedatabases van Kaspersky Security Network en tot andere statistische gegevens zonder gegevens naar KSN te versturen vanaf hun eigen computers. Privaat KSN is ontworpen voor bedrijven die niet kunnen deelnemen aan Kaspersky Security Network wegens een van de volgende redenen:
  - De lokale werkstations zijn niet verbonden met internet.
  - De verzending van gegevens naar het buitenland of andere netwerken dan het bedrijfsnetwerk is wettelijk verboden of beperkt door het beveiligingsbeleid van het bedrijf.

### Syntaxis van opdracht

```
KSN /global | /private <file name>
```

|  |  |
|--|--|
| <b>Privaat KSN-configuratiebestand</b> |  |
| <bestandsnaam>                         | Naam van het configuratiebestand met de instellingen van de KSN-proxyserver. Dit bestand heeft de extensie PKCS7 of PEM. |

Voorbeeld:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

## KESCLI-opdrachten

Met KESCLI-opdrachten kunt u informatie ontvangen over de status van computerbeveiliging met behulp van het OPSWAT-component, en kunt u standaardtaken uitvoeren, zoals virusscans en database-updates.

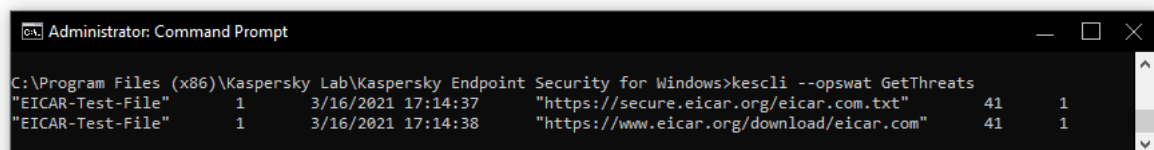
U kunt de lijst met KESCLI-opdrachten bekijken met de opdracht `--help` of de verkorte opdracht `-h`.

*Zo beheert u Kaspersky Endpoint Security vanaf de opdrachtregel:*

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

```
kescli <command> [options]
```

Kaspersky Endpoint Security zal nu de opdracht uitvoeren (zie onderstaande afbeelding).



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Het programma vanaf de opdrachtregel beheren

## Scan. Virusscan

Start de virusscantaak.

Om de taak uit te voeren, moet de beheerder [het gebruik van lokale taken in het beleid toestaan](#).

Syntaxis van opdracht

```
kescli --opswat Scan "<scanbereik>" <actie bij detectie van een dreiging>
```

U kunt de voltooiingsstatus van de taak *Volledige Scan* controleren met de opdracht [GetScanState](#) en kunt de datum en tijd van de laatste voltooiing zien met de opdracht [GetLastScanTime](#).

|                        |   |
|------------------------|---|
| <b>Scanbereik</b>      |   |
| <te scannen bestanden> | Een lijst met bestanden en mappen, gescheiden door ;-. Bijvoorbeeld: "C:\Program Files (x86)\Voorbeeldmap". |

|  |   |
|--|---|
| <b>Actie bij detectie van een dreiging</b> |   |
| 0  | Melden. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security de informatie over geïnfecteerde bestanden toe aan de lijst met actieve dreigingen wanneer deze bestanden worden gedetecteerd.  |
| 1  | Desinfecteren of verwijderen als desinfectie mislukt. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.<br><br>Deze actie is standaard geselecteerd. |

Voorbeeld:

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

## GetScanState. Status van voltooiing van scan

Ontvang informatie over de status van voltooiing van de taak *Volledige scan*:

- 1 – de scan wordt uitgevoerd.
- 0 – de scan wordt niet uitgevoerd.

Syntaxis van opdracht

```
--opswat GetScanState
```

Voorbeeld:

```
kescli --opswat GetScanState
```

## GetLastScanTime. De voltooiingstijd van de scan bepalen

Ontvang informatie over de datum en tijd van de laatste voltooiing van de taak *Volledige scan*.

Syntaxis van opdracht

```
kescli --opswat GetLastScanTime
```

## GetThreats. Gegevens verkrijgen over gedetecteerde bedreigingen

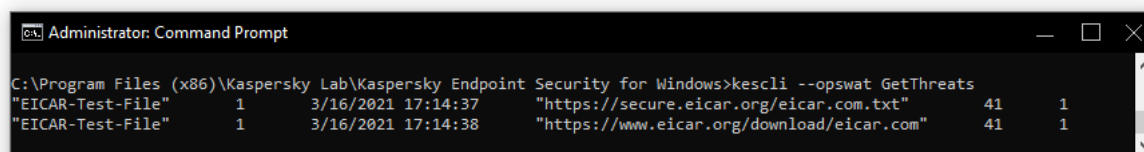
Ontvang een lijst met gedetecteerde bedreigingen (*dreigingsrapport*). Dit rapport bevat informatie over bedreigingen en virusactiviteiten gedurende de laatste 30 dagen voorafgaand aan het maken van het rapport.

### Syntaxis van opdracht

```
--opswat GetThreats
```

Wanneer deze opdracht wordt uitgevoerd, verzendt Kaspersky Endpoint Security een antwoord in de volgende indeling:

```
<naam van gedetecteerd object> <type object> <datum en tijd detectie> <pad naar bestand>  
<actie bij dreigingsdetectie> <gevaarniveau dreiging>
```



```
Administrator: Command Prompt  
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats  
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1  
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Het programma vanaf de opdrachtregel beheren

| Objecttype |  |
|------------|--|
| 0          | Niet gekend (Unknown).   |
| 1          | Virussen (Virware).  |
| 2          | Trojaanse programma's (Trojware).  |
| 3          | Kwaadaardige programma's (Malware).  |
| 4          | Advertentieprogramma's (Adware).   |
| 5          | Automatische inbelprogramma's (Pornware).  |
| 6          | Toepassingen die door een cybercrimineel kunnen worden gebruikt om de computer of gegevens van de gebruiker te beschadigen (Riskware). |
| 7          | Objecten die mogelijk zijn gecomprimeerd om schadelijke code te beschermen (Packed).   |
| 20         | Onbekende objecten (Xfiles).   |
| 21         | Gekend programma's (Software).   |
| 22         | Verborgene bestanden (Hidden).   |
| 23         | Programma's waarvoor aandacht vereist is (Pupware).  |
| 24         | Afwijkend gedrag (Anomaly).  |
| 30         | Niet bepaald (Undetect).   |
| 40         | Advertentiebanner (Banner).  |
| 50         | Netwerkaanval (Attack).  |
| 51         | Toegang tot register (Registry).   |

|     |  |
|-----|--|
| 52  | Verdacht activiteit (Suspicion).                               |
| 60  | Kwetsbaarheden (Vulnerability).                                |
| 70  | Phishing.  |
| 80  | Ongewenste e-mailbijlage (Attachment).                         |
| 90  | Malware gedetecteerd door Kaspersky Security Network (Urgent). |
| 100 | Onbekende link (Suspicious URL).                               |
| 110 | Andere malware (Behavioral).                                   |

| Actie bij detectie van een dreiging |  |
|-------------------------------------|--|
| 0                                   | Niet gekend (unknown).   |
| 1                                   | Dreiging werd opgelost (ok).   |
| 2                                   | Object was geïnfecteerd en niet gedesinfecteerd (infected).                                    |
| 5                                   | Object bevindt zich in een archief en is niet gedesinfecteerd (archive).                       |
| 9                                   | Object is gedesinfecteerd (disinfected).   |
| 10                                  | Object is niet gedesinfecteerd (not disinfected).  |
| 11                                  | Object is verwijderd (deleted).  |
| 13                                  | Er is een back-up van het object gemaakt (backupped).  |
| 15                                  | Object is verplaatst naar Back-up (quarantined).   |
| 23                                  | Het object wordt verwijderd bij het opnieuw opstarten van de computer (delete on reboot).      |
| 25                                  | Het object is gedesinfecteerd bij het opnieuw opstarten van de computer (disinfect on reboot). |
| 29                                  | Het object is door een gebruiker naar back-up verplaatst (added by user).                      |
| 30                                  | Het object is toegevoegd aan uitsluitingen (added to exclude).                                 |
| 31                                  | Het object werd verplaatst naar back-up bij herstart van computer (quarantine on reboot).      |
| 36                                  | Vals positief (false alarm).   |
| 38                                  | Het proces is beëindigd (terminated).  |
| 40                                  | Object is niet gedetecteerd (not found).   |
| 41                                  | Kan de dreiging niet oplossen (untreatable).   |
| 42                                  | Object is hersteld (rolled back).  |
| 43                                  | Het object is gemaakt als gevolg van bedreigingsactiviteit (produced by threat).               |
| 44                                  | Het object werd hersteld bij het opnieuw opstarten van de computer (roll back on reboot).      |
| 0xffffffff                          | Het object werd niet verwerkt (discarded).   |

|                       |  |
|-----------------------|--|
| Gevaarniveau dreiging |  |
|-----------------------|--|

|   |                                |
|---|--------------------------------|
| 0 | Onbekend                       |
| 1 | Hoog                           |
| 2 | Gemiddelde scan                |
| 4 | Laag                           |
| 8 | Info (minder dan <i>Laag</i> ) |

## UpdateDefinitions. Databases en softwaremodules van het programma bijwerken

Start de taak *Update*. Kaspersky Endpoint Security gebruikt de standaardbron: Kaspersky-updateservers.

Om de taak uit te voeren, moet de beheerder [het gebruik van lokale taken in het beleid toestaan](#).

### Syntaxis van opdracht

```
kescli --opswat UpdateDefinitions
```

Je kunt de uitgiftedatum en -tijd van de huidige antivirusdatabases bekijken door de opdrachtregel [GetDefinitionsetState](#) te gebruiken.

## GetDefinitionState. De voltooiingstijd van de update bepalen

Ontvang informatie over de uitgiftedatum en -tijd van de in gebruik zijnde antivirusdatabases.

### Syntaxis van opdracht

```
kescli --opswat GetDefinitionState
```

## EnableRTP. Beveiliging inschakelen

Schakel de beschermingsonderdelen van Kaspersky Endpoint Security in op de computer: File Threat Protection, Web Threat Protection, Mail Threat Protection, Network Threat Protection, Host Intrusion Prevention.

Om beschermingsonderdelen in te schakelen, moet de beheerder ervoor zorgen dat de relevante beleidsinstellingen kunnen worden gewijzigd (☑ attributen zijn open).

### Syntaxis van opdracht

```
kescli --opswat EnableRTP
```



Als gevolg hiervan worden beschermingsonderdelen ingeschakeld, zelfs als u de wijziging van programma-instellingen met [wachtwoordbeveiliging](#) hebt verboden.

U kunt controleren of File Threat Protection in- of uitgeschakeld is met de opdracht [GetRealTimeProtectionState](#).

## GetRealTimeProtectionState. Status van bescherming bestanden

Ontvang informatie over de bedrijfsstatus van de component File Threat Protection:

- 1 – het component is ingeschakeld.
- 0 – het component is uitgeschakeld.

### Syntaxis van opdracht

```
kescli --opswat GetRealTimeProtectionState
```

## Version. De versie van het programma bepalen

De versie van Kaspersky Endpoint Security voor Windows bepalen.

### Syntaxis van opdracht

```
--Version
```

U kunt ook de verkorte opdracht `-v` gebruiken.

Voorbeeld:  
`kescli -v`

## Opdrachten voor beheer van Detection and Response

U kunt de opdrachtregel gebruiken om de ingebouwde functionaliteit van Detection and Response-oplossingen te beheren (bijvoorbeeld Kaspersky Sandbox of Kaspersky Endpoint Detection and Response Optimum). U kunt Detection and Response-oplossingen beheren als beheer met de Kaspersky Security Center-console niet mogelijk is. De lijst met opdrachten voor het beheer van het programma kunt u bekijken door de opdracht `HELP` uit te voeren. Als u de syntaxis van een specifieke opdracht wilt lezen, typt u `HELP <opdracht>`.

*Ingebouwde functies van detectie- en responsoplossingen beheren via de opdrachtregel:*

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

```
avp.com <opdracht> [opties]
```

Kaspersky Endpoint Security zal nu de opdracht uitvoeren (zie onderstaande afbeelding).

## SANDBOX. Kaspersky Sandbox beheren

Opdrachten voor het beheren van het onderdeel Kaspersky Sandbox:

- Schakel het onderdeel Kaspersky Sandbox in of uit.  
Met het onderdeel Kaspersky Sandbox wordt interoperabiliteit met de Kaspersky Sandbox-oplossing mogelijk.
- Het onderdeel Kaspersky Sandbox configureren:
  - Verbind de computer met de Kaspersky Sandbox-servers.  
De servers gebruiken geïmplementeerde virtuele afbeeldingen van Microsoft Windows-besturingssystemen om objecten uit te voeren die moeten worden gescand. U kunt een IP-adres (IPv4 of IPv6) of een volledig gekwalificeerde domeinnaam invoeren. Raadpleeg voor details over het inzetten van virtuele afbeeldingen en het configureren van Kaspersky Sandbox-servers de [Kaspersky Sandbox-help](#).
  - Configureer de connectie-time-out voor Kaspersky Sandbox-server.  
Time-out voor het ontvangen van een reactie op een objectscanaanvraag van de Kaspersky Sandbox-server. Zodra de time-outperiode is verstreken, leidt Kaspersky Sandbox de aanvraag om naar de volgende server. De time-outwaarde hangt af van de snelheid en stabiliteit van de verbinding. De standaardwaarde is 5 seconden.
  - Configureer een vertrouwde verbinding tussen de computer en Kaspersky Sandbox-servers.  
Om een vertrouwde verbinding met Kaspersky Sandbox-servers te configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat toevoegen aan Kaspersky Sandbox-servers en het Kaspersky Endpoint Security-beleid. Voor details over het voorbereiden van het certificaat en het toevoegen van het certificaat aan servers, raadpleegt u [Kaspersky Sandbox Help](#).
- Toon de huidige instellingen van het component.

### Syntaxis van opdracht

```
stop sandbox [<profiel> /login=<gebruikersnaam> /password=<wachtwoord>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<serveradres>:<poort>] [--timeout=<connectie-
time-out Kaspersky Sandbox-server (ms)>] [--pinned-certificate=<pad naar het TLS-
certificaat>][/login=<gebruikersnaam> /password=<wachtwoord>]
sandbox /show
```

| Bewerking |  |
|-----------|--|
| stop      | Het onderdeel Kaspersky Sandbox uitschakelen.  |
| start     | Het onderdeel Kaspersky Sandbox inschakelen.   |
| set       | Het onderdeel Kaspersky Sandbox configureren. U kunt de volgende instellingen wijzigen: <ul style="list-style-type: none"><li>• Gebruik een vertrouwde verbinding (--tls);</li></ul> |

|       |  |
|-------|--|
|       | <ul style="list-style-type: none"> <li>• Voeg een TLS-certificaat (<code>--pinned-certificate</code>) toe;</li> <li>• Stel de connectie-time-out (<code>--timeout</code>) voor de Kaspersky Sandbox-server in;</li> <li>• Voeg Kaspersky Sandbox-servers (<code>--servers</code>) toe.</li> </ul>                  |
| tonen | Toon de huidige instellingen van het component. U krijgt de volgende reactie:<br><code>sandbox.timeout=&lt;connectie-time-out Kaspersky Sandbox-server (ms)&gt;</code><br><code>sandbox.tls=&lt;vertrouwde-verbindingstatus&gt;</code><br><code>sandbox.servers=&lt;lijst met Kaspersky Sandbox-servers&gt;</code> |

|   |   |
|---|---|
| <b>Authenticatie</b>  |   |
| <code>/login=&lt;gebruikersnaam&gt;</code><br><code>/password=&lt;wachtwoord&gt;</code> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

Voorbeeld:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

## PREVENTIE. Preventie van uitvoering beheren

Schakel Preventie van uitvoering uit of toon de huidige onderdeelinstellingen, inclusief de lijst met regels voor preventie van uitvoering.

### Syntaxis van opdracht

```
prevention disable
prevention /show
```

Bij het uitvoeren van de opdracht `prevention /show` krijg je de volgende reactie:

```
prevention.enable=true|false
```

```
prevention.mode=audit|prevent
```

```
prevention.rules
```

```
id: <regel-ID>
```

```
target: script|process|document
```

```
md5: <MD5-hash van het bestand>
```

```
sha256: <SHA256-hash van het bestand>
```

```
pattern: <pad naar het object>
```

```
case-sensitive: true|false
```

Resultaatwaarden opdracht:

- -1 betekent dat de opdracht niet wordt ondersteund door de versie van het programma dat op het apparaat is geïnstalleerd.
- 0 betekent dat de opdracht met succes is uitgevoerd.
- 1 betekent dat een verplicht argument niet is doorgegeven aan de opdracht.
- 2 betekent dat er zich een algemene fout heeft voorgedaan.
- 4 betekent dat er een syntaxfout was.
- 9 – verkeerde werking (bijvoorbeeld een poging om het component uit te schakelen wanneer het al is uitgeschakeld).

## ISOLATIE. Netwerkisolatie beheren

Schakel Netwerkisolatie van de computer uit of geef de huidige instellingen van het onderdeel weer. Componentinstellingen bevatten ook een lijst met netwerkverbindingen die zijn toegevoegd aan uitzonderingen.

### Syntaxis van opdracht:

```
isolation /OFF /login=<gebruikersnaam> /password=<wachtwoord>
isolation /STAT
```

Als resultaat van de opdracht `stat` ontvangt u de volgende reactie: `Network isolation on|off`.

## RESTORE. Bestanden terugzetten vanuit quarantaine

U kunt een bestand terugzetten vanuit quarantaine naar de oorspronkelijke map. Als de doelmap verwijderd is, plaatst het programma het bestand in een speciale map op de computer. Daarna moet u het bestand handmatig naar de bestemmingsmap verplaatsen. *Quarantaine* is een speciale lokale opslagplaats op de computer. De gebruiker kan bestanden die de gebruiker gevaarlijk acht voor de computer in quarantaine plaatsen. Bestanden in quarantaine worden in een geëncrypte staat bewaard en vormen geen bedreiging voor de beveiliging van de computer. Kaspersky Endpoint Security gebruikt Quarantaine alleen met de oplossingen Kaspersky Sandbox en Kaspersky Endpoint Detection and Response. In alle andere gevallen plaatst Kaspersky Endpoint Security het relevante bestand in [Back-up](#). Voor meer informatie over het beheer van Quarantaine als onderdeel van de oplossingen raadpleegt u de [Kaspersky Sandbox Help](#), [Kaspersky Endpoint Detection and Response Optimum Help](#), en [Kaspersky Endpoint Detection and Response Expert Help](#).

Voor het uitvoeren van deze opdracht [moet Wachtwoordbeveiliging ingeschakeld zijn](#). De gebruiker moet de machtiging **Terugzetten vanuit Back-up** hebben.

Het object wordt in quarantaine geplaatst onder de systeemaccount (SYSTEEM).

### Syntaxis van opdracht

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Geavanceerde instellingen

|                |   |
|----------------|---|
| /REPLACE       | Overschrijf een bestaand bestand.             |
| <bestandsnaam> | De naam van het bestand dat wordt teruggezet. |

|   |   |
|---|---|
| <b>Authenticatie</b>                              |   |
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

**Voorbeeld:**

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

Resultaatwaarden opdracht:

- -1 betekent dat de opdracht niet wordt ondersteund door de versie van het programma dat op het apparaat is geïnstalleerd.
- 0 betekent dat de opdracht met succes is uitgevoerd.
- 1 betekent dat een verplicht argument niet is doorgegeven aan de opdracht.
- 2 betekent dat er zich een algemene fout heeft voorgedaan.
- 4 betekent dat er een syntaxfout was.

## IOCSCAN. Scannen op loC's (Indicators of Compromise)

Voer de Scannen op Indicators of Compromise (IOC)-taak uit. Een *Indicator of Compromise (IOC)* is een set gegevens over een object of activiteit die wijst op onbevoegde toegang tot de computer (compromittering van gegevens). Vele mislukte aanmeldingen bij het systeem kunnen bijvoorbeeld een Indicator of Compromise zijn. Met de *IOC-scan* kunnen Indicators of Compromise op de computer worden gevonden en maatregelen als respons op deze dreiging worden genomen.

### Syntaxis van opdracht

```
IOCSCAN <volledig pad naar het IOC-bestand>[/path=<pad naar de IOC-bestandenmap>
[/process=on|off] [/hint=<volledig pad naar uitvoerbaar bestand van een proces
volledig bestand pad] [/bestand pad] [/bestand pad] [/bestand pad] [/bestand pad]
[/bestand pad] [/bestand pad] [/gebruikers bestand pad] [/bestand pad] [/bestand pad]
[/bestand pad evenement>] [/bestand pad met kanalen>] [/bestand pad] [/bestand pad]
[/bestand pad met uitsluitingen>][scope=<lijst met te scannen mappen>]
```

|                                     |   |
|-------------------------------------|---|
| <b>IOC-bestanden</b>                |   |
| <volledig pad naar het IOC-bestand> | Volledig pad naar het IOC-bestand dat u wilt gebruiken voor het scannen. U kunt meerdere IOC-bestanden opgeven, gescheiden door spaties. Voer het volledige pad naar het IOC-bestand in, zonder het argument /path.<br><br>Bijvoorbeeld C:\Users\Admin\Desktop\IOC\file1.ioc                                      |
| /path=<pad naar de map met          | Pad naar de map met IOC-bestanden die u wilt gebruiken voor het scannen. <i>IOC-bestanden</i> zijn bestanden die de verzameling indicatoren bevatten aan de hand waarvan het programma op zoek gaat naar hits die kunnen duiden op een dreiging. IOC-bestanden moet voldoen aan de <a href="#">OpenIOC-norm</a> . |

| Gegevenstype voor IOC-scannen  |   |
|--|---|
| /process=on off  | <p>Analyseer procesgegevens tijdens het uitvoeren van de IOC-scan (ProcessItem-term).</p> <p>Als de waarde van het argument <code>off</code> is, analyseert Kaspersky Endpoint Security de processen die tijdens de scan op de computer worden uitgevoerd niet. Als het IOC-bestand IOC-terminen van het ProcessItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security procesgegevens alleen als het ProcessItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| /hint=<volledig pad naar het uitvoerbare bestand van het proces volledig pad naar het bestand> | <p>Analyseer bestandsgegevens tijdens het uitvoeren van de IOC-scan (ProcessItem- en FileItem-terminen).</p> <p>U kunt op een van de volgende manieren een bestand selecteren:</p> <ul style="list-style-type: none"> <li>• &lt;volledig pad naar het uitvoerbare bestand van het proces&gt; – ProcessItem;</li> <li>• &lt;volledig pad naar het bestand&gt; – FileItem.</li> </ul>   |
| /registry=on off   | <p>Analyseer Windows-registeregegevens tijdens het uitvoeren van een IOC-scan (RegistryItem-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security het Windows-register niet. Als het IOC-bestand termen van het RegistryItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security het Windows-register alleen als het RegistryItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p> <p>Voor het gegevenstype RegistryItem scant Kaspersky Endpoint Security <a href="#">een reeks registersleutels</a>.</p> |
| /dnsentry=on off   | <p>Analyseer de gegevens over records in de lokale DNS-cache tijdens het uitvoeren van de IOC-scan (DnsEntryItem-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de lokale DNS-cache niet. Als het IOC-bestand termen van het DnsEntryItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security de lokale DNS-cache alleen als het DnsEntryItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| /arpentry=on off   | <p>Analyseer de gegevens over records in de ARP-tabel tijdens het uitvoeren van de IOC-scan (ArpEntryItem-term).</p>  |

|                                      |   |
|--------------------------------------|---|
|                                      | <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de ARP-tabel niet. Als het IOC-bestand termen van het <code>ArpEntryItem-IOC</code>-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security de ARP-tabel alleen als het <code>ArpEntryItem-IOC</code>-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| <p><code>/ports=on off</code></p>    | <p>Analyseer gegevens over poorten die openstaan voor luisteren tijdens het uitvoeren van de IOC-scan (<code>PortItem</code>-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de tabel met actieve verbindingen op het apparaat niet. Als het IOC-bestand termen van het <code>PortItem-IOC</code>-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security de tabel met actieve verbindingen alleen als het <code>PortItem-IOC</code>-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>                  |
| <p><code>/services=on off</code></p> | <p>Analyseer gegevens over services die zijn geïnstalleerd op het apparaat tijdens het uitvoeren van de IOC-scan (<code>ServiceItem</code>-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de gegevens over services die zijn geïnstalleerd op het apparaat niet. Als het IOC-bestand termen van het <code>ServiceItem-IOC</code>-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security servicegegevens alleen als het <code>ServiceItem-IOC</code>-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p> |
| <p><code>/system=on off</code></p>   | <p>Analyseer omgevingsgegevens tijdens het uitvoeren van de IOC-scan (<code>SystemInfoItem</code>-term).</p> <p>Als de waarde van het argument <code>off</code> is, analyseert Kaspersky Endpoint Security omgevingsgegevens niet. Als het IOC-bestand termen van het <code>SystemInfoItem-IOC</code>-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security omgevingsgegevens alleen als het <code>SystemInfoItem-IOC</code>-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| <p><code>/users=on off</code></p>    | <p>Analyseer gegevens over gebruikers tijdens het uitvoeren van de IOC-scan (<code>UserItem</code>-term).</p> <p>Als de waarde van het argument <code>off</code> is, analyseert Kaspersky Endpoint Security gegevens over gebruikers die zijn aangemaakt op het systeem niet. Als het IOC-bestand termen van het <code>UserItem-IOC</code>-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p>   |

|   |  |
|---|--|
|   | <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security gegevens over gebruikers die zijn aangemaakt in het systeem alleen als het UserItem-IOC-document is gedefinieerd is in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| <p><code>/volumes=on off</code></p>                               | <p>Analyseer gegevens over volumes tijdens het uitvoeren van de IOC-scan (Volumeltem-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de gegevens over volumes op het apparaat niet. Als het IOC-bestand termen van het Volumeltem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security volumegegevens alleen als het Volumeltem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>   |
| <p><code>/eventlog=on off</code></p>                              | <p>Analyseer de gegevens over records in het Windows Event-logboek tijdens het uitvoeren van de IOC-scan (EventLogItem-term).</p> <p>Als de waarde van het argument <code>off</code> is, scant Kaspersky Endpoint Security de records in het Windows-gebeurtenislogboek niet. Als het IOC-bestand termen van het EventLogItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security het Windows Event-logboek als het EventLogItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>   |
| <p><code>/datetime=&lt;publicatiedatum gebeurtenis&gt;</code></p> | <p>Houd bij het bepalen van het IOC-scanbereik voor het bijbehorende IOC-document rekening met de datum waarop de gebeurtenis is gepubliceerd in het Windows Event-logboek.</p> <p>Tijdens het uitvoeren van een IOC-scan scant Kaspersky Endpoint Security vermeldingen in het Windows-gebeurtenislogboek die zijn gepubliceerd vanaf de opgegeven tijd en datum tot het moment dat de taak is uitgevoerd.</p> <p>In Kaspersky Endpoint Security kan de publicatiedatum van de gebeurtenis worden opgegeven als de waarde van het argument. De scan wordt alleen uitgevoerd voor gebeurtenissen die na de opgegeven datum en vóór het uitvoeren van de scan in het Windows Event-logboek zijn gepubliceerd.</p> <p>Als er geen argument wordt opgegeven, scant Kaspersky Endpoint Security gebeurtenissen zonder rekening te houden met de publicatiedatum. De instelling <code>TaskSettings::BaseSettings::EventLogItem::datetime</code> kan niet worden bewerkt.</p> <p>De instelling wordt alleen gebruikt als het EventLogItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p> |
| <p><code>/channel=&lt;lijst met kanalen&gt;</code></p>            | <p>Lijst met (logboek)namen van kanalen waarvoor u een IOC-scan wilt uitvoeren.</p> <p>Als dit argument wordt opgegeven, scant Kaspersky Endpoint Security records die zijn gepubliceerd in de opgegeven logboeken. Het IOC-document moet een definitie bevatten van de EventLogItem-term.</p>   |



|   |  |
|---|--|
|   | <p>De naam van het logboek wordt aangegeven als een string overeenkomstig de naam van het logboek (kanaal) zoals aangegeven in de eigenschappen van het logboek (de Full Name-parameter) of in de gebeurteniseigenschappen (de &lt;Channel&gt;&lt;/Channel&gt;-parameter in het xml-schema van de gebeurtenis). U kunt meerdere kanalen opgeven, gescheiden door spaties.</p> <p>Als er geen argument wordt opgegeven, scant Kaspersky Endpoint Security records op de kanalen Application, System en Security.</p>  |
| /files=on off                           | <p>Analyseer bestandsgegevens tijdens het uitvoeren van de IOC-scan (FileItem-term).</p> <p>Als de waarde van het argument off is, analyseert Kaspersky Endpoint Security bestandsgegevens niet. Als het IOC-bestand termen uit het FileItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit').</p> <p>Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security bestandsgegevens alleen als het FileItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.</p>  |
| /drives=<all system critical custom>    | <p>Stel IOC-scanbereik in bij het analyseren van gegevens voor het FileItem-IOC-document.</p> <p>U kunt de volgende waarden instellen voor het scanbereik:</p> <ul style="list-style-type: none"> <li>• &lt;all&gt; voor alle beschikbare bestandsbereiken.</li> <li>• &lt;system&gt; voor bestanden in mappen waarin het besturingssysteem is geïnstalleerd.</li> <li>• &lt;critical&gt; voor tijdelijke bestanden in gebruiker- en systeemmappen.</li> <li>• &lt;custom&gt; voor bestanden in bereiken die door de gebruiker zijn gedefinieerd (/scope=&lt;lijst met mappen om te scannen&gt;).</li> </ul> <p>Als er geen argument wordt opgegeven, wordt de scan uitgevoerd voor kritieke gebieden.</p> |
| /excludes=<lijst met uitzonderingen>    | <p>Stel uitzonderingsbereik in bij het analyseren van gegevens voor het FileItem-IOC-document. U kunt meerdere paden opgeven, gescheiden door spaties.</p>   |
| /scope=<lijst met mappen om te scannen> | <p>Door gebruiker gedefinieerd IOC-scanbereik bij het analyseren van gegevens voor het FileItem IOC-document (/drives=custom). U kunt meerdere paden opgeven, gescheiden door spaties.</p>   |

Resultaatwaarden opdracht:

- -1 betekent dat de opdracht niet wordt ondersteund door de versie van eht programma dat op het apparaat is geïnstalleerd.
- 0 betekent dat de opdracht met succes is uitgevoerd.
- 1 betekent dat een verplicht argument niet is doorgegeven aan de opdracht.
- 2 betekent dat er zich een algemene fout heeft voorgedaan.

- 4 betekent dat er een syntaxfout was.

Als de opdracht succesvol is uitgevoerd (returnwaarde 0) en Indicators of Compromise zijn gedetecteerd, geeft Kaspersky Endpoint Security de volgende taakresultaten weer op de opdrachtregel:

|                           |  |
|---------------------------|--|
| UUID                      | ID van het IOC-bestand uit de header van de IOC-bestandsstructuur (de tag <ioc id="">)                           |
| Naam                      | Beschrijving van het IOC-bestand in de header van de IOC-bestandsstructuur (de tag <description></description> ) |
| Gematchte indicatie-items | Lijst met ID's van alle indicatoren die een hit opleverden.  |
| Gematchte objects         | Gegevens van elk IOC-document waarvoor een hit werd gevonden.  |

## MDRLICENSE. MDR-activering

Voer bewerkingen uit met het BLOB-configuratiebestand om Beheerde detectie en respons te activeren. Het BLOB-bestand bevat de client-ID en informatie over de licentie voor Kaspersky Beheerde detectie en respons. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Beheerde detectie en respons-console. Raadpleeg de [Help van Kaspersky Managed Detection and Response](#) voor gedetailleerde informatie over een BLOB-bestand.

Beheerdersbevoegdheden zijn vereist voor het uitvoeren van bewerkingen met een BLOB-bestand. Beheerde detectie- en responsinstellingen in het beleid moeten ook beschikbaar zijn voor bewerking (🔒).

### Syntaxis van opdracht

```
MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

| Bewerking              |  |
|------------------------|--|
| /ADD<br><bestandsnaam> | Pas het BLOB-configuratiebestand toe voor integratie met Kaspersky Beheerde detectie en respons (P7-bestandsindeling). U kunt slechts één BLOB-bestand toepassen. Als er al een BLOB-bestand aan de computer is toegevoegd, wordt het bestand vervangen. |
| /DEL                   | Verwijder het BLOB-configuratiebestand.  |

| Authenticatie                                     |   |
|---|---|
| /login=<gebruikersnaam><br>/password=<wachtwoord> | Gebruikersaccountgegevens met de vereiste machtigingen voor <a href="#">wachtwoordbeveiliging</a> . |

### Voorbeeld:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

## Foutcodes

Er kunnen fouten optreden wanneer u het programma met de opdrachtregel gebruikt. Wanneer er fouten optreden, toont Kaspersky Endpoint Security een foutbericht zoals Fout: Taak 'EntAppControl' kan niet worden gestart. Kaspersky Endpoint Security kan ook aanvullende informatie tonen in de vorm van een code, zoals error=8947906D (zie onderstaande tabel).

Foutcodes

| Foutcode | Beschrijving  |
|----------|---|
| 09479001 | Het licentiebestand voor Kaspersky Endpoint Security wordt al gebruikt op deze computer.                        |
| 0947901D | De licentie is verlopen. De databases kunnen niet worden geüpdatet.   |
| 89479002 | Code niet gevonden.   |
| 89479003 | Digitale handtekening ontbreekt of is beschadigd.   |
| 89479004 | Gegevens zijn beschadigd.   |
| 89479005 | Licentiebestand is beschadigd.  |
| 89479006 | Licentie is verlopen of licentiebestand is verlopen.  |
| 89479007 | Licentiebestand is niet opgegeven.  |
| 89479008 | Licentiebestand kan niet worden toegepast.  |
| 89479009 | Opslaan van gegevens is mislukt.  |
| 8947900A | Lezen van gegevens is mislukt.  |
| 8947900B | I/O-fout.   |
| 8947900C | Databases zijn niet gevonden.   |
| 8947900E | Licentiebibliotheek is niet geladen.  |
| 8947900F | Databases zijn beschadigd of handmatig geüpdatet.   |
| 89479010 | Databases zijn beschadigd.  |
| 89479011 | Kan geen ongeldig licentiebestand gebruiken om een reservelicentie toe te voegen.                               |
| 89479012 | Systeemfout.  |
| 89479013 | Denylist van licenties is beschadigd.   |
| 89479014 | Handtekening van bestand komt niet overeen met de digitale handtekening van Kaspersky.                          |
| 89479015 | Kan code voor niet-commerciële licentie niet gebruiken als code voor commerciële licentie.                      |
| 89479016 | De bètalicentie is vereist om de bètaversie van het programma te gebruiken.                                     |
| 89479017 | Licentiebestand is niet compatibel met dit programma.   |
| 89479018 | Code geblokkeerd door Kaspersky.  |
| 89479019 | Programma wordt al gebruikt met een evaluatielicentie. Evaluatiecode kan niet opnieuw worden toegevoegd.        |
| 8947901A | Licentiebestand is beschadigd.  |
| 8947901B | Digitale handtekening ontbreekt, is beschadigd of komt niet overeen met de digitale handtekening van Kaspersky. |

|          |   |
|----------|---|
| 8947901C | Licentie kan niet worden toegevoegd als de bijbehorende niet-commerciële licentie is verlopen.  |
| 8947901E | De datum waarop het licentiebestand is gemaakt of gebruikt is ongeldig. Controleer de systeemdatum.   |
| 8947901F | Kan geen code voor evaluatielicentie toevoegen: er is al een andere code voor een evaluatielicentie actief.   |
| 89479020 | Denylist van licenties is beschadigd of ontbreekt.  |
| 89479021 | Updatebeschrijving ontbreekt of is beschadigd.  |
| 89479022 | Fout in servicegegevens van licentiebestand.  |
| 89479023 | Kan geen ongeldig licentiebestand gebruiken om een reservelicentie toe te voegen.   |
| 89479025 | Fout bij verzending van aanvraag naar de activeringserver. Mogelijke redenen: fout bij internetverbinding of tijdelijke problemen met de activeringserver. Probeer het programma later te activeren met de activeringscode. Als de fout aanhoudt, neemt u contact op met de internetprovider. |
| 89479026 | Fout bij antwoord van activeringserver.   |
| 89479027 | Reactiestatus kan niet worden verkregen.  |
| 89479028 | Fout bij opslaan van tijdelijk bestand.   |
| 89479029 | Activeringscode is verkeerd ingevoerd of systeemdatum is onjuist. Controleer de systeemdatum op de computer.  |
| 8947902A | Code niet compatibel met dit programma of licentie verlopen. U kunt Kaspersky Endpoint Security niet activeren met een licentiebestand voor een ander programma.  |
| 8947902B | Ontvangst van licentiebestand is mislukt. Onjuiste activeringscode is ingevoerd.  |
| 8947902C | Activeringserver gaf fout 400.  |
| 8947902D | Activeringserver gaf fout 401.  |
| 8947902E | Activeringserver gaf fout 403.  |
| 8947902F | Activeringserver gaf fout 404.  |
| 89479030 | Activeringserver gaf fout 405.  |
| 89479031 | Activeringserver gaf fout 406.  |
| 89479032 | Authenticatie op proxyserver vereist. Controleer de netwerkopties.  |
| 89479033 | Time-out bij aanvraag.  |
| 89479034 | Activeringserver gaf fout 409.  |
| 89479035 | Activeringserver gaf fout 410.  |
| 89479036 | Activeringserver gaf fout 411.  |
| 89479037 | Activeringserver gaf fout 412.  |
| 89479038 | Activeringserver gaf fout 413.  |
| 89479039 | Activeringserver gaf fout 414.  |
| 8947903A | Activeringserver gaf fout 415.  |
| 8947903C | Interne serverfout.   |
| 8947903D | Functionaliteit wordt niet ondersteund.   |

|          |   |
|----------|---|
| 8947903E | Ongeldig antwoord van gateway. Controleer de netwerkopties.   |
| 8947903F | Service niet beschikbaar (HTTP-fout 503).   |
| 89479040 | Time-out bij reactie van gateway. Controleer de netwerkopties.  |
| 89479041 | Het protocol wordt niet ondersteund door de server.   |
| 89479043 | Onbekende HTTP-fout.  |
| 89479044 | Ongeldige bron-ID.  |
| 89479046 | Ongeldige URL.  |
| 89479047 | Ongeldige doelmap.  |
| 89479048 | Fout bij geheugentoe wijzing.   |
| 89479049 | Fout bij conversie van parameters naar ANSI-tekenreeks (URL, map, agent).   |
| 8947904A | Fout bij maken van werkthread.  |
| 8947904B | Werkthread is al actief.  |
| 8947904C | Werkthread is niet actief.  |
| 8947904D | Licentiebestand niet gevonden op activeringsserver.   |
| 8947904E | Licentie is geblokkeerd.  |
| 8947904F | Interne fout bij activeringsserver.   |
| 89479050 | Onvoldoende gegevens in activeringsaanvraag.  |
| 89479053 | Licentiebestand verlopen.   |
| 89479054 | Onjuiste systeemdatum op de computer.   |
| 89479055 | Evaluatielicentie is verlopen.  |
| 89479056 | De licentie is verlopen.  |
| 89479057 | Het maximale aantal programma-activeringen is voor de opgegeven code overschreden.  |
| 89479058 | Activeringsprocedure is met een systeemfout beëindigd.  |
| 89479059 | Kan code voor niet-commerciële licentie niet gebruiken als code voor commerciële licentie.                                |
| 8947905C | Activeringscode is vereist.   |
| 89479062 | Geen verbinding met activeringsserver mogelijk.   |
| 89479064 | Activeringsserver niet beschikbaar. Controleer de instellingen van de internetverbinding en probeer opnieuw te activeren. |
| 89479065 | De releasedatum van de database valt na de verloopdatum van licentie.   |
| 89479066 | Actieve licentie kan niet door een verlopen licentie worden vervangen.  |
| 89479067 | Reservelicentie kan niet worden toegevoegd als deze vóór de huidige licentie verloopt.                                    |
| 89479068 | Geüpdatete abonnementslicentie ontbreekt.   |
| 8947906A | Onjuiste activeringscode (controlesom komt niet overeen).   |
| 8947906B | Code al actief.   |
| 8947906C | Licentietypen die horen bij actieve en reservelicenties komen niet overeen.   |
| 8947906D | Onderdeel niet ondersteund door licentie.   |

|          |   |
|----------|---|
| 8947906E | Abonnementslicentie kan niet als reservelicentie worden toegevoegd.   |
| 89479213 | Algemene fout bij transportlaag.  |
| 89479214 | Verbinden met activeringsserver is mislukt.   |
| 89479215 | Ongeldige URL-indeling.   |
| 89479216 | Conversie van proxyserveradres is mislukt.  |
| 89479217 | Conversie van serveradres is mislukt. Controleer de instellingen van de internetverbinding.   |
| 89479218 | Verbinding met activeringsserver of proxyserver is mislukt.   |
| 89479219 | Toegang tot account geweigerd.  |
| 8947921A | Time-out voor reactie is verlopen.  |
| 8947921B | Fout bij verzending van HTTP-aanvraag.  |
| 8947921C | SSL-verbindingfout.   |
| 8947921D | Bewerking onderbroken door terugbellen.   |
| 8947921E | Te veel pogingen tot doorsturen.  |
| 8947921F | Controle van ontvanger is mislukt.  |
| 89479220 | Lege reactie van activeringsserver.   |
| 89479221 | Fout bij verzending van gegevens.   |
| 89479222 | Fout bij ontvangst van gegevens.  |
| 89479223 | Fout bij lokaal SSL-certificaat.  |
| 89479224 | Fout bij SSL-encryptie.   |
| 89479225 | Fout bij SSL-certificaat van server.  |
| 89479226 | Ongeldige inhoud van netwerkpakket.   |
| 89479227 | Toegang van gebruiker geweigerd.  |
| 89479228 | Ongeldig SSL-certificaatbestand.  |
| 89479229 | Maken van SSL-verbinding is mislukt.  |
| 8947922A | Verzending of ontvangst van netwerkpakket is mislukt. Probeer het later opnieuw.  |
| 8947922B | Ongeldig bestand met ingetrokken certificaten.  |
| 8947922C | Fout bij SSL-certificaataanvraag.   |
| 89479401 | Onbekende serverfout.   |
| 89479402 | Interne serverfout.   |
| 89479403 | Geen licentiebestand beschikbaar voor de ingevoerde activeringscode.  |
| 89479404 | Actieve licentie geblokkeerd.   |
| 89479405 | Vereiste parameters van aanvraag voor activering van programma ontbreken.   |
| 89479406 | Onjuiste gebruikersnaam of wachtwoord.  |
| 89479407 | Onjuiste activeringscode verstuurd naar server.   |
| 89479408 | Activeringscode is ongeldig voor Kaspersky Endpoint Security. U kunt Kaspersky Endpoint Security niet activeren met een licentiebestand voor een onbekend |

|          |  |
|----------|--|
|          | programma.   |
| 89479409 | Geen activeringscode in aanvraag.  |
| 8947940B | Licentie is verlopen (volgens gegevens van de activeringsserver).  |
| 8947940C | Het aantal activeringen met deze code is overschreden.   |
| 8947940D | Ongeldige structuur van aanvraagnummer.  |
| 8947940E | Activeringscode is ongeldig voor Kaspersky Endpoint Security. Activeringscode is bedoeld voor een ander Kaspersky-programma. |
| 8947940F | Licentiebestand kan niet worden geüpdatet.   |
| 89479410 | Activeringscode is ongeldig in deze regio.   |
| 89479411 | Activeringscode is ongeldig voor de taalversie van Kaspersky Endpoint Security.  |
| 89479412 | Extra toegang tot de activeringsserver is vereist.   |
| 89479413 | Activeringsserver gaf fout 643.  |
| 89479414 | Activeringsserver gaf fout 644.  |
| 89479415 | Activeringsserver gaf fout 645.  |
| 89479416 | Activeringsserver gaf fout 646.  |
| 89479417 | Structuur van activeringscode niet ondersteund door activeringsserver.   |
| 89479418 | Ongeldige structuur van activeringscode.   |
| 89479419 | Onjuiste systeemtijd op de computer.   |
| 8947941A | Activeringscode is ongeldig voor de versie van Kaspersky Endpoint Security.  |
| 8947941B | Abonnement verlopen.   |
| 8947941C | Aantal activeringen overschreden voor dit licentiebestand.   |
| 8947941D | Ongeldige digitale handtekening van licentiebestand.   |
| 8947941E | Er zijn aanvullende gegevens nodig.  |
| 8947941F | Verificatie van gegevens is mislukt.   |
| 89479420 | Abonnement inactief.   |
| 89479421 | Activeringsserver ondergaat onderhoud.   |
| 89479501 | Onbekende fout van Kaspersky Endpoint Security.  |
| 89479502 | Ongeldige parameter overgezet. Bijvoorbeeld: een lege lijst met adressen van activeringsservers.                             |
| 89479503 | Onjuiste activeringscode.  |
| 89479504 | Ongeldige gebruikersnaam.  |
| 89479505 | Ongeldig gebruikerswachtwoord.   |
| 89479506 | Ongeldige reactie van activeringsserver.   |
| 89479507 | Activeringsaanvraag onderbroken.   |
| 89479509 | Activeringsserver gaf een lege lijst voor doorsturen.  |

## Appendix. Programmaprofielen

Een *Profiel* is een onderdeel, taak of functie van Kaspersky Endpoint Security. Profielen worden gebruikt voor het beheer van het programma vanaf de opdrachtregel. U kunt profielen gebruiken om de opdrachten `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` en `IMPORT` uit te voeren. Met profielen kunt u programma-instellingen configureren (bijvoorbeeld `STOP DeviceControl`) of taken starten (bijvoorbeeld `START Scan_My_Computer`).

De volgende profielen zijn beschikbaar:

- `AdaptiveAnomaliesControl` – Adaptieve controle op afwijkingen.
- `AMSI` – AMSI-bescherming.
- `BehaviorDetection` – Gedragsdetectie.
- `DeviceControl` – Apparaatcontrole.
- `EntAppControl` – Programmacontrole.
- `File_Monitoring` of `FM` – File Threat Protection.
- `Firewall` of `FW` – Firewall.
- `HIPS` – Host Intrusion Prevention.
- `IDS` – Network Threat Protection.
- `IntegrityCheck` – Integriteitscontrole.
- `Mail_Monitoring` of `EM` – Mail Threat Protection.
- `Rollback` – Update terugdraaien.
- `Scan_ContextScan` – Scannen vanuit contextmenu.
- `Scan_IdleScan` – Achtergrondscan.
- `Scan_Memory` – Scan van kernelgeheugen.
- `Scan_My_Computer` – Volledige Scan.
- `Scan_Objects` – Aangepaste Scan.
- `Scan_Qscan` – Scan objecten die bij de opstart van het besturingssysteem worden geladen.
- `Scan_Removable_Drive` – Scan van verwisselbare schijven.
- `Scan_Startup` of `STARTUP` – Kritieke Gebiedenscan.
- `Updater` – Update.
- `Web_Monitoring` of `WM` – Web Threat Protection.



- WebControl – Webcontrole.

Kaspersky Endpoint Security ondersteunt ook serviceprofielen. Serviceprofielen zijn mogelijk vereist wanneer u contact opneemt met de Technische Support van Kaspersky.

## Het programma via de REST API beheren

In Kaspersky Endpoint Security kunt u programma-instellingen configureren, een scan starten, de antivirusdatabases updaten en andere taken met oplossingen van derden uitvoeren. Kaspersky Endpoint Security heeft hiervoor een API. De REST API van Kaspersky Endpoint Security werkt via HTTP en bestaat uit een reeks methoden met vraag en antwoord. U kunt dus Kaspersky Endpoint Security beheren via oplossingen van derden in plaats van de lokale programma-interface of de Beheerconsole van Kaspersky Security Center.

Als u aan de slag wilt met de REST API, moet u [Kaspersky Endpoint Security installeren met ondersteuning voor de REST API](#). De REST-client en Kaspersky Endpoint Security moeten op dezelfde computer geïnstalleerd zijn.

Een veilige interactie garanderen tussen Kaspersky Endpoint Security en de REST-client:

- Configureer de bescherming van de REST-client tegen ongeautoriseerde toegang volgens de aanbevelingen van de ontwikkelaar van de REST-client. Configureer de bescherming van de REST-clientmap tegen schrijven met behulp van Discretionary Access Control List - DACL.
- Gebruik een aparte account met beheerdersrechten om de REST-client uit te voeren. Weiger interactief aanmelden op het systeem voor deze account.

Het programma wordt beheerd via de REST API op `http://127.0.0.1` of `http://localhost`. Het is niet mogelijk om Kaspersky Endpoint Security op afstand te beheren via de REST API.



[DOCUMENTATIE VAN REST API OPENEN](#)

## Het programma installeren met de REST API

Voor het beheer van het programma via de REST API moet u Kaspersky Endpoint Security installeren met ondersteuning voor de REST API. Als u Kaspersky Endpoint Security via de REST API beheert, kunt u het programma niet beheren met Kaspersky Security Center.

### Installatie van het programma met REST API-ondersteuning voorbereiden

Voor de beveiligde interactie tussen Kaspersky Endpoint Security en de REST-client moet de identificatie van verzoeken worden geconfigureerd. Hiervoor moet u een certificaat installeren en vervolgens de payload van elk verzoek ondertekenen.

Als u een certificaat wilt aanmaken, kunt u bijvoorbeeld OpenSSL gebruiken.

Voorbeeld:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Gebruik het RSA-encryptiealgoritme met een sleutellengte van 2048 bits of meer.

Hiermee verkrijgt u een `cert.pem`-certificaat en een private `key.pem`-sleutel.

### Het programma met REST API-ondersteuning installeren

*Zo installeert u Kaspersky Endpoint Security met ondersteuning voor de REST API:*

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.

2. Ga naar de map met het distributiepakket voor Kaspersky Endpoint Security 11.2.0 of hoger.

3. Installeer Kaspersky Endpoint Security met de volgende instellingen:

- RESTAPI=1

- RESTAPI\_User=<User name>

Gebruikersnaam voor het beheer van het programma via de REST API. Voer de gebruikersnaam in de structuur <DOMEIN>\<Gebruikersnaam> in (bijvoorbeeld, RESTAPI\_User=BEDRIJF\Beheerder). U kunt alleen met dit account het programma via de REST API beheren. U kunt slechts één gebruiker kiezen die met de REST API mag werken.

- RESTAPI\_Port=<Poort>

Poort die wordt gebruikt voor de gegevensuitwisseling. Optionele parameter. Poort 6782 is standaard geselecteerd.

- RESTAPI\_Certificate=<Pad naar certificaat>

Certificaat voor de identificatie van verzoeken (bijvoorbeeld RESTAPI\_Certificate=C:\cert.pem).

U kunt het certificaat na de installatie van het programma installeren of het certificaat updaten nadat het verlopen is.

#### [Een certificaat voor de identificatie van REST API-aanvragen installeren](#)

1. Schakel [Zelfbescherming van Kaspersky Endpoint Security](#) uit

Het mechanisme Zelfbescherming voorkomt de wijziging of verwijdering van programmabestanden op de harde schijf, processen in het geheugen en vermeldingen in het systeemregister.

2. Ga naar de registersleutel met de REST API-instellingen:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest

3. Voer het pad naar het certificaat in, bijvoorbeeld Certificate = C:\Folder\cert.pem.

4. Schakel [Zelfbescherming van Kaspersky Endpoint Security](#) in.

5. [Herstart het programma](#).

- AdminKitConnector=1

Programmabeheer met beheersystemen. Het beheer is standaard toegestaan.

U kunt ook het bestand [setup.ini](#) gebruiken om de instellingen voor het werken met de REST API te definiëren.

Voorbeeld:

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator  
/pRESTAPI_Certificate=C:\cert.pem /s
```

U kunt nu het programma via de REST API beheren. Om de werking te controleren, opent u de documentatie van de REST API met een GET-aanvraag.

Voorbeeld:

```
GET http://localhost:6782/kes/v1/api-docs
```

Als u het programma met REST API-ondersteuning hebt geïnstalleerd, maakt Kaspersky Endpoint Security automatisch een regel voor toestaan in de instellingen van webcontrole voor toegang tot webbronnen (*service-regel voor REST API*). Deze regel is nodig om de REST-client te allen tijde toegang te geven tot Kaspersky Endpoint Security. Als u bijvoorbeeld beperkte gebruikerstoegang tot webbronnen hebt, heeft dit geen invloed op het beheer van het programma via de REST API. We raden u aan de regel niet te verwijderen of de instellingen *Service-regel voor REST API* niet te veranderen. Als u de regel hebt verwijderd, zal Kaspersky Endpoint Security deze herstellen nadat het programma opnieuw is opgestart.

## Werken met de API

Het is niet mogelijk om de toegang tot het programma via de REST API te beperken met [Wachtwoordbeveiliging](#). Zo kunt u bijvoorbeeld niet beletten dat een gebruiker de beveiliging uitschakelt via de REST API. U kunt Wachtwoordbeveiliging configureren via de REST API en de toegang van gebruikers tot het programma beperken via de lokale interface.

Als u het programma via de REST API beheert, moet u de REST-client starten met het account dat u hebt opgegeven wanneer u [het programma met ondersteuning voor de REST API hebt geïnstalleerd](#). U kunt slechts één gebruiker kiezen die met de REST API mag werken.



### [DOCUMENTATIE VAN REST API OPENEN](#)

Voer de volgende stappen uit om het programma via de REST API te beheeren:

1. Haal de huidige waarden van de programma-instellingen op. Stuur hiervoor een GET-aanvraag.

Voorbeeld:

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. Het programma stuurt een antwoord met de structuur en waarden van instellingen. Kaspersky Endpoint Security ondersteunt de indelingen XM en JSON.

Voorbeeld:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": true,
  "enabled": true
}
```

3. Bewerk de programma-instellingen. Gebruik de structuur van de instellingen die u in het antwoord op de GET-aanvraag hebt gekregen.

Voorbeeld:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. Sla de programma-instellingen (de payload) op in een JSON-bestand (payload.json).
5. Onderteken het JSON-bestand in de PKCS7-indeling.

Voorbeeld:

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
```

Hiermee verkrijgt u een ondertekend bestand met de payload van de aanvraag (`signed_payload.pem`).

6. Bewerk de programma-instellingen. Stuur hiervoor een POST-aanvraag en voeg het ondertekende bestand met de payload van de aanvraag toe (`signed_payload.pem`).

Het programma past de nieuwe instellingen toe en stuurt een reactie met de resultaten van de programmaconfiguratie (de reactie mag leeg zijn). Met een GET-aanvraag kunt u controleren of de instellingen zijn geüpdatet.

## Bronnen met informatie over het programma

### De pagina van Kaspersky Endpoint Security op de Kaspersky-website

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.

### Discussies over Kaspersky-programma's in de community voor gebruikers

Als uw vraag niet dringend is, kunt u uw vraag stellen aan Kaspersky-experts en andere gebruikers in onze [community](#).

In de Community kunt u bestaande onderwerpen bekijken, zelf commentaar posten en nieuwe discussieonderwerpen aanmaken.

# Contact opnemen met de Technische Support

Als u geen oplossing voor uw probleem vindt in de documentatie of in andere [informatiebronnen over Kaspersky Endpoint Security](#), raden we aan dat u contact opneemt met de Technische Support. De Technische Support beantwoordt graag al uw vragen over de installatie en het gebruik van Kaspersky Endpoint Security.

Kaspersky biedt ondersteuning voor Kaspersky Endpoint Security tijdens de levenscyclus van het programma (raadpleeg de pagina met de [levenscyclus van het programma](#)). 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 [Technische support-website te bezoeken](#)
- Door een verzoek naar de Technische Support van Kaspersky te sturen via de [Kaspersky CompanyAccount-portal](#)

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 het traceren 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 en gedetailleerde rapporten over de werking van programmaonderdelen.

Wanneer de diagnostische testen worden uitgevoerd, kunnen de experts van de Technische Support u vragen om programma-instellingen te wijzigen door:

- De functie voor het verkrijgen van uitgebreide diagnostische informatie te activeren.
- Configureer afzonderlijke componenten van het programma door speciale instellingen te wijzigen die niet toegankelijk zijn via de standaard gebruikersinterface.
- Instellingen voor de opslag van diagnostische informatie 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 gebruikt om de fout op te sporen en te corrigeren. De uitgebreide diagnostische informatie wordt op de computer van de gebruiker opgeslagen. De gegevens worden niet automatisch verstuurd naar Kaspersky.

De eerder vermelde handleidingen mogen alleen onder het toezicht van experts van de Technische Support worden uitgevoerd en hun instructies moeten strikt worden opgevolgd. Het zelf wijzigen van programma-instellingen op manieren die niet worden beschreven in de online help of in de aanbevelingen van de technische support kan leiden tot vertragingen en crashes van het besturingssysteem, het beveiligingsniveau van uw computer verlagen en de beschikbaarheid en integriteit van de verwerkte informatie schaden.

## Inhoud en opslag van traceringsbestanden

U bent persoonlijk verantwoordelijk voor de veiligheid van de gegevens die op uw computer worden opgeslagen, en in het bijzonder voor het bewaken en het beperken van de toegang tot deze gegevens totdat deze worden verstuurd naar Kaspersky.

Tracebestanden worden opslagen op de computer zolang het programma actief is en worden permanent verwijderd wanneer het programma wordt verwijderd.

Tracebestanden, behalve tracebestanden van Authenticatie-agent, worden opgeslagen in de map %ProgramData%\Kaspersky Lab\KES\Traces.

Tracebestanden krijgen de volgende naam: KES<versienummer van service\_datumXX.XX\_tijdXX.XX\_pidXXX.><type tracebestand>.log.

U kunt opgeslagen gegevens in tracebestanden bekijken.

Alle traceringsbestanden bevatten de volgende algemene gegevens:

- Het tijdstip van de gebeurtenis.
- Het nummer van de uitvoeringsthread.

Het tracebestand van Authenticatie-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.

Kaspersky Endpoint Security slaat wachtwoorden van gebruikers alleen in geëncrypte vorm op in een tracebestand.

## 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.
- Gegevens over de hardware die op de computer is geïnstalleerd (zoals BIOS/UEFI-firmwaregegevens). Deze gegevens worden naar tracebestanden geschreven bij het uitvoeren van Kaspersky Disk Encryption.
- De gebruikersnaam en het wachtwoord als die openbaar zijn verzonden. Deze gegevens kunnen tijdens het scannen van het internetverkeer worden 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.
- Gegevens over netwerkverkeer. Deze gegevens worden naar tracebestanden geschreven als verkeersbewakingscomponenten zijn ingeschakeld (zoals Webcontrole).
- Gegevens ontvangen van Kaspersky-servers (zoals de versie van antivirusdatabases).
- Statussen van Kaspersky Endpoint Security-componenten en hun bedrijfsgegevens.
- Gegevens over gebruikersactiviteit in het programma.
- Gebeurtenissen van besturingssysteem.

## 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 verbindingmodule van Kaspersky Security Center voordoen.

## Inhoud van bestanden met prestatietraces

Bestanden met prestatietraces krijgen de volgende naam:  
`KES<versienummer_datumXX.XX_tijdXX.XX_pidXXX.>PERF.HAND.etl.`

Naast de algemene gegevens bevatten bestanden met prestatietraces ook informatie over de belasting van de processor, informatie over de laadtijd van het besturingssysteem en programma's en informatie over actieve processen.

## Inhoud van tracebestand van AMSI-beschermingsonderdeel

Naast de algemene gegevens bevat het tracebestand AMSI.log ook informatie over de resultaten van scans die op verzoek van programma's van andere leveranciers worden uitgevoerd.

## Inhoud van tracebestanden van het onderdeel Mail Threat Protection

Het tracebestand mcou.OUTLOOK.EXE.log bevat naast de algemene gegevens mogelijk ook onderdelen van e-mailberichten, waaronder e-mailadressen.

## Inhoud van tracebestanden van het onderdeel Scannen vanuit contextmenu

Het tracebestand shelllex.dll.log bevat naast de algemene informatie ook informatie over de voltooiing van de scantaak en benodigde gegevens voor de probleemoplossing van het programma.

## Inhoud van tracebestanden van de webplug-in van het programma

Tracebestanden van de webplug-in van het programma worden in de map Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs opgeslagen op de computer waarop de Webconsole van Kaspersky Security Center is geïmplementeerd.

Tracebestanden van de webplug-in van het programma krijgen de volgende naam: logs-kes\_windows-<type tracebestand>.DESKTOP-<datum van bestandsupdate>.log. Webconsole begint na de installatie gegevens te schrijven en verwijdert de tracebestanden wanneer deze wordt verwijderd.

Tracebestanden van de webplug-in van het programma bevatten naast de algemene gegevens ook de volgende informatie:

- Wachtwoord van de KLAdmin-gebruiker voor de ontgrendeling van de Kaspersky Endpoint Security-interface ([Wachtwoordbeveiliging](#)).
- Tijdelijk wachtwoord voor de ontgrendeling van de Kaspersky Endpoint Security-interface ([Wachtwoordbeveiliging](#)).
- Gebruikersnaam en wachtwoord voor de SMTP-server ([E-mailmeldingen](#)).
- Gebruikersnaam en wachtwoord voor de internetproxyserver ([Proxyserver](#)).
- Gebruikersnaam en wachtwoord voor de taak [Programmaonderdelen wijzigen](#).
- Accountgegevens en paden die zijn opgegeven in Kaspersky Endpoint Security-taken en beleidseigenschappen.

## Inhoud van het tracebestand van Authenticatie-agent

Het tracebestand van Authenticatie-agent is in de map met informatie over systeemvolumes opgeslagen en heeft de volgende naam: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.

Naast de algemene gegevens bevat het tracebestand van Authenticatie-agent ook gegevens over de werking van Authenticatie-agent en de acties die de gebruiker met Authenticatie-agent uitvoert.

# Tracing van programmawerking

*Programmatracing* is een gedetailleerde record van de acties die door het programma zijn uitgevoerd en van berichten over gebeurtenissen tijdens de werking van het programma.

Programmatracing moet onder toezicht van de Technische Support van Kaspersky worden uitgevoerd.

*Zo maakt u een bestand met programmatraces aan:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Klik in het venster op de knop **Tools voor ondersteuning**.
3. Gebruik de schakelaar **Programmatracing inschakelen** om de tracing van de programmawerking in of uit te schakelen.
4. Selecteer in de vervolgkeuzelijst **Tracing** een modus voor de tracing van het programma:
  - **Met rotatie**. Sla traces op als een beperkt aantal bestanden met een beperkte grootte en overschrijf de oudere bestanden wanneer de maximale grootte wordt bereikt. Als deze modus is geselecteerd, dan kunt u het maximale aantal bestanden voor rotatie en de maximale grootte voor elk bestand definiëren.
  - **Schrijven naar een enkel bestand**. Sla één tracebestand op (geen maximale grootte).
5. Selecteer in de vervolgkeuzelijst **Niveau** het tracingniveau:  
U wordt aanbevolen om het vereiste tracingniveau met een expert van de Technische Support te bespreken. Zonder begeleiding van de Technische Support stelt u het traceniveau in op **Normaal (500)**.
6. Herstart Kaspersky Endpoint Security.
7. Om het traceringsproces te stoppen, keert u terug naar het venster **Tools voor ondersteuning** en schakelt u tractering uit.

U kunt ook tracebestanden maken wanneer u het programma vanaf de [opdrachtregel](#) installeert, inclusief met het [bestand setup.ini](#).

Hierdoor wordt een prestatietracebestand in de map %ProgramData%\Kaspersky Lab\KES\Traces gemaakt. Nadat het tracebestand is aangemaakt, verstuurt u het bestand naar de Technische Support van Kaspersky.


Kaspersky Endpoint Security verwijdert automatisch tracebestanden wanneer het programma wordt verwijderd. U kunt de bestanden ook handmatig verwijderen. Hiervoor moet u tracing uitschakelen en [het programma stoppen](#).

## Tracing van programmaprestaties

Met Kaspersky Endpoint Security kunt u informatie over problemen in de werking van de computer krijgen wanneer u het programma gebruikt. U kunt bijvoorbeeld informatie krijgen over vertragingen in het laden van het besturingssysteem nadat het programma is geïnstalleerd. Hiervoor maakt Kaspersky Endpoint Security [tracebestanden over de prestaties](#). Onder *prestatietracing* verstaan we de registratie van acties die door het programma worden uitgevoerd om problemen met de werking van Kaspersky Endpoint Security te analyseren. Voor het ontvangen van deze informatie gebruikt Kaspersky Endpoint Security de service Gebeurtenistracering voor Windows. De Technische Support van Kaspersky is verantwoordelijk voor het analyseren van problemen met Kaspersky Endpoint Security en het achterhalen van de oorzaak van die problemen.

Programmatracing moet onder toezicht van de Technische Support van Kaspersky worden uitgevoerd.

*Zo maakt u een bestand met prestatietraces aan:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Klik in het venster op de knop **Tools voor ondersteuning**.
3. Gebruik de schakelaar **Prestatietracing inschakelen** om het traceren van programmaprestaties in of uit te schakelen.
4. Selecteer in de vervolgkeuzelijst **Tracing** een modus voor de tracing van het programma:
  - **Met rotatie**. Sla traces op als een beperkt aantal bestanden met een beperkte grootte en overschrijf de oudere bestanden wanneer de maximale grootte wordt bereikt. Als deze modus is geselecteerd, kunt u de maximale grootte voor elk bestand definiëren.
  - **Schrijven naar een enkel bestand**. Sla één tracebestand op (geen maximale grootte).
5. Selecteer in de vervolgkeuzelijst **Niveau** het tracingniveau:
  - **Oppervlakkig**. Kaspersky Endpoint Security analyseert de belangrijkste processen van het besturingssysteem die zijn gerelateerd aan prestaties.
  - **Gedetailleerd**. Kaspersky Endpoint Security analyseert alle processen van het besturingssysteem die zijn gerelateerd aan prestaties.
6. Selecteer in de vervolgkeuzelijst **Type tracing** het type tracing:
  - **Basisinformatie**. Kaspersky Endpoint Security analyseert processen wanneer het besturingssysteem actief is. Gebruik dit type tracing als een probleem aanhoudt nadat het besturingssysteem is geladen, zoals een probleem met de toegang tot internet in de browser.
  - **Bij opnieuw opstarten**. Kaspersky Endpoint Security analyseert processen wanneer het besturingssysteem wordt geladen. Nadat het besturingssysteem is geladen, stopt Kaspersky Endpoint Security de tracing. Gebruik dit type tracing als het probleem te maken heeft met het vertraagd laden van het besturingssysteem.
7. Start de computer opnieuw op en probeer het probleem te reproduceren.
8. Om het traceringsproces te stoppen, keert u terug naar het venster **Tools voor ondersteuning** en schakelt u tracing uit.

Hierdoor wordt een prestatietracebestand in de map %ProgramData%\Kaspersky Lab\KES\Traces gemaakt. Nadat het tracebestand is aangemaakt, stuurt u het bestand naar de Technische Support van Kaspersky.


## Dump schrijven

Een dumpbestand bevat alle informatie over het werkgeheugen van Kaspersky Endpoint Security-processen op het moment dat het dumpbestand wordt aangemaakt.

Opgeslagen dumpbestanden bevatten mogelijk vertrouwelijke gegevens. U moet afzonderlijk de beveiliging verzekeren van dumpbestanden om toegang tot gegevens te controleren.

Dumpbestanden worden opslagen op de computer zolang het programma actief is en worden permanent verwijderd wanneer het programma wordt verwijderd. Dumpbestanden worden opgeslagen in de map %ProgramData%\Kaspersky Lab\KES\Traces.

*Zo schakelt u het schrijven naar een dump in en uit:*

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik in het blok **Foutopsporingsgegevens** het selectievakje **Schrijven naar dump inschakelen** om het schrijven van programma-dump in of uit te schakelen.
4. Sla uw wijzigingen op.


## Dump- en tracebestanden beschermen

Dump- en tracebestanden bevatten informatie over het besturingssysteem en bevatten mogelijk ook [gebruikersgegevens](#). 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. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Programma-instellingen** in het venster met de programma-instellingen.
3. Gebruik in het blok **Foutopsporingsgegevens** het selectievakje **Bescherming voor dump- en tracebestanden inschakelen** om bestandsbeveiliging in of uit te schakelen.
4. Sla uw wijzigingen op.

Dump- en tracebestanden waarnaar informatie is geschreven wanneer de bescherming actief was blijven zelfs na de uitschakeling van deze functie beschermd.

## Beperkingen en waarschuwingen

Kaspersky Endpoint Security heeft een aantal beperkingen die niet belangrijk zijn voor de werking van het programma.

[Het programma installeren](#) 

- Voor informatie over de ondersteuning voor Microsoft Windows 10, Microsoft Windows Server 2016 en Microsoft Windows Server 2019 raadpleegt u de [Knowledge Base van de Technische Support](#).
- Voor informatie over de ondersteuning voor Microsoft Windows Server 11 en Microsoft Windows Server 2022 raadpleegt u de [Knowledge Base van de Technische Support](#).
- Nadat het programma is geïnstalleerd op een geïnfecteerde computer, informeert het de gebruiker niet over de noodzaak om een computerscan uit te voeren. U kunt problemen ondervinden bij het [activeren van het programma](#). [Start een Kritieke Gebiedenscan](#) om deze problemen op te lossen.
- Als niet-ASCII-tekens (bijvoorbeeld Russische letters) worden gebruikt in de bestanden setup.ini en setup.reg, wordt u aangeraden het bestand te bewerken met notepad.exe en het bestand op te slaan in UTF-16LE-codering. Andere coderingen worden niet ondersteund.
- Het programma ondersteunt het gebruik van niet-ASCII-tekens niet bij het specificeren van het installatiepad van het programma in de [instellingen van het installatiepakket](#).
- Wanneer [programma-instellingen worden geïmporteerd uit een CFG-bestand](#), wordt de waarde van de instelling die deelname aan Kaspersky Security Network definieert, niet toegepast. Lees na het importeren van de instellingen de tekst van de Kaspersky Security Network-verklaring en bevestig uw toestemming voor deelname aan Kaspersky Security Network. U kunt de tekst van de verklaring lezen in de programma-interface of in het bestand ksn\_\*.txt in de map met de het distributiepakket van het programma.
- Als u de codering (FLE of FDE) of het onderdeel Apparaatbeheer wilt verwijderen en vervolgens opnieuw wilt installeren, moet u eerst het systeem opnieuw opstarten.
- Als u het Microsoft Windows 10-besturingssysteem gebruikt, moet u het systeem opnieuw opstarten nadat u het onderdeel File Level Encryption (FLE) hebt verwijderd.
- Wanneer u een versie van de AES Encryption Module probeert te installeren op een computer waarop Kaspersky Endpoint Security 11.9.0 voor Windows is geïnstalleerd, maar geen encryptieonderdelen, wordt de installatie van de Encryption Module beëindigd met een foutmelding dat er een nieuwere versie van het programma is geïnstalleerd. Vanaf Kaspersky Endpoint Security 10 voor Windows Service Pack 2 (versie 10.3.0.6294) is er geen afzonderlijk installatiebestand voor de Encryption Module. Encryptiebibliotheken maken deel uit van het distributiepakket van het programma. Kaspersky Endpoint Security 11.9.0 is incompatibel met AES-encryptiemodules. De vereiste bibliotheken voor de encryptiefunctie worden automatisch geïnstalleerd als Full Disk Encryption (FDE) of File Level Encryption (FLE) is geselecteerd.
- De installatie van het programma kan eindigen met de foutmelding dat er *een programma op uw computer is geïnstalleerd waarvan de naam ontbreekt of onleesbaar is*. Dit betekent dat incompatibele programma's of fragmenten daarvan op uw computer blijven staan. U kunt restanten van incompatibele programma's verwijderen door een verzoek met een gedetailleerde beschrijving van de situatie naar Kaspersky Technical Support te sturen via [Kaspersky CompanyAccount](#).
- Als u het verwijderen van het programma hebt geannuleerd, start u het herstel nadat de computer opnieuw is opgestart.
- Op computers met Windows 10 versie 1903 en 1909 kunnen upgrades van Kaspersky Endpoint Security 10 voor Windows Service Pack 2 Maintenance Release 3 (build 10.3.3.275), Service Pack 2 Maintenance Release 4 (build 10.3.3.304), 11.0.0 en 11.0.1 eindigen met een fout wanneer het onderdeel File Level Encryption (FLE) is geïnstalleerd. Dit komt doordat bestandsencryptie niet wordt ondersteund voor deze versies van Kaspersky Endpoint Security voor Windows in Windows 10 versie 1903 en 1909. Voordat u deze upgrade installeert, wordt u geadviseerd om [het onderdeel bestandsencryptie te verwijderen](#).
- Het programma vereist Microsoft .NET Framework 4.0 of hoger. Microsoft .NET Framework 4.6.1 bevat kwetsbaarheden. Als u Microsoft .NET Framework 4.6.1 gebruikt, moet u beveiligingsupdates installeren.

Voor informatie over Microsoft .NET Framework-beveiligingsupdates raadpleegt u de [Microsoft Ondersteuning-website](#).

- Als het programma niet wordt geïnstalleerd terwijl het onderdeel Kaspersky Endpoint Agent is geselecteerd in een serverbesturingssysteem en het venster *Windows Installer Coordinator Error* verschijnt, raadpleeg dan de instructies op de ondersteuningswebsite van Microsoft.
- Als het programma lokaal in niet-interactieve modus is geïnstalleerd, gebruikt u het meegeleverde [setup.ini-bestand](#) om de geïnstalleerde onderdelen te vervangen.
- Nadat Kaspersky Endpoint Security voor Windows is geïnstalleerd in sommige configuraties van Windows 7, blijft Windows Defender werken. U wordt geadviseerd om Windows Defender handmatig uit te schakelen om verminderde systeemprestaties te voorkomen.
- Als u het programma wilt installeren op computers met Windows 7 of Windows Server 2008 R2 waarop Veeam Backup & Replication-software is geïnstalleerd, moet u de computer mogelijk opnieuw opstarten en de installatie opnieuw uitvoeren.

[Het programma upgraden](#)



- Bij het upgraden vanaf Kaspersky Endpoint Security 10 voor Windows Service Pack 2 (build 10.3.0.6294), is [het onderdeel Host Intrusion Prevention ingeschakeld](#).
- Wanneer u Kaspersky Endpoint Security 10 voor Windows Service Pack 2 (build 10.3.0.6294) bijwerkt, worden de bestanden die in Back-up of Quarantaine zijn geplaatst door de vorige versie van het programma overgezet naar Back-up in de nieuwe versie van het programma. Deze bestanden worden niet overgezet voor eerdere versies dan Kaspersky Endpoint Security 10 voor Windows Service Pack 2 (build 10.3.0.6294). Om de bestanden op te slaan, moet u ze terugzetten vanuit Quarantaine en Back-up voordat u een upgrade uitvoert van het programma. Scan de teruggezette bestanden opnieuw nadat de upgrade is voltooid.
- Vanaf programmaversie 11.0.0 kunt u de MMC-plug-in Kaspersky Endpoint Security voor Windows installeren bovenop de vorige plug-inversie. Om terug te keren naar een vorige plug-inversie, verwijdert u de huidige plug-in en installeert u een eerdere versie van de plug-in.
- Bij het upgraden van Kaspersky Endpoint Security 11.0.0 of 11.0.1 voor Windows worden de [lokale instellingen voor taakplanning](#) voor de taken *Updaten*, *Kritieke Gebiedenscan*, *Aangepaste scan* en *Integriteitscontrole* niet opgeslagen.
- Op computers met Windows 10 versie 1903 en 1909 kunnen upgrades van Kaspersky Endpoint Security 10 voor Windows Service Pack 2 Maintenance Release 3 (build 10.3.3.275), Service Pack 2 Maintenance Release 4 (build 10.3.3.304), 11.0.0 en 11.0.1 eindigen met een fout wanneer het onderdeel File Level Encryption (FLE) is geïnstalleerd. Dit komt doordat bestandsencryptie niet wordt ondersteund voor deze versies van Kaspersky Endpoint Security voor Windows in Windows 10 versie 1903 en 1909. Voordat u deze upgrade installeert, wordt u geadviseerd om [het onderdeel bestandsencryptie te verwijderen](#).
- Het programma vereist Microsoft .NET Framework 4.0 of hoger. Microsoft .NET Framework 4.6.1 bevat kwetsbaarheden. Als u Microsoft .NET Framework 4.6.1 gebruikt, moet u beveiligingsupdates installeren. Voor informatie over Microsoft .NET Framework-beveiligingsupdates raadpleegt u de [Microsoft technische ondersteuningswebsite](#) <sup>2</sup>.
- Als u een eerdere versie van het programma upgradet naar versie 11.9.0 om Kaspersky Endpoint Agent te installeren, start u de computer opnieuw op en logt u in op het systeem met een account met lokale beheerdersrechten. Anders wordt Kaspersky Endpoint Agent niet geïnstalleerd tijdens de upgradeprocedure.
- Als u een upgrade uitvoert voor Kaspersky Endpoint Security 10 voor Windows Service Pack 2 Maintenance Release 4 met het component File Level Encryption (FLE) geïnstalleerd op computers met Windows 10 versie 1809, 1903 en 1909, worden er geen FDE-stuurprogramma's op de WinRE-image geïnstalleerd.
- Wanneer u een upgrade van Kaspersky Endpoint Security uitvoert, schakelt het programma het gebruik van KSN uit tot het Kaspersky Security Network-verklaring is aanvaard. Daarnaast kan de computerstatus worden veranderd naar *Essentieel* in Kaspersky Security Center; de gebeurtenis *KSN-servers niet beschikbaar* wordt ontvangen. Als u [Kaspersky Managed Detection and Response](#) gebruikt, ontvangt u gebeurtenissen over schendingen in de werking van de oplossing. Het gebruik van KSN is vereist voor de werking van Kaspersky Managed Detection and Response. Kaspersky Endpoint Security [schakelt het gebruik in van KSN](#) na het toepassen van het beleid waarin de beheerder de KSN-gebruiksvoorwaarden aanvaardt. Zodra de Kaspersky Security Network-verklaring is geaccepteerd, hervat Kaspersky Endpoint Security de werking.
- Nadat het programma is geüpgraded van eerdere versies dan Kaspersky Endpoint Security 11 voor Windows, moet de computer opnieuw worden opgestart.


- Het ReFS-bestandssysteem wordt ondersteund met beperkingen:
  - Kaspersky Endpoint Security kan gebeurtenissen over desinfecties van dreigingen onjuist verwerken. Als het programma bijvoorbeeld een schadelijk bestand heeft verwijderd, bevat het rapport mogelijk de vermelding 'Object niet verwerkt'. Tegelijk desinfecteert Kaspersky Endpoint Security dreigingen volgens de programma-instellingen. Kaspersky Endpoint Security kan ook een duplicaat van de gebeurtenis *Object wordt gedesinfecteerd bij herstart* maken voor hetzelfde object.
  - File Threat Protection kan ook bepaalde dreigingen overslaan. Tegelijk werkt Virusscan correct.
  - Nadat de antiviruscontrole van de server is gestart, worden scanuitsluitingen die met iChecker zijn toegevoegd, gereset wanneer de server opnieuw wordt opgestart.
  - De iSwift-technologie wordt niet ondersteund. Kaspersky Endpoint Security houdt geen rekening met scanuitzonderingen die met de iSwift-technologie zijn toegevoegd.
  - Kaspersky Endpoint Security detecteert bestanden van eicar.com en susp-eicar.com niet als het bestand meicar.exe op de computer bestond voordat Kaspersky Endpoint Security werd geïnstalleerd.
  - Kaspersky Endpoint Security kan meldingen over de desinfectie van dreigingen onjuist weergeven. Het programma kan bijvoorbeeld een melding over een dreiging weergeven voor een eerder gedesinfecteerde dreiging.
- File Level Encryption (FLE) en Kaspersky Disk Encryption (FDE)-technologieën worden niet ondersteund op serverplatforms. Tegelijk kan Kaspersky Endpoint Security gebeurtenissen over gegevensencryptie onjuist verwerken.
- In serverbesturingssystemen wordt geen waarschuwing weergegeven met betrekking tot de noodzaak van geavanceerde desinfectie.
- Microsoft Windows Server 2008 was uitgesloten van ondersteuning. - Het programma kan niet worden geïnstalleerd op een computer met het Microsoft Windows Server 2008-besturingssysteem.
- De Core-modus wordt ondersteund met beperkingen:
  - De lokale grafische gebruikersinterface is niet beschikbaar, inclusief meldingen, pop-upmeldingen en andere interfacebesturingselementen. De toepassing kan geen promptvensters weergeven, inclusief de volgende vensters:
    - Bevestigingsprompt voor programmaversie en module-upgrade;
    - Herstart van computer vereist;
    - Vragen om authenticatiegegevens voor de proxyserver.
    - Vragen om toegang tot een apparaat (Apparaatcontrole).
  - De volgende onderdelen zijn niet beschikbaar: Web Threat Protection, Mail Threat Protection, Webcontrole, BadUSB Attack Prevention.
  - Anti-Bridging is niet beschikbaar.
  - U kunt de Kaspersky Security Network-verklaring alleen accepteren in het programmabeleid in de Kaspersky Security Center-console.

- BitLocker-stationsversleuteling is alleen beschikbaar met een Trusted Platform Module (TPM). Een pincode/wachtwoord kan niet worden gebruikt voor encryptie, omdat het programma het wachtwoordpromptvenster voor preboot-authenticatie niet kan weergeven. Als het besturingssysteem de compatibiliteitsmodus Federal Information Processing Standard (FIPS) heeft ingeschakeld, sluit dan een verwisselbare schijf aan om de encryptiesleutel op te slaan voordat u begint met het coderen van de schijf.

### [Ondersteunde virtuele platforms](#)

- Full Disk Encryption (FDE) wordt op virtuele Hyper-V-computers niet ondersteund.
- Full Disk Encryption (FDE) wordt niet ondersteund op virtuele Citrix-platforms.
- Windows 10 Enterprise multi-sessie wordt ondersteund met beperkingen:
  - Kaspersky Endpoint Security desinfecteert actieve dreigingen zonder de gebruiker op de hoogte te stellen, net zoals bij het [desinfecteren van actieve dreigingen op servers](#). Omdat het besturingssysteem in de modus voor meerdere sessies blijft draaien, kunnen andere actieve gebruikers hun gegevens verliezen als de dreiging niet onmiddellijk wordt opgelost.
  - Full disk encryption (FDE) wordt niet ondersteund.
  - Het beheer van BitLocker wordt niet ondersteund.
  - Het gebruik van Kaspersky Endpoint Security met verwisselbare schijven wordt niet ondersteund. De Microsoft Azure-infrastructuur definieert verwisselbare schijven als netwerkschijven.
- Full Disk Encryption (FDE) en File Level Encryption (FLE) worden niet ondersteund op virtuele Citrix-platforms.
- Om Kaspersky Endpoint Security voor Windows compatibel te maken met Citrix PVS, voert u de installatie uit terwijl de optie [Controleer de compatibiliteit met Citrix PVS is ingeschakeld](#). Deze optie kunt u inschakelen in de [installatiewizard](#) of met de [opdrachtregelparameter](#) /pCITRIXCOMPATIBILITY=1. Bij een installatie op afstand moet het [KUD-bestand](#) worden bewerkt door de volgende parameter toe te voegen: /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop. Voordat u begint met klonen, moet [Zelfbescherming uitschakelen](#) om virtuele machines te klonen die vDisk gebruiken.
- Wanneer u een sjabloonmachine voorbereidt voor de Citrix XenDesktop-masterimage met vooraf geïnstalleerde Kaspersky Endpoint Security voor Windows en Kaspersky Security Center-netwerkagent, voegt u de volgende soorten uitzonderingen toe aan het configuratiebestand:
 

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Bezoek de [Citrix Support-website](#)  voor meer informatie over Citrix XenDesktop.
- In sommige gevallen kan een poging om een verwisselbare schijf veilig los te koppelen, mislukken op een virtuele machine die is geïmplementeerd op een VMware ESXi-hypervisor. Probeer het apparaat nogmaals veilig los te koppelen.

## [Compatibiliteit met kaspersky security center](#)

- Het onderdeel 'Adaptieve controle op afwijkingen' kan alleen via Kaspersky Security Center versie 11 of later worden beheerd.
- Het dreigingsrapport van Kaspersky Security Center 11 geeft mogelijk geen informatie weer over de actie die is ondernomen tegen dreigingen die door de AMSI-bescherming zijn gedetecteerd.
- De bedrijfsstatus van de onderdelen AMSI-bescherming en Adaptieve controle op afwijkingen is alleen beschikbaar in Kaspersky Security Center versie 11 of later. U kunt de bedrijfsstatus bekijken in de Kaspersky Security Center Console in de computereigenschappen in het gedeelte **Taken**. Rapporten voor deze componenten zijn ook alleen beschikbaar in Kaspersky Security Center versie 11 of hoger.

## Licentiebeheer

- Als het systeembericht *Fout bij ontvangst van gegevens* wordt weergegeven, controleert u of de computer waarop u activering uitvoert netwerktoegang heeft, of configureer de activeringsinstellingen via Kaspersky Security Center-activeringsproxy.
- Het programma kan niet worden geactiveerd door abonnement via het Kaspersky Security Center als de licentie is verlopen of als er een evaluatielicentie actief is op de computer. Wanneer u een evaluatielicentie of een nog maar beperkt geldige licentie wilt vervangen door een abonnementslicentie, [gebruikt u de taak voor licentiedistributie](#).
- In de programma-interface wordt de vervaldatum van de licentie weergegeven in de lokale tijd van de computer.
- Installatie van het programma met een ingesloten-licentiebestand op een computer met instabiele internettoegang kan resulteren in de tijdelijke weergave van gebeurtenissen die aangeven dat het programma niet is geactiveerd of dat de licentie de werking van onderdelen niet toestaat. Dit komt doordat het programma eerst de ingesloten evaluatielicentie installeert en probeert te activeren, en deze evaluatielicentie vereist internettoegang voor activering tijdens de installatieprocedure.
- Tijdens de proefperiode kan de installatie van een programma-upgrade of patch op een computer met instabiele internettoegang resulteren in de tijdelijke weergave van gebeurtenissen die aangeven dat het programma niet is geactiveerd. Dit komt doordat het programma opnieuw de ingesloten evaluatielicentie installeert en probeert te activeren, en deze evaluatielicentie vereist internettoegang voor activering bij het installeren van een upgrade.
- Als de evaluatielicentie automatisch is geactiveerd tijdens de installatie van het programma en vervolgens het programma is verwijderd zonder de licentiegegevens op te slaan, wordt het programma niet automatisch geactiveerd met de evaluatielicentie wanneer het opnieuw wordt geïnstalleerd. Activeer in dat geval het programma handmatig.
- Als u Kaspersky Security Center versie 11 en Kaspersky Endpoint Security versie 11.9.0 gebruikt, werken prestatierapporten van componenten mogelijk niet correct. Als u Kaspersky Endpoint Security-onderdelen hebt geïnstalleerd die niet in uw licentie zijn opgenomen, dan kan Network Agent statusfouten naar het Windows-gebeurtenislogboek sturen. Verwijder om fouten te vermijden de onderdelen die niet in uw licentie zijn opgenomen.

## Remediation Engine

- Het programma herstelt alleen bestanden op apparaten met een NTFS- of FAT32-bestandssysteem.
- Het programma kan bestanden met de volgende extensies herstellen: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls,xlsx, xlsx, xlsx, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srf, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Bestanden op netwerkschijven of op herschrijfbare cd's/dvd's kunnen niet worden hersteld.
- Bestanden die zijn geëncrypt met Encryption File System (EFS) kunnen niet worden hersteld. Voor meer informatie over de werking van EFS gaat u naar de [website van Microsoft](#).
- Het programma bewaakt geen wijzigingen aan bestanden die door processen op het niveau van de kernel van het besturingssysteem worden gemaakt.
- Het programma bewaakt geen wijzigingen aan bestanden die via een netwerkinterface worden gemaakt (bijvoorbeeld: een bestand is opgeslagen in een gedeelde map en een proces wordt op afstand gestart vanaf een andere computer).

## Firewall

- Filtratie van pakketten of verbindingen op lokaal adres, fysieke interface en packet-time-to-live (TTL) wordt ondersteund in de volgende gevallen:
  - Op lokaal adres voor uitgaande pakketten of verbindingen in programmaregels voor TCP en UDP en pakketregels.
  - Op lokaal adres voor inkomende pakketten of verbindingen (behalve UDP) in blokprogrammaregels en pakketregels.
  - Op packet-time-to-live (TTL) in blokpakketregels voor inkomende of uitgaande pakketten.
  - Via de netwerkinterface voor inkomende en uitgaande pakketten of verbindingen in pakketregels.
- In programmaversies 11.0.0 en 11.0.1 worden de gedefinieerde MAC-adressen onjuist toegepast. De MAC-adresinstellingen voor versie 11.0.0, 11.0.1 en 11.1.0 of hoger zijn niet compatibel. Na het upgraden van het programma of de plug-in van deze versies naar versie 11.1.0 of hoger, moet u de gedefinieerde MAC-adressen in Firewall-regels controleren en opnieuw configureren.
- Bij het upgraden van het programma van versie 11.1.1 en 11.2.0 naar versie 11.9.0, worden de statussen van machtigingen voor de volgende firewallregels niet gemigreerd:
  - Verzoeken aan DNS-server via TCP.
  - Verzoeken aan DNS-server via UDP.
  - Elke netwerkactiviteit.
  - ICMP-bestemming: onbereikbare inkomende reacties.
  - Inkomende ICMP-stream.
- Als u een netwerkadapter of pakket time to live (TTL) hebt geconfigureerd voor een toegestane pakketregel, dan is de prioriteit van deze regel lager dan die van een blokkerende programmaregel. Als netwerkactiviteit met andere woorden geblokkeerd is voor een programma (het programma bevindt zich bijvoorbeeld in de vertrouwensgroep *Zeer beperkt*), dan kunt u geen netwerkactiviteit van het programma toestaan door een pakketregel met deze instellingen te gebruiken. In alle andere gevallen is de prioriteit van een pakketregel hoger dan die van een programmanetwerkregel.
- Wanneer [Firewall-pakketregels worden geïmporteerd](#), kan Kaspersky Endpoint Security de regelnamen aanpassen. Het programma bepaalt regels met identieke sets van algemene parameters: protocol, regels, externe en lokale poorten, time-to-live (TTL) van pakketten. Als deze set algemene parameters identiek is voor meerdere regels, dan wijst het programma dezelfde naam toe aan deze regels of voegt het een parametertag toe aan de naam. Op deze manier importeert Kaspersky Endpoint Security alle pakketregels, maar de naam van regels met identieke algemene instellingen kan worden gewijzigd.
- Als u [rapportage van gebeurtenissen hebt ingeschakeld in een netwerkregel](#), bij het verplaatsen van het programma naar een andere vertrouwensgroep, worden de beperkingen van deze vertrouwensgroep niet toegepast. Als de toepassing zich dus in de vertrouwde vertrouwensgroep bevindt, heeft deze geen netwerkbeperkingen. Vervolgens hebt u gebeurtenisrapportage voor dit programma ingeschakeld en verplaatst naar de niet-vertrouwde vertrouwensgroep. Firewall legt geen netwerkbeperkingen op voor deze toepassing. We raden u aan het programma eerst naar de juiste vertrouwensgroep te verplaatsen en vervolgens gebeurtenisrapportage in te schakelen. Als deze methode niet geschikt is, kunt u handmatig beperkingen voor het programma configureren in de netwerkregelinstellingen. De beperking is alleen van toepassing op de lokale interface van het programma. Het verplaatsen van de toepassing tussen vertrouwensgroepen in het beleid werkt correct.

- De onderdelen Firewall en Intrusion Prevention hebben gemeenschappelijke instellingen: programmarechten en beschermde bronnen. Als u deze instellingen voor Firewall wijzigt, past Kaspersky Endpoint Security automatisch de nieuwe instellingen toe op intrusiepreventie. Als u bijvoorbeeld wijzigingen in de algemene instellingen van het Firewall-beleid hebt toegestaan (het hangslot is open), worden de instellingen voor intrusiepreventie ook bewerkbaar.
- Wanneer een [netwerkpakketregel](#) wordt geactiveerd in Kaspersky Endpoint Security 11.6.0 of eerder, geeft de kolom **Programmanaam** in het firewallrapport altijd de *Kaspersky Endpoint Security*-waarde weer. Daarnaast blokkeert de firewall de verbinding op pakketniveau voor alle programma's. Dit gedrag is gewijzigd voor Kaspersky Endpoint Security 11.7.0 of hoger. De kolom **Type regel** is toegevoegd aan het [firewallrapport](#). Wanneer een netwerkpakketregel wordt geactiveerd, blijft de kolom **Programmanaam** leeg.

## [BadUSB Attack Prevention](#)

- Kaspersky Endpoint Security stelt de time-out voor de vergrendeling van USB-apparaten opnieuw in wanneer de computer wordt vergrendeld (bijvoorbeeld na de time-out voor de schermvergrendeling). Als u dus meermaals een verkeerde autorisatiecode voor het USB-apparaat invoert waardoor het USB-apparaat wordt vergrendeld door het programma, kunt u met Kaspersky Endpoint Security de autorisatiepoging herhalen nadat u de computer hebt ontgrendeld. In dit geval wordt het USB-apparaat niet door Kaspersky Endpoint Security vergrendeld gedurende de opgegeven tijd in [Instellingen van het onderdeel BadUSB Attack Prevention](#).
- Kaspersky Endpoint Security stelt de time-out voor de vergrendeling van USB-apparaten opnieuw in wanneer de [computerbescherming wordt gepauzeerd](#). Als u dus meermaals een verkeerde autorisatiecode voor het USB-apparaat invoert waardoor het USB-apparaat wordt vergrendeld door het programma, kunt u met Kaspersky Endpoint Security de autorisatiepoging herhalen nadat u [de computerbescherming hebt hervat](#). In dit geval wordt het USB-apparaat niet door Kaspersky Endpoint Security vergrendeld gedurende de opgegeven tijd in [Instellingen van het onderdeel BadUSB Attack Prevention](#).

## [Programmacontrole](#)



- Alleen ZIP-archieven van minder dan 104 MB worden ondersteund tijdens het beheren van de regels van Programmacontrole in de Kaspersky Security Center-webconsole. Archieven in andere formaten, zoals RAR of 7z, worden niet ondersteund. Deze beperking bestaat niet als u met Programmacontrole-regels werkt in de Beheerconsole (MMC).
- Bij het werken in Microsoft Windows 10 in de modus denylist, kunnen blokkeringsregels onjuist worden toegepast waardoor programma's kunnen worden geblokkeerd die niet in regels zijn gespecificeerd.
- Wanneer progressieve web-apps (PWA) worden geblokkeerd door het onderdeel Programmacontrole, wordt appManifest.xml in het rapport aangegeven als de geblokkeerde app.
- Wanneer u de standaard Notepad-toepassing toevoegt aan een regel van programmacontrole voor Windows 11, is het niet aanbevolen om het pad naar het programma op te geven. Op computers met Windows 11 gebruikt het besturingssysteem Metro Notepad in de map C:\Program Files\WindowsApps\Microsoft.WindowsNotepad\*\Notepad\Notepad.exe. In eerdere versies van het besturingssysteem bevindt Notepad zich in de volgende mappen:
  - C:\Windows\notepad.exe
  - C:\Windows\System32\notepad.exe
  - C:\Windows\SysWOW64\notepad.exe

Wanneer u Notepad toevoegt aan een regel van programmacontrole, kunt u bijvoorbeeld de programmaam en de bestandshash specificeren vanuit de eigenschappen van het actieve programma.

## Apparaatcontrole

- De toegang tot printerapparaten die aan de vertrouwde lijst zijn toegevoegd, wordt geblokkeerd door blokkeringsregels voor apparaten en bussen.
- Voor MTP-apparaten wordt de controle van lees-, schrijf- en verbindingbewerkingen ondersteund als u de ingebouwde Microsoft-stuurprogramma's van het besturingssysteem gebruikt. Als een gebruiker een aangepast stuurprogramma installeert om met een apparaat te werken (bijvoorbeeld als onderdeel van iTunes of Android Debug Bridge), werkt de controle van de lees- en schrijfbewerkingen mogelijk niet.
- Wanneer u met MTP-apparaten werkt, worden de toegangsregels gewijzigd nadat het apparaat opnieuw is aangesloten.
- Het onderdeel Apparaatbeheer registreert gebeurtenissen die verband houden met bewaakte apparaten, zoals het verbinden van een apparaat en het verbreken van de verbinding met een apparaat, het lezen van een bestand van een apparaat, het schrijven van een bestand naar een apparaat en andere gebeurtenissen. Kaspersky Endpoint Security registreert evenementen voor verbroken-verbindingen alleen voor de volgende apparaattypes: Draagbare apparaten (MTP), Verwisselbare schijven, Diskettes, Cd-/dvd-stations. Voor andere apparaattypes registreert het programma evenementen voor verbroken-verbindingen niet. Het programma registreert de actie van het verbinden van een apparaat met de computer voor alle apparaattypes.
- Als u een apparaat aan de vertrouwde lijst toevoegt op basis van een modelmasker en tekens gebruikt die in de ID zijn opgenomen, maar niet in de modelnaam, worden deze apparaten niet toegevoegd. Op een werkstation worden deze apparaten op basis van een ID-masker toegevoegd aan de vertrouwde lijst.

## Webcontrole

- De indelingen OGV en WEBM worden niet ondersteund.
- Het RTMP-protocol wordt niet ondersteund.

## Adaptieve controle op afwijkingen

- Het wordt aanbevolen om automatisch uitsluitingen aan te maken op basis van de gebeurtenis. Wanneer u [handmatig een uitzondering](#) toevoegt, voegt u het `*`-teken toe aan het begin van het pad wanneer u het doelobject specificeert.
- Er kan [geen rapport met regels voor Adaptieve controle op afwijkingen worden gegenereerd](#) als de steekproef ook maar één gebeurtenis bevat waarvan de naam meer dan 260 tekens bevat.
- Uitzonderingen toevoegen vanuit de adaptieve controle op afwijkingen triggeren van regels-opslagplaats wordt niet ondersteund als de eigenschappen van een object of proces een waarde hebben die uit meer dan 256 tekens bestaat (bijvoorbeeld pad naar doelobject). U kunt handmatig [een uitzondering toevoegen in de beleidsinstellingen](#). U kunt ook een uitzondering toevoegen in het [rapport over getriggerde regels voor adaptieve controle op afwijkingen](#).

## Drive Encryption (FDE)

- Nadat u het programma hebt geïnstalleerd, moet u het besturingssysteem opnieuw opstarten om te zorgen dat encryptie van de harde schijf correct werkt.
- De Authenticatie-agent ondersteunt geen hiërogliefen of de speciale tekens `|` en `\`.
- Voor optimale computerprestaties na encryptie is het vereist dat de processor de AES-NI-instructieset ondersteunt (Intel Advanced Encryption Standard New Instructions). Als de processor AES-NI niet ondersteunt, kunnen de computerprestaties afnemen.
- Wanneer er processen zijn die proberen toegang te krijgen tot geëncrypte apparaten voordat het programma toegang tot dergelijke apparaten heeft verleend, geeft het programma een waarschuwing weer waarin staat dat dergelijke processen moeten worden beëindigd. Als de processen niet kunnen worden beëindigd, sluit u de gecodeerde apparaten opnieuw aan.
- De unieke ID's van harde schijven worden in geïnverteerde indeling weergegeven in de statistieken van apparaatencryptie.
- Het wordt niet aanbevolen om apparaten te formatteren terwijl ze van encryptie worden voorzien.
- Wanneer meerdere verwisselbare schijven tegelijkertijd op een computer zijn aangesloten, kan het encryptiebeleid maar op één verwisselbare schijf worden toegepast. Wanneer de verwijderbare apparaten opnieuw worden aangesloten, wordt het encryptiebeleid correct toegepast.
- De encryptie start mogelijk niet op een sterk gefragmenteerde harde schijf. Defragmenteer de harde schijf.
- Wanneer harde schijven van encryptie zijn voorzien, wordt de slaapstand geblokkeerd vanaf het moment dat de encryptietaak begint tot de eerste herstart van een computer met Microsoft Windows 7/8/8.1/10, en na installatie van encryptie van de harde schijf tot de eerste herstart van Microsoft Windows 8 /8.1/10. Wanneer harde schijven worden gedecrypt, wordt de slaapstand geblokkeerd vanaf het moment dat de opstartschijf volledig is gedecrypt tot de eerste herstart van het besturingssysteem. Als de optie **Snelle start** is ingeschakeld in Microsoft Windows 8/8.1/10, voorkomt het blokkeren van de slaapstand dat u het besturingssysteem afsluit.
- Windows 7-computers staan het wijzigen van het wachtwoord tijdens het herstel niet toe wanneer de schijf versleuteld is met BitLocker-technologie. Na het invoeren van de herstelsleutel en het laden van het besturingssysteem, vraagt Kaspersky Endpoint Security de gebruiker om het wachtwoord of de pincode te wijzigen. Het is dus onmogelijk om een nieuw wachtwoord of een pincode in te stellen. Dit probleem komt voort vanuit de specifieke kenmerken van het besturingssysteem. Om door te gaan, moet u de harde schijf opnieuw encrypten.
- Het wordt niet aanbevolen om de tool xbootmgr.exe te gebruiken als aanvullende providers zijn ingeschakeld. Bijvoorbeeld Dispatcher, Network of Drivers.
- Het formatteren van een geëncrypte verwisselbare schijf wordt niet ondersteund op een computer waarop Kaspersky Endpoint Security voor Windows is geïnstalleerd.
- Het formatteren van een geëncrypte verwisselbare schijf met het FAT32-bestandssysteem wordt niet ondersteund (de schijf wordt weergegeven als geëncrypt). Als u een schijf wilt formatteren, formatteert u deze opnieuw naar het NTFS-bestandssysteem.
- Voor details over het terugzetten van een besturingssysteem vanaf een reservekopie naar een geëncrypt GPT-apparaat, gaat u naar de [Technical Support Knowledge Base](#).
- Er kunnen niet meerdere downloadagents naast elkaar bestaan op één geëncrypte computer.

- Het is onmogelijk om toegang te krijgen tot een verwisselbare schijf die eerder op een andere computer van encryptie is voorzien als aan alle volgende voorwaarden wordt voldaan:
  - Er is geen verbinding met de Kaspersky Security Center-server.
  - De gebruiker probeert te autoriseren met een nieuw token of wachtwoord.

Start de computer opnieuw op als een vergelijkbare situatie zich voordoet. Nadat de computer opnieuw is opgestart, krijgt u toegang tot de geëncrypte verwisselbare schijf.

- Het detecteren van USB-apparaten door de Authenticatie-agent wordt mogelijk niet ondersteund wanneer xHCI-modus voor USB is ingeschakeld in de BIOS-instellingen.
- Kaspersky Disk Encryption (FDE) voor het SSD-gedeelte van een apparaat dat wordt gebruikt voor het cachen van de meest gebruikte gegevens, wordt niet ondersteund voor SSHD-apparaten.
- Encryptie van harde schijven in 32-bits Microsoft Windows 8/8.1/10-besturingssystemen die in UEFI-modus worden uitgevoerd, wordt niet ondersteund.
- Start de computer opnieuw op voordat u een gedecrypte harde schijf opnieuw versleuteld.
- De encryptie van de harde schijf is niet compatibel met Kaspersky Anti-Virus voor UEFI. Het wordt niet aanbevolen om encryptie van de harde schijf te gebruiken op computers waarop Kaspersky Anti-Virus for UEFI is geïnstalleerd.
- [Het maken van accounts voor Authenticatie-agent](#) op basis van Microsoft-accounts wordt ondersteund met de volgende beperkingen:
  - [Single Sign-On](#)-technologie wordt niet ondersteund.
  - Het automatisch maken van accounts voor Authenticatie-agent wordt niet ondersteund als de optie is geselecteerd om accounts te maken voor gebruikers die zich de afgelopen N dagen bij het systeem hebben aangemeld.
- Als de naam van een account voor Authenticatie-agent de indeling <domain>/<Windows-accountnaam> heeft, moet u na het wijzigen van de computernaam ook de namen wijzigen van accounts die zijn gemaakt voor lokale gebruikers van deze computer. Stel bijvoorbeeld dat er een lokale gebruiker genaamd Ivanov op de Ivanov-computer is en dat er een account voor Authenticatie-agent met de naam Ivanov/Ivanov is gemaakt voor deze gebruiker. Als de computernaam Ivanov wordt gewijzigd in Ivanov-PC, moet u de naam van het account voor Authenticatie-agent voor de gebruiker Ivanov wijzigen van Ivanov/Ivanov in Ivanov-PC/Ivanov. U kunt de accountnaam wijzigen met behulp van de lokale accountbeheertaak van de authenticatieagent. Voordat de naam van het account is gewijzigd, is authenticatie in de preboot-omgeving mogelijk met de oude naam (bijvoorbeeld Ivanov/Ivanov).
- Als een gebruiker alleen met een token toegang heeft tot een computer die van encryptie is voorzien met Kaspersky Disk Encryption-technologie en deze gebruiker de procedure voor toegangsherstel moet uitvoeren, zorg er dan voor dat deze gebruiker wachtwoordgebaseerde toegang tot deze computer krijgt nadat toegang tot de geëncrypte computer is hersteld. Het wachtwoord dat de gebruiker heeft ingesteld bij het herstellen van de toegang, wordt mogelijk niet opgeslagen. In dat geval moet de gebruiker de procedure om de toegang tot de geëncrypte computer te herstellen, opnieuw uitvoeren wanneer de computer opnieuw wordt opgestart.
- Bij het decrypten van een harde schijf met de [FDE Recovery Tool](#), kan het decoderingsproces eindigen met een fout als gegevens op het bronapparaat worden overschreven door geëncrypte gegevens. Een deel van de gegevens op de harde schijf blijft geëncrypt. Het wordt aanbevolen om de optie te kiezen om geëncrypte gegevens op te slaan in een bestand in de decryptie-instellingen van het apparaat wanneer u de FDE Recovery Tool gebruikt.

- Als het wachtwoord van de Authenticatie-agent is gewijzigd, wordt een bericht met de tekst *Uw wachtwoord is gewijzigd weergegeven*. Klik op *OK* verschijnt en de gebruiker start de computer opnieuw op. Het nieuwe wachtwoord wordt niet opgeslagen. Het oude wachtwoord moet worden gebruikt voor latere authenticatie in de preboot-omgeving.
- Schijfencryptie is niet compatibel met Intel Rapid Start-technologie.
- Schijfencryptie is niet compatibel met ExpressCache-technologie.
- In sommige gevallen, wanneer wordt geprobeerd een geëncrypte harde schijf te decrypten met behulp van de [FDE Recovery Tool](#), detecteert de tool de apparaatstatus foutief als 'niet-geëncrypt' nadat de 'Request-Response'-procedure is voltooid. Het logboek van de tool bevat een gebeurtenis waarin staat dat de decryptie van het apparaat met succes is uitgevoerd. In dat geval moet u de gegevensherstelprocedure opnieuw starten om het apparaat te decrypten.
- Nadat de Kaspersky Endpoint Security voor Windows-plug-in is bijgewerkt in de Webconsole, tonen de eigenschappen van de clientcomputer de BitLocker-herstelsleutel pas als de Web Console-service opnieuw is gestart.
- Voor de overige beperkingen van ondersteuning voor volledige schijfencryptie en een lijst met apparaten waarvoor encryptie van harde schijven met beperkingen wordt ondersteund, raadpleegt u de [Knowledge Base van de Technische Support](#).

## [File Level Encryption \(FLE\)](#)

- Encryptie van bestanden en mappen wordt niet ondersteund in besturingssystemen van de Microsoft Windows Embedded-familie.
- Nadat u het programma hebt geïnstalleerd, moet u het besturingssysteem opnieuw opstarten om te zorgen dat de encryptie van bestanden en mappen correct werkt.
- Als een geëncrypt bestand is opgeslagen op een computer met beschikbare encryptiefunctie en u het bestand opent vanaf een computer waarop geen encryptie beschikbaar is, krijgt u direct toegang tot dit bestand. Een geëncrypt bestand dat is opgeslagen in een netwerkmap op een computer met beschikbare encryptiefunctie, wordt in geëncrypte vorm gekopieerd naar een computer die geen beschikbare encryptiefunctie heeft.
- U wordt aangeraden om bestanden te decrypten die van encryptie zijn voorzien met Encrypting File System voordat u bestanden van encryptie voorziet met Kaspersky Endpoint Security voor Windows.
- Wanneer een bestand versleuteld is, neemt de grootte toe met 4 kB.
- Nadat een bestand is van encryptie voorzien, wordt het kenmerk *Archief* ingesteld in de bestandseigenschappen.
- Als een uitgepakt bestand uit een versleuteld archief dezelfde naam heeft als een reeds bestaand bestand op uw computer, dan wordt het laatste bestand overschreven door het nieuwe bestand dat uit een versleuteld archief wordt uitgepakt. De gebruiker wordt niet op de hoogte gebracht van de overschrijfbewerking.
- Voordat u een versleuteld archief uitpakt, moet u ervoor zorgen dat u voldoende vrije schijfruimte hebt voor de uitgepakte bestanden. Als u niet genoeg schijfruimte hebt, kan het uitpakken van het archief voltooid zijn, maar kunnen de bestanden beschadigd zijn. In dit geval is het mogelijk dat Kaspersky Endpoint Security geen foutmeldingen weergeeft.
- De interface van [Portable bestandsbeheer](#) geeft geen berichten weer over fouten die optreden tijdens de werking.
- Kaspersky Endpoint Security voor Windows start [Portable bestandsbeheer](#) niet op een computer waarop het onderdeel File Level Encryption is geïnstalleerd.
- U kunt [Portable bestandsbeheer](#) niet gebruiken om toegang te krijgen tot een verwisselbare schijf als alle volgende voorwaarden waar zijn:
  - Er is geen verbinding met Kaspersky Security Center.
  - Kaspersky Endpoint Security voor Windows is op de computer geïnstalleerd.
  - Gegevensencryptie (FDE of FLE) is niet uitgevoerd op de computer.

Toegang is niet mogelijk, zelfs als u het wachtwoord voor Portable bestandsbeheer kent.

- Wanneer bestandsencryptie wordt gebruikt, is het programma niet compatibel met de Sylpheed-mailclient.
- Kaspersky Endpoint Security voor Windows ondersteunt [de regels van beperkte toegang tot geëncrypte bestanden](#) niet voor sommige programma's. Dit is te wijten aan het feit dat sommige bestandsbewerkingen worden uitgevoerd door een programma van derden. Het kopiëren van bestanden wordt bijvoorbeeld uitgevoerd door de bestandsbeheerder, niet door het programma zelf. Op deze manier zal Kaspersky Endpoint Security, als de Outlook-e-mailclient toegang tot versleutelde bestanden wordt geweigerd, de e-mailclient toegang geven tot het versleutelde bestand, als de gebruiker bestanden naar het e-mailbericht heeft gekopieerd via het klembord of door te slepen en neerzetten. De kopieerbewerking werd uitgevoerd

door een bestandsbeheerder, waarvoor de regels voor beperking van de toegang tot versleutelde bestanden niet zijn gespecificeerd, dwz de toegang is toegestaan.

- Wanneer verwisselbare schijven zijn voorzien van encryptie met [ondersteuning voor portable modus](#), kan leeftijdscontrole met wachtwoorden niet worden uitgeschakeld.
- Het wijzigen van de instellingen van het paginabestand wordt niet ondersteund. Het besturingssysteem gebruikt de standaardwaarden in plaats van de opgegeven parameterwaarden.
- Gebruik veilige verwijdering bij het werken met geëncrypte verwisselbare schijven. We kunnen de gegevensintegriteit niet garanderen als de verwisselbare schijf niet veilig is verwijderd.
- Nadat bestanden van encryptie zijn voorzien, worden hun niet-geëncrypte originelen veilig verwijderd.
- Synchronisatie van offline bestanden met behulp van Client-Side Caching (CSC) wordt niet ondersteund. Het wordt aanbevolen om offline beheer van gedeelde bronnen op groepsbeleidsniveau te verbieden. Bestanden die zich in de offline modus bevinden, kunnen worden bewerkt. Na synchronisatie kunnen wijzigingen die in een offline bestand zijn aangebracht, verloren gaan. Voor details over ondersteuning voor Client-Side Caching (CSC) bij het gebruik van encryptie, verwijzen wij u naar de [Technical Support Knowledge Base](#).
- [Het aanmaken van een geëncrypt archief](#) in de root van de harde schijf van het systeem wordt niet ondersteund.
- U kunt problemen ondervinden bij het openen van geëncrypte bestanden via het netwerk. U wordt geadviseerd de bestanden naar een andere bron te verplaatsen of om ervoor te zorgen dat de computer die als bestandsserver wordt gebruikt, wordt beheerd door dezelfde Kaspersky Security Center Administration Server.
- Als u de toetsenbordindeling wijzigt, kan het venster voor wachtwoordinvoer voor een geëncrypt zelfuitpakkend archief vastlopen. U kunt dit probleem oplossen door het wachtwoordinvoervenster te sluiten, de toetsenbordindeling in uw besturingssysteem om te schakelen en het wachtwoord voor het geëncrypte archief opnieuw in te voeren.
- Als bestandsencryptie wordt gebruikt op systemen met meerdere partities op één schijf, wordt u aangeraden de optie te gebruiken die automatisch de grootte van het bestand pagefile.sys bepaalt. Nadat de computer opnieuw is opgestart, kan het bestand pagefile.sys tussen schijfpartities worden verplaatst.
- Na het toepassen van regels voor bestandsencryptie, inclusief bestanden in de map Mijn documenten, moet u ervoor zorgen dat gebruikers voor wie encryptie is toegepast, de geëncrypte bestanden kunnen openen. Om dit te doen, moet elke gebruiker zich bij het systeem aanmelden wanneer er verbinding is met Kaspersky Security Center. Als een gebruiker toegang probeert te krijgen tot geëncrypte bestanden zonder verbinding met Kaspersky Security Center, kan het systeem vastlopen.
- Als systeembestanden op de een of andere manier deel uitmaken van de encryptie op bestandsniveau, kunnen gebeurtenissen met betrekking tot fouten bij het encrypten van deze bestanden in rapporten worden vermeld. De bestanden die in deze gebeurtenissen zijn gespecificeerd, zijn niet daadwerkelijk van encryptie voorzien.
- Pico-processen worden niet ondersteund.
- Hoofdlettergevoelige paden worden niet ondersteund. Wanneer encryptie- of decryptieregels worden toegepast, worden de paden in productgebeurtenissen in kleine letters weergegeven.
- Het wordt niet aanbevolen om bestanden te encrypten die door het systeem worden gebruikt bij het opstarten. Als deze bestanden van encryptie zijn voorzien, kan een poging om toegang te krijgen tot geëncrypte bestanden zonder verbinding met Kaspersky Security Center ervoor zorgen dat het systeem vastloopt of dat er wordt gevraagd om toegang tot niet-geëncrypte bestanden.



- Als gebruikers gezamenlijk werken met een bestand via het netwerk onder FLE-regels via programma's die de file-to-memory-mappingmethode gebruiken (zoals WordPad of FAR) en via programma's die zijn ontworpen om met grote bestanden te werken (zoals Notepad ++), kan het bestand in niet-geëncrypte vorm voor onbepaalde tijd worden geblokkeerd zonder de mogelijkheid om er toegang toe te krijgen vanaf de computer waarop het zich bevindt.
- Kaspersky Endpoint Security versleutelt geen bestanden die zich in OneDrive-cloudopslag of in andere mappen met OneDrive als naam bevinden. Kaspersky Endpoint Security blokkeert ook het kopiëren van versleutelde bestanden naar OneDrive-mappen als die bestanden niet worden toegevoegd aan de [decryptieregel](#).
- Wanneer het onderdeel voor bestandsencryptie op bestandsniveau is geïnstalleerd, werkt het beheer van gebruikers en groepen niet in WSL-modus (Windows-substelsysteem voor Linux).
- Als het encryptieonderdeel op bestandsniveau is geïnstalleerd, wordt POSIX (Portable Operating System Interface) voor het hernoemen en verwijderen van bestanden niet ondersteund.
- Het wordt niet aanbevolen om tijdelijke bestanden te versleutelen, omdat dit gegevensverlies kan veroorzaken. Microsoft Word maakt bijvoorbeeld tijdelijke bestanden bij het verwerken van een document. Als tijdelijke bestanden versleuteld worden, maar het originele bestand niet, kan de gebruiker de foutmelding *Toegang geweigerd* krijgen wanneer hij probeert het document op te slaan. Bovendien kan Microsoft Word het bestand misschien wel opslaan, maar het document kan mogelijk de volgende keer niet worden geopend, dwz de gegevens gaan verloren. Om gegevensverlies te voorkomen, moet u [de map met tijdelijke bestanden uitsluiten van encryptieregels](#).
- Na het updaten van Kaspersky Endpoint Security voor Windows versie 11.0.1 of eerder, om toegang te krijgen tot versleutelde bestanden nadat de computer opnieuw is opgestart, moet u ervoor zorgen dat de netwerkgagent actief is. Netwerkgagent heeft een vertraagde opstart. Je hebt dus geen toegang tot de versleutelde bestanden direct nadat het besturingssysteem is geladen. U hoeft niet te wachten tot de netwerkgagent is gestart na de volgende opstart van de computer.

## [Andere beperkingen](#)



- Als het programma tijdens de werking fouten 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 encryptiefunctie 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.
- Webadressen die [aan de vertrouwde lijst zijn toegevoegd](#), worden mogelijk onjuist verwerkt.
- In de Kaspersky Security Center-console, kun je geen bestand naar de harde schijf van de **Advanced** → **Repositories** → **Active threats** map opslaan. Om het bestand op te slaan, moet je het geïnfecteerde bestand desinfecteren. Bij desinfecteren slaat het programma een kopie van het bestand op in Back-up. Nu kun je het bestand op de harde schijf opslaan vanuit de **Advanced** → **Repositories** → **Backup** map.
- Overname van instellingen van gegevensoverdracht naar Administration Server (**Algemene instellingen** → **Rapporten en Opslag** → **Gegevensoverdracht naar Administration Server**) is anders dan overname van andere instellingen. Als je de wijziging van gegevensoverdracht-instellingen in het beleid hebt toegestaan (het "hangslot" is open), worden deze instellingen opnieuw teruggezet naar de standaardwaarden in de lokale computereigenschappen in de console als deze niet eerder gedefinieerd waren. Als deze instellingen eerder gedefinieerd waren, dan worden hun waarden hersteld. Bij het verwijderen van een beleid, worden de instellingen op dezelfde manier overgenomen. In deze gevallen, worden andere instellingen in de lokale computereigenschappen overgenomen van het beleid.
- Kaspersky Endpoint Security bewaakt HTTP-verkeer dat volgbaar is met de RFC 2616, RFC 7540, RFC 7541, RFC 7301-normen. Als Kaspersky Endpoint Security een ander formaat voor gegevensuitwisseling detecteert in HTTP-verkeer, blokkeert het programma deze verbinding om te voorkomen dat schadelijke bestanden van het internet worden gedownload.
- Kaspersky Endpoint Security voorkomt communicatie via het QUIC-protocol. Browsers gebruiken het standaard transportprotocol (TLS of SSL), ongeacht of QUIC-ondersteuning is ingeschakeld in de browser of niet.
- Systeembewaking. Er wordt geen volledige informatie over processen weergegeven.
- Wanneer Kaspersky Endpoint Security voor Windows voor de eerste keer wordt gestart, kan een digitaal ondertekend programma tijdelijk in de verkeerde groep worden geplaatst. Het digitaal ondertekende programma wordt later in de juiste groep geplaatst.
- Wanneer u e-mail scant met de [Mail Threat Protection-extensie voor Microsoft Outlook](#), wordt u aangeraden Exchange-modus met cache te gebruiken (de optie Exchange-modus met cache gebruiken).
- [Virusscan-taak](#) ondersteunt 64-bitversie van Microsoft Outlook niet. Dit betekent dat Kaspersky Endpoint Security geen MS Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van MS Outlook op de computer is geïnstalleerd, zelfs als [e-mail is opgenomen in het scanbereik](#).
- Wanneer in Kaspersky Security Center wordt overgeschakeld van het gebruik van het wereldwijde Kaspersky Security Network naar het gebruik van een privé Kaspersky Security Network of vice versa, is de [optie om deel te nemen aan Kaspersky Security Network uitgeschakeld](#) in het beleid van het specifieke product. Lees na het overschakelen zorgvuldig de tekst van de Kaspersky Security Network-verklaring en bevestig uw toestemming voor deelname aan KSN. U kunt de tekst van de verklaring lezen in de programma-interface of bij het bewerken van het productbeleid.

- Tijdens een nieuwe scan van een schadelijk object dat werd geblokkeerd door software van derden, wordt de gebruiker niet op de hoogte gesteld wanneer de dreiging opnieuw wordt gedetecteerd. De gebeurtenis voor het opnieuw detecteren van de bedreiging wordt weergegeven in het programmerapport en in het Kaspersky Security Center-rapport.
- Het onderdeel [Endpoint Sensor](#) kan niet worden geïnstalleerd in Microsoft Windows Server 2008.
- Het rapport van Kaspersky Security Center over apparaatencryptie bevat geen informatie over apparaten die van encryptie zijn voorzien met Microsoft BitLocker op serverplatforms of op werkstations waarop het onderdeel Apparaatcontrole niet is geïnstalleerd.
- U kunt de weergave van alle rapportitems niet inschakelen in de webconsole van Kaspersky Security Center. In de webconsole kunt u alleen het aantal items wijzigen dat in rapporten wordt weergegeven. Kaspersky Security Center Web Console toont standaard 1000 rapportitems. U kunt de weergave van alle rapportitems inschakelen in de Administration Console (MMC).
- Het is niet mogelijk om de weergave van meer dan 1000 rapportitems in de Kaspersky Security Center Console in te stellen. Als u een waarde boven 1000 instelt, geeft de Kaspersky Security Center Console slechts 1000 rapportitems weer.
- Wanneer u een beleidshierarchie gebruikt, zijn de instellingen van de sectie Encryptie van verwisselbare schijven in een onderliggend beleid toegankelijk voor bewerking als het bovenliggende beleid wijziging van die instellingen verbiedt.
- U moet Aanmelden controleren inschakelen in de instellingen van het besturingssysteem om ervoor te zorgen dat de [uitzonderingen voor de bescherming van gedeelde mappen tegen externe encryptie goed werken](#).
- Als [bescherming van gedeelde mappen is ingeschakeld](#), controleert Kaspersky Endpoint Security voor Windows pogingen om gedeelde mappen te encrypten voor elke sessie voor externe toegang die werd gestart vóór het opstarten van Kaspersky Endpoint Security voor Windows, ook als de computer waarop de sessie werd gestart, is toegevoegd aan uitzonderingen. Als u niet wilt dat Kaspersky Endpoint Security voor Windows pogingen controleert om gedeelde mappen te encrypten voor sessies voor externe toegang die zijn gestart vanaf een computer die is toegevoegd aan uitzonderingen en die zijn gestart vóór het opstarten van Kaspersky Endpoint Security voor Windows, beëindigt en start u de sessie voor externe toegang opnieuw of start u de computer waarop Kaspersky Endpoint Security voor Windows is geïnstalleerd opnieuw op.
- Als de [updatetaak wordt uitgevoerd met de machtigingen van een specifiek gebruikersaccount](#), worden productpatches niet gedownload bij het updaten vanaf een bron die autorisatie vereist.
- Het programma start mogelijk niet, vanwege onvoldoende systeemprestaties. Om dit probleem op te lossen, gebruikt u de optie Ready Boot of verhoogt u de time-out van het besturingssysteem voor het starten van services.
- Het programma werkt niet in Veilige modus.
- Om ervoor te zorgen dat Kaspersky Endpoint Security voor Windows-versies 11.5.0 en 11.6.0 correct kunnen werken met Cisco AnyConnect-software, moet u Compliance Module versie 4.3.183.2048 of hoger installeren. Lees meer over compatibiliteit met Cisco Identity Services Engine in de [Cisco-documentatie](#).
- We kunnen niet garanderen dat Audio Control werkt tot na de eerste herstart na installatie van het programma.
- In de beheerconsole (MMC), in de instellingen voor intrusiepreventie in het venster voor het configureren van programmamachtigingen, is de knop **Verwijderen** niet beschikbaar. U kunt een programma uit een vertrouwensgroep verwijderen via het contextmenu van het programma.

- In de lokale interface van het programma, in de instellingen voor Intrusion Prevention, zijn programmamachtigingen en beveiligde bronnen niet beschikbaar voor weergave als de computer wordt beheerd door een beleid. Scrollen, zoeken, filteren en andere bedieningselementen zijn niet beschikbaar. U kunt de programmamachtigingen bekijken in de beleidseigenschappen in de Kaspersky Security Center Console.
- Als grote tracebestanden zijn ingeschakeld, worden er geen traces gemaakt voor de AMSI-component en de Outlook-plug-in.
- Prestatietraces kunnen niet handmatig worden verzameld in Windows Server 2008.
- Prestatietraces voor het tracetype 'Opnieuw opstarten' worden niet ondersteund.
- Dumpregistratie wordt niet ondersteund voor pico-processen.
- De beschikbaarheidscontrole van KSN wordt niet langer ondersteund.
- Als u de optie 'Extern beheer van systeemservices uitschakelen' uitschakelt, kunt u de service van het programma dat is geïnstalleerd met de parameter AMPPL=1, niet stoppen (standaard is de parameterwaarde ingesteld op 1, vanaf Windows versie 10RS2). De AMPPL-parameter met een waarde van 1 maakt het gebruik van de Protection Processes-technologie voor de productservice mogelijk.
- Om een aangepaste scan van een map uit te voeren, moet de gebruiker die de aangepaste scan start, de machtigingen hebben om de kenmerken van deze map te lezen. Anders is het scannen van de aangepaste map onmogelijk en eindigt dit met een fout.
- Wanneer een scanregel die is gedefinieerd in een beleid, een pad bevat zonder het teken \ aan het eind, bijvoorbeeld C:\map1\map2, wordt de scan uitgevoerd voor het pad C:\map1\.
- Bij het upgraden van het programma van versie 11.1.0 naar 11.9.0 worden de instellingen van de AMSI-bescherming opnieuw ingesteld op hun standaardwaarden.
- Als u een softwarerestrictiebeleid (software restriction policy of SRP) gebruikt, wordt de computer mogelijk niet geladen (zwart scherm). U wordt aangeraden om de SRP-instellingen als volgt te wijzigen: stel de waarde **Alle softwarebestanden behalve bibliotheken (zoals DLL)** in voor de parameter **Softwarerestrictiebeleid toepassen op de volgende objectenparameter**, en voeg regels toe met het beveiligingsniveau **Onbeperkt** voor paden naar bestanden van het programma (C:\Program Files\Common Files\Kaspersky Lab en C:\Program Files\Kaspersky Lab). Voor meer informatie over het gebruik van SRP raadpleegt u de [Microsoft-documentatie](#).
- Als de computer deel uitmaakt van een domein onder Windows Group Policy Object (GPO) met de parameter DriverLoadPolicy ingesteld op 8 (alleen goed), veroorzaakt het opnieuw opstarten van de computer terwijl Kaspersky Endpoint Security is geïnstalleerd een BSOD. Om een fout te voorkomen, moet de parameter Early Launch Antimalware (ELAM) in Groepsbeleid worden ingesteld op 1 (Goed en onbekend). ELAM-instellingen bevinden zich in het beleid onder: **Computer Configuratie** → **Beheersjablonen** → **Systeem** → **Early Launch Antimalware**.
- Beheer van Outlook-plug-in-instellingen via Rest API wordt niet ondersteund.
- Taakuitvoeringinstellingen voor een specifieke gebruiker kunnen niet tussen apparaten worden overgedragen via een configuratiebestand. Geef de gebruikersnaam en het wachtwoord handmatig op nadat de instellingen zijn toegepast vanuit een configuratiebestand.
- Na het installeren van een update werkt de integriteitscontroletaak pas als het systeem opnieuw is opgestart om de update toe te passen.

- Wanneer het geroteerde tracingniveau wordt gewijzigd via het hulpprogramma voor diagnose op afstand, geeft Kaspersky Endpoint Security voor Windows ten onrechte een lege waarde voor het tracingniveau weer. Tracebestanden worden echter geschreven op basis van het juiste traceniveau. Wanneer het geroteerde tracingniveau wordt gewijzigd via de lokale interface van het programma, wordt het tracingniveau correct gewijzigd, maar geeft het hulpprogramma voor diagnose op afstand het verkeerde tracingniveau weer dat het laatst door het hulpprogramma is gedefinieerd. Dit kan ertoe leiden dat de beheerder geen up-to-date informatie heeft over het huidige tracingniveau en dat er relevante informatie kan ontbreken in traces als een gebruiker het tracingniveau handmatig wijzigt in de lokale interface van het programma.
- In de lokale interface staan de instellingen van wachtwoordbeveiliging niet toe om de naam van het beheerdersaccount te wijzigen (standaard KLAdmin). Om de naam van het beheerdersaccount te wijzigen, moet u de wachtwoordbeveiliging uitschakelen, vervolgens de wachtwoordbeveiliging inschakelen en een nieuwe naam voor het beheerdersaccount opgeven.
- U kunt geen objecten scannen die in quarantaine zijn geplaatst met de taak [Plaats bestand in Quarantaine](#).
- Kaspersky Endpoint Security voert geen [IOC Scan](#)-taken uit op netwerkstation als de bestandsmap in de taakeigenschappen begint met de letter van een station. Kaspersky Endpoint Security alleen het UNC-padformaat voor [IOC Scantaken](#) op netwerkstations. Bijvoorbeeld `\\server\shared_folder`.
- Een [import van een programma-configuratiebestand](#) eindigt met een fout als de instelling [integratie met Kaspersky Sandbox](#) ingeschakeld is in het configuratiebestand. Schakel Kaspersky Sandbox uit voordat u de programma-instellingen exporteert. Voer vervolgens de export-/importprocedure uit. Schakel Kaspersky Sandbox in na het importeren van het configuratiebestand.
- Wanneer een indicator van compromis wordt gedetecteerd tijdens het uitvoeren van de taak [IOC Scan](#), plaatst de toepassing een bestand alleen in quarantaine voor de FileItem-term. Het in quarantaine plaatsen van een bestand voor andere termen wordt niet ondersteund.
- Het is niet mogelijk om een Alternatieve Gegevensstroom (ADS) van meer dan 4 MB in quarantaine te plaatsen. Kaspersky Endpoint Security slaat alle gegevensstromen van deze grootte over zonder de gebruiker op de hoogte te stellen.
- Kaspersky Endpoint Security for Windows web plug-in 11.7.0 of hoger is vereist voor het beheren van detectiedetails. Alarmgegevens zijn nodig wanneer er gewerkt wordt met [Endpoint Detection and Response](#)-oplossingen (EDR Optimum en EDR Expert). Detectiegegevens zijn alleen beschikbaar in Kaspersky Security Center Web Console en Kaspersky Security Center Cloud Console.
- Het Kaspersky Endpoint Security-programma wanneer deze is geïnstalleerd op een Windows Server 2019-server is niet compatibel met Docker. Het implementeren van Docker-containers op een computer met Kaspersky Endpoint Security veroorzaakt een crash (BSOD).
- De compatibiliteit van Kaspersky Endpoint Security en Secret Net Studio-software is beperkt:
  - Het Kaspersky Endpoint Security-programma is niet compatibel met de antiviruscomponent van Secret Net Studio-software.  
Het programma kan niet worden geïnstalleerd op een computer waar Secret Net Studio is ingezet met de antiviruscomponent. Om interoperabiliteit mogelijk te maken, moet u het onderdeel antivirus verwijderen uit Secret Net Studio.
  - Secret Net Studio is niet compatibel met het onderdeel File Level Encryption (FLE) van Kaspersky Endpoint Security.  
Wanneer u Kaspersky Endpoint Security installeert met het onderdeel File Level Encryption (FLE), kan Secret Net Studio werken met fouten. Om interoperabiliteit te garanderen, moet u het onderdeel File Level Encryption (FLE) verwijderen uit Kaspersky Endpoint Security.

- Het migreren van de [KES + KEA] configuratie naar [KES + ingebouwde agent] kan voltooid worden met een fout in het verwijderen van het Kaspersky Endpoint Agent-programma. De programmaverwijderingsfout is opgelost in de nieuwste versie van Kaspersky Endpoint Agent. Om Kaspersky Endpoint Agent te verwijderen, start u de computer opnieuw op en maakt u een taak voor het verwijderen van programma's.

# Woordenlijst

## Actieve licentie

Een code die momenteel door het programma wordt gebruikt.

## Antivirusdatabases

Databases die informatie bevatten over dreigingen voor de computerbeveiliging die zijn gekend door Kaspersky sinds de uitgave van de antivirusdatabases. De handtekeningen in de antivirusdatabases helpen schadelijke code in gescande objecten te vinden. De antivirusdatabases worden gemaakt door deskundigen van Kaspersky 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.

## Authenticatie-agent

Interface voor het verifiëren van de identiteit om toegang tot geëncrypte harde schijven te krijgen en het besturingssysteem te laden nadat de opstartbare harde schijf is geëncrypt.

## 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 het onderdeel Essential Threat Protection wanneer het actief is. De beschermde bereiken van de verschillende onderdelen hebben verschillende eigenschappen.

## Database met phishing-webadressen

Een lijst met webadressen die volgens Kaspersky-specialisten te maken hebben met phishing. De database wordt periodiek geüpdatet en is een onderdeel van het distributiepakket van het Kaspersky-programma.

## Database met schadelijke webadressen

Een lijst met webadressen waarvan de inhoud mogelijk gevaarlijk is. De lijst wordt door specialisten van Kaspersky gemaakt. Het wordt periodiek bijgewerkt en opgenomen in 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.

## Extra licentie

Een code die het recht op het gebruik van het programma certificeert maar momenteel niet wordt gebruikt.

## Geïnfecteerd bestand

Een bestand met schadelijke code (code van bekende malware die tijdens het scannen van het bestand is gedetecteerd). Kaspersky raadt aan dat u zulke bestanden niet gebruikt 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 gebruikersnaam, het wachtwoord en de 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).

Wat de werking van de beschermingsonderdelen betreft, dient het normaliseren van adressen van webbronnen 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`.

## Infecteerbaar bestand

Een bestand dat, wegens de structuur of de indeling ervan, door criminelen kan worden gebruikt als een 'container' om schadelijke code op te slaan en te verspreiden. Doorgaans zijn deze bestanden uitvoerbare bestanden met bestandsextensies zoals `.com`, `.exe` en `.dll`. Er bestaat een vrij hoog risico op het binnendringen van kwaadaardige code in dergelijke bestanden.

## IOC

Indicator of Compromise Een verzameling gegevens over een schadelijk object of schadelijke activiteit.

## IOC-bestand

Een bestand dat een verzameling Indicators of Compromise bevat aan de hand waarvan het programma op zoek gaat naar hits die kunnen duiden op een dreiging. De kans op detectie is mogelijk hoger als aan de hand van de scan exacte hits met meerdere IOC-bestanden worden gevonden voor het object.

## Licentiecertificaat

Een document dat Kaspersky samen met het licentiebestand of de activeringscode verstrekt aan de gebruiker. Het bevat informatie over de licentie die aan de gebruiker is verleend.

## Masker

Voorstelling van een bestandsnaam en extensie met behulp van jokertekens.

Bestandsmaskers kunnen alle tekens bevatten die in bestandsnamen zijn toegestaan, inclusief jokertekens:

- Het teken `*` (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\*\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
- Twee opeenvolgende sterretjes `**` stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in de map `Voorbeeld` en de submappen ervan bevinden. Het masker moet ten minste één genest niveau bevatten. Het masker `C:\**\*.txt` is geen geldig masker. Het masker `**` is alleen beschikbaar voor het maken van scanuitzonderingen.
- Het teken `?` (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Voorbeeld` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

## 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.



## 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.

## OpenIOC

Open standaard voor Indicator of Compromise (IOC)-definities op basis van XML met meer dan 500 verschillende Indicators of Compromise.

## 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 encryptiefunctiefunctionaliteit op de computer beschikbaar is.

## 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.

## 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.

## 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 lijkt op de definitie van een virus.

## Verlener van certificaat

Certificeringsinstantie die het certificaat heeft verleend.

# Bijlagen

Dit gedeelte bevat informatie ter aanvulling op de inhoud van het document.

## Appendix 1. Programma-instellingen

U kunt een [beleid](#), [taken](#) of de programma-[interface](#) gebruiken om Kaspersky Endpoint Security te configureren. Gedetailleerde informatie over programmaonderdelen vindt u in de overeenkomstige secties.

### File Threat Protection

Met het onderdeel File Threat Protection voorkomt u dat het bestandssysteem van de computer geïnfecteerd raakt. Standaard bevindt het onderdeel File Threat Protection zich permanent in het RAM van de computer. Het onderdeel scant bestanden op alle schijven van de computer, evenals op aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Het onderdeel scant de bestanden waartoe de gebruiker of het programma toegang heeft. Als een schadelijk bestand wordt gedetecteerd, blokkeert Kaspersky Endpoint Security de bestandsbewerking. Het programma desinfecteert of verwijdert vervolgens het schadelijke bestand, afhankelijk van de instellingen van het onderdeel File Threat Protection.

Als u probeert een bestand te openen waarvan de inhoud is opgeslagen in de OneDrive-cloud, downloadt en scant Kaspersky Endpoint Security de bestandsinhoud.

Instellingen van het onderdeel File Threat Protection

| Parameter  | Beschrijving   |
|--|--|
| <b>Beveiligingsniveau</b><br><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i> | <p>Voor File Threat Protection kan Kaspersky Endpoint Security verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden <i>beveiligingsniveaus</i> genoemd:</p> <ul style="list-style-type: none"><li>• <b>Hoog.</b> Als dit beschermingsniveau is geselecteerd, past het onderdeel File Threat Protection de strikte controle toe op alle bestanden die worden geopend, opgeslagen en gestart. Het onderdeel File Threat Protection scant alle soorten bestanden op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Het onderdeel scant ook archieven, installatiepakketten en ingebede OLE-objecten.</li><li>• <b>Aanbevolen.</b> Dit bestandsbeveiligingsniveau wordt aanbevolen door experts van Kaspersky Lab. Het onderdeel File Threat Protection scant alleen de opgegeven soorten bestanden op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer, alsook ingebede OLE-objecten. Het onderdeel File Threat Protection scant geen archieven of installatiepakketten.</li><li>• <b>Laag.</b> De instellingen van dit bestandsbeveiligingsniveau zorgen voor maximale scansnelheid. Het onderdeel File Threat Protection scant alleen bestanden met de opgegeven extensies op alle harde schijven, verwisselbare schijven en netwerkschijven van de computer. Het onderdeel File Threat Protection scant geen samengestelde bestanden.</li></ul> |

|  |  |
|--|--|
| <p><b>Bestandstypen</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p>                                       | <p><b>Alle bestanden.</b> Als deze instelling is ingeschakeld, worden alle bestanden gecontroleerd door Kaspersky Endpoint Security, zonder uitzondering (alle indelingen en extensies).</p> <p><b>Bestanden gescand op indeling.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. Alvorens een bestand te scannen op schadelijke code, wordt de interne header van het bestand geanalyseerd om de indeling van het bestand te bepalen (bijvoorbeeld .txt, .doc, of .exe). De scan zoekt ook naar bestanden met bepaalde bestandsextensies.</p> <p><b>Bestanden gescand op extensie.</b> Als deze instelling is ingeschakeld, worden <a href="#">alleen infecteerbare bestanden</a> gescand door Kaspersky Endpoint Security. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.</p>        |
| <p><b>Protection scope</b></p>   | <p>Bevat objecten die worden gescand door het onderdeel File Threat Protection. Een scanobject kan een harde schijf, verwisselbare schijf, netwerkschijf, map, bestand of meerdere bestanden van een masker zijn.</p> <p>Het onderdeel File Threat Protection scant standaard bestanden die op harde schijven, verwisselbare schijven of netwerkschijven worden gestart. Het beschermd bereik voor deze objecten kan niet worden gewijzigd of verwijderd. U kunt ook voorkomen dat een object (zoals een verwisselbare schijf) wordt gescand.</p>  |
| <p><b>Machine learning en analyse op basis van definities</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p> | <p>De methode 'Machine learning en analyse op basis van definities' gebruikt de Kaspersky Endpoint Security-databases die beschrijvingen van bekende dreigingen en neutralisatiemethoden bevatten. Een bescherming die gebruikmaakt van deze methode zorgt voor een minimale beveiliging.</p> <p>Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.</p>  |
| <p><b>Heuristische analyse</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p>                                | <p>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.</p> <p>Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingsstelsel en de duur van de heuristische analyse.</p>  |
| <p><b>Actie bij detectie van een dreiging</b></p>  | <p><b>Desinfecteren of verwijderen als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Mocht de desinfectie mislukken, dan worden de bestanden door Kaspersky Endpoint Security verwijderd.</p> <p><b>Desinfecteren of blokkeren als desinfectie mislukt.</b> Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Als geen desinfectie mogelijk is, voegt Kaspersky Endpoint Security de informatie over de gevonden geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.</p> <p><b>Blokkeren.</b> Als deze optie is geselecteerd, blokkeert het onderdeel File Threat Protection automatisch alle geïnfecteerde bestanden zonder eerst te proberen om ze te desinfecteren.</p> |

|   |  |
|---|--|
|   | <p>Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt Kaspersky Endpoint Security een reservekopie van het bestand voor het geval u <a href="#">het bestand moet herstellen of als het in de toekomst kan worden gedesinfecteerd</a>.</p>   |
| <b>Scan alleen nieuwe en gewijzigde bestanden</b>   | <p>Scant alleen nieuwe bestanden en die bestanden die zijn gewijzigd sinds de laatste keer dat ze werden gescand. Op deze manier wordt de duur van een scan ingekort. Deze modus is zowel op enkelvoudige als op samengestelde bestanden van toepassing.</p>   |
| <b>Scan archieven</b>   | <p>ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling. Bij het controleren van archieven voert het programma een recursief uitpakken uit. Zo kunnen bedreigingen worden gedetecteerd in archieven op meerdere niveaus (archief in een archief).</p>   |
| <b>Scan distributiepakketten</b>  | <p>Dit selectievakje schakelt het scannen van distributiepakketten van andere fabrikanten in of uit.</p>   |
| <b>Scan files in Microsoft Office formats</b>   | <p>Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.</p>   |
| <b>Pak grote samengestelde bestanden niet uit</b>   | <p>Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde.</p> <p>Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.</p> </div>   |
| <b>Unpack compound files in the background</b>  | <p>Als het selectievakje is ingeschakeld, verleent Kaspersky Endpoint Security toegang tot samengestelde bestanden die groter zijn dan de opgegeven waarde voordat deze bestanden worden gescand. In dit geval zal Kaspersky Endpoint Security samengestelde bestanden op de achtergrond uitpakken en scannen.</p> <p>Kaspersky Endpoint Security biedt alleen toegang tot samengestelde bestanden die kleiner zijn dan deze waarde na het uitpakken en scannen van deze bestanden.</p> <p>Als het selectievakje is uitgeschakeld, verleent Kaspersky Endpoint Security pas toegang tot samengestelde bestanden nadat bestanden van elke grootte zijn uitgepakt en gescand.</p>                    |
| <b>Scanmodus</b><br><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i> | <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security scant bestanden waartoe de gebruiker, het besturingssysteem of een programma dat onder het gebruikersaccount wordt uitgevoerd, toegang heeft.</p> </div> <p><b>Intelligente modus.</b> In deze modus scant File Threat Protection een object op basis van een analyse van acties die zijn uitgevoerd op het object. Wanneer u bijvoorbeeld werkt met een Microsoft Office-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.</p> |

|  |   |
|--|---|
|  | <p><b>Bij openen en wijzigen.</b> In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze te openen of te wijzigen.</p> <p><b>Bij openen.</b> In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze te openen.</p> <p><b>Bij uitvoeren.</b> In deze modus scant File Threat Protection objecten wanneer er wordt geprobeerd om ze uit te voeren.</p>  |
| <p><b>iSwift-technologie</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p>              | <p>Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iSwift-technologie is een verbeterde versie van de iChecker-technologie voor het NTFS-bestandssysteem.</p>   |
| <p><b>iChecker-technologie</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p>            | <p>Met deze technologie kan de scansnelheid toenemen door bepaalde bestanden uit te sluiten van de scan. Met behulp van een speciaal algoritme dat rekening houdt met de releasedatum van de Kaspersky Endpoint Security-databases, de datum waarop bestanden voor het laatst zijn gescand en eventuele wijzigingen in de scaninstellingen wordt bepaald welke bestanden niet worden gescand. De iChecker-technologie heeft enkele beperkingen: de technologie werkt niet met grote bestanden en is alleen van toepassing op objecten met een structuur die door het programma wordt herkend (bijvoorbeeld bestanden met de extensie EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP en RAR).</p> |
| <p><b>File Threat Protection pauzeren</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p> | <p>Hierdoor wordt de werking van File Threat Protection voor bestanden tijdelijk en automatisch onderbroken op het opgegeven tijdstip of bij het werken met de opgegeven programma's.</p>   |

## Web Threat Protection

Het onderdeel Web Threat Protection voorkomt downloads van schadelijke bestanden vanaf het internet en blokkeert ook schadelijke en phishingwebsites. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Kaspersky Endpoint Security scant HTTP-, HTTPS- en FTP-verkeer. Kaspersky Endpoint Security scant URL's en IP-adressen. U kunt [opgeven welke poorten Kaspersky Endpoint Security moet bewaken](#) of gewoon alle poorten selecteren.

Voor de bewaking van HTTPS-verkeer moet u [Versleutelde verbindingen scannen](#) inschakelen.

Wanneer een gebruiker een schadelijke website of phishingwebsite probeert te openen, blokkeert Kaspersky Endpoint Security de toegang en wordt er een waarschuwing weergegeven (zie onderstaande afbeelding).



### Toegang geweigerd

Het opgevraagde webadres kan niet worden weergegeven

http://kl-test-page.avp.ru/new\_ksn\_samples/AVS\_RISKWARE-KSN\_BAD.exe

**Reden:**

object is geïnfecteerd met [UDS:DangerousObject.Multi.Generic](#)

Bericht gemaakt op: 10/12/2020 7:37:31 PM

kaspersky

Bericht over geweigerde toegang tot website

Instellingen van het onderdeel Web Threat Protection

| Parameter  | Beschrijving  |
|--|---|
| <b>Beveiligingsniveau</b><br><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i> | <p>Voor Web Threat Protection kan Kaspersky Endpoint Security verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden <i>beveiligingsniveaus</i> genoemd:</p> <ul style="list-style-type: none"><li>• <b>Hoog.</b> Het beveiligingsniveau waarmee het internetverkeer dat de computer via de protocollen HTTP en FTP ontvangt zeer grondig wordt gescand door het onderdeel Web Threat Protection. Web Threat Protection scant alle objecten uit het internetverkeer in detail door de complete programmadatabases te gebruiken en voert de meest gedetailleerde <a href="#">heuristische analyse</a> uit.</li><li>• <b>Aanbevolen.</b> Het beschermingsniveau dat het optimale evenwicht tussen prestaties van Kaspersky Endpoint Security en beveiliging van internetverkeer biedt. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit. Dit beschermingsniveau voor internetverkeer wordt door experts van Kaspersky aanbevolen.</li><li>• <b>Laag.</b> De instellingen van dit beschermingsniveau voor webverkeer zorgen voor maximale scansnelheid van webverkeer. Het onderdeel Web Threat Protection voert de heuristische analyse op het niveau Gemiddelde scan uit.</li></ul> |
| <b>Actie bij detectie van een dreiging</b>   | <p><b>Download blokkeren.</b> Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, blokkeert het onderdeel Web Threat Protection de toegang tot het object en toont het een bericht in de browser.</p> <p><b>Melden.</b> Als deze optie wordt geselecteerd bij de detectie van een geïnfecteerd object in het internetverkeer, staat Kaspersky Endpoint Security toe dat het object wordt gedownload naar de computer maar voegt het informatie over het geïnfecteerde object toe aan de lijst met actieve dreigingen.</p>   |
| <b>Controleer of het webadres</b>  | <p>Door de koppelingen te scannen om te bepalen of ze zijn opgenomen in de database met kwaadaardige webadressen, kunt u websites volgen die aan de denylist zijn</p>   |

|  |  |
|--|--|
| <p><b>voorkomt in de database met schadelijke webadressen</b></p> <p><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i></p>                     | <p>toegevoegd. De database van kwaadaardige webadressen wordt door Kaspersky onderhouden, bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security geüpdatet.</p>   |
| <p><b>Gebruik heuristische analyse</b></p> <p><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i></p>  | <p>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.</p> <p>Wanneer webverkeer wordt gescand op virussen en andere toepassingen die een bedreiging vormen, voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.</p> |
| <p><b>Controleer of het webadres voorkomt in de database met phishingadressen</b></p> <p><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i></p> | <p>De database van phishing-webadressen bevat de webadressen van bekende websites die voor phishing-aanvallen worden gebruikt. Kaspersky vult deze database met phishing-koppelingen aan met adressen die zijn verkregen van de internationale organisatie gekend als Anti-Phishing Working Group. De database van phishing-adressen wordt bij het installatiepakket van het programma meegeleverd en tijdens database-updates van Kaspersky Endpoint Security bijgewerkt.</p>   |
| <p><b>Do not scan web traffic from trusted web addresses</b></p>   | <p>Als het selectievakje is ingeschakeld, wordt de inhoud van webpagina's of websites waarvan de adressen voorkomen in de lijst met vertrouwde webadressen niet gescand door het onderdeel Web Threat Protection. U kunt zowel het specifieke adres als het adresmasker van een webpagina of website toevoegen aan de lijst met vertrouwde webadressen.</p>  |

## Mail Threat Protection

Het onderdeel Mail Threat Protection scant de bijlagen van inkomende en uitgaande e-mailberichten op virussen en andere dreigingen. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de [Kaspersky Security Network-cloudservice](#) en heuristische analyse.

Mail Threat Protection kan zowel inkomende als uitgaande berichten scannen. Het programma ondersteunt POP3, SMTP, IMAP en NNTP in de volgende e-mailprogramma's:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Microsoft Outlook Express



- Windows Mail

Mail Threat Protection ondersteunt geen andere protocollen en e-mailprogramma's.

Mail Threat Protection kan niet altijd toegang op *protocol-niveau* verkrijgen tot berichten (bijvoorbeeld bij gebruik van de Microsoft Exchange-oplossing). Daarom bevat Mail Threat Protection een [extensie voor Microsoft Office Outlook](#). De extensie maakt het scannen van berichten mogelijk op het *niveau van het e-mailprogramma*. De extensie Mail Threat Protection ondersteunt bewerkingen met Outlook 2010, 2013, 2016 en 2019.

Het onderdeel Mail Threat Protection scant geen berichten als de e-mailclient in een browser is geopend.

Wanneer een schadelijk bestand in een bijlage wordt gedetecteerd, hernoemt Kaspersky Endpoint Security het onderwerp van het bericht als volgt: `[Bericht heeft uw deelname nodig voor verwerking] <onderwerp bericht>` of `[Bericht is verwerkt] <onderwerp bericht>`.

Instellingen van het onderdeel Mail Threat Protection

| Parameter  | Beschrijving  |
|--|---|
| <b>Beveiligingsniveau</b><br><i>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</i> | <p>Voor Mail Threat Protection past Kaspersky Endpoint Security verschillende groepen instellingen toe. Deze groepen van instellingen die in het programma zijn opgeslagen, worden <i>beveiligingsniveaus</i> genoemd:</p> <ul style="list-style-type: none"> <li>• <b>Hoog.</b> Als dit beveiligingsniveau voor e-mails is geselecteerd, worden e-mailberichten zeer grondig gescand door het onderdeel Mail Threat Protection. Het onderdeel Mail Threat Protection scant inkomende en uitgaande e-mailberichten en voert een gedetailleerde heuristische analyse uit. Het hoge e-mailbeveiligingsniveau wordt aanbevolen voor omgevingen met een hoog risico. Een voorbeeld van zulk een omgeving is een verbinding met een gratis e-mailservice vanaf een thuisnetwerk dat niet is beveiligd door een centrale e-mailbescherming.</li> <li>• <b>Aanbevolen.</b> Het beveiligingsniveau voor e-mails dat het optimale evenwicht tussen prestaties van Kaspersky Endpoint Security en e-mailbeveiliging biedt. Het onderdeel Mail Threat Protection scant inkomende en uitgaande e-mailberichten en voert een normale heuristische analyse uit. Dit beveiligingsniveau voor e-mails wordt door experts van Kaspersky aanbevolen.</li> <li>• <b>Laag.</b> Als dit beveiligingsniveau voor e-mails is geselecteerd, scant het onderdeel Mail Threat Protection alleen inkomende e-mailberichten, voert het een oppervlakkige heuristische analyse uit en scant het geen archieven die aan e-mailberichten zijn toegevoegd. Met dit beveiligingsniveau voor e-mails scant het onderdeel Mail Threat Protection e-mailberichten op maximale snelheid en gebruikt het zeer weinig bronnen van het besturingssysteem. Het beveiligingsniveau voor e-mails Laag wordt aanbevolen voor gebruik in een goed beveiligde omgeving. Een voorbeeld van zo'n omgeving is een bedrijfsnetwerk met een centrale e-mailbeveiliging.</li> </ul> |
| <b>Actie bij detectie van een dreiging</b>   | <p><b>Desinfecteren of verwijderen als desinfectie mislukt.</b> Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. De gebruiker krijgt dan toegang tot het bericht met een veilige bijlage. Als het object niet kan worden gedesinfecteerd, verwijdert Kaspersky Endpoint Security het geïnfecteerde object. Kaspersky Endpoint Security voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht: <code>[Bericht is verwerkt] &lt;onderwerp van bericht&gt;</code>.</p>   |



|   |  |
|---|--|
|   | <p><b>Desinfecteren of blokkeren als desinfectie mislukt.</b> Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. De gebruiker krijgt dan toegang tot het bericht met een veilige bijlage. Als het object niet kan worden gedesinfecteerd, voegt Kaspersky Endpoint Security een waarschuwing toe aan het onderwerp van het bericht: [Bericht heeft uw medewerking nodig voor verwerking] &lt;onderwerp van bericht&gt;. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert Kaspersky Endpoint Security de verzending van het bericht en toont het e-mailprogramma een fout.</p> <p><b>Blokkeren.</b> Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt Kaspersky Endpoint Security een waarschuwing toe aan het onderwerp van het bericht: [Bericht heeft uw deelname nodig voor verwerking] &lt;onderwerp van bericht&gt;. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert Kaspersky Endpoint Security de verzending van het bericht en toont het e-mailprogramma een fout.</p> |
| <p><b>Beschermd bereik</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p>     | <p>Het <i>beschermd bereik</i> omvat objecten die door het onderdeel worden gecontroleerd wanneer het wordt uitgevoerd: inkomende en uitgaande berichten of alleen inkomende berichten.</p> <p>Om uw computers te beschermen, hoeft u alleen inkomende berichten te scannen. U kunt het scannen op uitgaande berichten inschakelen om te voorkomen dat geïnfecteerde bestanden in archieven worden verzonden. U kunt ook het scannen van uitgaande berichten inschakelen als u wilt voorkomen dat bestandformaten worden verzonden, zoals audio- en videobestanden.</p>  |
| <p><b>Scan POP3-, SMTP-, NNTP- en IMAP-verkeer</b></p>  | <p>Met het selectievakje schakelt u de optie in of uit waarmee u verkeer via de protocollen POP3, SMTP, NNTP en IMAP kunt laten scannen door het onderdeel Mail Threat Protection.</p>   |
| <p><b>Verbind Microsoft Outlook-extensie</b></p>  | <p>Als het selectievakje is ingeschakeld, worden de e-mailberichten die via de POP3-, SMTP-, NNTP- en IMAP-protocollen worden verstuurd gescand met behulp van de extensie die in Microsoft Outlook is geïntegreerd.</p> <p>Als e-mail wordt gescand met de extensie voor Microsoft 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 <a href="#">Microsoft Knowledge Base</a>.</p>  |
| <p><b>Heuristische analyse</b><br/>(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)</p> | <p>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.</p> <p>Bij het scannen van bestanden op een schadelijke code voert de heuristische analysator instructies uit in de uitvoerbare bestanden. Het aantal instructies dat door de heuristische analysator wordt uitgevoerd, is afhankelijk van het niveau dat is gespecificeerd voor de heuristische analyse. Dit niveau van de heuristische analyse verzekert een evenwicht tussen de grondigheid bij het zoeken naar nieuwe dreigingen, de belasting van de bronnen in het besturingssysteem en de duur van de heuristische analyse.</p>  |
| <p><b>Scan toegevoegde archieven</b></p>  | <p>ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling</p>   |

|  |  |
|--|--|
|  | <p>Als Kaspersky Endpoint Security tijdens de scan een wachtwoord voor een archief in de tekst van het bericht detecteert, wordt dit wachtwoord gebruikt om de inhoud van het archief te scannen op kwaadaardige programma's. In dit geval wordt het wachtwoord niet opgeslagen. Een archief wordt tijdens het scannen uitgepakt. Als er een programmafout optreedt tijdens het uitpakken, kunt u de uitgepakte bestanden handmatig verwijderen. Deze bestanden worden opgeslagen in het volgende pad: %systemroot%\temp. De bestanden hebben het voorvoegsel PR.</p>  |
| <b>Scan Microsoft Office-bijlagen</b>              | Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.  |
| <b>Scan geen archiefbestanden groter dan N MB.</b> | Als dit selectievakje is ingeschakeld, worden archieven die aan e-mailberichten zijn toegevoegd en die groter dan de opgegeven waarde zijn niet gescand door het onderdeel Mail Threat Protection. Als het selectievakje is uitgeschakeld, worden toegevoegde archieven van elke grootte gescand door het onderdeel Mail Threat Protection.  |
| <b>Scan archieven niet langer dan N sec</b>        | Als het selectievakje is ingeschakeld, is de toegestane scanduur voor archieven die aan e-mailberichten zijn toegevoegd beperkt tot de opgegeven tijd.   |
| <b>Filter voor bijlagen</b>                        | <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Het bijlagenfilter wordt niet toegepast op uitgaande e-mailberichten.</p> </div> <p><b>Filteren uitschakelen.</b> Als deze optie is geselecteerd, worden bestanden die aan e-mailberichten zijn toegevoegd niet gefilterd door het onderdeel Mail Threat Protection.</p> <p><b>Naam van geselecteerde typen bijlagen wijzigen.</b> Als deze optie geselecteerd is, zal het onderdeel Mail Threat Protection het laatste extensie-teken in de bijgevoegde bestanden van de gespecificeerde types vervangen door het onderstrepingsteken (bijvoorbeeld bijlage.doc_). Dus om het bestand te openen, moet de gebruiker het bestand hernoemen.</p> <p><b>Geselecteerde typen bijlagen verwijderen.</b> Als deze optie is geselecteerd, verwijdert het onderdeel Mail Threat Protection de opgegeven soorten toegevoegde bestanden uit e-mailberichten.</p> <p>In de lijst met bestandsmaskers kunt u opgeven welke soorten bijlagen moeten worden hernoemd of verwijderd uit e-mailberichten.</p> |

## Network Threat Protection

Het onderdeel Network Threat Protection scant inkomend netwerkverkeer op activiteit die kenmerkend is voor netwerkaanvallen. Wanneer Kaspersky Endpoint Security een poging tot netwerkaanval op de computer van een gebruiker detecteert, blokkeert het de netwerkverbinding met de aanvallende computer. 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 Threat Protection wordt bijgewerkt wanneer [de databases en de modules van het programma worden bijgewerkt](#).

| Parameter  | Beschrijving   |
|--|--|
| <b>Behandel poortscans en flooding als aanvallen</b> | <p><i>Network Flooding</i> is een aanval op netwerkbronnen van een organisatie (zoals webserver). Deze aanval bestaat uit het verzenden van een groot aantal verzoeken om de bandbreedte van netwerkbronnen te overbelasten. Wanneer dit gebeurt, hebben gebruikers geen toegang meer tot de netwerkbronnen van de organisatie.</p> <p>Een <i>Port Scanning</i>-aanval bestaat uit het scannen van de UDP-poorten, TCP-poorten en netwerkservices op de computer. Met deze aanval kan de aanvaller de mate van kwetsbaarheid van de computer bepalen voordat hij gevaarlijkere netwerkaanvallen uitvoert. Met Port Scanning kan de aanvaller ook het besturingssysteem op de computer identificeren en de juiste netwerkaanvallen voor dit besturingssysteem kiezen.</p> <p>Als dit selectievakje is ingeschakeld, bewaakt Kaspersky Endpoint Security netwerkverkeer om deze aanvallen te detecteren. Als er een aanval wordt gedetecteerd, waarschuwt het programma de gebruiker en stuurt de desbetreffende gebeurtenis naar Kaspersky Security Center. Het programma geeft informatie over de aanvallende computer, die nodig is voor tijdige acties als reactie op bedreigingen.</p> <p>U kunt de detectie van dit soort aanvallen uitschakelen voor het geval dat sommige van uw toegestane programma's bewerkingen uitvoeren die typisch zijn voor dit soort aanvallen. Dit helpt om vals alarm te voorkomen.</p> |
| <b>Blokkeer aanvallende apparaten voor N min</b>     | <p>Als het selectievakje is ingeschakeld, voegt Network Threat Protection de aanvallende computer toe aan de lijst met geblokkeerde computers. Dit betekent dat de netwerkverbinding met de aanvallende computer na de eerste netwerkaanval een bepaalde tijd wordt geblokkeerd door het onderdeel Network Threat Protection. Deze blokkering beschermt de gebruiker automatisch tegen mogelijke nieuwe netwerkaanvallen vanaf hetzelfde adres. De minimale tijd die een aanvallende computer in de blokkeerlijst moet doorbrengen, is één minuut. De maximale tijd is 32 768 minuten.</p> <p>U kunt de blokkeerlijst bekijken in het venster van het <a href="#">Netwerkmonitor-tool</a>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security wist de blokkeerlijst wanneer het programma opnieuw wordt opgestart en wanneer de instellingen voor Network Threat Protection worden gewijzigd.</p> </div>  |
| <b>Uitzonderingen</b>                                | <p>De lijst bevat IP-adressen die Network Threat Protection niet blokkeert als er netwerkaanvallen vanaf die IP-adressen plaatsvinden.</p> <p>Het programma registreert geen informatie over netwerkaanvallen vanaf de IP-adressen die op de lijst met uitzonderingen staan.</p>   |
| <b>MAC spoofing-bescherming</b>                      | <p>Bij een <i>MAC-spoofing-aanval</i> wordt het MAC-adres van een netwerkapparaat (netwerkaart) gewijzigd. Als gevolg hiervan kan een aanvaller gegevens die naar een apparaat zijn verzonden, omleiden naar een ander apparaat en toegang krijgen tot deze gegevens. Via Kaspersky Endpoint Security kunt u MAC-adresvervalsing blokkeren en meldingen over deze aanvallen ontvangen.</p>   |

## Firewall

De Firewall blokkeert ongeautoriseerde verbindingen met de computer tijdens het werken op internet of een lokaal netwerk. De Firewall controleert ook de netwerkactiviteit van programma's op de computer. Hierdoor kunt u uw bedrijfs-LAN beschermen tegen identiteitsdiefstal en andere aanvallen. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en vooraf gedefinieerde *netwerkregels*.

Network Agent wordt gebruikt voor interactie met Kaspersky Security Center. Firewall maakt automatisch netwerkregels die nodig zijn voor de werking van het programma en de netwerkagent. Als gevolg hiervan opent de firewall verschillende poorten op de computer. Welke poorten worden geopend, is afhankelijk van de rol van de computer (bijvoorbeeld distributiepunt). Raadpleeg de [help van Kaspersky Security Center](#) voor meer informatie over de poorten die op de computer worden geopend.

## Netwerkregels

U kunt netwerkregels op de volgende niveaus configureren:

- *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. Kaspersky Endpoint Security heeft vooraf gedefinieerde netwerkpakketregels met machtigingen die worden aanbevolen door Kaspersky-experts.
- *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.

Beheerde toegang van programma's tot bronnen, processen en persoonlijke gegevens van het besturingssysteem wordt geleverd door het [Host Intrusion Prevention-onderdeel](#) met behulp van *programmarechten*.

Wanneer een programma voor de eerste keer wordt opgestart, voert de Firewall de volgende acties uit:

1. Controleert de beveiliging van het programma aan de hand van gedownloade antivirusdatabases.

2. Controleert in Kaspersky Security Network of de website veilig is.

Het wordt aanbevolen [deel te nemen aan Kaspersky Security Network](#) zodat het onderdeel Firewall efficiënter kan werken.

3. Zet het programma in één van de *vertrouwensgroepen*: Vertrouwd, Deels beperkt, Zeer beperkt, of Niet vertrouwd.

Een [vertrouwensgroep definieert de rechten](#) die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd. Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep, afhankelijk van het risico dat dit programma voor de computer kan opleveren.

Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep voor de onderdelen Firewall en Host Intrusion Prevention. U kunt de vertrouwensgroep niet uitsluitend voor de firewall of voor Host Intrusion Prevention wijzigen.

Als deelname aan KSN hebt geweigerd of als er geen netwerk is, plaatst Kaspersky Endpoint Security het programma in een vertrouwensgroep, afhankelijk van de [instellingen van het Host Intrusion Prevention-onderdeel](#). Nadat de reputatie van het programma is ontvangen van KSN, kan de vertrouwensgroep automatisch worden gewijzigd.

4. Dit blokkeert de netwerkactiviteit van het programma, afhankelijk van de vertrouwensgroep. Programma's in de vertrouwensgroep 'Zeer beperkt' mogen bijvoorbeeld geen netwerkverbindingen gebruiken.

De volgende keer dat het programma wordt gestart, controleert Kaspersky Endpoint Security de integriteit van het programma. Als het programma niet is gewijzigd, gebruikt het onderdeel de huidige netwerkregels ervoor. Als het programma is gewijzigd, analyseert Kaspersky Endpoint Security het programma alsof het voor het eerst wordt gestart.

## Prioriteiten voor netwerkregels

Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als netwerkactiviteit aan meerdere regels wordt toegevoegd, regelt de Firewall de netwerkactiviteit volgens de regel met de hoogste prioriteit.

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.

## Status van netwerkverbinding

U kunt met de Firewall de netwerkactiviteit beheren, afhankelijk van de status van de netwerkverbinding. Kaspersky Endpoint Security ontvangt de netwerkverbindingstatus van het besturingssysteem van de computer. De status van de netwerkverbinding in het besturingssysteem wordt door de gebruiker ingesteld bij het opzetten van de verbinding. U kunt [de status van de netwerkverbinding wijzigen in de instellingen van Kaspersky Endpoint Security](#). De firewall controleert de netwerkactiviteit afhankelijk van de netwerkstatus in de Kaspersky Endpoint Security-instellingen en niet in het besturingssysteem.

De netwerkverbinding kan de volgende status hebben:

- **Openbaar netwerk.** Het netwerk wordt niet beschermd door antivirusprogramma's, firewalls of filters (zoals wifi in een café). 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.** Netwerk voor gebruikers met beperkte toegang tot bestanden en printers op deze computer (zoals voor een bedrijfsnetwerk of thuisnetwerk).
- **Vertrouwd netwerk.** 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.

| Parameter                            | Beschrijving  |
|--------------------------------------|---|
| <b>Regels voor netwerkpakketten.</b> | <p>Een tabel met een lijst met regels voor netwerkpakketten. Regels voor netwerkpakketten dienen om beperkingen voor netwerkpakketten in te stellen, ongeacht het programma. Zulke regels beperken het inkomende en uitgaande netwerkverkeer via specifieke poorten van het geselecteerde gegevensprotocol.</p> <p>De tabel bevat vooraf geconfigureerde regels voor netwerkpakketten die door Kaspersky zijn aanbevolen voor een optimale bescherming van het netwerkverkeer van computers met een Microsoft Windows-besturingssysteem.</p> <p>Firewall stelt de prioriteit van uitvoering van elke regel voor netwerkpakketten in. Firewall verwerkt regels voor netwerkpakketten in de volgorde waarin ze in de lijst met regels voor netwerkpakketten verschijnen, van boven naar beneden. Firewall zoekt de bovenste regel voor netwerkpakketten die geschikt is voor de netwerkverbinding en past deze toe door de netwerkactiviteit toe te staan of te blokkeren. Firewall negeert dan alle daaropvolgende regels voor netwerkpakketten voor de specifieke netwerkverbinding.</p> <p>Regels voor netwerkpakketten hebben een hogere prioriteit dan netwerkregels voor programma's.</p> |
| <b>Netwerkverbindingen</b>           | <p>Deze tabel bevat informatie over netwerkverbindingen die Firewall op de computer detecteert.</p> <div data-bbox="512 954 1493 1077" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>De status <i>Openbaar netwerk</i> wordt standaard toegewezen aan het internet. U kunt de status van het internet niet wijzigen.</p> </div>  |
| <b>Netwerkregels</b>                 | <p><b>Programma's</b></p> <p>Tabel met programma's die worden beheerd door het onderdeel Firewall. Programma's worden aan vertrouwensgroepen toegewezen. Een vertrouwensgroep definieert de rechten die door Kaspersky Endpoint Security worden gebruikt bij het beheren van netwerkactiviteit van programma's.</p> <p>U kunt een programma selecteren in een enkele lijst met alle programma's die onder invloed van een beleid op computers zijn geïnstalleerd, en de programma's toevoegen aan een vertrouwensgroep.</p> <p><b>Netwerkregels</b></p> <p>Een tabel met netwerkregels voor programma's die in een vertrouwensgroep zijn geplaatst. Firewall regelt overeenkomstig deze regels de netwerkactiviteit van programma's.</p> <p>De tabel toont de vooraf gedefinieerde netwerkregels die worden aanbevolen door Kaspersky-experts. Deze netwerkregels zijn toegevoegd om het netwerkverkeer van computers met Windows-besturingssystemen optimaal te beschermen. Het is niet mogelijk om de voorgedefinieerde netwerkregels te verwijderen.</p>   |

## 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. Als gevolg hiervan kan het virus opdrachten uitvoeren onder uw gebruikersaccount om bijvoorbeeld malware te downloaden.



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 besturingssysteem 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 het [Schermtoetsenbord \(als dit beschikbaar is\)](#) (zie onderstaande afbeelding). Deze procedure noemen we de toetsenbordautorisatie.

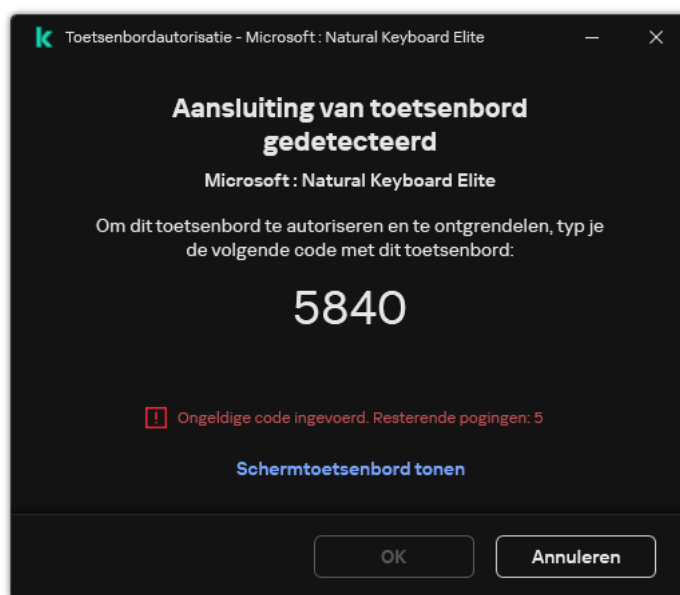
Als de code juist is ingevoerd, slaat het programma de identificatieparameters op (VID/PID van het toetsenbord en het nummer van de poort waarop het is aangesloten) in de lijst met geautoriseerde toetsenborden. U hoeft de toetsenbordautorisatie niet te herhalen wanneer het toetsenbord opnieuw wordt aangesloten 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 kunt [het aantal pogingen voor de invoer van de numerieke code configureren](#). Als de numerieke code meermaals verkeerd wordt ingevoerd of als het venster voor de toetsenbordautorisatie wordt gesloten (zie onderstaande afbeelding), blokkeert het programma de invoer van dit toetsenbord. Wanneer de tijd voor de blokkering van het USB-apparaat verstrijkt of het besturingssysteem opnieuw wordt opgestart, wordt de gebruiker door het programma gevraagd om de toetsenbordautorisatie opnieuw uit te voeren.

Het programma staat het gebruik van een geautoriseerd toetsenbord toe en blokkeert een toetsenbord dat niet is geautoriseerd.

Het onderdeel BadUSB Attack Prevention wordt niet standaard geïnstalleerd. Als u het onderdeel BadUSB Attack Prevention nodig hebt, kunt u het onderdeel toevoegen aan de eigenschappen van het [installatiepakket](#) voordat u het programma installeert of [de beschikbare programmaonderdelen wijzigen](#) nadat u het programma hebt geïnstalleerd.



Toetsenbordautorisatie

Instellingen van het onderdeel BadUSB Attack Prevention

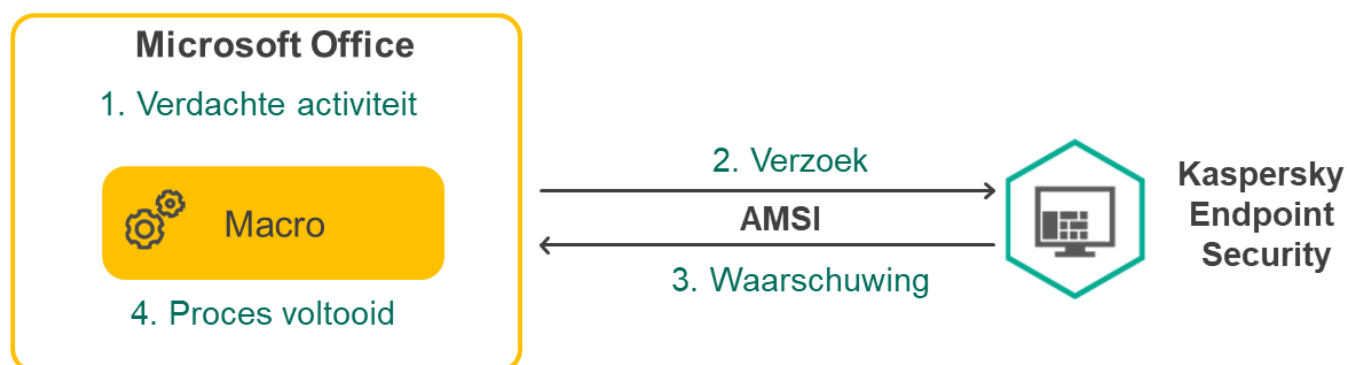
| Parameter   | Beschrijving   |
|-------------|--|
| Gebruik van | Als het selectievakje is ingeschakeld, wordt het gebruik van Schermtoetsenbord |

|   |  |
|---|--|
| <b>Schermtoetsenbord voor autorisatie van USB-apparaten verbieden</b> | voor de autorisatie van een USB-apparaat waarmee geen autorisatiecode kan worden ingevoerd geblokkeerd door het programma.   |
| <b>Maximaal aantal pogingen tot autorisatie van USB-apparaten</b>     | Het USB-apparaat wordt automatisch geblokkeerd als de autorisatiecode het opgegeven aantal keer verkeerd wordt ingevoerd. Geldige waarden zijn 1 tot en met 10. Als u dus 5 pogingen voor de invoer van de autorisatiecode invoert, wordt het USB-apparaat na de vijfde poging geblokkeerd. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd hebt u weer 5 pogingen om de autorisatiecode in te voeren. |
| <b>Time-out als het maximale aantal pogingen is bereikt</b>           | De duur van de blokkering van het USB-apparaat na het opgegeven aantal mislukte pogingen om de autorisatiecode in te voeren. Geldige waarden zijn 1 tot en met 180 (minuten).  |

## AMSI-bescherming

AMSI-beschermingsonderdeel is ontwikkeld als ondersteuning voor de Antimalware Scan Interface van Microsoft. Dankzij de *Antimalware Scan Interface (AMSI)* kunnen programma's van andere leveranciers met AMSI-ondersteuning objecten (bijvoorbeeld PowerShell-scripts) versturen naar Kaspersky Endpoint Security om ze te laten scannen en om vervolgens de resultaten van de scans voor deze objecten te ontvangen. Programma's van andere leveranciers zijn bijvoorbeeld Microsoft Office-programma's (zie onderstaande afbeelding). Voor meer informatie over AMSI raadpleegt u de [Microsoft-documentatie](#).

De AMSI-bescherming kan alleen dreigingen detecteren en meldingen over dreigingen versturen naar programma's van andere leveranciers. Nadat het andere programma een melding heeft ontvangen, kunnen geen schadelijke acties worden uitgevoerd (bijvoorbeeld een beëindiging van een proces).



Voorbeeld van AMSI-werking

AMSI-bescherming kan een verzoek van een ander programma weigeren als dit programma bijvoorbeeld het maximale aantal verzoeken binnen een bepaalde tijd overschrijdt. Kaspersky Endpoint Security stuurt informatie over een geweigerd verzoek van een ander programma naar Administration Server. De AMSI Protection-component weigert geen verzoeken van programma's van derden waarvoor: [continue integratie met de AMSI Protection-component](#) is ingeschakeld.

AMSI-bescherming is beschikbaar voor de volgende besturingssystemen voor werkstations en servers:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;



- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

#### Instellingen van AMSI-bescherming

| Parameter   | Beschrijving  |
|---|---|
| <b>Scan archieven</b>                             | ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Kaspersky Endpoint Security scant bestanden niet alleen per extensie, maar ook per indeling. Bij het controleren van archieven voert het programma een recursief uitpakken uit. Zo kunnen bedreigingen worden gedetecteerd in archieven op meerdere niveaus (archief in een archief).   |
| <b>Scan distributiepakketten</b>                  | Dit selectievakje schakelt het scannen van distributiepakketten van andere fabrikanten in of uit.   |
| <b>Scan Microsoft Office-bestanden</b>            | Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten.   |
| <b>Pak grote samengestelde bestanden niet uit</b> | Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde.<br>Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door Kaspersky Endpoint Security.<br>Kaspersky Endpoint Security scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet. |

## Exploit-preventie

Het onderdeel Exploit-preventie detecteert programmacode die kwetsbaarheden op de computer uitbuit om bevoegdheden van beheerders te misbruiken of om schadelijke activiteit uit te voeren. Exploits kunnen bijvoorbeeld aanvallen met bufferoverschrijdingen gebruiken. Hiervoor verstuurt de exploit een grote hoeveelheid gegevens naar een kwetsbaar programma. Wanneer deze gegevens worden verwerkt, voert het kwetsbare programma schadelijke code uit. Door deze aanval kan de exploit een onbevoegde installatie van malware starten. Wanneer er zonder medeweten van de gebruiker wordt geprobeerd om een uitvoerbaar bestand te starten met een kwetsbaar programma, belet Kaspersky Endpoint Security dat het bestand wordt gestart en brengt het de gebruiker op de hoogte.

#### Instellingen van het onderdeel Exploit-preventie

| Parameter  | Beschrijving   |
|--|--|
| <b>Bij detectie van exploit</b>                                  | <b>Bewerking blokkeren.</b> Als deze optie wordt geselecteerd wanneer een exploit is gedetecteerd, blokkeert Kaspersky Endpoint Security de bewerkingen van deze exploit en registreert het informatie over deze exploit.<br><b>Melden.</b> Als deze optie wordt geselecteerd wanneer een exploit wordt gedetecteerd, registreert Kaspersky Endpoint Security informatie over de exploit en voegt het informatie over deze exploit toe aan de <a href="#">lijst met actieve dreigingen</a> . |
| <b>Bescherming voor systeemprocessen in geheugen inschakelen</b> | Als deze schakelaar is ingeschakeld, blokkeert Kaspersky Endpoint Security externe processen die toegang proberen te krijgen tot het geheugen van de systeemprocessen.   |

# Gedragsdetectie

Het onderdeel Gedragsdetectie ontvangt gegevens over de acties van programma's op de computer en geeft deze gegevens door aan andere beschermingsonderdelen om hun prestaties te verbeteren. Het onderdeel Gedragsdetectie gebruikt definities van gedragspatronen (BSS) voor programma's. Als een programma-activiteit overeenkomt met een behavior stream signature, voert Kaspersky Endpoint Security de geselecteerde responsieve actie uit. De functionaliteit van Kaspersky Endpoint Security op basis van de definities van gedragspatronen levert een proactieve bescherming voor de computer.

Instellingen van het onderdeel Gedragsdetectie

| Parameter  | Beschrijving  |
|--|---|
| <b>Bij detectie van malware-activiteit</b>                                 | <ul style="list-style-type: none"><li>• <b>Bestand verwijderen.</b> Als deze optie is geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, verwijdert Kaspersky Endpoint Security het uitvoerbare bestand van het schadelijke programma en maakt het een back-up van het bestand in Back-up.</li><li>• <b>Programma beëindigen.</b> Als deze optie wordt geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, beëindigt Kaspersky Endpoint Security dit programma.</li><li>• <b>Melden.</b> Als deze optie is geselecteerd wanneer schadelijke activiteit van een programma wordt gedetecteerd, beëindigt Kaspersky Endpoint Security dit programma niet maar voegt het wel informatie over de schadelijke activiteit van dit programma toe aan de lijst met actieve dreigingen.</li></ul>  |
| <b>Bescherming van gedeelde mappen tegen externe encryptie inschakelen</b> | <p>Als de schakelaar is ingeschakeld, analyseert Kaspersky Endpoint Security activiteit in gedeelde mappen. Als deze activiteit overeenkomt met een definitie van gedragspatronen die kenmerkend is voor externe encryptie, voert Kaspersky Endpoint Security de geselecteerde actie uit.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"><p>Kaspersky Endpoint Security voorkomt de externe encryptie alleen voor bestanden op media die het NTFS-bestandssysteem gebruiken en niet zijn geëncrypt door het EFS-systeem.</p></div> <ul style="list-style-type: none"><li>• <b>Melden.</b> Als deze optie is geselecteerd wanneer een poging tot het wijzigen van bestanden in gedeelde mappen wordt gedetecteerd, voegt Kaspersky Endpoint Security informatie over deze poging tot het wijzigen van bestanden in gedeelde mappen toe aan de lijst met actieve dreigingen.</li><li>• <b>Blokkeer verbinding N min.</b> Als Kaspersky Endpoint Security een poging tot wijziging van bestanden in gedeelde mappen detecteert wanneer deze optie is geselecteerd, blokkeert het de netwerkactiviteit van de computer die de bestanden probeert te wijzigen en maakt het back-ups van gewijzigde bestanden.</li></ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"><p>Als het onderdeel Remediation Engine is ingeschakeld en de optie <b>Blokkeer verbinding N min</b> is geselecteerd, worden gewijzigde bestanden teruggezet vanuit back-ups.</p></div> |
| <b>Uitzonderingen</b>  | Lijst met computers waarvoor geen pogingen tot het encrypten van gedeelde mappen  |

worden gemonitord.

Als u de lijst met computers waarvoor gedeelde mappen niet moeten worden beschermd tegen externe encryptie wilt toepassen, moet u 'Aanmelden controleren' in het Windows-beveiligingsbeleid inschakelen. 'Aanmelden controleren' is standaard uitgeschakeld. Voor meer informatie over een Windows-beveiligingsbeleid gaat u naar de [Microsoft-website](#).

## Host Intrusion Prevention

Het onderdeel Host Intrusion Prevention voorkomt dat programma's acties uitvoeren die mogelijk gevaarlijk zijn voor het besturingssysteem en controleert de toegang tot bronnen van het besturingssysteem en persoonlijke gegevens. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases en de Kaspersky Security Network-cloudservice.

Het onderdeel regelt de werking van programma's door gebruik te maken van *programmarechten*. Programmarechten omvatten de volgende toegangsparameters:

- Toegang tot besturingssysteembronnen (bijvoorbeeld automatische-opstartopties, registersleutels)
- Toegang tot persoonlijke gegevens (zoals bestanden en programma's)

De netwerkactiviteit van programma's wordt beheerd door de [firewall](#) met behulp van *netwerkregels*.

Wanneer een programma voor de eerste keer wordt opgestart, voert het Host Intrusion Prevention-onderdeel de volgende acties uit:

1. Controleert de beveiliging van het programma aan de hand van gedownloade antivirusdatabases.
2. Controleert in Kaspersky Security Network of de website veilig is.

U wordt aanbevolen [deel te nemen aan Kaspersky Security Network](#) zodat het onderdeel Host Intrusion Prevention efficiënter kan werken.

3. Zet het programma in één van de *vertrouwensgroepen*: Vertrouwd, Deels beperkt, Zeer beperkt, of Niet vertrouwd.

Een [vertrouwensgroep definieert de rechten](#) die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd. Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep, afhankelijk van het risico dat dit programma voor de computer kan opleveren.

Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep voor de onderdelen Firewall en Host Intrusion Prevention. U kunt de vertrouwensgroep niet uitsluitend voor de firewall of voor Host Intrusion Prevention wijzigen.

Als deelname aan KSN hebt geweigerd of als er geen netwerk is, plaatst Kaspersky Endpoint Security het programma in een vertrouwensgroep, afhankelijk van de [instellingen van het Host Intrusion Prevention-onderdeel](#). Nadat de reputatie van het programma is ontvangen van KSN, kan de vertrouwensgroep automatisch worden gewijzigd.

4. Blokkeert acties van programma's afhankelijk van de vertrouwensgroep. Programma's uit de vertrouwensgroep 'Zeer beperkt' krijgen bijvoorbeeld geen toegang tot de modules van het besturingssysteem.

De volgende keer dat het programma wordt gestart, controleert Kaspersky Endpoint Security de integriteit van het programma. Als het programma niet is gewijzigd, gebruikt het onderdeel de huidige programmarechten ervoor. Als het programma is gewijzigd, analyseert Kaspersky Endpoint Security het programma alsof het voor het eerst wordt gestart.

#### Instellingen van het onderdeel Host Intrusion Prevention

| Parameter                  | Beschrijving  |
|----------------------------|---|
| <b>Application rights</b>  | <p><b>Applications</b></p> <p>Tabel met programma's die worden bewaakt door het onderdeel Host Intrusion Prevention. Programma's worden aan vertrouwensgroepen toegewezen. Een vertrouwensgroep definieert de rechten die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd.</p> <p>U kunt een programma selecteren in een enkele lijst met alle programma's die onder invloed van een beleid op computers zijn geïnstalleerd, en de programma's toevoegen aan een vertrouwensgroep.</p> <p>Toegangsrechten voor programma's worden weergegeven in de volgende tabellen:</p> <ul style="list-style-type: none"> <li>• <b>Files and system registry.</b> Deze tabel bevat de rechten van programma's in een vertrouwensgroep voor de toegang tot besturingssysteembronnen en persoonlijke gegevens.</li> <li>• <b>Rights.</b> In deze kolom ziet u het recht van programma's in een vertrouwensgroep om toegang tot processen en bronnen van het besturingssysteem te hebben.</li> <li>• <b>Network rules.</b> Een tabel met netwerkregels voor programma's die in een vertrouwensgroep zijn geplaatst. <a href="#">Firewall</a> regelt overeenkomstig deze regels de netwerkactiviteit van programma's. De tabel toont de vooraf gedefinieerde netwerkregels die worden aanbevolen door Kaspersky-experts. Deze netwerkregels zijn toegevoegd om het netwerkverkeer van computers met Windows-besturingssystemen optimaal te beschermen. Het is niet mogelijk om de voorgedefinieerde netwerkregels te verwijderen.</li> </ul> |
| <b>Protected resources</b> | <p><b>Name</b></p> <p>De tabel bevat gecategoriseerde computerbronnen. Host Intrusion Prevention monitort pogingen van andere programma's om toegang tot bronnen in de tabel te verkrijgen. Een bron kan een registercategorie, bestand of map, of registersleutel zijn.</p> <p><b>Applications</b></p> <p>Tabel met programma's die worden bewaakt door het onderdeel Host Intrusion Prevention voor de geselecteerde bron. Programma's worden aan vertrouwensgroepen toegewezen. Een vertrouwensgroep definieert de rechten die Kaspersky Endpoint Security raadpleegt wanneer de programma-activiteit wordt gecontroleerd.</p>   |
| <b>Trust group for</b>     | Een vertrouwensgroep waarin Kaspersky Endpoint Security programma's plaatst die   |

|  |  |
|--|--|
| <p><b>applications launched before Kaspersky Endpoint Security for Windows starts working</b></p>      | <p>eerder worden gestart dan Kaspersky Endpoint Security.</p>  |
| <p><b>Update rights for previously unknown applications from KSN database</b></p>                      | <p>Als het selectievakje is ingeschakeld, worden de rechten voor eerder onbekende programma's bijgewerkt door het onderdeel Host Intrusion Prevention met behulp van de Kaspersky Security Network-database.</p>   |
| <p><b>Trust digitally signed applications</b></p>  | <p>Als dit selectievakje is ingeschakeld, plaatst het onderdeel Host Intrusion Prevention de digitale handtekening van vertrouwde leveranciers in de vertrouwde groep.</p> <p><i>Vertrouwde leveranciers</i> zijn de softwareleveranciers die Kaspersky vertrouwt. U kunt het <a href="#">leverancierscertificaat ook handmatig aan het vertrouwde certificaatarchief toevoegen</a>.</p> <p>Als dit selectievakje is uitgeschakeld, beschouwt het onderdeel Host Intrusion Prevention dergelijke programma's niet als vertrouwd en gebruikt het andere parameters om de vertrouwensgroep van die programma's te bepalen.</p>   |
| <p><b>Delete rules for applications that have not been started for longer than (days, 1 to 90)</b></p> | <p>Als het selectievakje is ingeschakeld, verwijdert Kaspersky Endpoint Security automatisch informatie over het programma (vertrouwensgroep en toegangsrechten) indien aan de volgende voorwaarden wordt voldaan:</p> <ul style="list-style-type: none"> <li>• U hebt het programma handmatig in een vertrouwensgroep geplaatst of hebt de toegangsrechten ervan handmatig geconfigureerd.</li> <li>• Het programma is niet binnen de opgegeven periode gestart.</li> </ul> <p>Als de vertrouwensgroep en rechten van een programma automatisch zijn bepaald, verwijdert Kaspersky Endpoint Security na 30 dagen informatie over dit programma. Het is niet mogelijk om de opslagduur voor programma-informatie te wijzigen of om de automatische verwijdering uit te schakelen.</p> <p>De volgende keer dat u dit programma start, analyseert Kaspersky Endpoint Security het programma alsof het voor de eerste keer wordt gestart.</p> |
| <p><b>Trust group for applications that could not be added to existing groups</b></p>                  | <p>De opties in deze vervolgkeuzelijst bepalen aan welke vertrouwensgroep een onbekend programma wordt toegewezen door Kaspersky Endpoint Security.</p> <p>U kunt één van de volgende opties kiezen:</p> <ul style="list-style-type: none"> <li>• <b>Low Restricted.</b></li> <li>• <b>High Restricted.</b></li> <li>• <b>Untrusted.</b></li> </ul>  |

Via Remediation Engine kan Kaspersky Endpoint Security acties van malware in het besturingssysteem terugdraaien.

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

- **Bestandsactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het verwijdert uitvoerbare bestanden die door malware zijn aangemaakt (op alle media behalve netwerkschijven).
- Het verwijdert uitvoerbare bestanden die zijn gemaakt door programma's die door malware zijn geïnfecteerd.
- Het herstelt bestanden die door malware zijn gewijzigd of verwijderd.

De functie voor bestandsherstel heeft een [aantal beperkingen](#).

- **Registeractiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het verwijdert registersleutels die door malware zijn aangemaakt.
- Het herstelt geen registersleutels die door malware zijn gewijzigd of verwijderd.

- **Systeemactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het beëindigt processen die door malware zijn gestart.
- Het beëindigt processen waarin een schadelijk programma is binnengedrongen.
- Het hervat geen processen die door malware zijn gestopt.

- **Netwerkactiviteit**

Kaspersky Endpoint Security voert de volgende acties uit:

- Het blokkeert de netwerkactiviteit van malware.
- het blokkeert de netwerkactiviteit van processen waarin malware is binnengedrongen.

Het terugdraaien van malwareacties kan door het onderdeel [File Threat Protection](#) of [Gedragsdetectie](#) worden gestart, of tijdens een [virusscan](#).

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.

## Kaspersky Security Network

Voor een efficiëntere bescherming van uw computer gebruikt Kaspersky Endpoint Security gegevens die het van gebruikers over de hele wereld ontvangt. Kaspersky Security Network is ontworpen om deze 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 dreigingen maar verbetert ook de prestaties van bepaalde beschermingsonderdelen en verlaagt de kans op false positives. Als u deelneemt aan Kaspersky Security Network, ontvangt Kaspersky Endpoint Security van de KSN-services informatie over de categorie en reputatie van gescande bestanden, alsook informatie over de reputatie van gescande webadressen.

Het gebruik van Kaspersky Security Network is vrijwillig. U wordt tijdens de initiële configuratie van het programma gevraagd om aan KSN deel te nemen. Gebruikers kunnen hun deelname aan KSN op elk moment starten of stoppen.

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 Kaspersky Security Network-verklaring wordt bij het [distributiepakket](#) van het programma meegeleverd.

Om de belasting van de KSN-servers te verminderen, kunnen Kaspersky-experts programma-updates beschikbaar maken die verzoeken aan Kaspersky Security Network tijdelijk uitschakelen of deels beperken. In dit geval is de status van de verbinding met KSN in de lokale interface van het programma *Ingeschakeld met beperkingen*.

## Infrastructuur van KSN

Kaspersky Endpoint Security ondersteunt de volgende infrastructurele KSN-oplossingen:

- *Wereldwijd KSN* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky Security Network en sturen Kaspersky informatie over objecten die op hun computers worden gedetecteerd. Dankzij deze informatie worden de objecten dan verder onderzocht door Kaspersky-analisten en worden ze toegevoegd aan de Kaspersky Security Network-databases die reputatie-informatie en statistische gegevens bevatten.
- *Privaat KSN* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang verkrijgen tot reputatiedatabases van Kaspersky Security Network en tot andere statistische gegevens zonder gegevens naar KSN te versturen vanaf hun eigen computers. Privaat KSN is ontworpen voor bedrijven die niet kunnen deelnemen aan Kaspersky Security Network wegens een van de volgende redenen:
  - De lokale werkstations zijn niet verbonden met internet.
  - De verzending van gegevens naar het buitenland of andere netwerken dan het bedrijfsnetwerk is wettelijk verboden of beperkt door het beveiligingsbeleid van het bedrijf.

Kaspersky Security Center gebruikt standaard Wereldwijd KSN. U kunt het gebruik van Privaat KSN configureren in de Beheerconsole (MMC) en de Webconsole van Kaspersky Security Center en in de [opdrachtregel](#). U kunt het gebruik van Privaat KSN niet in de Cloudconsole van Kaspersky Security Center configureren.

Voor meer informatie over Privaat KSN raadpleegt u de documentatie van Kaspersky Private Security Network.

## KSN-proxy



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.
- De service KSN-proxy plaatst verwerkte gegevens in de cache waardoor de externe netwerkcommunicatie minder belast raakt en de informatie die gevraagd wordt door de computer van de gebruiker sneller ontvangen wordt.

Voor meer informatie over de service KSN-proxy raadpleegt u de [Help van Kaspersky Security Center](#).

Instellingen van Kaspersky Security Network

| Parameter  | Beschrijving  |
|--|---|
| <b>Uitgebreide KSN-modus inschakelen</b>   | <p>De <i>uitgebreide KSN-modus</i> is een modus waarin Kaspersky Endpoint Security <a href="#">aanvullende gegevens</a> naar Kaspersky verstuurt. Kaspersky Endpoint Security gebruikt KSN om dreigingen te detecteren, ongeacht de schakelpositie.</p>   |
| <b>Cloudmodus inschakelen</b>  | <p><i>Cloudmodus</i> verwijst naar de modus waarin Kaspersky Endpoint Security een beperkte versie van de antivirusdatabases gebruikt. Kaspersky Security Network ondersteunt de werking van het programma wanneer een beperkte versie van de antivirusdatabases worden gebruikt. Met de beperkte versie van de antivirusdatabases verbruikt u ongeveer de helft van het RAM van de computer dat anders met de normale databases zou worden gebruikt. Als u niet deelneemt aan Kaspersky Security Network of als de cloudmodus is uitgeschakeld, downloadt Kaspersky Endpoint Security de volledige versie van de antivirusdatabases vanaf de Kaspersky-servers.</p> <p>Als de schakelaar is ingeschakeld, gebruikt Kaspersky Endpoint Security de beperkte versie van de antivirusdatabases zodat de bronnen van het besturingssysteem niet te veel belast raken.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security downloadt de beperkte versie van de antivirusdatabases tijdens de volgende update nadat u het selectievakje hebt ingeschakeld.</p></div> <p>Als de schakelaar is uitgeschakeld, gebruikt Kaspersky Endpoint Security de complete versie van de antivirusdatabases.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security downloadt de complete versie van de antivirusdatabases tijdens de volgende update nadat u het selectievakje hebt uitgeschakeld.</p></div> |
| <b>Computer status when KSN servers are unavailable</b><br><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i> | <p>De opties in deze vervolgkeuzelijst bepalen de status van een computer in Kaspersky Security Center wanneer de KSN-servers niet beschikbaar zijn.</p>  |



|  |  |
|--|--|
| <p><b>Use KSN Proxy</b><br/>(alleen beschikbaar in de Kaspersky Security Center-console)</p>                                   | <p>Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security de service KSN-proxy. U kunt de instellingen van de KSN-proxy-service configureren in de eigenschappen van Administration Server.</p>   |
| <p><b>Use KSN servers when KSN Proxy is not available</b><br/>(alleen beschikbaar in de Kaspersky Security Center-console)</p> | <p>Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN-proxy-service niet beschikbaar is. KSN-servers kunnen eigendom van zowel Kaspersky (wanneer wereldwijd KSN wordt gebruikt) als derden (wanneer privaat KSN wordt gebruikt) zijn.</p> |

## Webcontrole

Webcontrole beheert de toegang van gebruikers tot webbronnen. Het onderdeel helpt zo het verkeersvolume en het misbruik van werkuren verminderen. Wanneer een gebruiker een website probeert te openen die wordt beperkt door Webcontrole, dan blokkeert Kaspersky Endpoint Security de toegang of wordt er een waarschuwing weergegeven (zie onderstaande afbeelding).

Kaspersky Endpoint Security bewaakt alleen HTTP- en HTTPS-verkeer.

Voor de bewaking van HTTPS-verkeer moet u [Versleutelde verbindingen scannen](#) inschakelen.

## Methoden voor het beheer van de toegang tot websites

Met Webcontrole kunt u de toegang tot websites configureren met de volgende methoden:

- **Websitecategorie.** Websites worden gecategoriseerd volgens de Kaspersky Security Network-cloudservice, heuristische analyse en de database van bekende websites (een onderdeel van de programmadatabases). U kunt bijvoorbeeld de gebruikerstoegang beperken tot de categorie "Sociale netwerken" of tot [andere categorieën](#).
- **Gegevenstype.** U kunt de toegang van gebruikers beperken voor gegevens op websites en bijvoorbeeld afbeeldingen verbergen. Kaspersky Endpoint Security bepaalt het gegevenstype op basis van de bestandsindeling en niet op basis van de extensie.

Kaspersky Endpoint Security scant geen bestanden in archieven. Als een archief bijvoorbeeld afbeeldingen bevat, identificeert Kaspersky Endpoint Security de gegevens als 'Archieven' en niet als 'Grafische bestanden'.

- **Individueel adres.** U kunt een webadres invoeren of [maskers gebruiken](#).

U kunt meerdere methoden tegelijk gebruiken om de toegang tot websites te regelen. Zo kunt u bijvoorbeeld de toegang tot het gegevenstype 'Office-bestanden' alleen beperken voor de categorie 'Webmail'.

## Regels voor toegang tot websites

Webcontrole beheert de toegang van gebruikers tot websites met behulp van *toegangsregels*. U kunt de volgende geavanceerde instellingen configureren voor een regel voor toegang tot websites:

- Gebruikers waarop de regel van toepassing is.  
U kunt bijvoorbeeld de internettoegang via een browser beperken voor alle gebruikers van het bedrijf, behalve voor de IT-afdeling.
- Regelplanning.  
U kunt bijvoorbeeld de internettoegang via een browser tijdens de werkuren beperken.

## Prioriteiten voor toegangsregels

Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als een website is toegevoegd aan meerdere regels, regelt Webcontrole de toegang tot de website volgens de regel met de hoogste prioriteit. Kaspersky Endpoint Security kan bijvoorbeeld een bedrijfsportal identificeren als een sociaal netwerk. Wilt u de toegang tot sociale netwerken verbieden maar toch toegang tot de webportal van het bedrijf verlenen, dan maakt u twee regels: een regel die de websitecategorie 'Sociale netwerken' blokkeert en een regel die de webportal van het bedrijf toestaat. De toegangsregel voor de webportal van het bedrijf moet een hogere prioriteit hebben dan de toegangsregel voor sociale netwerken.



De gevraagde webpagina kan niet worden geopend.

Adres: <http://kaspersky.ru/>.

De webpagina is geblokkeerd door de regel test\_block.

Reden: de webbron behoort tot de Onbepaald inhoudscategorie(ën) en de Onbepaald gegevenscategorie(ën).

Deze webbron is verboden binnen het bedrijf. Als je vindt dat de blokkering een vergissing is of als je toegang tot deze webbron nodig hebt, neem je contact op met de beheerder van het lokale bedrijfsnetwerk ([Toegang vragen](#)).

Bericht gemaakt op: 10/29/2020 4:16:12 AM



De opgevraagde webpagina is mogelijk onveilig of verboden door het bedrijfsbeleid.

Adres: <http://kaspersky.com/>.

De webpagina is geblokkeerd door de regel test\_warning.

Reden: de webbron behoort tot de inhoudscategorieën Onbepaald en de gegevenscategorieën Onbepaald.

Klik op de koppeling <http://kaspersky.com/> om de opgevraagde webpagina te openen.

Klik op de koppeling [http://kaspersky.com/\\*](http://kaspersky.com/*) om toegang te krijgen tot de volledige inhoud van de website, waarvan de webpagina deel uitmaakt.

Klik op de koppeling [\\*/\\*.kaspersky.com/\\*](*/*.kaspersky.com/*) om toegang te krijgen tot alle bestaande domeinen van een niveau dat lager is dan of gelijk is aan het niveau met het "\*".

De toegang tot de hierboven vermelde webbronnen wordt tijdens de huidige sessie van het programma toegestaan.

Als je een waarschuwing ziet die berust op een vergissing, neem je contact op met de beheerder van het lokale bedrijfsnetwerk ([Toegang vragen](#)).

Bericht gemaakt op: 10/29/2020 4:20:00 AM

#### Berichten van Webcontrole

#### Instellingen van het onderdeel Webcontrole

| Parameter                             | Beschrijving   |
|---------------------------------------|--|
| <b>Toegangsregels voor webbronnen</b> | Lijst met toegangsregels voor webbronnen. Elke regel heeft een prioriteit. Hoe hoger een regel in de lijst staat, hoe hoger de prioriteit ervan. Als een website is toegevoegd aan meerdere regels, regelt Webcontrole de toegang tot de website volgens de regel met de hoogste prioriteit.   |
| <b>Standaardregel</b>                 | De <i>Standaardregel</i> is een regel voor toegang tot webbronnen die niet in andere regels is vastgelegd. De volgende opties zijn beschikbaar: <ul style="list-style-type: none"> <li>• <b>Alles toestaan behalve de regellijst</b>, ook wel als de denylist-modus voor verboden websites genoemd.</li> <li>• <b>Alles weigeren behalve de regellijs</b>, ook wel de allowlist-modus voor toegestane websites genoemd.</li> </ul> |

|   |   |
|---|---|
| <p><b>Berichtsjablonen</b></p>                              | <ul style="list-style-type: none"> <li>• <b>Waarschuwing.</b> Het invoerveld bestaat uit een sjabloon van het bericht dat wordt weergegeven als een regel voor een waarschuwing over pogingen tot toegang tot een ongewenste webbron wordt geactiveerd.</li> <li>• <b>Bericht over blokkering.</b> Het invoerveld bevat het sjabloon van het bericht dat wordt weergegeven als een regel die de toegang tot een webbron blokkeert wordt geactiveerd.</li> <li>• <b>Bericht aan beheerder.</b> Sjabloon van het bericht dat naar de netwerkbeheerder wordt verstuurd als de gebruiker vindt dat de blokkering een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: <b>Bericht over blokkering van toegang tot webpagina aan beheerder.</b> De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie <b>User requests</b>. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.</li> </ul> |
| <p><b>Registreer het openen van toegestane pagina's</b></p> | <p>Kaspersky Endpoint Security registreert gegevens over bezoeken aan websites, waaronder toegestane websites. Kaspersky Endpoint Security verstuurt gebeurtenissen naar Kaspersky Security Center, naar <a href="#">het lokale logboek van Kaspersky Endpoint Security</a> en naar het Windows-gebeurtenislogboek. Als u de activiteit van gebruikers op het internet wilt bewaken, moet u <a href="#">de instellingen voor het opslaan van gebeurtenissen configureren</a>.</p> <div data-bbox="413 1081 1493 1240" style="background-color: #f8d7da; padding: 10px; border: 1px solid #f5c6cb;"> <p>Browsers die de bewakingsfunctie ondersteunen: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Het monitoren van gebruikersactiviteit werkt niet in andere browsers.</p> </div> <div data-bbox="413 1283 1493 1406" style="border: 1px solid #d6d8db; padding: 10px; margin-top: 10px;"> <p>De bewaking van de activiteit van gebruikers op het internet vereist meer computerbronnen bij de decryptie van HTTPS-verkeer.</p> </div>  |

## Apparaatcontrole

Apparaatcontrole beheert de toegang van gebruikers tot apparaten die zijn geïnstalleerd in of aangesloten op de computer (bijvoorbeeld harde schijven, camera's of wifi-apparaten). Met dit onderdeel kunt u de computer beschermen tegen infecties en datalekken voorkomen wanneer zulke apparaten worden aangesloten.


### Niveaus voor toegang tot apparaten

Apparaatcontrole beheert de toegang op de volgende niveaus:

- **Apparaattype.** Bijvoorbeeld printers, verwisselbare schijven en cd-/dvd-stations.

Zo kunt u de toegang tot apparaten configureren:



- Toestaan – ✓.
  - Blokkeren – .
  - Afhankelijk van de verbindingbus (behalve wifi) – .
  - Blokkeren met uitzonderingen (alleen wifi) – .
- **Verbindingbus.** Een *verbindingbus* is een interface voor de aansluiting van apparaten op de computer (bijvoorbeeld USB of FireWire). U kunt dus de aansluiting van alle apparaten beperken, bijvoorbeeld via USB. Zo kunt u de toegang tot apparaten configureren:

- Toestaan – ✓.
  - Blokkeren – .
- **Vertrouwde apparaten.** *Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

U kunt vertrouwde apparaten toevoegen op basis van de volgende gegevens:

- **Apparaten per ID** Elk apparaat heeft een uniek ID (Hardware-ID of HWID). U kunt het ID in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Voorbeeld van een apparaat-ID:  
SCSI\CDROM&VEN\_NECVMWAR&PROD\_VMWARE\_SATA\_CD00\5&354AE4D7&0&000000. Apparaten toevoegen per ID is handig als u meerdere specifieke apparaten wilt toevoegen.
- **Apparaten per model** Elk apparaat heeft een leverancier-ID (VID) en een product-ID (PID). U kunt de ID's in de apparaateigenschappen bekijken met behulp van de hulpprogramma's van het besturingssysteem. Sjabloon voor de invoer van het VID en PID: VID\_1234&PID\_5678. Apparaten toevoegen per model is handig als u een bepaald model apparaten in uw bedrijf gebruikt. Op deze manier kunt u alle apparaten van dit model toevoegen.
- **Apparaten per ID-masker** Als u meerdere apparaten met vergelijkbare ID's gebruikt, kunt u maskers gebruiken om apparaten toe te voegen aan de lijst met vertrouwde apparaten. Het teken \* vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken ? bij de invoer van een masker. Bijvoorbeeld WDC\_C\*.
- **Apparaten per modelmasker** Als u meerdere apparaten met vergelijkbare VID's of PID's gebruikt (bijvoorbeeld apparaten van dezelfde fabrikant), kunt u maskers gebruiken om apparaten aan de lijst met vertrouwde apparaten toe te voegen. Het teken \* vervangt een willekeurige reeks tekens. Kaspersky Endpoint Security biedt geen ondersteuning voor het teken ? bij de invoer van een masker. Bijvoorbeeld VID\_05AC & PID\_ \*.

Apparaatcontrole beheert de toegang van gebruikers tot apparaten met behulp van [toegangsregels](#). Via Apparaatcontrole kunt u ook gebeurtenissen zoals het aansluiten of loskoppelen van apparaten opslaan. Voor het opslaan van gebeurtenissen moet u in een beleid de registratie van gebeurtenissen configureren.

Als de toegang tot een apparaat afhangt van de aansluitbus (de status ) , slaat Kaspersky Endpoint Security geen informatie over het aansluiten of loskoppelen van apparaten op. Als u wilt dat Kaspersky Endpoint Security informatie over het aansluiten of loskoppelen van apparaten opslaat, staat u de toegang tot het desbetreffende soort apparaat toe (de status ) of voegt u het apparaat aan de vertrouwde lijst toe.

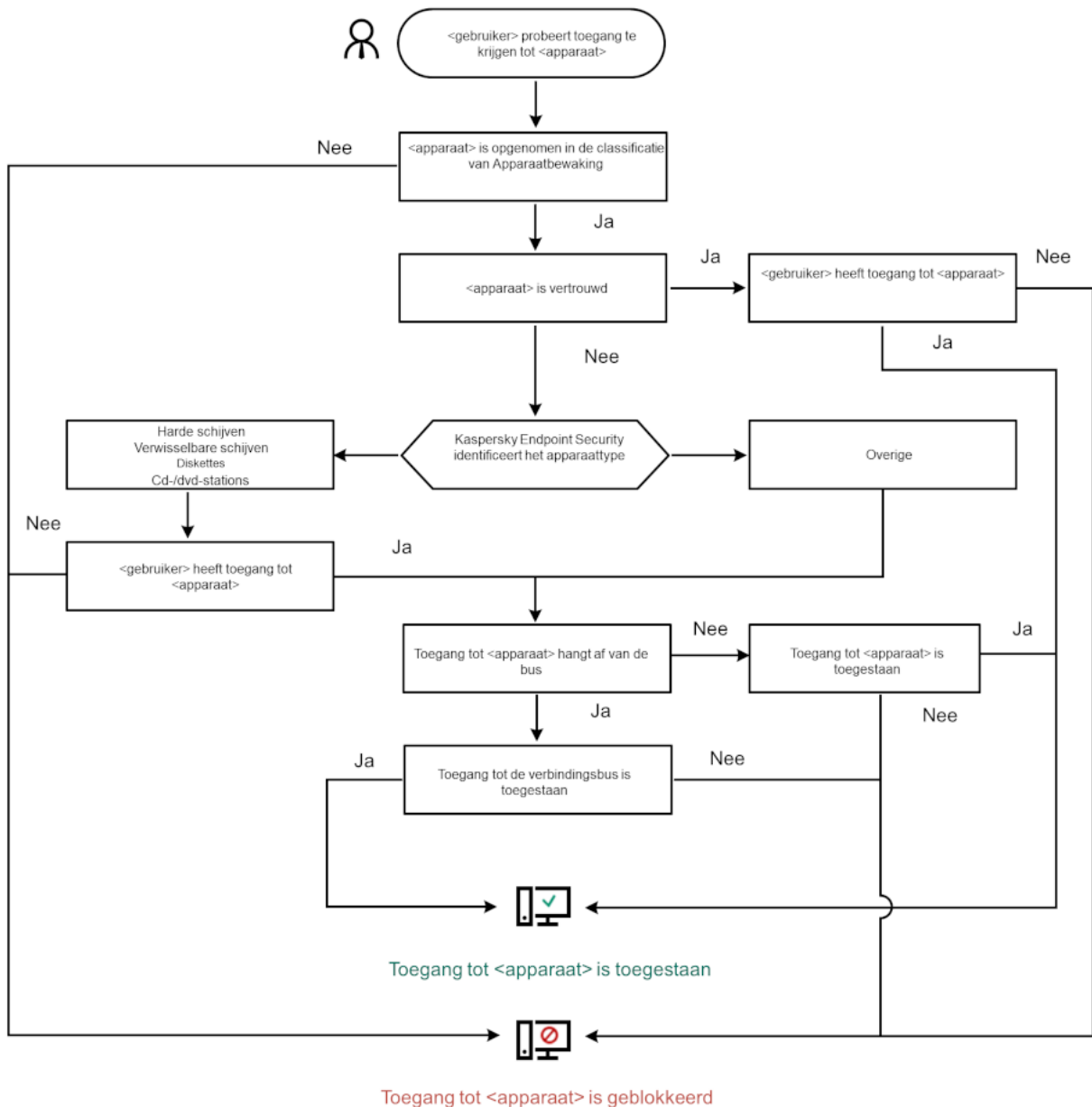
Wanneer een apparaat dat wordt geblokkeerd door Apparaatcontrole wordt aangesloten op de computer, blokkeert Kaspersky Endpoint Security de toegang en toont het een melding (zie onderstaande afbeelding).



Melding van Apparaatcontrole

## Algoritme voor werking van Apparaatcontrole

Kaspersky Endpoint Security beslist of de toegang tot een apparaat moet worden verleend nadat de gebruiker het apparaat op de computer heeft aangesloten (zie onderstaande afbeelding).



Algoritme voor werking van Apparaatcontrole

Als een apparaat wordt aangesloten en de toegang wordt verleend, kunt u de toegangsregel bewerken om de toegang te blokkeren. In dit geval blokkeert Kaspersky Endpoint Security de toegang de volgende keer dat iemand probeert toegang te krijgen tot het apparaat (bewerkingen zoals het weergeven van de mapstructuur of het lezen of schrijven van data). 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](#).

Instellingen van het onderdeel Apparaatcontrole

| Parameter  | Beschrijving  |
|--|---|
| <b>Aanvragen voor tijdelijke toegang toestaan</b><br><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i> | Als het selectievakje is ingeschakeld, wordt de knop <b>Toegang vragen</b> in de lokale interface van Kaspersky Endpoint Security weergegeven. Met een klik op deze knop opent u het venster <b>Toegang tot apparaat vragen</b> . In dit venster kan de gebruiker tijdelijke toegang tot een geblokkeerd apparaat aanvragen.  |
| <b>Apparaten en wifi-netwerken</b>   | In deze tabel ziet u alle mogelijke soorten apparaten volgens de classificatie van het onderdeel Apparaatcontrole, inclusief de respectieve toegangsstatus.   |
| <b>Verbindingsbussen</b>   | Een lijst met alle beschikbare verbindingbussen volgens de classificatie van Apparaatcontrole, inclusief de respectieve toegangsstatus.   |
| <b>Vertrouwde apparaten</b>  | Lijst met vertrouwde apparaten en gebruikers die toegang hebben tot deze apparaten.   |
| <b>Anti-Bridging</b>   | <p>Anti-Bridging belet het maken van netwerkbruggen door het gelijktijdig maken van meerdere netwerkverbindingen op een computer te voorkomen. Hiermee kunt u een bedrijfsnetwerk beschermen tegen aanvallen via onbeveiligde, onbevoegde netwerken.</p> <p>Anti-Bridging blokkeert het maken van meerdere verbindingen volgens de prioriteiten van apparaten. Hoe hoger een apparaat in de lijst staat, hoe hoger de prioriteit ervan.</p> <p>Als een actieve verbinding en een nieuwe verbinding van hetzelfde type zijn (bijvoorbeeld wifi), blokkeert Kaspersky Endpoint Security de actieve verbinding en staat het toe dat de nieuwe verbinding wordt gemaakt.</p> <p>Als een actieve verbinding en een nieuwe verbinding van een ander type zijn (bijvoorbeeld een netwerkadapter en wifi), blokkeert Kaspersky Endpoint Security de verbinding met de laagste prioriteit en staat het de verbinding met de hoogste prioriteit toe.</p> <p>Anti-Bridging ondersteunt de volgende soorten apparaten: netwerkadapter, wifi en modem.</p> |
| <b>Berichtsjablonen</b>  | <b>Bericht over blokkering.</b> Sjabloon van het bericht dat verschijnt wanneer een geblokkeerd apparaat toegang tot een geblokkeerd apparaat probeert te krijgen. Dit bericht verschijnt ook wanneer een gebruiker een bewerking met inhoud op een apparaat probeert uit voeren wanneer die bewerking werd geblokkeerd voor die gebruiker.   |

**Bericht aan beheerder.** Een sjabloon van het bericht dat naar de netwerkbeheerder wordt verstuurd als de gebruiker vindt dat de geblokkeerde toegang tot het apparaat of het verboden gebruik van de inhoud op het apparaat een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: **Bericht over blokkering van toegang tot apparaat aan beheerder**. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie **User requests**. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.

## Programmacontrole

Programmacontrole beheert het opstarten van applicaties op de computers van gebruikers. Hiermee kunt u een bedrijfsbeveiligingsbeleid implementeren bij het gebruik van programma's. Programmacontrole vermindert ook het risico op computerinfectie door de toegang tot programma's te beperken.

De configuratie van programmacontrole bestaat uit de volgende stappen:

### 1. [Categorieën van programma's aanmaken](#).

De beheerder maakt categorieën applicaties die de beheerder wil beheren. Programmacategorieën zijn bedoeld voor alle computers in het bedrijfsnetwerk, ongeacht de beheergroepen. Om een categorie aan te maken, kunt u de volgende criteria gebruiken: KL-categorie (bijvoorbeeld, *Browsers*), bestandshash, programmaverkoper en andere criteria.

### 2. [Regels van programmacontrole maken](#).

De beheerder maakt regels van programmacontrole in het beleid voor de beheergroep. De regel omvat de categorieën van programma's en de opstartstatus van programma's uit deze categorieën: geblokkeerd of toegestaan.

### 3. [De modus van Programmacontrole selecteren](#).

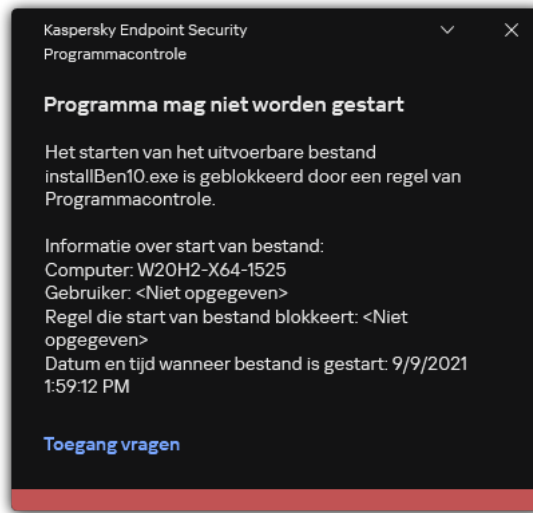
De beheerder kiest de modus voor het werken met programma's die niet zijn opgenomen in een van de regels (programma denylist en allowlist).

Wanneer een gebruiker probeert een verboden programma te starten, blokkeert Kaspersky Endpoint Security het starten van het programma en wordt er een melding weergegeven (zie de onderstaande afbeelding).

Er is een *testmodus* beschikbaar om de configuratie van programmacontrole te controleren. In deze modus doet Kaspersky Endpoint Security het volgende:

- Staat het opstarten van programma's toe, inclusief verboden programma's.
- Geeft een melding weer over het opstarten van een verboden programma en voegt informatie toe aan het rapport op de computer van de gebruiker.
- Stuurt gegevens over het opstarten van verboden programma's naar Kaspersky Security Center.





Melding van programmacontrole

## Over de uitvoermodi van programmacontrole

Het onderdeel Programmacontrole werkt in twee modi:

- **Denylist** In deze modus staat programmacontrole toe dat alle gebruikers alle programma's starten, behalve de programma's die verboden zijn in programmacontrole.

Deze modus van Programmacontrole is standaard ingeschakeld.

- **Allowlist** In deze modus staat Programmacontrole niet toe dat de gebruikers alle programma's starten, behalve de programma's die toegestaan zijn en niet verboden zijn in de regels van Programmacontrole.

Als de Toestaan-regels van Programmacontrole 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.

U kunt de [aanbevelingen voor de configuratie van regels voor programmacontrole in de modus allowlist](#) lezen.

De werking van Programmacontrole 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](#).

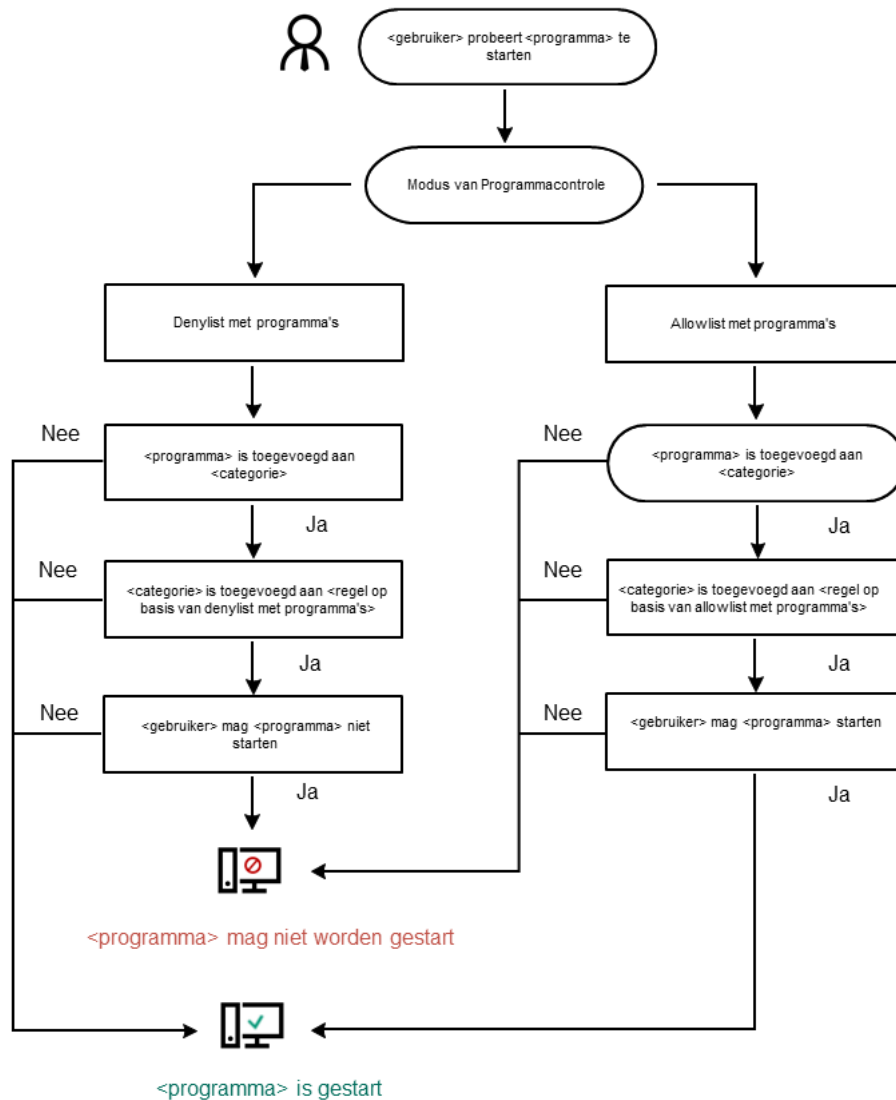
De regels van Programmacontrole die worden aangemaakt in de Beheerconsole van Kaspersky Security Center zijn gebaseerd op aangepaste categorieën van programma's en niet op uitvoerings- of uitzonderingsvoorwaarden zoals in de lokale interface van Kaspersky Endpoint Security.

- [Informatie over geïnstalleerde programma's op netwerkcomputers ontvangen](#).

Dit is de reden waarom u wordt aanbevolen om Kaspersky Security Center te gebruiken voor de configuratie van de werking van het onderdeel Programmacontrole.

## Algoritme voor werking van programmacontrole

Kaspersky Endpoint Security gebruikt een algoritme om een beslissing te nemen over het starten van een programma (zie onderstaande afbeelding).



Algoritme voor werking van programmacontrole

Instellingen van het onderdeel Programmacontrole

| Parameter                | Beschrijving   |
|--------------------------|--|
| Test mode                | Als de schakelaar is ingeschakeld, staat Kaspersky Endpoint Security toe dat een programma dat wordt geblokkeerd in de huidige modus van Programmacontrole wordt gestart en registreert het informatie over de opstart van dat programma in het rapport.   |
| Application Control Mode | <p>U kunt één van de volgende opties kiezen:</p> <ul style="list-style-type: none"> <li><b>Denylist</b> Als deze optie is geselecteerd, staat Programmacontrole toe dat alle gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de blokkeringsregels van Programmacontrole is voldaan.</li> <li><b>Allowlist</b> Als deze optie is geselecteerd, staat Programmacontrole niet toe dat gebruikers programma's starten, behalve in gevallen waarbij aan de voorwaarden van de uitvoeringsregels van Programmacontrole is voldaan.</li> </ul> <p>Wanneer de modus <b>Allowlist</b> is geselecteerd, worden twee regels van Programmacontrole automatisch aangemaakt:</p> <ul style="list-style-type: none"> <li><b>Golden Image:</b></li> </ul> |

|   |  |
|---|--|
|   | <ul style="list-style-type: none"> <li>• <b>Vertrouwde updaters:</b></li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>U kunt de instellingen van automatisch aangemaakte regels niet bewerken, noch kunt u die regels verwijderen. U kunt deze regels inschakelen of uitschakelen.</p> </div>  |
| <p><b>Control DLL modules load (significantly increases the load on the system)</b></p> | <p>Als het selectievakje is ingeschakeld, wordt het laden van DLL-modules wanneer gebruikers programma's proberen te starten gecontroleerd door Kaspersky Endpoint Security. Informatie over de DLL-module en het programma dat deze DLL-module heeft geladen, wordt in het rapport geregistreerd.</p> <div style="border: 1px solid black; background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Wanneer u de controle over het laden van DLL-modules en stuurprogramma's inschakelt, moet u in de instellingen van programmacontrole controleren of een van de volgende regels is ingeschakeld: de standaard <b>Golden Image</b>-regel of een andere regel die de KI-categorie "Vertrouwde certificaten" bevat en ervoor zorgt dat vertrouwde DLL-modules en stuurprogramma's worden geladen voordat Kaspersky Endpoint Security wordt gestart. Als u de controle van het laden van DLL-modules en stuurprogramma's inschakelt wanneer de regel <b>Golden Image</b> is uitgeschakeld, kan het besturingssysteem instabiel worden.</p> </div> <p>Kaspersky Endpoint Security bewaakt alleen DLL-modules en stuurprogramma's die zijn geladen nadat het selectievakje werd ingeschakeld. Nadat u het selectievakje hebt geselecteerd, wordt aanbevolen om de computer opnieuw op te starten om ervoor te zorgen dat het programma alle DLL-modules en stuurprogramma's controleert, inclusief degenen die zijn geladen voordat Kaspersky Endpoint Security opstart.</p> |
| <p><b>Message templates</b></p>   | <p><b>Message about blocking</b> Sjabloon van het bericht dat wordt weergegeven bij de activering van een regel van Programmacontrole die de start van een programma blokkeert.</p> <p><b>Message to administrator</b> Sjabloon van het bericht dat een gebruiker naar de LAN-beheerder van het bedrijf kan sturen als de gebruiker denkt dat een programma per ongeluk is geblokkeerd. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: <b>Bericht over blokkering van programmastart aan beheerder</b>. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie <b>User requests</b>. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.</p>  |

## Adaptieve controle op afwijkingen

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

Het onderdeel Adaptieve controle op afwijkingen bewaakt en blokkeert acties die niet kenmerkend zijn voor de computers in het bedrijfsnetwerk. Adaptieve controle op afwijkingen gebruikt een aantal regels om afwijkend gedrag bij te houden (bijvoorbeeld de regel *Start van Windows PowerShell via Office-programma*). Regels worden door Kaspersky-experts gemaakt op basis van kenmerkende scenario's van malware-activiteit. U kunt configureren hoe Adaptieve controle op afwijkingen elke regel moet gebruiken en bijvoorbeeld toestaan dat PowerShell-scripts voor de automatisering van bepaalde workflows worden uitgevoerd. Kaspersky Endpoint Security updatet de reeks regels samen met de programmadatabases. Updates voor deze regels moeten [handmatig worden bevestigd](#).

## Instellingen van Adaptieve controle op afwijkingen

De configuratie van Adaptieve controle op afwijkingen bestaat uit de volgende stappen:

### 1. Adaptieve controle op afwijkingen trainen.

Nadat u Adaptieve controle op afwijkingen hebt ingeschakeld, werken de regels ervan in de *trainingsmodus*. Tijdens de training bewaakt Adaptieve controle op afwijkingen de activering van regels en verstuurt het activeringsgebeurtenissen naar Kaspersky Security Center. Elke regel heeft een eigen trainingsduur. De duur van de trainingsmodus is door experts van Kaspersky vastgelegd. Normaal is de trainingsmodus twee weken actief.

Als een regel tijdens de training niet één keer is geactiveerd, zal Adaptieve controle op afwijkingen de acties die zijn gekoppeld aan deze regel als niet typisch beschouwen. Kaspersky Endpoint Security blokkeert dan alle acties die aan die regel zijn gekoppeld.

Als een regel tijdens de training is geactiveerd, registreert Kaspersky Endpoint Security gebeurtenissen in het [rapport over de activering van regels](#) en de opslagplaats **Triggering of rules in Smart Training state**.

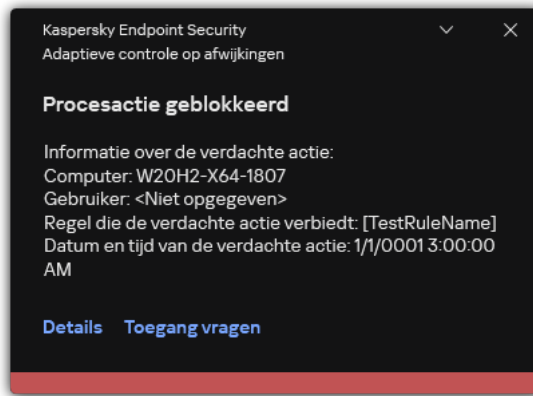
### 2. Rapport over activering van regels analyseren.

De beheerder analyseert het [rapport over de activering van regels](#) of de inhoud van de opslagplaats **Triggering of rules in Smart Training state**. Daarna kan de beheerder het gedrag van Adaptieve controle op afwijkingen selecteren wanneer de regel wordt geactiveerd: blokkeren of toestaan. De beheerder kan ook verder bewaken hoe de regel werkt en de duur van de training verlengen. Als de beheerder geen actie onderneemt, blijft het programma ook werken in de trainingsmodus. De periode van de trainingsmodus wordt dan herstart.

Adaptieve controle op afwijkingen wordt in realtime geconfigureerd. Adaptieve controle op afwijkingen wordt via de volgende kanalen geconfigureerd:

- Adaptieve controle op afwijkingen begint automatisch de acties te blokkeren voor de regels die nooit zijn geactiveerd in de trainingsmodus.
- Kaspersky Endpoint Security voegt nieuwe regels toe of verwijdert oude regels.
- De beheerder configureert de werking van Adaptieve controle op afwijkingen na de controle van het rapport over de activering van regels en de inhoud van de opslagplaats **Triggering of rules in Smart Training state**. U wordt aanbevolen het rapport over de activering van regels en de inhoud van de opslagplaats **Triggering of rules in Smart Training state** te controleren.

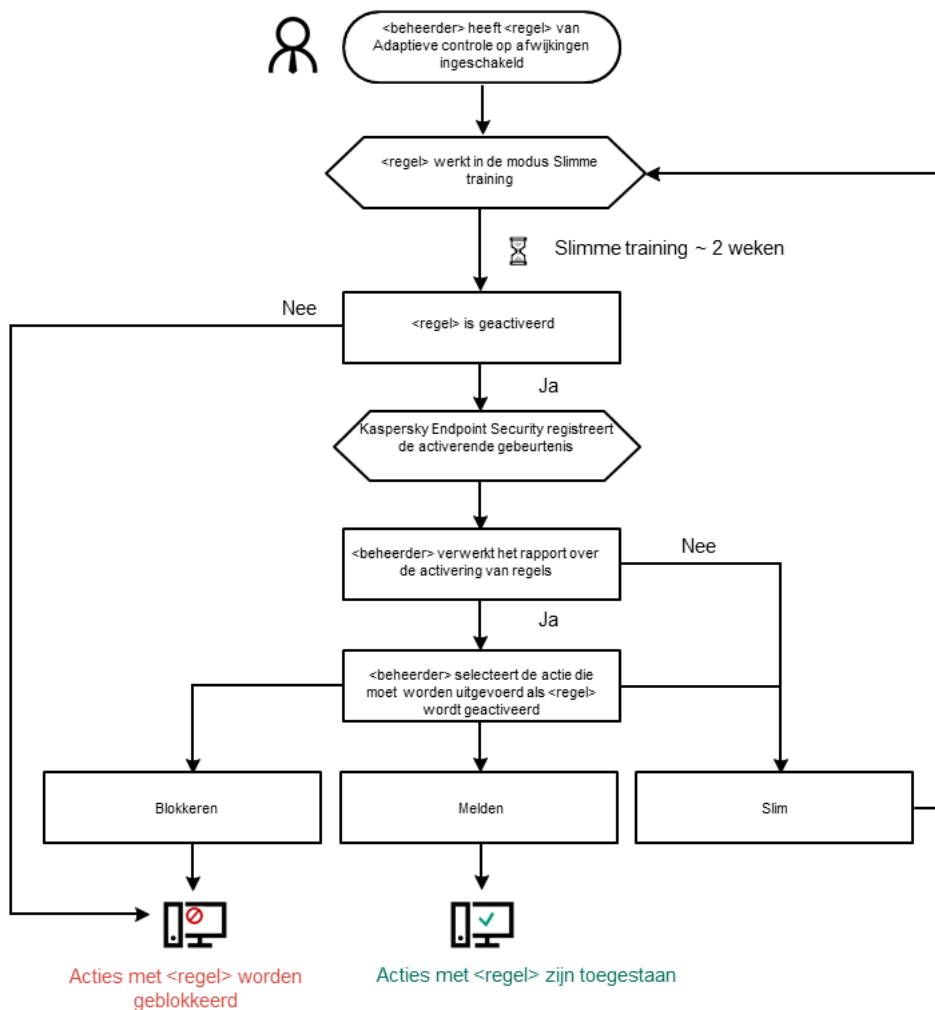
Wanneer een schadelijk programma een actie probeert uit te voeren, blokkeert Kaspersky Endpoint Security de actie en toont het een melding (zie onderstaande afbeelding).



Melding van Adaptieve controle op afwijkingen

## Algoritme voor de werking van Adaptieve controle op afwijkingen

Op basis van het volgende algoritme (zie onderstaande afbeelding) beslist Kaspersky Endpoint Security of een actie van een regel al dan niet mag worden uitgevoerd.



Instellingen van het onderdeel Adaptieve controle op afwijkingen

| Parameter  | Beschrijving  |
|--|---|
| <p><b>Rapport over status van regels voor Adaptieve controle op afwijkingen</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p>   | <p>Dit rapport bevat informatie over de status van de detectieregels van Adaptieve controle op afwijkingen (bijvoorbeeld <i>Uit of Blokkeren</i>). Het rapport wordt voor alle beheergroepen gegenereerd.</p>   |
| <p><b>Rapport over geactiveerde regels voor Adaptieve controle op afwijkingen</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p>Dit rapport bevat informatie over afwijkende acties die door Adaptieve controle op afwijkingen zijn gedetecteerd. Het rapport wordt voor alle beheergroepen gegenereerd.</p>   |
| <p><b>Regels</b></p>   | <p>Tabel met regels voor Adaptieve controle op afwijkingen. Regels worden door Kaspersky-experts gemaakt op basis van kenmerkende scenario's van potentiële schadelijke activiteit.</p>   |
| <p><b>Sjablonen</b></p>  | <p><b>Bericht over blokkering.</b> Sjabloon van het bericht dat wordt weergegeven aan een gebruiker wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd voor de blokkering van een afwijkende actie.</p> <p><b>Bericht aan beheerder.</b> Sjabloon van het bericht dat een gebruiker kan versturen naar de beheerder van het lokale bedrijfsnetwerk als de gebruiker vindt dat de blokkering een vergissing is. Nadat de gebruiker toegang heeft gevraagd, stuurt Kaspersky Endpoint Security een gebeurtenis naar Kaspersky Security Center: <b>Bericht over blokkering van programma-activiteit aan beheerder</b>. De beschrijving van de gebeurtenis bevat een bericht aan de beheerder met vervangende variabelen. U kunt deze gebeurtenissen in de Kaspersky Security Center-console bekijken met de voorgedefinieerde gebeurtenisselectie <b>User requests</b>. Als uw organisatie Kaspersky Security Center niet heeft geïmplementeerd of als er geen verbinding is met de beheerserver, stuurt het programma een bericht aan de beheerder naar het opgegeven e-mailadres.</p> |

## Endpoint Sensor

Endpoint Sensor is geen onderdeel van Kaspersky Endpoint Security 11.4.0.

U kunt de Endpoint Sensor beheeren in de Webconsole van Kaspersky Security Center en in de Beheerconsole van Kaspersky Security Center. Het is niet mogelijk om Endpoint Sensor met de Cloudconsole van Kaspersky Security Center te beheeren.

*Endpoint Sensor* is ontworpen voor gebruik met Kaspersky Anti Targeted Attack Platform. Kaspersky *Anti Targeted Attack Platform* is een oplossing voor de tijdige detectie van geavanceerde dreigingen, zoals doelgerichte aanvallen, geavanceerde aanhoudende dreigingen (Advanced Persistent Threats, APT), en zero-day-aanvallen en anderen. Kaspersky Anti Targeted Attack platform omvat twee functionele blokken: Kaspersky Targeted Attack (hierna ook wel 'KATA' genoemd) en Kaspersky Endpoint Detection and Response (hierna ook wel 'KEDR' genoemd). U kunt KEDR afzonderlijk aanschaffen. Voor informatie over de oplossing raadpleegt u de [Help van Kaspersky Anti Targeted Attack Platform](#).

Bij het beheer van Endpoint Sensor zijn er de volgende beperkingen:

- U kunt Endpoint Sensor-instellingen in een beleid configureren op voorwaarde dat u versie 11.0.0 tot 11.3.0 van Kaspersky Endpoint Security gebruikt op de computer. Voor meer informatie over de configuratie van Endpoint Sensor-instellingen via het beleid leest u de [Help-artikelen voor de vorige versies van Kaspersky Endpoint Security](#).
- Als u Kaspersky Endpoint Security 11.4.0 of hoger gebruikt op de computer, kunt u geen Endpoint Sensor-instellingen in een beleid configureren.

Endpoint Sensor is op clientcomputers geïnstalleerd. Op deze computers bewaakt het onderdeel voortdurend processen, actieve netwerkverbindingen en bestanden die worden gewijzigd. Endpoint Sensor stuurt de informatie door naar de KATA-server.

De functionaliteit van het onderdeel is beschikbaar op de volgende besturingssystemen:

- Windows 7 Service Pack 1 Home/Professional/Enterprise
- Windows 8.1 Professional/Enterprise
- Windows 10 RS3 Home/Pro/Education/Enterprise
- Windows 10 RS4 Home/Pro/Education/Enterprise
- Windows 10 RS5 Home/Pro/Education/Enterprise
- Windows 10 RS6 Home/Pro/Education/Enterprise
- Windows Server 2008 R2 Foundation/Standard/Enterprise (64-bits)
- Windows Server 2012 Foundation/Standard/Enterprise (64-bits)
- Windows Server 2012 R2 Foundation/Standard/Enterprise (64-bits)
- Windows Server 2016 Essentials/Standard (64-bits)

Voor gedetailleerde informatie over de werking van KATA raadpleegt u de [Help van Kaspersky Anti Targeted Attack Platform](#).

# Kaspersky Sandbox

Kaspersky Endpoint Security 11.7.0 heeft nu een ingebouwde agent voor integratie met de Kaspersky Sandbox-oplossing. *De Kaspersky Sandbox-oplossing* detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Kaspersky Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Kaspersky Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Kaspersky Sandbox-servers). Voor meer informatie over de oplossing gaat u naar de [Help van Kaspersky Sandbox](#).

Het onderdeel kan alleen worden beheerd met behulp van de Kaspersky Security Center-webconsole. U kunt dit onderdeel niet beheren met de Beheerconsole (MMC).

## Kaspersky Sandbox-componentinstellingen

| Parameter                              | Beschrijving  |
|--|---|
| <b>Server TLS certificate</b>          | Om een vertrouwde verbinding met Kaspersky Sandbox-servers te configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat toevoegen aan Kaspersky Sandbox-servers en het Kaspersky Endpoint Security-beleid. Voor details over het voorbereiden van het certificaat en het toevoegen van het certificaat aan servers, raadpleegt u <a href="#">Kaspersky Sandbox Help</a> .  |
| <b>Timeout</b>                         | Verbindingstime-out voor Kaspersky Sandbox-server. Nadat de geconfigureerde time-out is verstreken, stuurt Kaspersky Endpoint Security een verzoek naar de volgende server. U kunt de verbindingstime-out voor Kaspersky Sandbox verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder.   |
| <b>Kaspersky Sandbox request queue</b> | Grootte van de verzoekwachtrijmap. Wanneer een object op de computer wordt geopend (uitvoerbaar bestand gestart of document geopend, bijvoorbeeld in DOCX- of PDF-indeling), dan kan Kaspersky Endpoint Security het object ook verzenden om te worden gescand door Kaspersky Sandbox. Als er meerdere verzoeken zijn, maakt Kaspersky Endpoint Security een verzoekwachtrij aan. Standaard is de grootte van de verzoekwachtrijmap beperkt tot 100 MB. Nadat de maximale grootte is bereikt, stopt Kaspersky Sandbox met het toevoegen van nieuwe verzoeken aan de wachtrij en stuurt het de bijbehorende gebeurtenis naar Kaspersky Security Center. U kunt de grootte van de verzoekwachtrijmap configureren, afhankelijk van uw serverconfiguratie.   |
| <b>Kaspersky Sandbox servers</b>       | Kaspersky Sandbox server-verbindinginstellingen. De servers gebruiken geïmplementeerde virtuele afbeeldingen van Microsoft Windows-besturingssystemen om objecten uit te voeren die moeten worden gescand. U kunt een IP-adres (IPv4 of IPv6) of een volledig gekwalificeerde domeinnaam invoeren.  |
| <b>Action on threat detection</b>      | <p><b>Move copy to Quarantine, delete object.</b> Als deze optie is geselecteerd, verwijdert Kaspersky Endpoint Security het schadelijke object dat op de computer is gevonden. Voordat het object wordt verwijderd, maakt Kaspersky Endpoint Security een back-up voor het geval dat het object later moet worden teruggezet. Kaspersky Endpoint Security plaatst de back-up in Quarantaine.</p> <p><b>Run scan of critical areas.</b> Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak <a href="#">Kritieke Gebiedenscan</a>. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.</p> <p><b>Create IOC scan task.</b> Als deze optie geselecteerd is, maakt Kaspersky Endpoint Security automatisch de <a href="#">IOC scant</a>taak (autonome IOC-scant). Voor deze taak kunt u de uitvoermodus, het scanbereik en de actie voor IOC-detectie configureren: object verwijderen, de taak <a href="#">Kritieke gebiedenscan</a> uitvoeren. Om andere instellingen van de <a href="#">IOC-scant</a>taak te wijzigen, gaat u naar de taakinstellingen.</p> |



|                          |   |
|--------------------------|---|
| <b>IOC scan scope</b>    | <p><b>Critical file areas.</b> Als deze optie geselecteerd is, voert Kaspersky Endpoint Security alleen een IOC-scan uit in kritieke bestandsgebieden van de computer: kernelgeheugen en opstartsectoren.</p> <p><b>File areas on system drives of the computer.</b> ALS deze optie geselecteerd is, voert Kaspersky Endpoint Security een IOC-scan uit op het systeemstation van de computer.</p>  |
| <b>Run IOC scan task</b> | <p><b>Manually.</b> Scan uitvoeren waarin u de <i>IOC-scant</i>taak handmatig kunt uitvoeren wanneer u dat wil.</p> <p><b>After threat is detected.</b> Uitvoermodus waarin Kaspersky Endpoint Security de <i>IOC-scant</i>taak automatisch wordt uitgevoerd wanneer een dreiging wordt gedetecteerd.</p> <p><b>Run only when the computer is idle.</b> Uitvoermodus waarin Kaspersky Endpoint Security de <i>IOC-scant</i>taak uitvoert als de screensaver actief is of het scherm wordt vergrendeld. Als de gebruiker de computer ontgrendelt, pauzeert Kaspersky Endpoint Security de scant</p> taak. Dit betekent dat de taak enkele dagen in beslag kan nemen. |

## Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 heeft nu een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing (hierna ook 'EDR Optimum' genoemd). Kaspersky Endpoint Security 11.8.0 heeft nu een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Expert-oplossing (hierna ook 'EDR Expert' genoemd). *Kaspersky Endpoint Detection and Response Optimum* is een bereik van oplossingen die de IT-infrastructuur van het bedrijf beschermt tegen geavanceerde digitale dreigingen. De functionaliteit van de oplossingen combineert de automatische detectie van dreigingen met de respons op deze dreigingen om geavanceerde aanvallen te neutraliseren, zoals nieuwe exploits, ransomware, bestandsloze aanvallen en methoden met legitieme hulpprogramma's van het systeem. EDR Expert biedt meer bewaking van dreigingen en reactiefunctiefunctionaliteit dan EDR Optimum. Voor details over de oplossingen, bekijk [Kaspersky Endpoint Detection and Response Optimum Help](#) en [Kaspersky Endpoint Detection and Response Expert Help](#).

Kaspersky Endpoint Detection and Response controleert en analyseert de ontwikkeling van dreigingen en geeft *beveiligingspersoneel* of *beheerders* informatie over de potentiële aanval die noodzakelijk is voor een tijdige reactie. Kaspersky Endpoint Detection and Response geeft detectiegegevens in een apart venster weer. *Detectiegegevens* zijn een hulpmiddel waar alle verzamelde informatie over een gedetecteerde dreiging zichtbaar is. Deze detectiegegevens bevatten bijvoorbeeld de geschiedenis van bestanden die op de computer terechtkomen. Voor details over het beheren van detectiegegevens, raadpleegt u de [Help van Kaspersky Endpoint Detection and Response Optimum](#) en de [Help van Kaspersky Endpoint Detection and Response Expert](#).

U kunt de EDR Optimum component configureren in Webconsole en Cloud Console. Componentinstellingen voor EDR Expert zijn alleen beschikbaar in Cloud Console.

### Instellingen Endpoint Detection and Response

| Parameter                | Beschrijving   |
|--------------------------|--|
| <b>Network isolation</b> | <p>Automatische isolatie van de computer van het netwerk als reactie op gedetecteerde bedreigingen.</p> <p>Wanneer netwerkisolatie is ingeschakeld, verbreekt het programma alle actieve verbindingen en blokkeert alle nieuwe TCP/IP-verbindingen op de computer. Het programma laat alleen de volgende verbindingen actief:</p> <ul style="list-style-type: none"> <li>• Verbindingen die worden vermeld in uitzonderingen voor netwerkisolatie.</li> <li>• Verbindingen gestart door Kaspersky Endpoint Security-services.</li> <li>• Verbindingen gestart door de Kaspersky Security Center Administration-agent.</li> </ul> |

|  |  |
|--|--|
| <p><b>Automatically unlock isolated computer in N uren</b></p>   | <p>Netwerkisolatie kan na een bepaalde tijd automatisch of handmatig worden uitgeschakeld. Standaard schakelt Kaspersky Endpoint Security netwerkisolatie 5 uur na het begin van de isolatie uit.</p>  |
| <p><b>Network isolation exclusions</b></p>                       | <p>Lijst van regels voor uitzonderingen van netwerkisolatie. Netwerkverbindingen die overeenkomen met de regels, worden niet geblokkeerd op computers wanneer netwerkisolatie is ingeschakeld.</p> <p>Om uitzonderingen van netwerkisolatie te configureren, kunt u een lijst gebruiken van <i>standaard netwerkprofielen</i>. Standaard omvatten uitzonderingen netwerkprofielen die regels bevatten die zorgen voor een ononderbroken werking van apparaten met de DNS/DHCP-server en DNS/DHCP-clientrollen. U kunt ook de instellingen van standaard netwerkprofielen wijzigen of uitzonderingen handmatig definiëren.</p> <div style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p>Uitzonderingen die zijn opgegeven in beleidseigenschappen worden alleen toegepast als netwerkisolatie automatisch wordt ingeschakeld als reactie op een gedetecteerde dreiging. Uitzonderingen opgegeven in computereigenschappen worden alleen toegepast als netwerkisolatie handmatig is ingeschakeld in computereigenschappen in de Kaspersky Security Center-console of in alarmdetails.</p> </div> |
| <p><b>Execution prevention</b></p>                               | <p>Beheer de uitvoering van uitvoerbare bestanden en scripts en het openen van bestanden in office-bestandsindelingen. U kunt bijvoorbeeld voorkomen dat onveilige toepassingen op de geselecteerde computer worden uitgevoerd. Preventie van uitvoering ondersteunt <a href="#">een reeks office-bestandsextensies</a> en <a href="#">een reeks scriptinterpreters</a>.</p>   |
| <p><b>Action on execution or opening of forbidden object</b></p> | <p><b>Block and write to report.</b> In deze modus blokkeert het programma de uitvoering van objecten of het openen van documenten die voldoen aan de criteria van regels voor preventie van uitvoering. Het programma publiceert ook een gebeurtenis over pogingen om objecten uit te voeren of documenten te openen naar het Windows-gebeurtenislogboek en het Kaspersky Security Center-gebeurtenislogboek.</p> <p><b>Log events only.</b> In deze modus publiceert Kaspersky Endpoint Security een gebeurtenis over pogingen om uitvoerbare objecten uit te voeren of documenten te openen die voldoen aan de criteria van de regel voor preventie voor het Windows-gebeurtenislogboek en Kaspersky Security Center, maar blokkeert niet de poging om het object of document uit te voeren of te openen. Deze modus is standaard geselecteerd.</p>   |
| <p><b>Regels voor preventie van uitvoering</b></p>               | <p>Lijst van regels voor preventie van uitvoering van objecten. <i>Regels voor preventie van uitvoering</i> is een set criteria waarmee het programma rekening houdt bij het reageren op een objectuitvoering, bijvoorbeeld bij het blokkeren van objectuitvoering. Het programma identificeert bestanden aan de hand van hun paden of checksums berekend met behulp van MD5- en SHA256-hash-algoritmen.</p>   |

## Full Disk Encryption

U kunt een encryptietechnologie selecteren: Kaspersky Disk Encryption of BitLocker-stationsversleuteling (hierna ook gewoon "BitLocker" genoemd).

### Kaspersky Disk Encryption

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 [Authenticatie-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 aangesloten op de computer worden ingevoerd of moeten de gebruikersnaam en het wachtwoord van de Authenticatie-agent-account worden ingevoerd. Dit account is door de lokale netwerkbeheerder aangemaakt met taken voor het [beheer van accounts voor Authenticatie-agenten](#). Dit account is gebaseerd op een Microsoft Windows-account waarmee een gebruiker zich bij het besturingssysteem aanmeldt. U kunt ook [Enmalige aanmelding \(SSO\)-technologie gebruiken](#), waarmee u zich automatisch bij het besturingssysteem kunt aanmelden met de gebruikersnaam en het wachtwoord van de account voor authenticatie-agent.

De gebruikersauthenticatie in Authenticatie-agent kan op twee manieren worden uitgevoerd:

- Typ de naam en het wachtwoord van het account in Authenticatie-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.

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.

## BitLocker-stationsversleuteling

*BitLocker* is een encryptietechnologie die is ingebouwd in Windows-besturingssystemen. Met Kaspersky Endpoint Security kunt u BitLocker beheeren. BitLocker zorgt voor de encryptie van logische volumes. BitLocker kan niet worden gebruikt voor de encryptie van verwisselbare schijven. Voor meer informatie over BitLocker raadpleegt u de [Microsoft-documentatie](#).

BitLocker biedt veilige opslag van toegangssleutels met behulp van een vertrouwde platformmodule. Een *Trusted Platform Module (TPM)* is een microchip die ontwikkeld is om basisfuncties voor beveiliging te leveren (bijvoorbeeld de opslag van encryptiesleutels). Een Trusted Platform Module wordt meestal op het moederbord van de computer geïnstalleerd en werkt via de hardwarebus samen met alle andere systeemonderdelen. Het gebruik van TPM is de veiligste manier om BitLocker-toegangssleutels op te slaan, aangezien TPM pre-opstartverificatie van de systeemintegriteit biedt. U kunt nog steeds schijven encrypten op een computer zonder een TPM. In dat geval wordt de toegangssleutel geëncrypt met een wachtwoord. BitLocker gebruikt de volgende authenticatiemethoden:

- TPM.
- TPM en pincode.
- Wachtwoord.

Na het encrypten van een schijf, maakt BitLocker een hoofdsleutel aan. Kaspersky Endpoint Security stuurt de hoofdsleutel naar Kaspersky Security Center zodat u [de toegang tot de schijf kunt herstellen](#), bijvoorbeeld als een gebruiker het wachtwoord is vergeten.

Als een gebruiker een schijf van encryptie voorziet met BitLocker, stuurt Kaspersky Endpoint Security [informatie over schijfencryptie naar Kaspersky Security Center](#). Kaspersky Endpoint Security stuurt de hoofdsleutel echter niet naar Kaspersky Security Center. Hierdoor is het niet mogelijk om de toegang tot de schijf te herstellen met Kaspersky Security Center. Om te zorgen dat BitLocker correct werkt met Kaspersky Security Center, moet u [de schijf decrypten](#) en [de schijf opnieuw encrypten](#) met een beleid. U kunt een schijf lokaal decrypten of een beleid gebruiken.

Na het encrypten van de harde schijf van het systeem, moet de gebruiker BitLocker-verificatie doorlopen om het besturingssysteem op te starten. Na de authenticatieprocedure kunnen gebruikers met BitLocker inloggen. BitLocker ondersteunt geen technologie voor eenmalige aanmelding (SSO).

Als u Windows-groepsbeleid gebruikt, schakelt u BitLocker-beheer uit in de beleidsinstellingen. De beleidsinstellingen van Windows kunnen in strijd zijn met de beleidsinstellingen van Kaspersky Endpoint Security. Bij het encrypten van een schijf kunnen er fouten optreden.

#### Onderdeelininstellingen van Kaspersky Disk Encryption

| Parameter   | Beschrijving   |
|---|--|
| <b>Encryptiemodus</b>   | <p><b>Alle harde schijven encrypten.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle harde schijven geëncrypt door het programma.</p> <p>Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om het programma te installeren.</p> <p><b>Alle harde schijven decrypten.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle eerder geëncrypte harde schijven gedecrypt door het programma.</p> <p><b>Leave unchanged.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden schijven in hun eerdere staat gelaten door het programma. Als de schijf geëncrypt was, blijft deze geëncrypt. Als de schijf gedecrypt was, blijft deze gedecrypt. Deze optie is standaard geselecteerd.</p>  |
| <b>Accounts in Authenticatie-agent automatisch voor Windows-gebruikers aanmaken tijdens encryptie</b> | <p>Als dit selectievakje is ingeschakeld, maakt het programma Authenticatie-agent-accounts op basis van de lijst met Windows-gebruikersaccounts op de computer. Kaspersky Endpoint Security gebruikt standaard alle lokale en domeinaccounts waarmee de gebruiker zich de afgelopen 30 dagen heeft aangemeld bij het besturingssysteem.</p>  |
| <b>Instellingen voor aanmaak van account in Authenticatie-agent</b>                                   | <p><b>Alle accounts op de computer.</b> All accounts op de computer die op enig moment actief zijn geweest.</p> <p><b>Alle domeinaccounts op de computer.</b> Alle accounts op de computer die behoren tot een bepaald domein en die op enig moment actief zijn geweest.</p> <p><b>Alle lokale accounts op de computer.</b> Alle lokale accounts op de computer die op enig moment actief zijn geweest.</p> <p><b>Service-account met een eenmalig wachtwoord.</b> De service-account is nodig om toegang te krijgen tot de computer, bijvoorbeeld wanneer de gebruiker het wachtwoord vergeet. U kunt de service-account ook gebruiken als reserve-account. U moet de naam invoeren van de service-account (standaard, ServiceAccount). Kaspersky Endpoint Security maakt automatisch een wachtwoord aan. U kunt het wachtwoord vinden in de <a href="#">Kaspersky Security Center-console</a>.</p> <p><b>Lokale beheerder.</b> Kaspersky Endpoint Security maakt een authenticatie-agent-gebruikersaccount voor de lokale beheerder van de computer.</p> <p><b>Computerbeheerder.</b> Kaspersky Endpoint Security maakt een authenticatie-agent-gebruikersaccount aan voor de account van de computerbeheerder. In Active Directory kunt u zien welke account de rol van computerbeheerder heeft in de eigenschappen van de computer. Standaard is de rol van computerbeheerder niet gedefinieerd, dat wil zeggen dat deze niet overeenkomt met een account.</p> |

|  |   |
|--|---|
|  | <p><b>Actief account.</b> Kaspersky Endpoint Security maakt automatisch een authenticatie-agent-account aan voor de account die actief is op het moment van schijfversleuteling.</p>  |
| <p><b>Accounts in Authenticatie-agent automatisch aanmaken voor alle gebruikers van deze computer bij aanmelding</b></p> | <p>Als dit selectievakje is ingeschakeld, zoekt het programma informatie over Windows-gebruikersaccounts op de computer voordat Authenticatie-agent wordt gestart. Als Kaspersky Endpoint Security een Windows-gebruikersaccount detecteert die geen Authenticatie-agent-account heeft, maakt het programma een nieuw account aan voor toegang tot geëncrypte schijven. Het nieuwe Authenticatie-agent-account heeft de volgende standaardinstellingen: alleen met wachtwoord beveiligde aanmelding en wachtwoordwijziging bij eerste authenticatie. Daarom hoeft u niet <a href="#">handmatig Authenticatie-agent-accounts</a> toe te voegen met de taak <i>Authenticatie-agent-accounts beheren</i> voor computers met reeds versleutelde stations.</p>   |
| <p><b>Ingevoerde gebruikersnaam in Authenticatie-agent opslaan</b></p>   | <p>Als het selectievakje is ingeschakeld, slaat het programma de naam van het account in Authenticatie-agent op. U hoeft de accountnaam niet in te voeren de volgende keer dat u in Authenticatie-agent de Authenticatie met hetzelfde account probeert te voltooien.</p>   |
| <p><b>Alleen gebruikte schijfruimte encrypten (snellere encryptie)</b></p>   | <p>Dit selectievakje schakelt de optie in of uit waarmee u het encryptiegebied beperkt tot de gebruikte sectoren van de harde schijf. Via deze beperking kunt u de encryptie verkorten.</p> <div data-bbox="507 891 1493 1081" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>De in- of uitschakeling van de functie <b>Encrypt used disk space only (Windows 8 and later versions)</b> na het starten van de encryptie wijzigt deze instelling niet tenzij de harde schijven zijn gedecrypt. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.</p> </div> <p>Als het selectievakje is ingeschakeld, worden alleen delen van de harde schijf die door bestanden worden ingenomen geëncrypt. Kaspersky Endpoint Security encrypt automatisch nieuwe gegevens wanneer die worden toegevoegd.</p> <p>Als het selectievakje is uitgeschakeld, wordt de gehele harde schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden.</p> <div data-bbox="507 1384 1493 1615" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Deze optie wordt aanbevolen voor nieuwe harde schijven waarvan de gegevens niet zijn gewijzigd of verwijderd. Als u een encryptie toepast op een harde schijf die al wordt gebruikt, wordt u aanbevolen de gehele harde schijf te encrypten. Op deze manier zijn alle gegevens beschermd, zelfs verwijderde gegevens die mogelijk kunnen worden hersteld.</p> </div> <p>Dit selectievakje is standaard uitgeschakeld.</p> |
| <p><b>Ondersteuning voor verouderde USB-apparaten gebruiken (niet aanbevolen)</b></p>                                    | <p>Dit selectievakje schakelt de functie Ondersteuning voor verouderde USB-apparaten in of uit. <i>Ondersteuning voor verouderde USB-apparaten</i> is een BIOS/UEFI-functie waarmee u USB-apparaten (zoals een beveiligingstoken) kunt gebruiken tijdens de opstart van de computer voordat het besturingssysteem wordt gestart (BIOS-modus). Ondersteuning voor verouderde USB-apparaten is niet van invloed op de ondersteuning voor USB-apparaten nadat het besturingssysteem is gestart.</p> <p>Als het selectievakje is ingeschakeld, wordt de ondersteuning voor USB-apparaten tijdens de initiële opstart van de computer ingeschakeld.</p>  |

|                               |   |
|-------------------------------|---|
|                               | <p>Wanneer de functie Ondersteuning voor verouderde USB-apparaten is ingeschakeld, biedt de Authenticatie-agent in de BIOS-modus geen ondersteuning voor het werken met tokens via USB. U wordt aanbevolen deze optie alleen te gebruiken als er een probleem met de compatibiliteit van de hardware is en voor computers waarop het probleem is opgetreden.</p>  |
| <b>Wachtwoordinstellingen</b> | <p>Instellingen voor wachtwoordsterkte voor Authenticatie-agent-accounts. U kunt ook de technologie Eenmalige aanmelding (SSO) inschakelen.</p> <p>Met SSO-technologie kunt u dezelfde accountgegevens gebruiken om toegang tot geëncrypte harde schijven te krijgen en u bij het besturingssysteem aan te melden.</p> <p>Als het selectievakje is ingeschakeld, moet u de accountgegevens invoeren om toegang te krijgen tot de geëncrypte harde schijven en om vervolgens automatisch aangemeld te worden bij het besturingssysteem.</p> <p>Als het selectievakje is uitgeschakeld, moet u voor toegang tot de geëncrypte harde schijven en de daaropvolgende aanmelding bij het besturingssysteem eerst de gebruikersgegevens voor toegang tot de geëncrypte harde schijven invoeren en vervolgens de gegevens van het gebruikersaccount voor het besturingssysteem.</p> |
| <b>Helpteksten</b>            | <p><b>Authenticatie.</b> Helptekst die wordt weergegeven in het venster Authenticatie-agent bij het invoeren van aanmeldingsgegevens voor een account.</p> <p><b>Wachtwoord wijzigen.</b> Helptekst die wordt weergegeven in het venster Authenticatie-agent wanneer het wachtwoord voor het Authenticatie-agent-account wordt gewijzigd.</p> <p><b>Wachtwoord herstellen.</b> Helptekst die wordt weergegeven in het venster Authenticatie-agent wanneer het wachtwoord voor het Authenticatie-agent-account wordt hersteld.</p>   |

Instellingen component BitLocker-stationsversleuteling

| Parameter   | Beschrijving  |
|---|---|
| <b>Encryptiemodus</b>   | <p><b>Alle harde schijven encrypten.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle harde schijven geëncrypt door het programma.</p> <p>Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om het programma te installeren.</p> <p><b>Alle harde schijven decrypten.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle eerder geëncrypte harde schijven gedecrypt door het programma.</p> <p><b>Leave unchanged.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden schijven in hun eerdere staat gelaten door het programma. Als de schijf geëncrypt was, blijft deze geëncrypt. Als de schijf gedecrypt was, blijft deze gedecrypt. Deze optie is standaard geselecteerd.</p> |
| <b>Gebruik van BitLocker-authenticatie inschakelen die preboot-</b> | <p>Dit selectievakje schakelt het gebruik van een authenticatie met gegevensinvoer vóór de opstart in of uit, zelfs als het platform niet geschikt is voor invoer tijdens de opstart (bijvoorbeeld met toetsenborden op aanraakschermen van tablets).</p>   |



|  |  |
|--|--|
| <p><b>toetsenbordinvoer op tablets vereist</b></p>                           | <div data-bbox="451 73 1493 232" style="border: 1px solid black; padding: 5px;"> <p>Het touchscreen van tabletcomputers is niet beschikbaar in de preboot-omgeving. Om de BitLocker-authenticatie op tabletcomputers te voltooien, moet de gebruiker bijvoorbeeld een USB-toetsenbord aansluiten.</p> </div> <p>Als het selectievakje is ingeschakeld, is het gebruik van een authenticatie met invoer vóór de opstart toegestaan. U wordt aanbevolen deze instelling alleen te gebruiken voor apparaten die beschikken over alternatieve middelen voor gegevensinvoer vóór de opstart, zoals een USB-toetsenbord naast schermtoetsenborden.</p> <p>Als het selectievakje is uitgeschakeld, is BitLocker-stationsversleuteling niet mogelijk op tablets.</p>   |
| <p><b>Hardware-encryptie gebruiken</b></p>                                   | <p>Als het selectievakje is ingeschakeld, past het programma een hardware-encryptie toe. Hiermee kunt u sneller encrypten en gebruikt u minder computerbronnen.</p>  |
| <p><b>Alleen gebruikte schijfruimte encrypten (Windows 8 en nieuwer)</b></p> | <p>Dit selectievakje schakelt de optie in of uit waarmee u het encryptiegebied beperkt tot de gebruikte sectoren van de harde schijf. Via deze beperking kunt u de encryptie verkorten.</p> <div data-bbox="451 801 1493 994" style="border: 1px solid black; padding: 5px;"> <p>De in- of uitschakeling van de functie <b>Encrypt used disk space only (Windows 8 and later versions)</b> na het starten van de encryptie wijzigt deze instelling niet tenzij de harde schijven zijn gedecrypt. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.</p> </div> <p>Als het selectievakje is ingeschakeld, worden alleen delen van de harde schijf die door bestanden worden ingenomen geëncrypt. Kaspersky Endpoint Security encrypt automatisch nieuwe gegevens wanneer die worden toegevoegd.</p> <p>Als het selectievakje is uitgeschakeld, wordt de gehele harde schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden.</p> <div data-bbox="451 1296 1493 1525" style="border: 1px solid black; padding: 5px;"> <p>Deze optie wordt aanbevolen voor nieuwe harde schijven waarvan de gegevens niet zijn gewijzigd of verwijderd. Als u een encryptie toepast op een harde schijf die al wordt gebruikt, wordt u aanbevolen de gehele harde schijf te encrypten. Op deze manier zijn alle gegevens beschermd, zelfs verwijderde gegevens die mogelijk kunnen worden hersteld.</p> </div> <p>Dit selectievakje is standaard uitgeschakeld.</p> |
| <p><b>Authenticatie-instellingen</b></p>                                     | <p><b>Use password (Windows 8 and later versions)</b></p> <p>Als deze optie is geselecteerd, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om een wachtwoord in te voeren als die toegang tot een geëncrypte schijf probeert te krijgen.</p> <p>Deze optie kan worden geselecteerd als geen Trusted Platform Module (TPM) wordt gebruikt.</p> <p><b>Use Trusted Platform Module (TPM)</b></p> <p>Als deze optie is geselecteerd, gebruikt BitLocker een Trusted Platform Module (TPM).</p>  |

Een *Trusted Platform Module (TPM)* is een microchip die ontwikkeld is 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.

Voor computers met Windows 7 of Windows Server 2008 R2 is alleen encryptie met een TPM-module beschikbaar. Als geen TPM-module is geïnstalleerd, is BitLocker-encryptie niet mogelijk. Het gebruik van een wachtwoord op deze computers wordt niet ondersteund.

Een apparaat met een Trusted Platform Module kan encryptiesleutels aanmaken die alleen met het apparaat kunnen worden gedecrypt. Een Trusted Platform Module encrypt encryptiesleutels met een eigen rootopslagsleutel. De rootopslagsleutel wordt in de Trusted Platform Module opgeslagen. Dit biedt meer bescherming tegen pogingen om de encryptiesleutels te hacken.

Deze actie is standaard geselecteerd.

U kunt een extra beveiligingslaag instellen voor toegang tot de encryptiesleutel en de sleutel coderen met een wachtwoord of een pincode:

- **Use PIN for TPM.** Als dit selectievakje geselecteerd is, dan kan een gebruiker een pincode gebruiken om toegang tot een encryptiesleutel te krijgen die in een Trusted Platform Module (TPM) is opgeslagen. Als dit selectievakje is uitgeschakeld, mogen gebruikers geen pincodes gebruiken. Om toegang te krijgen tot de encryptiesleutel, moet een gebruiker het wachtwoord invoeren. U kunt de gebruiker toestaan om een geavanceerde pincode te gebruiken. Met *Geavanceerde pincode* kunt u naast cijfers ook andere tekens gebruiken: hoofdletters en kleine letters, speciale tekens en spaties.
- **Use Trusted Platform Module (TPM); if it is unavailable - use password.** Als het selectievakje is ingeschakeld, kan de gebruiker een wachtwoord gebruiken om toegang tot encryptiesleutels te krijgen wanneer geen Trusted Platform Module (TPM) beschikbaar is.

Als het selectievakje is uitgeschakeld en de TPM niet beschikbaar is, zal de volledige schijfencryptie niet starten.

## File Level Encryption

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 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.



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

Bestandsencryptie heeft de volgende speciale kenmerken:

- 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.
- Kaspersky Endpoint Security encrypt geen bestanden die het besturingssysteem en geïnstalleerde programma's kunnen beschadigen als ze worden gewijzigd. De volgende bestanden en mappen met alle geneste mappen staan bijvoorbeeld op de lijst met encryptie-uitzonderingen:
  - %WINDIR%;
  - %PROGRAMFILES% en %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 bestandsencryptie.

Onderdeelinstellingen voor File Level Encryption

| Parameter        | Beschrijving  |
|------------------|---|
| Encryptiemodus   | <p><b>Ongewijzigd laten.</b> Als deze optie is geselecteerd, laat Kaspersky Endpoint Security bestanden en mappen ongewijzigd door ze niet te encrypten of te decrypten.</p> <p><b>Volgens regels.</b> Als deze optie is geselecteerd, zal Kaspersky Endpoint Security bestanden en mappen encrypten volgens de encryptieregels, bestanden en mappen decrypten volgens de decryptieregels en de toegang van programma's tot geëncrypte bestanden regelen volgens de programmaregels.</p> <p><b>Alles decrypten.</b> Als deze optie is geselecteerd, worden alle geëncrypte bestanden en mappen gedecrypt door Kaspersky Endpoint Security.</p>  |
| Encryption rules | <p>Op dit tabblad ziet u encryptieregels voor bestanden die op lokale schijven zijn opgeslagen. U kunt als volgt bestanden toevoegen:</p> <ul style="list-style-type: none"><li>• <b>Vooraf gedefinieerde mappen.</b> In Kaspersky Endpoint Security kunt u de volgende gebieden toevoegen:<ul style="list-style-type: none"><li><b>Documenten.</b> Bestanden in de standaardmap <i>Documenten</i> van het besturingssysteem, en de submappen ervan.</li><li><b>Favorieten.</b> Bestanden in de standaardmap <i>Favorieten</i> van het besturingssysteem en de submappen ervan.</li><li><b>Bureaublad.</b> Bestanden in de standaardmap <i>Bureaublad</i> van het besturingssysteem, en de submappen ervan.</li><li><b>Tijdelijke bestanden.</b> Tijdelijke bestanden voor de werking van op de computer geïnstalleerde programma's. Microsoft Office-programma's maken bijvoorbeeld tijdelijke bestanden aan die back-ups van documenten bevatten.</li><li><b>Outlook-bestanden.</b> Bestanden voor de werking van het e-mailprogramma Outlook: gegevensbestanden (PST), offline gegevensbestanden (OST), offline adresboekbestanden (OAB) en persoonlijk-adresboekbestanden (PAB).</li></ul></li><li>• <b>Aangepaste map.</b> U kunt het pad naar de map typen. Houd u bij het toevoegen van een mappad aan de volgende regels:</li></ul> |

|  |   |
|--|---|
|  | <p>Gebruik een omgevingsvariabele (bijvoorbeeld %FOLDER%\UserFolder\). U kunt een omgevingsvariabele slechts één keer gebruiken en alleen aan het begin van het pad.</p> <p>Gebruik geen relatieve paden.</p> <p>Gebruik de tekens * en ? niet.</p> <p>Gebruik geen UNC-paden.</p> <p>Gebruik ; of , als scheidingsteken.</p> <ul style="list-style-type: none"> <li>• <b>Bestanden op extensie.</b> U kunt extensiegroepen in de lijst selecteren, zoals de extensiegroep <i>Archieven</i>. U kunt de bestandsextensie ook handmatig toevoegen.</li> </ul> |
| <b>Decryption rules</b>                    | Op dit tabblad ziet u decryptieregels voor bestanden die op lokale schijven zijn opgeslagen.  |
| <b>Rules for applications</b>              | Op het tabblad ziet u een tabel met toegangsregels voor geëncrypte bestanden voor programma's en encryptieregels voor bestanden die door individuele programma's zijn aangemaakt of gewijzigd.  |
| <b>Encrypted package password settings</b> | Wachtwoordsterkte-eisen waaraan moet worden voldaan bij het maken van geëncrypte pakketten.   |

## Encryptie van verwisselbare schijven

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

Kaspersky Endpoint Security ondersteunt de encryptie van bestanden in FAT32- en NTFS-bestandssystemen. Als een verwisselbare schijf met een niet-ondersteund bestandssysteem is aangesloten op de computer, wordt de encryptietaak voor deze verwisselbare schijf beëindigd met een fout en wijst Kaspersky Endpoint Security de alleen-lezenstatus toe aan de verwisselbare schijf.

Om gegevens op verwisselbare schijven te beschermen, kunt u de volgende soorten encryptie gebruiken:

- Full Disk Encryption (FDE)

Encryptie van de volledige verwisselbare schijf, inclusief het bestandssysteem.

Het is niet mogelijk om toegang te krijgen tot geëncrypte gegevens buiten het bedrijfsnetwerk. Het is ook onmogelijk om toegang te krijgen tot geëncrypte gegevens binnen het bedrijfsnetwerk als de computer niet is verbonden met Kaspersky Security Center (bijvoorbeeld op een gastcomputer).

- File Level Encryption (FLE).

Encryptie van alleen bestanden op een verwisselbare schijf. Het bestandssysteem blijft ongewijzigd.

Encryptie van bestanden op verwisselbare schijven biedt de mogelijkheid om toegang te krijgen tot gegevens buiten het bedrijfsnetwerk met behulp van een speciale modus met de naam [\*portable modus\*](#).

Tijdens de encryptie maakt Kaspersky Endpoint Security een hoofdsleutel aan. Kaspersky Endpoint Security slaat de hoofdsleutel op in de volgende opslagplaatsen:

- Kaspersky Security Center.

- Gebruikerscomputer.

De hoofdsleutel is geëncrypt met de geheime sleutel van de gebruiker.

- Verwisselbare schijf.

De hoofdsleutel is gecodeerd met de openbare sleutel van Kaspersky Security Center.

Nadat de encryptie is voltooid, zijn de gegevens op de verwisselbare schijf toegankelijk binnen het bedrijfsnetwerk alsof ze zich op een gewone niet geëncrypte verwisselbare schijf bevinden.

## Toegang tot geëncrypte gegevens

Wanneer een verwisselbare schijf met geëncrypte gegevens is aangesloten, voert Kaspersky Endpoint Security de volgende acties uit:

1. Controleert op een hoofdsleutel in de lokale opslag op de computer van de gebruiker.

Als de hoofdsleutel wordt gevonden, krijgt de gebruiker toegang tot de gegevens op de verwisselbare schijf.

Als de hoofdsleutel niet wordt gevonden, voert Kaspersky Endpoint Security de volgende acties uit:

- a. Stuurt een verzoek naar Kaspersky Security Center.

Na ontvangst van het verzoek stuurt Kaspersky Security Center een antwoord met de hoofdsleutel.

- b. Kaspersky Endpoint Security slaat de hoofdsleutel op in de lokale opslag op de computer van de gebruiker voor daaropvolgende bewerkingen met de geëncrypte verwisselbare schijf.

2. Decrypt de gegevens.

## Speciale functies voor encryptie van verwisselbare schijf

Encryptie van verwisselbare schijven heeft de volgende speciale functies:

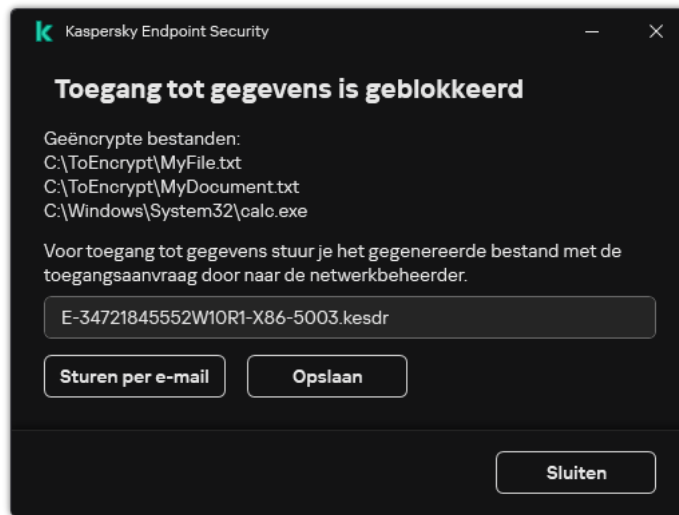
- Het beleid met vooraf geconfigureerde instellingen voor de encryptie van verwisselbare schijven is opgesteld voor een specifieke groep beheerde computers. Daarom is het resultaat van de toepassing van het geconfigureerde Kaspersky Security Center-beleid voor de encryptie of decryptie van verwisselbare schijven afhankelijk van de computer waarop de verwisselbare schijf is aangesloten.
- Kaspersky Endpoint Security encrypt of decrypt geen alleen-lezenbestanden die op verwisselbare schijven zijn opgeslagen.
- 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

| Parameter                           | Beschrijving   |
|-------------------------------------|--|
| <b>Manage encryption</b>            | <p><b>Encrypt entire removable drive.</b> Als deze optie is geselecteerd wanneer het beleid met de opgegeven encryptie-instellingen voor verwisselbare schijven wordt toegepast, worden verwisselbare schijven sector per sector geëncrypt door Kaspersky Endpoint Security (inclusief de bestandssystemen).</p> <p><b>Encrypt all files.</b> Als deze optie is geselecteerd wanneer het 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. De inhoud van het bestandssysteem van een verwisselbare schijf, inclusief de mapstructuur en de namen van geëncrypte bestanden, zijn niet geëncrypt en blijven toegankelijk.</p> <p><b>Encrypt new files only.</b> Als deze optie is geselecteerd wanneer het 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 of gewijzigd op verwisselbare schijven geëncrypt door Kaspersky Endpoint Security. Deze encryptiemodus is handig als een verwisselbare schijf zowel voor persoonlijk als professioneel gebruik wordt ingezet. Met deze encryptiemodus kunt u alle oude bestanden ongewijzigd laten en alleen de bestanden encrypten die de gebruiker aanmaakt op een werkcomputer waarop Kaspersky Endpoint Security is geïnstalleerd en de encryptiefunctie is ingeschakeld. Hierdoor is de toegang tot persoonlijke bestanden altijd beschikbaar, ongeacht of Kaspersky Endpoint Security met ingeschakelde encryptiefunctie is geïnstalleerd op de computer.</p> <p><b>Decrypt entire removable drive.</b> Als deze optie is geselecteerd wanneer het 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.</p> <p><b>Leave unchanged.</b> Als deze optie is geselecteerd wanneer het beleid is toegepast, worden schijven in hun eerdere staat gelaten door het programma. Als de schijf geëncrypt was, blijft deze geëncrypt. Als de schijf gedecrypt was, blijft deze gedecrypt. Deze optie is standaard geselecteerd.</p> |
| <b>Portable mode</b>                | <p>Dit selectievakje schakelt de voorbereiding van een verwisselbare schijf in of uit die de toegang tot bestanden op deze verwisselbare schijf mogelijk maakt op computers buiten het bedrijfsnetwerk.</p> <p>Als dit selectievakje is ingeschakeld en het beleid wordt toegepast, wordt de gebruiker door Kaspersky Endpoint Security gevraagd om een wachtwoord op te geven alvorens de bestanden op een verwisselbare schijf worden geëncrypt. Het wachtwoord is vereist om toegang tot geëncrypte bestanden op een verwisselbare schijf te krijgen op computers buiten het bedrijfsnetwerk. U kunt de wachtwoordsterkte configureren.</p> <p>De portable modus is beschikbaar voor de modi <b>Encrypt all files</b> of <b>Encrypt new files only</b>.</p>   |
| <b>Encrypt used disk space only</b> | <p>Met dit selectievakje kunt u de encryptiemodus waarin alleen gebruikte schijfsectoren worden geëncrypt inschakelen of uitschakelen. Deze modus wordt aanbevolen voor nieuwe schijven waarvan de gegevens niet zijn gewijzigd of verwijderd.</p> <p>Als het selectievakje is ingeschakeld, worden alleen delen van de schijf die door bestanden worden ingenomen geëncrypt. Kaspersky Endpoint Security encrypt automatisch nieuwe gegevens wanneer die worden toegevoegd.</p> <p>Als het selectievakje is uitgeschakeld, wordt de gehele schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden.</p> <p>De mogelijkheid om alleen gebruikte ruimte te encrypten is alleen beschikbaar voor de modus <b>Encrypt entire removable drive</b>.</p>  |

|   |   |
|---|---|
|   | <p>Na de start van de encryptie wordt deze instelling niet gewijzigd door de inschakeling of uitschakeling van de functie <b>Encrypt used disk space only</b>. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.</p>   |
| <b>Encryption rules for selected devices</b>                | <p>In deze tabel ziet u de apparaten waarvoor aangepaste encryptieregels zijn gedefinieerd. U kunt op de volgende manieren encryptieregels maken voor afzonderlijke verwisselbare schijven:</p> <ul style="list-style-type: none"> <li>• Een verwisselbare schijf toevoegen uit de lijst met vertrouwde apparaten voor apparaatbeheer.</li> <li>• Handmatig een verwisselbare schijf toevoegen: <ul style="list-style-type: none"> <li>• Op apparaat-ID (Hardware-ID of HWID)</li> <li>• Op apparaatmodel: Leverancier-ID (VID) en product-ID (PID)</li> </ul> </li> </ul>  |
| <b>Allow encryption of removable drives in offline mode</b> | <p>Als dit selectievakje is ingeschakeld, worden verwisselbare schijven door Kaspersky Endpoint Security geëncrypt zelf als er geen verbinding met Kaspersky Security Center is. In dit geval worden de vereiste gegevens voor de decryptie van verwisselbare schijven bewaard op de harde schijf van de computer waarop de verwisselbare schijf is aangesloten en worden deze niet naar Kaspersky Security Center verstuurd.</p> <p>Als het selectievakje is uitgeschakeld, worden verwisselbare schijven niet geëncrypt door Kaspersky Endpoint Security als er geen verbinding met Kaspersky Security Center is.</p> |
| <b>Portable mode password settings</b>                      | <p>Wachtwoordsterkte-instellingen voor Portable bestandsbeheer.</p>   |

## Sjablonen (gegevensencryptie)

Na gegevensencryptie kan Kaspersky Endpoint Security de toegang tot gegevens beperken, bijvoorbeeld vanwege een wijziging in de infrastructuur van de organisatie en een wijziging in de Kaspersky Security Center Administration Server. Als een gebruiker geen toegang heeft tot geëncrypte gegevens, kan de gebruiker de beheerder om toegang tot de gegevens vragen. Met andere woorden, de gebruiker moet een bestand met een toegangsverzoek naar de beheerder sturen. De gebruiker moet vervolgens het antwoordbestand dat hij of zij van de beheerder heeft ontvangen, uploaden naar Kaspersky Endpoint Security. Met Kaspersky Endpoint Security kunt u via e-mail toegang tot gegevens aanvragen bij de beheerder (zie onderstaande afbeelding).



Toegang tot geëncrypte gegevens aanvragen

Er wordt een sjabloon verstrekt voor het melden van onvoldoende toegang tot geëncrypte gegevens. Om het de gebruiker gemakkelijk te maken kunt u de volgende velden invullen:

- **To.** Voer het e-mailadres in van de beheerdersgroep met rechten voor de functies voor gegevensencryptie.
- **Subject.** Voer het onderwerp van de e-mail in met uw verzoek voor toegang tot geëncrypte bestanden. U kunt bijvoorbeeld labels toevoegen om berichten te filteren.
- **Bericht.** Wijzig zo nodig de inhoud van het bericht. U kunt variabelen gebruiken om de benodigde gegevens op te halen (bijvoorbeeld de % USER\_NAME%-variabele).

## Uitzonderingen

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.

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. Een beheerder kan een gebruiker ook toestaan om zijn eigen lokale vertrouwde zone voor een specifieke computer te creëren. Op deze manier kunnen gebruikers hun eigen lokale lijsten met uitsluitingen en vertrouwde programma's maken naast de algemene vertrouwde zone in een beleid.

## Scanuitzonderingen

Een *scanuitzondering* is een reeks voorwaarden waaraan moet worden voldaan zodat een bepaald object niet door Kaspersky Endpoint Security wordt gescand op virussen en andere dreigingen.

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 dit soort programma's door indringers worden gebruikt als een hulpmiddel. Voor informatie over legitieme software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen, raadpleegt u de [website van de IT-encyclopedie van Kaspersky](#).

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 IT-encyclopedie van Kaspersky toe aan de vertrouwde zone. Voorbeeld: u gebruikt vaak het Radmin-programma voor het externe beheer van computers. 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 IT-encyclopedie van Kaspersky voorkomt.

Als een programma dat informatie verzamelt en deze ter verwerking verstuurt op uw computer is geïnstalleerd, kan Kaspersky Endpoint Security dit programma classificeren als malware. 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:

- [Gedragsdetectie](#).
- [Exploit-preventie](#).
- [Host Intrusion Prevention](#).
- [File Threat Protection](#).
- [Web Threat Protection](#).
- [Mail Threat Protection](#).
- [Scantaken](#).

## Lijst met vertrouwde programma's

De *lijst met vertrouwde programma's* is een lijst met programma's waarvan de bestands- en netwerkactiviteit (inclusief schadelijke 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. Een programma dat toegevoegd is aan de lijst met vertrouwde programma's, wordt echter uitgesloten van scans door Kaspersky Endpoint Security.


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.

Instellingen van uitzonderingen

| Parameter                             | Beschrijving  |
|---------------------------------------|---|
| <b>Soorten gedetecteerde objecten</b> | <p>Kaspersky Endpoint Security detecteert en blokkeert altijd virussen, wormen en Trojans, ongeacht de geconfigureerde programma-instellingen. Ze kunnen de computer immers grote schade toebrengen.</p> <ul style="list-style-type: none"><li>• <a href="#">Virussen en wormen</a> </li></ul> |



**Subcategorie:** virussen en wormen (Virussen\_en\_Wormen)

**Veiligheidsrisico:** hoog

Klassieke virussen en wormen voeren acties uit die niet door de gebruiker zijn toegestaan. Ze kunnen kopieën van zichzelf maken die zichzelf kunnen repliceren.

### **Klassiek virus**

Wanneer een klassiek virus de computer binnendringt, infecteert het een bestand, wordt het actief, voert het schadelijke acties uit en voegt het kopieën van zichzelf toe aan andere bestanden.

Een klassiek virus vermenigvuldigt zich alleen in lokale bronnen van de computer; het kan zelf geen andere computers binnendringen. Het kan alleen op een andere computer terechtkomen als het een kopie van zichzelf toevoegt aan een bestand dat in een gedeelde map of op een geplaatste cd is opgeslagen of als de gebruiker een e-mailbericht met een geïnfecteerd bestand als bijlage doorstuurt.

Klassieke viruscode kan diverse delen van computers, besturingssystemen en programma's binnendringen. Afhankelijk van de omgeving worden virussen verdeeld in *bestandsvirussen*, *opstartvirussen*, *scriptvirussen* en *macrovirussen*.

Virussen kunnen bestanden infecteren door middel van diverse technieken. *Overschrijvende* virussen schrijven hun code over de licentie van het bestand dat wordt geïnfecteerd, waardoor de inhoud van het bestand wordt gewist. Het geïnfecteerde bestand werkt niet meer en kan niet worden hersteld. *Parasitaire* virussen wijzigen bestanden waardoor ze volledig of deels functioneel blijven. *Aanvullende virussen* wijzigen geen bestanden maar maken duplicaten. Wanneer een geïnfecteerd bestand wordt geopend, wordt een duplicaat ervan (wat eigenlijk een virus is) gemaakt. De volgende soorten virussen komen ook voor: *gekoppelde virussen*, *OBJ-virussen*, *LIB-virussen*, *broncodevirussen* en vele andere.

### **Worm**

Net als bij een klassiek virus wordt de code van een worm geactiveerd en voert deze schadelijke acties uit nadat deze een computer is binnengedrongen. Wormen hebben hun naam gekregen vanwege hun mogelijkheid om van de ene computer naar de andere te "kruipen" en kopieën via talrijke gegevenskanalen te verspreiden zonder toestemming van de gebruiker.

Wormen onderscheiden zich vooral van elkaar door de wijze waarop ze zich verspreiden. In de volgende tabel ziet u een overzicht van diverse soorten wormen die zijn geclassificeerd volgens de wijze waarop ze zich verspreiden.

Wijzen waarop wormen zich verspreiden

| Type | Naam       | Beschrijving                 |
|------|------------|------------------------------|
| E-   | E-mailworm | Deze verspreiden zich via e- |

|                 |                        |   |
|-----------------|------------------------|---|
| <b>mailworm</b> |                        | <p>mail.</p> <p>Een geïnfecteerd e-mailbericht bevat een bijlage met een kopie van een worm of een koppeling naar een bestand dat is geüpload naar een website die mogelijk gehackt is of speciaal voor dat doel is gemaakt. Wanneer u de bijlage opent, wordt de worm geactiveerd. Wanneer u op de koppeling klikt en vervolgens het bestand downloadt en opent, begint de worm ook schadelijke acties uit te voeren. Daarna verspreidt de worm kopieën van zichzelf, zoekt die andere e-mailadressen en verstuurt die geïnfecteerde berichten ernaar.</p> |
| <b>IM-Worm</b>  | Wormen voor IM-clients | <p>Deze verspreiden zich via instant messengers.</p> <p>Doorgaans gebruiken zulke wormen de lijst met contactpersonen van de gebruiker om berichten met een koppeling naar een bestand met een kopie van de worm op een website te versturen. Als de gebruiker het bestand downloadt en opent, wordt de worm geactiveerd.</p>   |
| <b>IRC-Worm</b> | Online chatwormen      | <p>Deze verspreiden zich via Internet Relay Chats, servicesystemen waarmee mensen met elkaar kunnen communiceren in real time via het internet.</p> <p>Deze wormen publiceren een bestand met een kopie van zichzelf of een kopie naar het bestand in een chat. Als de gebruiker het bestand downloadt en opent, wordt de worm geactiveerd.</p>   |
| <b>Net-worm</b> | Netwerkwormen          | Deze wormen verspreiden zich via computernetwerken.   |

|                 |                                   |   |
|-----------------|-----------------------------------|---|
|                 |                                   | <p>In tegenstelling tot andere wormen kan een normale netwerkworm zich verspreiden zonder hulp van de gebruiker. De worm zoekt in het lokale netwerk naar computers die programma's met kwetsbaarheden bevatten. Hiertoe stuurt de worm een speciaal netwerkpakket (exploit) dat de wormcode of een deel ervan bevat. Als er een 'kwetsbare' computer in het netwerk is, ontvangt die computer zo'n netwerkpakket. Wanneer de worm de computer volledig is binnengedrongen, activeert die zichzelf.</p>   |
| <b>P2P-worm</b> | Netwerkwormen voor bestandsdeling | <p>Deze verspreiden zich via peer-to-peernetwerken voor bestandsdeling.</p> <p>Om een P2P-netwerk te infiltreren, kopieert de worm zichzelf naar een map voor bestandsdeling die doorgaans op de computer van de gebruiker staat. Het P2P-netwerk toont informatie over dit bestand zodat de gebruiker het geïnfecteerde bestand in het netwerk kan "vinden", zoals andere bestanden, en het bestand vervolgens kan downloaden en openen.</p> <p>Meer geavanceerde wormen emuleren het netwerkprotocol van een specifiek P2P-netwerk: ze geven positieve antwoorden op zoekopdrachten en bieden kopieën van zichzelf aan die de gebruiker dan kan downloaden.</p> |
| <b>Worm</b>     | Andere soorten wormen             | <p>Enkele andere soorten wormen zijn:</p> <ul style="list-style-type: none"> <li>• Wormen die kopieën van zichzelf verspreiden via netwerkbronnen. Met behulp van de functies van het besturingssysteem zoeken ze beschikbare netwerkmappen, maken ze verbinding met computers via het internet en proberen ze volledige toegang tot hun stations te krijgen. In tegenstelling tot de eerder beschreven wormen kunnen</li> </ul>  |

andere soorten wormen zichzelf niet activeren en moet de gebruiker een bestand met een kopie van de worm openen om de worm te activeren.

- Wormen die een andere methode dan de methoden in de eerdere tabel gebruiken om zich te verspreiden (bijvoorbeeld wormen die zich verspreiden via mobiele telefoons).

- [Trojans \(inclusief ransomware\)](#) 

## Subcategorie: Trojans

### Veiligheidsrisico: hoog

In tegenstelling tot wormen en virussen kunnen Trojans zich niet zelf repliceren. Ze dringen bijvoorbeeld de computer binnen via e-mail of een browser wanneer de gebruiker een geïnfecteerde webpagina bezoekt. Trojans worden met de hulp van de gebruiker gestart. Net nadat ze zijn gestart, beginnen ze schadelijke acties uit te voeren.

Verskillende Trojans gedragen zich anders op geïnfecteerde computers. De belangrijkste functies van Trojans zijn het blokkeren, wijzigen of vernietigen van gegevens en het uitschakelen van computers of netwerken. Trojans kunnen ook bestanden ontvangen of versturen, bestanden uitvoeren, berichten op het scherm weergeven, webpagina's opvragen, programma's downloaden en installeren en de computer opnieuw opstarten.

Hackers gebruiken vaak "sets" van verschillende Trojans.

In de volgende tabel leest u hoe Trojans zich kunnen gedragen.

Gedrag van Trojans op een geïnfecteerde computer

| Type                  | Naam                       | Beschrijving  |
|-----------------------|----------------------------|---|
| <b>Trojan-ArcBomb</b> | Trojans – "archiefbommen"  | Tijdens het uitpakken worden deze archieven zo groot dat de werking van de computer wordt beïnvloed.<br><br>Als de gebruiker zo'n archief probeert uit te pakken, kan de computer vertragen of geblokkeerd raken. De harde schijf wordt gevuld met "lege" gegevens.<br>"Archiefbommen" zijn in het bijzonder gevaarlijk voor bestands- en mailservers. Als de server een automatisch systeem voor de verwerking van inkomende gegevens gebruikt, kan de "archiefbom" de server laten crashen. |
| <b>Backdoor</b>       | Trojans voor extern beheer | Deze worden beschouwd als de gevaarlijkste soort Trojan. Hun werking is vergelijkbaar met programma's voor extern beheer die op computers zijn geïnstalleerd.   |

|                       |                      |   |
|-----------------------|----------------------|---|
|                       |                      | Deze programma's installeren zichzelf ongemerkt op de computer, waardoor de indringer de computer op afstand kan beheren.   |
| <b>Trojan</b>         | Trojans              | <p>Deze omvatten de volgende schadelijke programma's:</p> <ul style="list-style-type: none"> <li>• <b>Klassieke Trojans.</b> Deze programma's voeren alleen de voornaamste functies van Trojans uit: gegevens blokkeren, wijzigen of vernietigen en computers of netwerken uitschakelen. In tegenstelling tot de andere soorten Trojans die in de tabel zijn beschreven, hebben ze geen geavanceerde functies.</li> <li>• <b>Veelzijdige Trojans.</b> Deze programma's hebben geavanceerde functies die kenmerken zijn voor diverse soorten Trojans.</li> </ul> |
| <b>Trojan-Ransom</b>  | Trojans voor losgeld | Ze "gijzelen" de gegevens van de gebruiker, wijzigen of blokkeren ze of beïnvloeden de werking van de computer zodanig dat de gebruiker geen gegevens kan gebruiken. De indringer vraagt een geldsom aan de gebruiker in ruil voor een programma waarmee de werking van de computer en de toegang tot de gegevens op de computer kan worden hersteld.   |
| <b>Trojan-Clicker</b> | Trojan clickers      | Deze openen webpagina's vanaf de computer van de gebruiker door zelf opdrachten naar een browser te sturen of door de opgegeven webadressen in de bestanden van het besturingssysteem te wijzigen.  |

|                          |                    |   |
|--------------------------|--------------------|---|
|                          |                    | Met behulp van deze programma's voeren indringers netwerkaanvallen uit en verhogen ze bezoeken aan websites om zo het aantal weergaven van banners te verhogen.   |
| <b>Trojan-Downloader</b> | Trojan downloaders | Deze gaan naar de webpagina van de indringer, downloaden andere schadelijke programma's vanaf de webpagina en installeren de programma's op de computer van de gebruiker. Mogelijk bevatten ze de bestandsnaam van het schadelijke programma dat wordt gedownload of ontvangen ze die vanaf de bezochte webpagina.  |
| <b>Trojan-Dropper</b>    | Trojan droppers    | <p>Deze bevatten andere Trojans die ze op de harde schijf plaatsen en vervolgens installeren.</p> <p>Indringers kunnen programma's van het type Trojan Dropper gebruiken voor het volgende:</p> <ul style="list-style-type: none"> <li>• Een schadelijk programma ongemerkt installeren: programma's van het type Trojan Dropper geven geen berichten weer of geven valse berichten weer met meldingen over bijvoorbeeld een fout in een archief of een incompatibele versie van het besturingssysteem.</li> <li>• De detectie van een ander schadelijk programma voorkomen: niet alle antivirussoftware kan een schadelijk programma in een programma van het type Trojan Dropper detecteren.</li> </ul> |
| <b>Trojan-Notifier</b>   | Trojan notifiers   | Deze melden een indringer dat de geïnfecteerde computer toegankelijk is   |

|                     |   |   |
|---------------------|---|---|
|                     |   | <p>door informatie over de computer te versturen naar de indringer: IP-adres, nummer van geopende poort of e-mailadres. Ze maken verbinding met de indringer via e-mail of FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.</p> <p>Programma's van het type Trojan Notifier worden vaak gebruikt in sets die uit meerdere Trojans bestaan. Ze melden de indringer dat andere Trojans met succes zijn geïnstalleerd op de computer van de gebruiker.</p>   |
| <b>Trojan-Proxy</b> | Trojan-proxy's                            | Deze geven de indringer de mogelijkheid om webpagina's anoniem te bezoeken met de computer van de gebruiker. Ze worden vaak gebruikt voor het versturen van spam.   |
| <b>Trojan-PSW</b>   | Software voor het stelen van wachtwoorden | <p>PSW is een soort Trojan die gebruikersaccounts steelt, zoals registratiegegevens van software. Deze Trojans vinden vertrouwelijke gegevens in systeembestanden en het register en versturen die naar de "aanvaller" per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.</p> <p>Sommige van deze Trojans zijn afzonderlijk gecategoriseerd per type zoals in deze tabel is beschreven. Deze zijn Trojans die gegevens van bankrekeningen stelen (Trojan-Banker), gegevens van gebruikers van instant messengers (Trojan-IM), en gegevens van gebruikers van online games (Trojan-GameThief).</p> |
| <b>Trojan-Spy</b>   | Trojan-spionnen                           | Deze bespioneren de gebruiker door informatie te verzamelen over de acties van de gebruiker terwijl die met de computer werkt. Ze kunnen de   |



|                    |   |  |
|--------------------|---|--|
|                    |   | gegevens die de gebruiker invoert met het toetsenbord onderscheppen, schermafbeeldingen maken of lijsten met actieve programma's verzamelen. Nadat ze de informatie hebben ontvangen, versturen ze die naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Trojan-DDoS</b> | Trojan-netwerkaanvallers  | Deze versturen een groot aantal verzoeken van de computer van de gebruiker naar een externe server. De server heeft onvoldoende bronnen om alle verzoeken te verwerken en stopt met werken (Denial of Service, of kortom DoS). Hackers infecteren vaak veel computers met deze programma's zodat ze de computers kunnen gebruiken om een enkele server tegelijk aan te vallen.<br><br>DoS-programma's voeren een aanval uit vanaf een enkele computer met het medeweten van de gebruiker. DDoS-programma's (Distributed DoS) voeren gedistribueerde aanvallen uit vanaf verschillende computers zonder dat de gebruiker van de geïnfecteerde computer dit opmerkt. |
| <b>Trojan-IM</b>   | Trojans die gegevens van gebruikers van Instant messengers stelen | Deze stelen accountnummers en wachtwoorden van gebruikers van instant messengers. Ze versturen de gegevens naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Rootkit</b>     | Rootkits  | Deze maskeren andere schadelijke programma's en hun activiteit waardoor de   |

|                          |   |  |
|--------------------------|---|--|
|                          |   | programma's langer in het besturingssysteem aanwezig blijven. Ze kunnen ook bestanden, processen in het geheugen van een geïnfecteerde computer of registersleutels verbergen die schadelijke programma's uitvoeren. De rootkits kunnen een gegevensoverdracht tussen programma's op de computer van de gebruiker en andere computers in het netwerk maskeren. |
| <b>Trojan-SMS</b>        | Trojans in de vorm van sms-berichten                        | Deze infecteren mobiele telefoons door sms-berichten naar betalende telefoonnummers te versturen.  |
| <b>Trojan-GameThief</b>  | Trojans die gegevens van gebruikers van online games stelen | Deze stelen accountgegevens van gebruikers van online games, waarna ze de gegevens naar de indringer versturen per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier.  |
| <b>Trojan-Banker</b>     | Trojans die gegevens van bankrekeningen stelen              | Deze stelen gegevens van bankrekeningen of e-money-systeemgegevens en sturen die dan naar de hacker per e-mail, via FTP, met een bezoek aan de webpagina van de hacker of op een andere manier.  |
| <b>Trojan-Mailfinder</b> | Trojans die e-mailadressen verzamelen                       | Deze verzamelen e-mailadressen die op een computer zijn opgeslagen en versturen ze naar de indringer per e-mail, via FTP, met een bezoek aan de webpagina van de indringer of op een andere manier. Indringers kunnen spam naar de verzamelde adressen versturen.  |

- [Schadelijke tools](#) ?

**Subcategorie:** schadelijke tools

**Veiligheidsrisico:** gemiddeld

In tegenstelling tot andere soorten malware voeren schadelijke tools hun acties niet direct na hun start uit. Ze kunnen veilig worden opgeslagen en gestart op de computer van de gebruiker. Indringers gebruiken vaak de functies van deze programma's om virussen, wormen en Trojans te maken, netwerkaanvallen op externe servers uit te voeren, computers te hacken of andere schadelijke acties uit te voeren.

Diverse functies van schadelijke tools zijn gegroepeerd op type en worden in de volgende tabel beschreven.

Functies van schadelijke tools

| Type                | Naam             | Beschrijving  |
|---------------------|------------------|---|
| <b>Constructeur</b> | Constructeurs    | Hiermee kunnen nieuwe virussen, wormen en Trojans worden gemaakt. Bepaalde constructeurs hebben een standaardinterface met vensters waarin de gebruiker kan kiezen welk type schadelijk programma moet worden gemaakt, hoe debuggers moeten worden tegengegaan, en andere functies.                   |
| <b>Dos</b>          | Netwerkaanvallen | Deze versturen een groot aantal verzoeken van de computer van de gebruiker naar een externe server. De server heeft onvoldoende bronnen om alle verzoeken te verwerken en stopt met werken (Denial of Service, of kortom DoS).  |
| <b>Exploit</b>      | Exploits         | Een <i>exploit</i> is een reeks gegevens of een programmalicentie die kwetsbaarheden van het programma waarin deze wordt verwerkt gebruikt om een schadelijke actie op een computer uit te voeren. Een exploit kan bijvoorbeeld bestanden schrijven of lezen of "geïnfecteerde" webpagina's opvragen. |

|                    |  |  |
|--------------------|--|--|
|                    |  | <p>Verschillende exploits gebruiken kwetsbaarheden in verschillende programma's of netwerkservices. Vermomd als een netwerkpakket wordt een exploit via het netwerk verstuurd naar heel veel computers, op zoek naar computers met kwetsbare netwerkservices. Een exploit in een DOC-bestand gebruikt de kwetsbaarheden van een teksteditor. Deze kan de acties beginnen uitvoeren die door de hacker vooraf zijn geprogrammeerd wanneer de gebruiker het geïnfecteerde bestand opent. Een exploit die is ingebed in een e-mailbericht zoekt naar kwetsbaarheden in een e-mailprogramma. Deze kan een schadelijke actie beginnen uitvoeren zodra de gebruiker het geïnfecteerde bericht in dit e-mailprogramma opent.</p> <p>Net-Worms verspreiden zich via netwerken door middel van exploits. Nuker exploits zijn netwerkpakketten die computers uitschakelen.</p> |
| <b>FileCryptor</b> | Encryptors                                     | Deze encrypten andere schadelijke programma's om ze te verbergen voor het antivirusprogramma.  |
| <b>Flooder</b>     | Programma's voor het besmetten van "netwerken" | Deze versturen een groot aantal berichten via netwerkkanalen. Dit type tools omvat bijvoorbeeld programma's die Internet Relay Chats besmetten.  |

|                 |                       |   |
|-----------------|-----------------------|---|
|                 |                       | Tools van het type Flooder zijn geen programma's die kanalen "besmetten" die door e-mail, instant messengers en mobiele communicatiesystemen worden gebruikt. Deze programma's worden beschouwd als afzonderlijke types die in de tabel worden beschreven (Email-Flooder, IM-Flooder en SMS-Flooder).   |
| <b>HackTool</b> | Tools om te hacken    | Deze maken het mogelijk om de computer waarop ze zijn geïnstalleerd te hacken of om een andere computer aan te vallen (bijvoorbeeld door nieuwe systeemaccounts toe te voegen zonder de toestemming van de gebruiker of door systeemlogboeken te wissen om sporen van hun aanwezigheid in het besturingssysteem te verbergen). Dit type tools omvat bepaalde sniffers die schadelijke functies hebben, zoals het onderscheppen van wachtwoorden. Sniffers zijn programma's waarmee netwerkverkeer kan worden bekeken. |
| <b>Hoax</b>     | Hoaxes                | Deze alarmeren de gebruiker met virusachtige berichten: ze kunnen "een virus detecteren" in een niet-geïnfecteerd bestand of de gebruiker melden dat de schijf is geformatteerd hoewel dit niet het geval is.   |
| <b>Spoofers</b> | Tools voor vervalsing | Deze versturen berichten en netwerkaanvragen met een vals adres van de zender. Indringers gebruiken tools van het type Spoofer om zich bijvoorbeeld voor te doen als de echte afzender van berichten.   |
|                 |                       |   |

|                      |  |  |
|----------------------|--|--|
| <b>VirTool</b>       | Tools die schadelijke programma's aanpassen                    | Deze kunnen worden gebruikt om malware aan te passen en ze te verbergen voor antivirusprogramma's.   |
| <b>Email-Flooder</b> | Programma's die e-mailadressen "besmetten"                     | Deze versturen een groot aantal berichten naar diverse e-mailadressen, waardoor ze "besmet raken". Een groot aantal inkomende berichten belet dat gebruikers de gewenste berichten in hun postvakken zien. |
| <b>IM-Flooder</b>    | Programma's die het verkeer van instant messengers "besmetten" | Deze overspoelen gebruikers van instant messengers met berichten. Een groot aantal berichten belet dat gebruikers de gewenste inkomende berichten zien.  |
| <b>SMS-Flooder</b>   | Programma's die het verkeer van sms-berichten "besmetten"      | Deze versturen een groot aantal sms-berichten naar mobiele telefoons.  |

- [Adware](#) 

**Subcategorie:** software voor advertenties (Adware);

**Veiligheidsrisico:** gemiddeld

Adware toont advertenties aan de gebruiker. Adwareprogramma's tonen banners in de interfaces van andere programma's en verwijzen zoekopdrachten door naar webpagina's met advertenties. Sommige ervan verzamelen marketinginformatie over de gebruiker en versturen die naar de ontwikkelaar: deze informatie bevat mogelijk de namen van de websites die de gebruiker bezoekt of de inhoud van de zoekopdrachten van de gebruiker. In tegenstelling tot programma's van het type Trojan-Spy stuurt adware deze informatie naar de ontwikkelaar met de toestemming van de gebruiker.

- [Automatische inbelprogramma's](#) 

**Subcategorie:** legitieme software die criminelen kunnen gebruiken om uw computer of persoonlijke gegevens te beschadigen.

**Veiligheidsrisico:** gemiddeld

De meeste van deze programma's zijn nuttig, waardoor veel gebruikers ze hebben. Deze programma's zijn onder andere IRC-clients, automatische inbelprogramma's, programma's om bestanden te downloaden, monitors voor de systeemactiviteit, hulpprogramma's voor wachtwoorden en internet servers voor FTP, HTTP en Telnet.

Als indringers echter toegang tot deze programma's krijgen of als ze die programma's op de computer van de gebruiker plaatsen, kunnen bepaalde functies van de programma's worden gebruikt om de beveiliging aan te tasten.

Deze programma's verschillen naargelang functie. De verschillende types worden in de onderstaande tabel beschreven.

| Type              | Naam                                      | Beschrijving  |
|-------------------|---|---|
| <b>Client-IRC</b> | Online chatprogramma's                    | Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.  |
| <b>Inbeller</b>   | Automatische inbelprogramma's             | Deze kunnen verborgen verbindingen via een telefoonmodem tot stand brengen.   |
| <b>Downloader</b> | Programma's voor downloads                | Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.  |
| <b>Monitor</b>    | Programma's voor monitoring               | Hiermee kan de activiteit op de computer waarop ze zijn geïnstalleerd worden gemonitord (zien welke programma's actief zijn en hoe ze gegevens met geïnstalleerde programma's op andere computers uitwisselen). |
| <b>PSWTool</b>    | Programma's om wachtwoorden te herstellen | Hiermee kunnen wachtwoorden worden bekeken en   |

|                     |                                |   |
|---------------------|--------------------------------|---|
|                     |                                | <p>vergeten wachtwoorden worden hersteld. Indringers plaatsen ze ongemerkt op computers van gebruikers met hetzelfde doel.</p>  |
| <b>RemoteAdmin</b>  | Programma's voor extern beheer | <p>Deze worden veel gebruikt door systeembeheerders. Met deze programma's kan toegang tot de interface van een externe computer worden verkregen om die computer te monitoren en te beheren. Indringers plaatsen ze in het geheim op computers van gebruikers met hetzelfde doel: externe computers monitoren en beheren.</p> <p>Legitieme programma's voor extern beheer verschillen van Trojans van het type Backdoor voor extern beheer. Trojans kunnen het besturingssysteem zelfstandig binnendringen en zichzelf installeren terwijl legitieme programma's dit niet kunnen.</p> |
| <b>Server-FTP</b>   | FTP-servers                    | <p>Deze werken als FTP-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via FTP.</p>   |
| <b>Server-Proxy</b> | Proxyservers                   | <p>Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.</p>  |



|                      |   |  |
|----------------------|---|--|
| <b>Server-Telnet</b> | Telnet-servers                            | Deze werken als Telnet-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via Telnet.   |
| <b>Server-Web</b>    | Webservers                                | Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.   |
| <b>RiskTool</b>      | Tools om op een lokale computer te werken | Deze geven de gebruiker extra opties wanneer die aan de computer van de gebruiker zelf zit. De gebruiker kan de tool gebruiken om bestanden of vensters van actieve programma's te verbergen en om actieve processen te beëindigen.                                    |
| <b>NetTool</b>       | Netwerkprogramma's                        | Deze geven de gebruiker extra opties tijdens het werken met andere computers in het netwerk. Met deze tools kunnen de computers opnieuw worden opgestart, kunnen open poorten worden gedetecteerd en kunnen geïnstalleerde programma's op de computers worden gestart. |
| <b>Client-P2P</b>    | P2P-netwerkprogramma's                    | Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.  |
| <b>Client-SMTP</b>   | SMTP-clients                              | Deze versturen e-mailberichten zonder medeweten van de gebruiker. Indringers plaatsen ze op de computer van de gebruiker om spam   |

|                   |                   |  |
|-------------------|-------------------|--|
|                   |                   | onder de naam van de gebruiker te versturen.   |
| <b>WebToolbar</b> | Online werkbalken | Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.   |
| <b>FraudTool</b>  | Pseudoprogramma's | Deze doen zichzelf voor als andere programma's. Er zijn bijvoorbeeld pseudo-antivirusprogramma's die berichten over gevonden malware weergeven. In werkelijkheid vinden of desinfecteren deze programma's niets. |

- [Detecteer andere software die criminelen kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen](#) 

**Subcategorie:** legitieme software die criminelen kunnen gebruiken om uw computer of persoonlijke gegevens te beschadigen.

**Veiligheidsrisico:** gemiddeld

De meeste van deze programma's zijn nuttig, waardoor veel gebruikers ze hebben. Deze programma's zijn onder andere IRC-clients, automatische inbelprogramma's, programma's om bestanden te downloaden, monitors voor de systeemactiviteit, hulpprogramma's voor wachtwoorden en internetserveren voor FTP, HTTP en Telnet.

Als indringers echter toegang tot deze programma's krijgen of als ze die programma's op de computer van de gebruiker plaatsen, kunnen bepaalde functies van de programma's worden gebruikt om de beveiliging aan te tasten.

Deze programma's verschillen naargelang functie. De verschillende types worden in de onderstaande tabel beschreven.

| Type              | Naam                                      | Beschrijving  |
|-------------------|---|---|
| <b>Client-IRC</b> | Online chatprogramma's                    | Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.  |
| <b>Inbeller</b>   | Automatische inbelprogramma's             | Deze kunnen verborgen verbindingen via een telefoonmodem tot stand brengen.   |
| <b>Downloader</b> | Programma's voor downloads                | Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.  |
| <b>Monitor</b>    | Programma's voor monitoring               | Hiermee kan de activiteit op de computer waarop ze zijn geïnstalleerd worden gemonitord (zien welke programma's actief zijn en hoe ze gegevens met geïnstalleerde programma's op andere computers uitwisselen). |
| <b>PSWTool</b>    | Programma's om wachtwoorden te herstellen | Hiermee kunnen wachtwoorden worden bekeken en   |

|                     |                                |   |
|---------------------|--------------------------------|---|
|                     |                                | <p>vergeten wachtwoorden worden hersteld. Indringers plaatsen ze ongemerkt op computers van gebruikers met hetzelfde doel.</p>  |
| <b>RemoteAdmin</b>  | Programma's voor extern beheer | <p>Deze worden veel gebruikt door systeembeheerders. Met deze programma's kan toegang tot de interface van een externe computer worden verkregen om die computer te monitoren en te beheren. Indringers plaatsen ze in het geheim op computers van gebruikers met hetzelfde doel: externe computers monitoren en beheren.</p> <p>Legitieme programma's voor extern beheer verschillen van Trojans van het type Backdoor voor extern beheer. Trojans kunnen het besturingssysteem zelfstandig binnendringen en zichzelf installeren terwijl legitieme programma's dit niet kunnen.</p> |
| <b>Server-FTP</b>   | FTP-servers                    | <p>Deze werken als FTP-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via FTP.</p>   |
| <b>Server-Proxy</b> | Proxyservers                   | <p>Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.</p>  |

|                      |   |  |
|----------------------|---|--|
| <b>Server-Telnet</b> | Telnet-servers                            | Deze werken als Telnet-servers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via Telnet.   |
| <b>Server-Web</b>    | Webservers                                | Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.   |
| <b>RiskTool</b>      | Tools om op een lokale computer te werken | Deze geven de gebruiker extra opties wanneer die aan de computer van de gebruiker zelf zit. De gebruiker kan de tool gebruiken om bestanden of vensters van actieve programma's te verbergen en om actieve processen te beëindigen.                                    |
| <b>NetTool</b>       | Netwerkprogramma's                        | Deze geven de gebruiker extra opties tijdens het werken met andere computers in het netwerk. Met deze tools kunnen de computers opnieuw worden opgestart, kunnen open poorten worden gedetecteerd en kunnen geïnstalleerde programma's op de computers worden gestart. |
| <b>Client-P2P</b>    | P2P-netwerkprogramma's                    | Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.  |
| <b>Client-SMTP</b>   | SMTP-clients                              | Deze versturen e-mailberichten zonder medeweten van de gebruiker. Indringers plaatsen ze op de computer van de gebruiker om spam   |

|                   |                   |  |
|-------------------|-------------------|--|
|                   |                   | onder de naam van de gebruiker te versturen.   |
| <b>WebToolbar</b> | Online werkbalken | Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.   |
| <b>FraudTool</b>  | Pseudoprogramma's | Deze doen zichzelf voor als andere programma's. Er zijn bijvoorbeeld pseudo-antivirusprogramma's die berichten over gevonden malware weergeven. In werkelijkheid vinden of desinfecteren deze programma's niets. |

- [Objecten die mogelijk zijn gecomprimeerd om schadelijke code te beschermen](#) 

Kaspersky Endpoint Security scant gecomprimeerde objecten en de decompressiemodule in SFX-archieven (zelfuitpakkende archieven).

Om gevaarlijke programma's te verbergen voor antivirusprogramma's, archiveren indringers ze met speciale compressieprogramma's of maken ze meermaals ingepakte bestanden aan.

Kaspersky-virusanalisten hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.

Als Kaspersky Endpoint Security een dergelijk compressieprogramma in een bestand detecteert, bevat het bestand wellicht een kwaadaardig programma of een programma dat criminelen kunnen gebruiken om schade aan uw computer of persoonlijke gegevens te berokkenen.

Kaspersky Endpoint Security onderscheidt de volgende soorten programma's:

- *Ingepakte bestanden die mogelijk schadelijk zijn* – gebruikt voor het comprimeren van malware, zoals virussen, wormen en Trojans.
- *Meermaals ingepakte bestanden* (gemiddeld veiligheidsrisico) – het object is drie keer gecomprimeerd door een of meerdere compressieprogramma's.

- [Meermaals ingepakte objecten](#) 

Kaspersky Endpoint Security scant gecomprimeerde objecten en de decompressiemodule in SFX-archieven (zelfuitpakkende archieven).

Om gevaarlijke programma's te verbergen voor antivirusprogramma's, archiveren indringers ze met speciale compressieprogramma's of maken ze meermaals ingepakte bestanden aan.

Kaspersky-virusanalisten hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.

Als Kaspersky Endpoint Security een dergelijk compressieprogramma in een bestand detecteert, bevat het bestand wellicht een kwaadaardig programma of een programma dat criminelen kunnen gebruiken om schade aan uw computer of persoonlijke gegevens te berokkenen.

Kaspersky Endpoint Security onderscheidt de volgende soorten programma's:

- *Ingepakte bestanden die mogelijk schadelijk zijn* – gebruikt voor het comprimeren van malware, zoals virussen, wormen en Trojans.
- *Meermaals ingepakte bestanden* (gemiddeld veiligheidsrisico) – het object is drie keer gecomprimeerd door een of meerdere compressieprogramma's.

## Uitzonderingen

Deze tabel bevat informatie over scanuitzonderingen.

Op de volgende manieren kunt u voorkomen dat objecten niet worden gescand:

- Geef het pad naar het bestand of de map op.
- Voer de objecthash in.
- Gebruik maskers:
  - Het teken `*` (sterretje), dat een willekeurige reeks tekens voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\*\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen op de C-schijf bevinden, maar niet in submappen.
  - Twee opeenvolgende sterretjes `**` stellen een willekeurige reeks tekens voor (inclusief een lege reeks) in de bestands- of mapnaam, inclusief de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het masker `C:\Voorbeeld\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in de map `Voorbeeld` en de submappen ervan bevinden. Het masker moet ten minste één genest niveau bevatten. Het masker `C:\**\*.txt` is geen geldig masker.
  - Het teken `?` (vraagteken), dat een enkel willekeurig teken voorstelt, behalve de tekens `\` en `/` (scheidingstekens van de namen van bestanden en mappen in paden naar bestanden en mappen). Het

|   |   |
|---|---|
|   | <p>masker C:\Voorbeeld\???.txt omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam Voorbeeld bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.</p> <ul style="list-style-type: none"> <li>• Voer de naam van het object in volgens de classificatie van de <a href="#">encyclopedie van Kaspersky</a> (bijvoorbeeld E-mailworm, Rootkit of RemoteAdmin). U kunt maskers gebruiken met het teken ? (vervangt een willekeurig teken) en het teken * (vervangt een willekeurig aantal tekens). Als bijvoorbeeld het Client *-masker is opgegeven, sluit Kaspersky Endpoint Security Client-IRC-, Client-P2P- en Client-SMTP-objecten uit van scans.</li> </ul>   |
| <p><b>Vertrouwde programma's</b></p>  | <p>In deze tabel ziet u vertrouwde programma's waarvan de activiteit niet wordt gemonitord door Kaspersky Endpoint Security tijdens de werking ervan.</p> <p>Het onderdeel Programmacontrole controleert de opstart van elk programma, ongeacht of het programma voorkomt in de tabel met vertrouwde programma's.</p>   |
| <p><b>Merge values when inheriting</b><br/><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p>  | <p>Hiermee wordt de lijst met scanuitsluitingen en vertrouwde programma's samengevoegd in het bovenliggende en onderliggende beleid van Kaspersky Security Center. Voor het samenvoegen van lijsten moet het onderliggende beleid geconfigureerd zijn om de instellingen van het bovenliggende beleid van Kaspersky Security Center over te nemen.</p> <p>Als het selectievakje is ingeschakeld, worden lijstitems van het bovenliggende beleid van Kaspersky Security Center weergegeven in onderliggende beleidsregels. Op deze manier kunt u bijvoorbeeld een geconsolideerde lijst met vertrouwde programma's voor de hele organisatie maken.</p> <p>Overgenomen lijstitems in een onderliggend beleid kunnen niet worden verwijderd of bewerkt. Items op de lijst met scanuitsluitingen en de lijst met vertrouwde programma's die tijdens het overnemen worden samengevoegd, kunnen alleen in het bovenliggende beleid worden verwijderd en bewerkt. U kunt wel items van een onderliggend beleid bewerken en verwijderen, of zelfs items toevoegen.</p> <p>Als items op lijsten van het onderliggende beleid en het bovenliggende beleid overeenkomen, worden deze items weergegeven als hetzelfde item van het bovenliggende beleid.</p> <p>Als het selectievakje is uitgeschakeld, worden items van lijsten niet samengevoegd wanneer de instellingen van het Kaspersky Security Center-beleid worden overgenomen.</p> |
| <p><b>Allow use of local exclusions / Allow use of local trusted applications</b><br/><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p><i>Lokale uitsluitingen en lokale vertrouwde programma's (lokale vertrouwde zone)</i> – door de gebruiker gedefinieerde lijst met objecten en programma's in Kaspersky Endpoint Security voor een specifieke computer. Kaspersky Endpoint Security controleert objecten en programma's niet vanuit de lokale vertrouwde zone. Op deze manier kunnen gebruikers <a href="#">hun eigen lokale lijsten met uitsluitingen en vertrouwde programma's maken</a> naast de algemene vertrouwde zone in een beleid.</p> <p>Als het selectievakje is ingeschakeld, kan een gebruiker een lokale lijst met scanuitsluitingen en een lokale lijst met vertrouwde programma's maken. Een beheerder kan Kaspersky Security Center gebruiken om items in de computereigenschappen te bekijken, toe te voegen, te bewerken of te verwijderen.</p>  |



|   |  |
|---|--|
|   | Als het selectievakje is uitgeschakeld, heeft een gebruiker alleen toegang tot de algemene lijsten met scansluitingen en vertrouwde programma's die in het beleid zijn gegenereerd.  |
| <b>Vertrouwde systeemcertificatenopslag</b> | <p>Als een van de vertrouwde systeemcertificatenopslagplaatsen is geselecteerd, sluit Kaspersky Endpoint Security programma's uit die zijn ondertekend met een vertrouwde digitale handtekening van scans. Kaspersky Endpoint Security wijst dergelijke programma's automatisch toe aan de groep <i>Vertrouwd</i>.</p> <p>Als <b>Niet gebruiken</b> is geselecteerd, scant Kaspersky Endpoint Security de programma's, ongeacht of ze wel of niet een digitale handtekening. Kaspersky Endpoint Security plaatst een programma in een vertrouwensgroep, afhankelijk van het risico dat dit programma voor de computer kan opleveren.</p> |

## Programma-instellingen

U kunt de volgende algemene instellingen van het programma configureren:

- Uitvoermodus
- Zelfbescherming
- Prestaties
- Foutopsporingsgegevens
- Computerstatus wanneer instellingen worden toegepast

Programma-instellingen

| Parameter   | Beschrijving   |
|---|--|
| <b>Kaspersky Endpoint Security voor Windows starten bij opstart van computer</b>      | <p>Als het selectievakje is ingeschakeld, wordt Kaspersky Endpoint Security na de opstart van het besturingssysteem gestart. Kaspersky Endpoint Security beschermt de computer gedurende de hele sessie.</p> <p>Als het selectievakje is uitgeschakeld, wordt Kaspersky Endpoint Security niet na de opstart van het besturingssysteem gestart. Kaspersky Endpoint Security wordt pas gestart wanneer de gebruiker dit handmatig doet. Computerbescherming is uitgeschakeld en de gegevens van de gebruiker lopen mogelijk gevaar.</p>   |
| <b>Gebruik Geavanceerde desinfectietechnologie (vereist heel wat computerbronnen)</b> | <p>Als het selectievakje is ingeschakeld, verschijnt een pop-upmelding op het scherm wanneer schadelijke activiteit in het besturingssysteem wordt gedetecteerd. In de melding wordt de gebruiker door Kaspersky Endpoint Security aangeboden om een geavanceerde desinfectie op de computer uit te voeren. Nadat de gebruiker deze procedure heeft goedgekeurd, wordt de dreiging door Kaspersky Endpoint Security geneutraliseerd. Na de voltooiing van de geavanceerde desinfectieprocedure herstart Kaspersky Endpoint Security de computer. De geavanceerde desinfectietechnologie gebruikt heel wat computerbronnen waardoor andere programma's mogelijk trager gaan werken.</p> |

|   |   |
|---|---|
|   | <p>Wanneer het programma een actieve infectie detecteert, kan bepaalde functionaliteit van het besturingssysteem niet beschikbaar zijn. Het besturingssysteem is weer volledig beschikbaar nadat de Geavanceerde desinfectie is voltooid en de computer opnieuw is opgestart.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Windows for Servers, toont Kaspersky Endpoint Security de melding niet. Daarom kan de gebruiker geen actie selecteren om een actieve dreiging te desinfecteren. Voor de desinfectie van een dreiging moet u <a href="#">de technologie Geavanceerde desinfectie inschakelen</a> in de programma-instellingen en <a href="#">directe Geavanceerde desinfectie inschakelen</a> in de instellingen van de taak <i>Virusscan</i>. Vervolgens moet u de <i>virusscantaak</i> starten.</p> </div> |
| <p><b>Kaspersky Security Center gebruiken als proxyserver voor activering</b><br/><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p>Als het selectievakje is ingeschakeld, wordt Administration Server van Kaspersky Security Center als een proxyserver gebruikt tijdens de activering van het programma.</p>   |
| <p><b>Zelfbescherming inschakelen</b></p>   | <p>Als dit selectievakje is ingeschakeld, voorkomt Kaspersky Endpoint Security de wijziging of de verwijdering van programmabestanden op de harde schijf, processen in het geheugen en vermeldingen in het systeemregister.</p>   |
| <p><b>Toestaan dat instellingen van Kaspersky Endpoint Security worden beheerd via apps voor extern beheer</b></p>  | <p>Als dit selectievakje is ingeschakeld, kunnen vertrouwde programma's voor extern beheer (zoals TeamViewer, LogMeln Pro en Remotely Anywhere) de instellingen van Kaspersky Endpoint Security wijzigen. Niet-vertrouwde programma's voor extern beheer mogen de instellingen van Kaspersky Endpoint Security niet wijzigen, zelfs niet als het selectievakje is ingeschakeld.</p>   |
| <p><b>Extern beheer van services inschakelen</b></p>  | <p>Als het selectievakje is ingeschakeld, kunt u in Kaspersky Endpoint Security programmaservices beheren vanaf een externe computer. Bij een poging tot het extern beheer van de programmaservices wordt een melding boven het pictogram van het programma in de Microsoft Windows-taakbalk weergegeven (tenzij de meldingen zijn uitgeschakeld door de gebruiker).</p>  |
| <p><b>Geplande taken uitstellen bij werking op accustroom</b></p>   | <p>Als het selectievakje is ingeschakeld, is de energiebesparingsmodus ingeschakeld. Kaspersky Endpoint Security stelt geplande taken uit. U kunt indien nodig scan- en updatetaken handmatig starten.</p>  |
| <p><b>Bronnen aan andere programma's geven</b></p>  | <p>Het verbruik van computerbronnen door Kaspersky Endpoint Security bij het scannen van de computer kan de belasting van de CPU en de subsystemen van de harde schijf verhogen. Dit kan andere programma's vertragen. Om de prestaties te optimaliseren, biedt Kaspersky Endpoint Security een <i>modus voor het overbrengen van bronnen naar andere programma's</i>. In deze modus kan het besturingssysteem de prioriteit van de scantaakthreads van Kaspersky Endpoint Security verlagen als de CPU-belasting hoog is. Hierdoor kunnen de bronnen van het besturingssysteem opnieuw worden gedistribueerd naar andere programma's. Scantaken krijgen dus minder CPU-tijd. Als gevolg hiervan zal Kaspersky Endpoint Security er langer over doen om de computer te scannen. Standaard is het programma geconfigureerd om bronnen aan andere programma's af te staan.</p>  |

|   |  |
|---|--|
| <p><b>Schrijven naar dump inschakelen</b></p>   | <p>Als het selectievakje is ingeschakeld, schrijft Kaspersky Endpoint Security dumps wanneer het crasht.</p> <p>Als het selectievakje is uitgeschakeld, schrijft Kaspersky Endpoint Security geen dumps. Het programma verwijdert ook bestaande dumpbestanden op de harde schijf van de computer.</p>  |
| <p><b>Bescherming voor dump- en tracebestanden inschakelen</b></p>  | <p>Als het selectievakje is ingeschakeld, krijgen systeembeheerders, lokale beheerders en de gebruiker die het schrijven van dumpbestanden heeft ingeschakeld toegang tot dumpbestanden. Alleen systeembeheerders en lokale beheerders hebben toegang tot tracebestanden.</p> <p>Als het selectievakje is uitgeschakeld, hebben alle gebruikers toegang tot dump- en tracebestanden.</p> |
| <p><b>Computerstatus wanneer instellingen worden toegepast</b></p> <p><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i></p> | <p>Instellingen voor de weergave van de status van clientcomputers waarop Kaspersky Endpoint Security is geïnstalleerd in de Webconsole wanneer fouten optreden tijdens het toepassen van een beleid of het uitvoeren van een taak. De opties <i>OK</i>, <i>Waarschuwing</i> en <i>Kritiek</i> voor de status zijn beschikbaar.</p>  |

## Rapporten en Opslag

### Rapporten

Informatie over de werking van elk Kaspersky Endpoint Security-onderdeel, de gebeurtenissen die zijn gerelateerd aan gegevensencryptie, de prestaties van elke scantaak, updatetaak, integriteitscontrole en de algemene werking van het programma wordt in rapporten vastgelegd.

Rapporten worden opgeslagen in de map `C:\ProgramData\Kaspersky Lab\KES\Report`.

### Back-up

*Back-up* bewaart back-ups van bestanden die tijdens de desinfectie zijn verwijderd of gewijzigd. Een *back-up* is een kopie van het bestand die is gemaakt voordat het bestand werd gedesinfecteerd of verwijderd. Back-ups van bestanden worden in een speciale indeling opgeslagen en zijn niet gevaarlijk.

Back-ups van bestanden worden opgeslagen in de map `C:\ProgramData\Kaspersky Lab\KES\QB`.

Gebruikers in de groep Beheerders hebben de benodigde machtigingen om deze map te openen. De gebruiker wiens account is gebruikt om Kaspersky Endpoint Security te installeren heeft beperkte toegangsrechten voor deze map.

Kaspersky Endpoint Security biedt de mogelijkheid niet om machtigingen voor de toegang tot back-ups van bestanden te configureren.

### Quarantaine

Quarantaine is een speciale lokale opslagplaats op de computer. De gebruiker kan bestanden die de gebruiker gevaarlijk acht voor de computer in quarantaine plaatsen. Bestanden in quarantaine worden in een geëncrypte staat bewaard en vormen geen bedreiging voor de beveiliging van de computer. Kaspersky Endpoint Security gebruikt Quarantaine alleen met de oplossingen Kaspersky Sandbox en Kaspersky Endpoint Detection and Response. In alle andere gevallen plaatst Kaspersky Endpoint Security het relevante bestand in [Back-up](#). Voor meer informatie over het beheer van Quarantaine als onderdeel van de oplossingen raadpleegt u de [Kaspersky Sandbox Help](#), [Kaspersky Endpoint Detection and Response Optimum Help](#), en [Kaspersky Endpoint Detection and Response Expert Help](#).

Quarantaine kan alleen via Webconsole worden geconfigureerd. U kunt ook Webconsole gebruiken om objecten in quarantaine te beheren (terugzetten, verwijderen, toevoegen, etc.). U kunt bestanden lokaal op de computer terugzetten met de [opdrachtregel](#).

Kaspersky Endpoint Security gebruikt het systeemaccount (SYSTEEM) om bestanden in quarantaine te plaatsen.

#### Instellingen van rapporten en opslag

| Parameter  | Beschrijving  |
|--|---|
| <b>Bewaar rapporten niet langer dan N dagen</b>  | Als het selectievakje is ingeschakeld, is de maximale opslagduur van rapporten beperkt tot het opgegeven tijdsinterval. De standaard maximale opslagduur voor rapporten is 30 dagen. Na die tijd worden de oudste gegevens uit het rapportbestand automatisch verwijderd door Kaspersky Endpoint Security.  |
| <b>Beperk grootte van rapportbestand tot N MB</b>  | Als het selectievakje is ingeschakeld, is de maximale bestandsgrootte van rapporten beperkt tot de opgegeven waarde. De maximale bestandsgrootte 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.                        |
| <b>Bewaar objecten niet langer dan N dagen</b>   | Als het selectievakje is ingeschakeld, is de maximale opslagduur van bestanden beperkt tot het opgegeven tijdsinterval. De standaard maximale opslagduur voor bestanden is 30 dagen. Na het verlopen van de maximale opslagduur verwijdert Kaspersky Endpoint Security de oudste bestanden in Back-up.  |
| <b>Beperk de grootte van Back-up tot N MB</b>  | Als het selectievakje is ingeschakeld, is de maximale opslaggrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 100 MB. Om te vermijden dat de maximale opslaggrootte wordt overschreden, worden de oudste bestanden in de opslag automatisch verwijderd door Kaspersky Endpoint Security wanneer de maximale opslaggrootte wordt bereikt.  |
| <b>Limit the size of Quarantine to N MB</b><br><i>(Alleen beschikbaar in Webconsole)</i>                 | Maximale grootte van Quarantaine in MB. U kunt de maximale grootte van Quarantaine bijvoorbeeld instellen op 200 MB. Wanneer Quarantaine dan de maximale grootte bereikt, stuurt Kaspersky Endpoint Security de desbetreffende gebeurtenis naar Kaspersky Security Center en publiceert het de gebeurtenis in het Windows-gebeurtenislogboek. Inmiddels stopt het programma nieuwe objecten in quarantaine plaatsen. U moet de quarantaine handmatig legen. |
| <b>Notify when the Quarantine storage reaches N percent</b><br><i>(Alleen beschikbaar in Webconsole)</i> | Drempelwaarde voor de Quarantaine. U kunt de drempel van Quarantaine bijvoorbeeld instellen op 50%. Wanneer Quarantaine dan de drempel bereikt, stuurt Kaspersky Endpoint Security de desbetreffende gebeurtenis naar Kaspersky Security Center en publiceert het de gebeurtenis in het Windows-gebeurtenislogboek. Inmiddels blijft het programma nieuwe objecten in quarantaine plaatsen.   |
| <b>Data transfer</b>   | Categorieën van gebeurtenissen op clientcomputers waarvan de informatie moet  |

to  
Administration  
Server

(alleen  
beschikbaar in  
Kaspersky  
Security  
Center)

worden verstuurd naar de Administration Server.

## Netwerkinstellingen

U kunt de proxyserver voor het maken van verbinding met internet en het updaten van antivirusdatabases configureren, de bewakingsmodus voor netwerkpoorten selecteren en de scans van geëncrypte verbindingen configureren.

### Netwerkopties

| Parameter  | Beschrijving   |
|--|--|
| <b>Beperk verkeer bij verbindingen met datalimiet</b>                      | <p>Als dit selectievakje is ingeschakeld, beperkt het programma het eigen netwerkverkeer wanneer de internetverbinding een datalimiet heeft. Kaspersky Endpoint Security identificeert een mobiele internetverbinding als een verbinding met een datalimiet en identificeert een Wi-Fi-verbinding als een verbinding zonder datalimiet.</p> <p>Kostenbewuste netwerkverbinding werkt op computers met Windows 8 of hoger.</p>  |
| <b>Injecteer script in internetverkeer voor interactie met webpagina's</b> | <p>Als het selectievakje is ingeschakeld, injecteert Kaspersky Endpoint Security een script voor interactie met webpagina's in het internetverkeer. Dit script zorgt ervoor dat het onderdeel Webcontrole correct werkt. Het script maakt de registratie van Webcontrole-gebeurtenissen mogelijk. Zonder dit script kunt u <a href="#">de bewaking van de internetactiviteit van gebruikers</a> niet inschakelen.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"><p>Kaspersky-experts raden aan om dit interactiescript voor webpagina's in het verkeer te injecteren om een correcte werking van Webcontrole te garanderen.</p></div> |
| <b>Proxy server</b>  | <p>Instellingen van de proxyserver die gebruikers van clientcomputers gebruiken om verbinding te maken met internet. Kaspersky Endpoint Security gebruikt deze instellingen voor bepaalde beschermingsonderdelen en om de databases en programmamodules bij te werken.</p> <p>Voor de automatische configuratie van een proxyserver gebruikt Kaspersky Endpoint Security het WPAD-protocol (Web Proxy Auto-Discovery Protocol). Als het IP-adres van de proxyserver niet kan worden bepaald met dit protocol, gebruikt Kaspersky Endpoint Security het adres van de proxyserver dat in de instellingen van Microsoft Internet Explorer is opgegeven.</p>             |
| <b>Bypass proxy server for local addresses</b>                             | <p>Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security geen proxyserver wanneer een update vanuit een gedeelde map wordt uitgevoerd.</p>   |
| <b>Bewaakte poorten</b>  | <p><b>Alle netwerkpoorten bewaken.</b> In deze bewakingsmodus voor netwerkpoorten bewaken de beschermingsonderdelen (File Threat Protection, Web Threat Protection, Mail Threat Protection) gegevensstromen die via alle open netwerkpoorten van de computer worden verstuurd.</p>   |

**Alleen geselecteerde netwerkpoorten bewaken.** In deze modus voor het bewaken van netwerkpoorten, controleren de beschermingsonderdelen de geselecteerde poorten van de computer en de netwerkactiviteit van de geselecteerde programma's. De lijst met netwerkpoorten die normaal worden gebruikt voor de verzending van e-mail en netwerkverkeer wordt geconfigureerd volgens de aanbevelingen van Kaspersky-experts.

**Bewaak alle poorten voor de programma's die voorkomen op de lijst aanbevolen door Kaspersky.** Dit gebruikt een vooraf gedefinieerde lijst met programma's waarvan de netwerkpoorten worden bewaakt door Kaspersky Endpoint Security. Deze lijst bevat bijvoorbeeld Google Chrome, Adobe Reader, Java en andere programma's.

**Bewaak alle poorten voor de opgegeven programma's.** Dit gebruikt een lijst met programma's waarvan de netwerkpoorten worden bewaakt door Kaspersky Endpoint Security:

### Versleutelde verbindingen scannen

Kaspersky Endpoint Security scant versleuteld netwerkverkeer dat wordt verzonden via de volgende protocollen:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Kaspersky Endpoint Security ondersteunt de volgende scanmodi voor versleutelde verbindingen:

- **Versleutelde verbindingen niet scannen.** Kaspersky Endpoint Security heeft geen toegang tot de inhoud van websites waarvan het adres begint met <https://>.
- **Versleutelde verbindingen scannen op verzoek van beschermingsonderdelen.** Kaspersky Endpoint Security scant versleuteld verkeer alleen wanneer daarom wordt gevraagd door de onderdelen File Threat Protection, Mail Threat Protection en Web Control.
- **Versleutelde verbindingen altijd scannen.** Kaspersky Endpoint Security scant versleuteld netwerkverkeer, zelfs als de beschermingsonderdelen zijn uitgeschakeld.

Kaspersky Endpoint Security scant geen versleutelde verbindingen die tot stand zijn gebracht door [vertrouwde programma's waarvoor het scannen van verkeer is uitgeschakeld](#). Kaspersky Endpoint Security scant geen versleutelde verbindingen uit de vooraf gedefinieerde lijst met vertrouwde websites. De vooraf gedefinieerde lijst met vertrouwde websites is gemaakt door Kaspersky-experts. Deze lijst wordt bijgewerkt met de antivirusdatabases van het programma. U kunt de vooraf gedefinieerde lijst met vertrouwde websites alleen in de Kaspersky Endpoint Security-interface bekijken. U kunt de lijst niet bekijken in de Kaspersky Security Center Console.

### Vetrouwde rootcertificaten

Lijst met vertrouwde rootcertificaten. Met Kaspersky Endpoint Security kunt u vertrouwde rootcertificaten op gebruikerscomputers installeren als u bijvoorbeeld een nieuw certificeringscentrum moet implementeren. Met het programma kunt u een certificaat toevoegen aan een speciaal Kaspersky Endpoint Security-certificaatarchief. In dit geval wordt het certificaat alleen als vertrouwd beschouwd voor de Kaspersky Endpoint Security-programma. De gebruiker kan met andere woorden toegang krijgen tot een website met het nieuwe certificaat in de browser. Als een ander programma toegang probeert te krijgen tot de website, kunt u een verbindingfout krijgen vanwege



|  |  |
|--|--|
|  | <p>een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.</p>  |
| <p><b>Bij een bezoek aan een domein met een niet-vertrouwd certificaat</b></p>     | <ul style="list-style-type: none"> <li>• <b>Toestaan.</b> Wanneer een domein met een niet-vertrouwd certificaat wordt bezocht, staat Kaspersky Endpoint Security <a href="#">de netwerkverbinding niet toe</a>. Wanneer een domein met een niet-vertrouwd certificaat wordt geopend in een browser, toont Kaspersky Endpoint Security een HTML-pagina met een waarschuwing en de reden waarom een bezoek aan dat domein niet wordt aanbevolen. Een gebruiker kan klikken op de koppeling op de HTML-waarschuwingspagina om toegang tot de opgevraagde webbron te krijgen. Als een programma of dienst van derden een verbinding tot stand brengt met een domein met een niet-vertrouwd certificaat, maakt Kaspersky Endpoint Security een eigen certificaat om verkeer te scannen. Het nieuwe certificaat heeft de status <i>Niet vertrouwd</i>. Dit is nodig om het programma van derden te waarschuwen voor de niet-vertrouwde verbinding, omdat de HTML-pagina in dit geval niet kan worden weergegeven en de verbinding in de achtergrondmodus kan worden gemaakt.</li> <li>• <b>Verbinding blokkeren.</b> Wanneer een domein met een niet-vertrouwd certificaat wordt bezocht, staat Kaspersky Endpoint Security de netwerkverbinding niet toe. Wanneer een domein met een niet-vertrouwd certificaat wordt geopend in een browser, toont Kaspersky Endpoint Security een HTML-pagina met de reden waarom dat domein is geblokkeerd.</li> </ul> |
| <p><b>Bij fouten tijdens het scannen van geëncrypte verbindingen</b></p>           | <ul style="list-style-type: none"> <li>• <b>Verbinding blokkeren.</b> Als deze optie is geselecteerd wanneer een fout tijdens het scannen van een beveiligde verbinding optreedt, blokkeert Kaspersky Endpoint Security de netwerkverbinding.</li> <li>• <b>Domein toevoegen aan uitzonderingen.</b> Als deze optie is geselecteerd wanneer een fout tijdens het scannen van een geëncrypte verbinding optreedt, zal Kaspersky Endpoint Security het domein dat aan de basis lag van de fout toevoegen aan de lijst met domeinen met scanfouten en zal het geen geëncrypt netwerkverkeer bewaken wanneer dit domein wordt bezocht. Alleen in de lokale interface van het programma kunt u een lijst met domeinen zien waarvoor fouten tijdens het scannen van de geëncrypte verbindingen zijn opgetreden. Als u de inhoud van de lijst wilt wissen, moet u <b>Verbinding blokkeren</b> selecteren. Kaspersky Endpoint Security genereert ook een gebeurtenis voor de fout bij het scannen van de versleutelde verbinding.</li> </ul>   |
| <p><b>Block SSL 2.0 connections (recommended)</b></p>                              | <p>Als het selectievakje is ingeschakeld, blokkeert Kaspersky Endpoint Security netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht.</p> <p>Als het selectievakje is uitgeschakeld, blokkeert Kaspersky Endpoint Security geen netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht en bewaakt het geen netwerkverkeer dat via deze verbindingen wordt verstuurd of ontvangen.</p>  |
| <p><b>Decrypt encrypted connections with websites that use EV certificates</b></p> | <p>EV-certificaten (Certificaten voor uitgebreide validatie) bevestigen de authenticiteit van websites en verbeteren de beveiliging van de verbinding. Browsers tonen een hangslot in de adresbalk om aan te geven dat een website een EV-certificaat heeft. Browsers kunnen de adresbalk ook volledig of gedeeltelijk in een groene kleur weergeven.</p> <p>Als het selectievakje is ingeschakeld, decrypt en bewaakt Kaspersky Endpoint Security geëncrypte verbindingen met websites die een EV-certificaat gebruiken.</p> <p>Als het selectievakje is uitgeschakeld, heeft Kaspersky Endpoint Security geen toegang tot de inhoud van HTTPS-verkeer. Om deze reden bewaakt het programma HTTPS-verkeer alleen op basis van het webadres, zoals <code>https://bing.com</code>.</p>  |


|  |  |
|--|--|
|  | <p>Als u een website met een EV-certificaat voor het eerst opent, wordt de beveiligde verbinding gedecrypt ongeacht of het selectievakje is ingeschakeld.</p>  |
| <p><b>Trusted addresses</b></p>  | <p>Dit gebruikt een lijst met webadressen waarvoor Kaspersky Endpoint Security geen netwerkverbindingen scant. U kunt een domeinnaam of een IP-adres invoeren. Kaspersky Endpoint Security ondersteunt het teken * voor de invoer van een masker in de domeinnaam.</p> <div data-bbox="416 347 1493 539" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security ondersteunt geen maskers voor IP-adressen. U kunt een bereik van IP-adressen invoeren in de lokale programma-interface (bijvoorbeeld 198.51.100.0/24). U kunt geen bereik van IP-adressen invoeren in de Kaspersky Security Center-console.</p> </div> <p>Voorbeelden:</p> <ul style="list-style-type: none"> <li>• <code>domein.nl</code> – de record bevat de volgende adressen: <code>https://domein.nl</code>, <code>https://www.domein.nl</code>, <code>https://domein.nl/pagina123</code>. De record bevat geen subdomeinen (bijvoorbeeld <code>subdomein.domein.nl</code>).</li> <li>• <code>subdomein.domein.nl</code> – de record bevat de volgende adressen: <code>https://subdomein.domein.nl</code>, <code>https://subdomein.domein.nl/pagina123</code>. De record bevat niet het domein <code>domein.nl</code>.</li> <li>• <code>*.domein.nl</code> – de record bevat de volgende adressen: <code>https://films.domein.nl</code>, <code>https://afbeeldingen.domein.nl/pagina123</code>. De record bevat niet het domein <code>domein.nl</code>.</li> </ul> |
| <p><b>Trusted applications</b></p>   | <p>Lijst met programma's waarvan de activiteit niet wordt bewaakt door Kaspersky Endpoint Security tijdens de werking ervan. U kunt kiezen welke programma-activiteit niet moet worden bewaakt door Kaspersky Endpoint Security (bijvoorbeeld: geen netwerkverkeer scannen). Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de * en ?-tekens bij het invoeren van een masker.</p>  |
| <p><b>Gebruik de geselecteerde certificaatopslag om versleutelde verbindingen in Mozilla-programma's te scannen</b></p> <p><i>(alleen beschikbaar in de Kaspersky Endpoint Security-interface)</i></p> | <p>Als dit selectievakje is ingeschakeld, scant Kaspersky Endpoint Security geëncrypt verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient. Het openen van bepaalde websites via het HTTPS-protocol wordt mogelijk geblokkeerd.</p> <div data-bbox="416 1435 1493 1628" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Om verkeer in de Mozilla Firefox-browser en de Thunderbird-mailclient te scannen, moet u de <a href="#">versleutelde verbindingen scannen inschakelen</a>. Als Versleutelde verbindingen scannen ingeschakeld is, scant Kaspersky Endpoint Security geen versleuteld verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient.</p> </div> <p>Kaspersky Endpoint Security gebruikt het Kaspersky-rootcertificaat om geëncrypt verkeer te decrypten en te analyseren. U kunt de certificaatopslag voor het Kaspersky-rootcertificaat selecteren.</p> <ul style="list-style-type: none"> <li>• <b>Windows-certificaatarchief gebruiken (aanbevolen).</b> Het Kaspersky-rootcertificaat wordt aan deze opslag toegevoegd tijdens de installatie van Kaspersky Endpoint Security.</li> <li>• <b>Mozilla-certificaatarchief gebruiken.</b> Mozilla Firefox en Thunderbird gebruiken hun eigen certificaatopslag. Als de Mozilla-certificaatopslag is geselecteerd, moet u het Kaspersky-rootcertificaat handmatig aan deze opslag toevoegen via de browsereigenschappen.</li> </ul>                                       |



# Interface

U kunt de instellingen van de programma-interface configureren.

## Interface-instellingen

| Parameter  | Beschrijving  |
|--|---|
| <b>Interactie met gebruiker</b><br><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i> | <p><b>With simplified interface.</b> Op een clientcomputer is het hoofdvenster van het programma niet toegankelijk en is alleen het <a href="#">pictogram in het Windows-systeemvak</a> beschikbaar. Via het contextmenu van het pictogram kan de gebruiker <a href="#">een beperkt aantal bewerkingen met Kaspersky Endpoint Security uitvoeren</a>. Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.</p> <p><b>With full interface.</b> Op een clientcomputer zijn het hoofdvenster van Kaspersky Endpoint Security en het <a href="#">pictogram in het Windows-systeemvak</a> beschikbaar. Via het contextmenu van het pictogram kan de gebruiker bewerkingen met Kaspersky Endpoint Security uitvoeren. Kaspersky Endpoint Security toont ook meldingen boven het pictogram van het programma.</p> <p><b>Hide Application Activity Monitor section.</b> Op de clientcomputer is de knop <b>Bewaking van programma-activiteit</b> niet beschikbaar in het hoofdvenster van Kaspersky Endpoint Security. <i>Bewaking van programma-activiteit</i> is een tool ontworpen voor de realtime weergave van informatie over de activiteit van de computer van een gebruiker.</p> <p><b>No interface.</b> Op een clientcomputer wordt de werking van Kaspersky Endpoint Security niet aangegeven. Het <a href="#">pictogram in het Windows-systeemvak</a> en de meldingen zijn niet beschikbaar.</p> |
| <b>Instellingen voor meldingen</b>   | Een tabel met de instellingen voor meldingen over gebeurtenissen van een verschillend belang die zich tijdens de werking van een onderdeel, een taak of het gehele programma kunnen voordoen. Kaspersky Endpoint Security toont meldingen over deze gebeurtenissen op het scherm, verstuurt ze per e-mail of registreert ze.  |
| <b>Instellingen voor e-mailmeldingen</b>   | De SMTP-serverinstellingen voor de levering van meldingen over gebeurtenissen die zich tijdens de werking van het programma voordoen.   |
| <b>Toon status van het programma in het systeemvak</b>   | Categorieën van programmeergebeurtenissen die ervoor zorgen dat het <a href="#">Kaspersky Endpoint Security-pictogram</a> in het systeemvak van de Microsoft Windows-taakbalk wijzigt (  of  ) en leiden tot een pop-upmelding.  |
| <b>Statusmeldingen over lokale antivirusdatabase</b>   | Instellingen van meldingen over verouderde antivirusdatabases die door het programma worden gebruikt.   |
| <b>Wachtwoordbeveiliging</b>   | <p>Als de schakelaar is ingeschakeld, vraagt Kaspersky Endpoint Security een wachtwoord wanneer de gebruiker een bewerking probeert uit te voeren die is opgenomen in het bereik van Wachtwoordbeveiliging. Het bereik van Wachtwoordbeveiliging omvat verboden bewerkingen (zoals de uitschakeling van beschermingsonderdelen) en de gebruikersaccounts waarop het bereik van Wachtwoordbeveiliging is toegepast.</p> <p>Na de inschakeling van Wachtwoordbeveiliging wordt u door Kaspersky Endpoint Security gevraagd om een wachtwoord voor het uitvoeren van bewerkingen in te stellen.</p>  |
| <b>Technical Support web resources</b>   | Lijst met koppelingen naar webbronnen met informatie over technische ondersteuning voor Kaspersky Endpoint Security. Toegevoegde koppelingen  |

|   |   |
|---|---|
| <i>(alleen beschikbaar in de Kaspersky Security Center-console)</i>                               | worden in plaats van de standaardkoppelingen weergegeven in het venster <b>Support</b> van de lokale Kaspersky Endpoint Security-interface. |
| <b>Message to user</b><br><br><i>(alleen beschikbaar in de Kaspersky Security Center-console)</i> | Bericht dat wordt weergegeven in het venster <b>Support</b> van de lokale interface van Kaspersky Endpoint Security.                        |

## Instellingen beheren

U kunt de huidige Kaspersky Endpoint Security-instellingen opslaan in een bestand en ze gebruiken om het programma snel op een andere computer te configureren. U kunt ook een configuratiebestand gebruiken wanneer u het programma implementeert via Kaspersky Security Center met een [installatiepakket](#). U kunt de standaardinstellingen op elk moment herstellen.

De instellingen voor het beheer van programmaconfiguratie zijn alleen beschikbaar in de Kaspersky Endpoint Security-interface.

Beheerinstellingen voor programmaconfiguratie

| Instellingen       | Beschrijving   |
|--------------------|--|
| <b>Importeren</b>  | Pak de programma-instellingen uit een bestand met CFG-indeling uit en pas ze toe.  |
| <b>Exporteren</b>  | Sla de huidige programma-instellingen in een bestand met CFG-indeling op.  |
| <b>Terugzetten</b> | U kunt de instellingen die zijn aanbevolen door Kaspersky lab voor Endpoint Security op elk moment herstellen. Wanneer de instellingen zijn hersteld, wordt het <b>Aanbevolen</b> beveiligingsniveau ingesteld voor alle beschermingsonderdelen. |

## Databases en softwaremodules van het programma bijwerken

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 dreigingen en methoden om ze onschadelijk te maken. Voor een snelle detectie van dreigingen wordt u aanbevolen de databases en programmamodules regelmatig te updaten.

Voor periodieke updates hebt u een actieve licentie nodig. Zonder actieve licentie kunt u maar één keer een update uitvoeren.

De updateservers van Kaspersky zijn de voornaamste updatebron voor Kaspersky Endpoint Security.

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 proxyserver aanpassen.

Updates worden gedownload via het HTTPS-protocol. Ze kunnen ook via het HTTP-protocol worden gedownload als ze niet via het HTTPS-protocol kunnen worden gedownload.

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 dreigingen 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 geüpdatet met records van nieuwe dreigingen 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).

Informatie over de huidige staat van de Kaspersky Endpoint Security-databases is zichtbaar in het hoofdvenster van het programma of de knopinfo die u ziet als u de muisaanwijzer over het pictogram van het programma in het systeemvak beweegt.

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.

Instellingen voor programmamodule en database-update

| Parameter                            | Beschrijving  |
|--------------------------------------|---|
| <b>Planning van database-updates</b> | <p><b>Automatisch.</b> In deze modus controleert Kaspersky Endpoint Security met een bepaalde regelmaat de updatebron op nieuwe beschikbare updatepakketten. De controles op updatepakketten worden tijdens virusuitbraken vaker uitgevoerd en worden minder vaak uitgevoerd als er geen virusuitbraken zijn. Nadat een nieuw updatepakket is gevonden, wordt het door Kaspersky Endpoint Security gedownload en geïnstalleerd op de computer.</p> <p><b>Handmatig.</b> Met deze uitvoermodus voor updatetaken kunt u een updatetaak handmatig starten.</p> <p><b>Volgens schema.</b> In deze uitvoermodus voor updatetaken wordt de updatetaak door Kaspersky Endpoint Security uitgevoerd volgens het opgegeven schema. Als deze uitvoermodus voor updatetaken is geselecteerd, kunt u de updatetaak van Kaspersky Endpoint Security ook handmatig starten.</p> |
| <b>Overgeslagen taken starten</b>    | <p>Als het selectievakje is ingeschakeld, wordt de overgeslagen updatetaak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De updatetaak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de begintijd van de updatetaak.</p> <p>Als het selectievakje is uitgeschakeld, worden overgeslagen updatetaken niet gestart door Kaspersky Endpoint Security. In plaats daarvan start het de volgende updatetaak volgens het huidige schema.</p>   |
| <b>Update source</b>                 | Een <i>updatebron</i> 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.

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.

Kaspersky Endpoint Security ondersteunt geen updates van HTTPS-servers, tenzij het de updateservers van Kaspersky zijn.

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.

#### Start database-updates namens

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 een updatebron waarvoor authenticatie bij de proxyserver vereist is niet geconfigureerd is. 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.

#### Updates voor programmamodules downloaden

Het downloaden van programmamodule-updates met programmadatabase-updates.

Als het selectievakje is ingeschakeld, wordt de gebruiker door Kaspersky Endpoint Security verwittigd over de beschikbare updates voor programmamodules en worden de updates voor programmamodules aan het updatepakket toegevoegd tijdens het uitvoeren van de updatetaak. De toepassing van de updates voor programmamodules wordt door de volgende instellingen bepaald:

- **Essentiële en goedgekeurde updates installeren.** Als deze optie is geselecteerd en updates voor programmamodules beschikbaar zijn, installeert Kaspersky Endpoint Security essentiële updates automatisch en alle andere updates voor programmamodules pas nadat de installatie ervan lokaal is goedgekeurd via de programma-interface of via Kaspersky Security Center.
- **Alleen goedgekeurde updates installeren.** Als deze optie is geselecteerd en updates voor programmamodules beschikbaar zijn, installeert Kaspersky Endpoint Security updates pas nadat de installatie ervan lokaal is goedgekeurd via de programma-interface of via Kaspersky Security Center. Deze optie is standaard geselecteerd.

Als het selectievakje is uitgeschakeld, wordt de gebruiker niet door Kaspersky Endpoint Security verwittigd over de beschikbare updates voor programmamodules en worden de updates voor programmamodules niet aan het updatepakket toegevoegd tijdens het uitvoeren van de updatetaak.

Als voor de updates voor de programmamodules de voorwaarden van de Gebruiksrechtovereenkomst moeten worden doorgenomen en aanvaard, installeert het programma de updates nadat de voorwaarden van de Gebruiksrechtovereenkomst zijn aanvaard.

|   |   |
|---|---|
|   | Dit selectievakje is standaard ingeschakeld.  |
| <b>Updates naar map kopiëren</b>  | Als dit selectievakje is ingeschakeld, kopieert Kaspersky Endpoint Security het updatepakket naar de gedeelde map die onder het selectievakje is opgegeven. Daarna kunnen andere computers in het netwerk het updatepakket in deze gedeelde map ophalen. Hierdoor vermindert u het internetverkeer omdat het updatepakket slechts één keer wordt gedownload. De volgende map is standaard opgegeven: C:\ProgramData\Kaspersky Lab\KES\Update distribution\.   |
| <b>Proxyserver voor updates</b><br><i>(alleen beschikbaar in de Kaspersky Endpoint Security-interface)</i>                      | Proxyserverinstellingen voor internettoegang van gebruikers van clientcomputers om programmamodules en databases bij te werken.<br><br>Voor de automatische configuratie van een proxyserver gebruikt Kaspersky Endpoint Security het WPAD-protocol (Web Proxy Auto-Discovery Protocol). Als het IP-adres van de proxyserver niet kan worden bepaald met dit protocol, gebruikt Kaspersky Endpoint Security het adres van de proxyserver dat in de instellingen van Microsoft Internet Explorer is opgegeven. |
| <b>Gebruik geen proxyserver voor lokale adressen</b><br><i>(alleen beschikbaar in de Kaspersky Endpoint Security-interface)</i> | Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security geen proxyserver wanneer een update vanuit een gedeelde map wordt uitgevoerd.   |

## Appendix 2. Vertrouwensgroepen voor programma's

Kaspersky Endpoint Security categoriseert alle programma's die op de computer worden gestart in vertrouwensgroepen. Programma's worden in vertrouwensgroepen gecategoriseerd naargelang het veiligheidsrisico die de programma's voor het besturingssysteem vormen.

De vertrouwensgroepen zijn de volgende:

- **Vertrouwd.** Deze groep bevat programma's die aan een of meer van de volgende voorwaarden voldoen:
  - De programma's zijn digitaal ondertekend door vertrouwde leveranciers.
  - De programma's komen voor in de Kaspersky Security Network-database van vertrouwde programma's.
  - De gebruiker heeft programma in de groep 'Vertrouwd' geplaatst.

Deze programma's mogen alle bewerkingen uitvoeren.

- **Deels beperkt.** Deze groep bevat programma's die aan de volgende voorwaarden voldoen:
  - De programma's zijn niet digitaal ondertekend door vertrouwde leveranciers.
  - De programma's komen niet voor in de Kaspersky Security Network-database van vertrouwde programma's.
  - De gebruiker heeft programma in de groep 'Deels beperkt' geplaatst.

Zulke programma's hebben minimale beperkingen voor de toegang tot bronnen van het besturingssysteem.

- **Zeer beperkt.** Deze groep bevat programma's die aan de volgende voorwaarden voldoen:

- De programma's zijn niet digitaal ondertekend door vertrouwde leveranciers.
- De programma's komen niet voor in de Kaspersky Security Network-database van vertrouwde programma's.
- De gebruiker heeft programma in de groep 'Zeer beperkt' geplaatst.

Zulke programma's hebben een zeer beperkte toegang tot bronnen van het besturingssysteem.

- **Niet vertrouwd.** Deze groep bevat programma's die aan de volgende voorwaarden voldoen:
  - De programma's zijn niet digitaal ondertekend door vertrouwde leveranciers.
  - De programma's komen niet voor in de Kaspersky Security Network-database van vertrouwde programma's.
  - De gebruiker heeft programma in de groep 'Niet vertrouwd' geplaatst.

Voor deze programma's worden alle bewerkingen geblokkeerd.

## Appendix 3. Bestandsextensies voor snelle scan van verwisselbare schijven

com – uitvoerbaar bestand van een programma dat niet groter is dan 64 kB

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 – dynamische link-bibliotheek

scr – Microsoft Windows-welkomstscherf

cpl – module van Microsoft Windows-configuratiescherf

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

tsp – programma in gedeelde-tijd-modus

drv – stuurprogramma van apparaat

vxd – virtueel-apparaatstuurprogramma van Microsoft Windows

pif – programma-informatiebestand

lnk – Microsoft Windows-koppelingsbestand

reg – licentiebestand 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 – hypertextdocument

htt – Microsoft Windows-hypertekstkop

hta – hypertextprogramma 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 – Microsoft Windows 95-bureaubladbestand

hlp – Win Help-bestand

eml – Microsoft Outlook Express-e-mailbericht

nws – nieuw Microsoft Outlook Express-e-mailbericht

msg – Microsoft Mail-e-mailbericht

plg – e-mailbericht

mbx – opgeslagen Microsoft Office Outlook-e-mailbericht

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

dot\* – Microsoft Office Word-documentjablonen zoals: dot voor Microsoft Office Word-documentjablonen, dotx voor Microsoft Office Word 2007-documentjablonen, dotm voor Microsoft Office Word 2007-documentjablonen 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-bestandsformaat;

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, xlsxm 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

## Appendix 4. Bestandstypen voor het bijlagefilter van Mail Threat Protection

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



Als u het filteren van e-mailbijlagen hebt ingeschakeld, kan het onderdeel Mail Threat Protection bestanden met de volgende extensies hernoemen of verwijderen:

com – uitvoerbaar bestand van een programma dat niet groter is dan 64 kB

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 – dynamische link-bibliotheek

scr – Microsoft Windows-welkomstscherf

cpl – module van Microsoft Windows-configuratiescherf

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

tsp – programma in gedeelde-tijd-modus

drv – stuurprogramma van apparaat

vxd – virtueel-apparaatstuurprogramma van Microsoft Windows

pif – programma-informatiebestand

lnk – Microsoft Windows-koppelingsbestand

reg – licentiebestand 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 – hypertextdocument

htt – Microsoft Windows-hypertekstkop

hta – hypertextprogramma 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 – Microsoft Windows 95-bureaubladbestand

hlp – Win Help-bestand

eml – Microsoft Outlook Express-e-mailbericht

nws – nieuw Microsoft Outlook Express-e-mailbericht

msg – Microsoft Mail-e-mailbericht

plg – e-mailbericht

mbx – opgeslagen Microsoft Office Outlook-e-mailbericht

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

dot\* – Microsoft Office Word-documentjablonen zoals: dot voor Microsoft Office Word-documentjablonen, dotx voor Microsoft Office Word 2007-documentjablonen, dotm voor Microsoft Office Word 2007-documentjablonen 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-bestandsformaat;

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, xslm 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

## Appendix 5. Netwerkinstellingen voor interactie met externe services

Kaspersky Endpoint Security gebruikt de volgende netwerkinstellingen voor interactie met externe services.

### Netwerkinstellingen

| Adres  | Beschrijving  |
|--|---|
| activation-v2.kaspersky.com/activation-service/activation-service.svc<br>Protocol: HTTPS<br>Poort: 443   | Programma activeren.                                      |
| s00.upd.kaspersky.com<br>s01.upd.kaspersky.com<br>s02.upd.kaspersky.com<br>s03.upd.kaspersky.com<br>s04.upd.kaspersky.com<br>s05.upd.kaspersky.com<br>s06.upd.kaspersky.com<br>s07.upd.kaspersky.com | Databases en softwaremodules van het programma bijwerken. |

s08.upd.kaspersky.com  
s09.upd.kaspersky.com  
s10.upd.kaspersky.com  
s11.upd.kaspersky.com  
s12.upd.kaspersky.com  
s13.upd.kaspersky.com  
s14.upd.kaspersky.com  
s15.upd.kaspersky.com  
s16.upd.kaspersky.com  
s17.upd.kaspersky.com  
s18.upd.kaspersky.com  
s19.upd.kaspersky.com  
cm.k.kaspersky-labs.com

Protocol: HTTPS

Poort: 443

downloads.upd.kaspersky.com

Protocol: HTTPS

Poort: 443

- Databases en softwaremodules van het programma bijwerken.
- Controleren of Kaspersky-servers toegankelijk zijn. Als toegang tot de servers met behulp van het DNS-systeem niet mogelijk is, dan maakt het programma gebruik van openbare DNS. Dit is noodzakelijk om ervoor te zorgen dat anti-virusdatabases worden bijgewerkt en het niveau van beveiliging wordt gehandhaafd voor de computer. Kaspersky Endpoint Security gebruikt de volgende lijst met openbare DNS-servers in de volgende volgorde:

1. Google Public DNS (8.8.8.8).

2. Cloudflare DNS (1.1.1.1).

3. Alibaba Cloud DNS (223.6.6.6).

4. Quad9 DNS (9.9.9.9).

5. CleanBrowsing (185.228.168.168).

|  |  |
|--|--|
|  | <p>Verzoeken die door het programma worden verzonden, kunnen adressen van domeinen en het openbare IP-adres van de gebruiker bevatten, omdat het programma een TCP/UDP-verbinding met de DNS-server tot stand brengt. Deze informatie is bijvoorbeeld nodig om het certificaat van een webbron te valideren bij het gebruik van https. Als Kaspersky Endpoint Security een openbare DNS-server gebruikt, wordt de gegevensverwerking geregeld door het privacybeleid van de betreffende service. Als u wilt voorkomen dat Kaspersky Endpoint Security een openbare DNS-server gebruikt, dient u contact op te nemen met Technische support voor een privé-patch.</p> |
| <p>touch.kaspersky.com<br/>Protocol: HTTP</p>  | <ul style="list-style-type: none"> <li>• Het ontvangen van de vertrouwde tijd voor het controleren van de geldigheidsperiode van het certificaat (TLS-verbinding).</li> <li>• Waarschuwing over het weigeren van toegang tot een webbron in de browser (Web Threat Protection en Webcontrole)</li> </ul>   |
| <p>p00.upd.kaspersky.com<br/>p01.upd.kaspersky.com<br/>p02.upd.kaspersky.com<br/>p03.upd.kaspersky.com<br/>p04.upd.kaspersky.com<br/>p05.upd.kaspersky.com<br/>p06.upd.kaspersky.com<br/>p07.upd.kaspersky.com<br/>p08.upd.kaspersky.com<br/>p09.upd.kaspersky.com</p> | <p>Databases en softwaremodules van het programma bijwerken.</p>   |

|   |   |
|---|---|
| <p>p10.upd.kaspersky.com<br/> p11.upd.kaspersky.com<br/> p12.upd.kaspersky.com<br/> p13.upd.kaspersky.com<br/> p14.upd.kaspersky.com<br/> p15.upd.kaspersky.com<br/> p16.upd.kaspersky.com<br/> p17.upd.kaspersky.com<br/> p18.upd.kaspersky.com<br/> p19.upd.kaspersky.com<br/> downloads.kaspersky-labs.com<br/> cm.k.kaspersky-labs.com</p> <p>Protocol: HTTP</p> <p>Poort: 80</p> |   |
| <p>ds.kaspersky.com</p> <p>Protocol: HTTPS</p> <p>Poort: 443</p>  | Bij het gebruik van Kaspersky Security Network. |
| <p>ksn-a-stat-geo.kaspersky-labs.com<br/> ksn-file-geo.kaspersky-labs.com<br/> ksn-verdict-geo.kaspersky-labs.com<br/> ksn-url-geo.kaspersky-labs.com<br/> ksn-a-p2p-geo.kaspersky-labs.com<br/> ksn-info-geo.kaspersky-labs.com<br/> ksn-cinfo-geo.kaspersky-labs.com</p> <p>Protocol: Any</p> <p>Poort: 443, 1443</p>   | Bij het gebruik van Kaspersky Security Network. |
| <p>click.kaspersky.com<br/> redirect.kaspersky.com</p> <p>Protocol: HTTPS</p>   | Volg links vanuit de interface.                 |
| <p>cr1.kaspersky.com<br/> ocsp.kaspersky.com</p> <p>Protocol: HTTP</p> <p>Poort: 80</p>   | Public Key Infrastructure (PKI).                |

## Appendix 6. Programma-gebeurtenissen

Informatie over de werking van elk Kaspersky Endpoint Security-onderdeel, de gebeurtenissen die zijn gerelateerd aan gegevensencryptie, de voltooiing van elke scantaak, updatetaak, integriteitscontrole en de algemene werking van het programma wordt vastgelegd in het Kaspersky Security Center-gebeurtenissenlogboek en Windows-gebeurtenislogboek.

Kaspersky Endpoint Security genereert de volgende soorten gebeurtenissen: algemene gebeurtenissen en specifieke gebeurtenissen. Specifieke gebeurtenissen worden alleen gemaakt door Kaspersky Endpoint Security for Windows. Specifieke gebeurtenissen hebben een eenvoudige ID, zoals 000000cb. Specifieke gebeurtenissen bevatten de volgende vereiste parameters:

- GNRL\_EA\_DESCRIPTION is de inhoud van de gebeurtenis.
- GNRL\_EA\_ID is de service-ID van de gebeurtenis.
- GNRL\_EA\_SEVERITY is de status van de gebeurtenis. 1 – Informatief bericht ⓘ, 2 – Waarschuwing ⚠, 3 – Functionele fouten ❗, 4 – Essentieel ❗.
- EVENT\_TYPE\_DISPLAY\_NAME is de titel van de gebeurtenis.
- TASK\_DISPLAY\_NAME is de naam van het programmacomponent dat de gebeurtenis heeft gestart.

Algemene gebeurtenissen kunnen worden aangemaakt door Kaspersky Endpoint Security for Windows en door andere Kaspersky-programma's (bijvoorbeeld Kaspersky Security for Windows Server). Algemene gebeurtenissen hebben een meer complexe ID, zoals GNRL\_EV\_VIRUS\_FOUND. Naast de vereiste instellingen bevatten algemene gebeurtenissen geavanceerde instellingen.

## Kritieke gebeurtenissen

### [End User License Agreement violated ⓘ](#)

|  |                            |
|--|----------------------------|
| Status   | ❗                          |
| Onderdeel  | Systeemaudit               |
| Windows-gebeurtenissen ID                                | 201                        |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_LICENSE_EXPIRATION |
| Windows gebeurtenislogboek - EventLogItem.               | ✓                          |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓                          |

### [License has almost expired ⓘ](#)

|  |              |
|--|--------------|
| Status   | ❗            |
| Onderdeel  | Systeemaudit |
| Windows-gebeurtenissen ID                                | 203          |
| Kaspersky Security Center gebeurtenis ID                 | 000000cb     |
| Windows gebeurtenislogboek - EventLogItem.               | –            |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓            |

### [Databases are missing or corrupted ⓘ](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 206   |
| Kaspersky Security Center gebeurtenis ID                 | 000000ce  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |


#### [Databases are extremely out of date](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 207   |
| Kaspersky Security Center gebeurtenis ID                 | 000000cf  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Application autorun is disabled](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 209   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d1  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Activation error](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 229   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Active threat detected. Advanced Disinfection should be started](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 231   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e7  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [KSN servers unavailable](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2023  |
| Kaspersky Security Center gebeurtenis ID                 | 000007e7  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Not enough space in Quarantine storage](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 343   |
| Kaspersky Security Center gebeurtenis ID                 | 00000157  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object not restored from Quarantine](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 346   |
| Kaspersky Security Center gebeurtenis ID                 | 0000015a  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object not deleted from Quarantine](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 348   |
| Kaspersky Security Center gebeurtenis ID                 | 0000015c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |




**Er is verbinding gemaakt met een domein met een niet-vertrouwd certificaat** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 57  |
| Kaspersky Security Center gebeurtenis ID                 | 00000039  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |




**We konden een versleutelde verbinding niet controleren. Het domein is aan de lijst met uitzonderingen toegevoegd.** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 60  |
| Kaspersky Security Center gebeurtenis ID                 | 0000003c  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |




**Malicious object detected (local bases)** 

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Gedragsdetectie<br>Exploit-preventie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 302   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_VIRUS_FOUND   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [Malicious object detected \(KSN\)](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Gedragsdetectie<br>Exploit-preventie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 302   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_VIRUS_FOUND_BY_KSN  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/>Programmacomponent (<a href="#">engine</a>).<br/>Threat detection technology (<a href="#">methode</a>).<br/>Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/>EDR-versie.<br/>Identificatie van dreiging in EDR.<br/>MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

## [Disinfection impossible](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>Virusscan  |
| Windows-gebeurtenissen ID                                | 312   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_NOTCURED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |


### Cannot be deleted

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Host Intrusion Prevention<br>Gedragsdetectie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 313   |
| Kaspersky Security Center gebeurtenis ID                 | 00000139  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |


### Processing error

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>AMSI-bescherming<br>Virusscan |
| Windows-gebeurtenissen ID                                | 317   |
| Kaspersky Security Center gebeurtenis ID                 | 0000013d  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |




### Process terminated

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Host Intrusion Prevention<br>Gedragsdetectie<br>Virusscan |
| Windows-gebeurtenissen ID                                | 452   |
| Kaspersky Security Center gebeurtenis ID                 | 000001c4  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### Unable to terminate process

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Host Intrusion Prevention<br>Gedragsdetectie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 453   |
| Kaspersky Security Center gebeurtenis ID                 | 000001c5  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### Dangerous link blocked

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Web Threat Protection  |
| Windows-gebeurtenissen ID                                | 362  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_VIRUS_FOUND_AND_BLOCKED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is het pad naar het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

[Dangerous link opened](#) 




|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Web Threat Protection  |
| Windows-gebeurtenissen ID                                | 363  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_VIRUS_FOUND_AND_REPORTED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is het pad naar het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

[Previously opened dangerous link detected](#) 





|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Web Threat Protection  |
| Windows-gebeurtenissen ID                                | 1201   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_VIRUS_FOUND_AND_PASSED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is het pad naar het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

[Process action blocked](#) 

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Adaptieve controle op afwijkingen  |
| Windows-gebeurtenissen ID                                | 2200   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ADSEC_DETECT   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de naam van de regel voor Adaptieve controle op afwijkingen.</li> <li>• GNRL_EA_PARAM_2 is de ID van de heuristische regel.</li> <li>• GNRL_EA_PARAM_3 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_4 is het bronproces.</li> <li>• GNRL_EA_PARAM_5 is het bronobject.</li> <li>• GNRL_EA_PARAM_6 is het doelproces.</li> <li>• GNRL_EA_PARAM_7 is het doelobject.</li> <li>• GNRL_EA_PARAM_8 is bijkomende informatie over het gedetecteerde object:<br/>Hashes van bronproces / object en doelproces / object.<br/>Proces geblokkeerd (verdict_type): true of false.<br/>User security ID (SID).</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

### [Keyboard not authorized](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | BadUSB Attack Prevention  |
| Windows-gebeurtenissen ID                                | 2051  |
| Kaspersky Security Center gebeurtenis ID                 | 00000803  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




### [AMSI request was blocked](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | AMSI-bescherming  |
| Windows-gebeurtenissen ID                                | 2200  |
| Kaspersky Security Center gebeurtenis ID                 | 00000898  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



### Network activity blocked

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Firewall  |
| Windows-gebeurtenissen ID                                | 602   |
| Kaspersky Security Center gebeurtenis ID                 | 00000329  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



### Network attack detected

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Network Threat Protection  |
| Windows-gebeurtenissen ID                                | 651  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ATTACK_DETECTED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de naam van de aanval.</li> <li>• GNRL_EA_PARAM_2 is het protocol.</li> <li>• GNRL_EA_PARAM_3 is het IP-adres van de computer die fungeert als de bron van de netwerkaanval. Het IP-adres wordt aangegeven in de byte order van de host. Bijvoorbeeld 2886729929 voor 172.16.0.201.</li> <li>• GNRL_EA_PARAM_4 is het poortnummer.</li> <li>• GNRL_EA_PARAM_5 is een IPv6-adres, bijvoorbeeld 12B012B012B012B012B012B012B012B012B012B012B0.</li> <li>• GNRL_EA_PARAM_6 is het IP-adres van de computer waarop de netwerkaanval is gericht. Het IP-adres wordt aangegeven in de byte order van de host. Bijvoorbeeld 2886729929 voor 172.16.0.201.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

### [Application startup prohibited](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Programmacontrole  |
| Windows-gebeurtenissen ID                                | 702  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_APPLICATION_LAUNCH_DENIED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de handmatig aangemaakte categorie-ID.</li> <li>• GNRL_EA_PARAM_4 is de programmacategorie-ID.</li> <li>• GNRL_EA_PARAM_5 is informatie over de digitale handtekening van het programma.</li> <li>• GNRL_EA_PARAM_6 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe).</li> <li>• GNRL_EA_PARAM_7 is het pad naar het uitvoerbare bestand.</li> <li>• GNRL_EA_PARAM_8 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_9 is de versie van het programma die de gebruiker probeert uit te voeren.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |


### [Prohibited process was started before Kaspersky Endpoint Security startup](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Programmacontrole   |
| Windows-gebeurtenissen ID                                | 710   |
| Kaspersky Security Center gebeurtenis ID                 | 000002c6  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



### [Access denied \(local bases\)](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Webcontrole  |
| Windows-gebeurtenissen ID                                | 752  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_WEB_URL_BLOCKED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de URL.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |



### [Access denied \(KSN\)](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Webcontrole  |
| Windows-gebeurtenissen ID                                | 752  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_WEB_URL_BLOCKED_BY_KSN   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de URL.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |



### [Operation with the device prohibited](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 802   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_DEVCTRL_DEV_PLUG_DENIED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de Hardware-ID (HWID).</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [Network connection blocked](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 809   |
| Kaspersky Security Center gebeurtenis ID                 | 00000329  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Error updating component](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1011  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f3  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Error distributing component updates](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1012  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f4  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Local update error](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1014  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f6  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Network update error](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1015  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f7  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Cannot start two tasks at the same time](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1017  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f9  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Error verifying application databases and modules](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1018  |
| Kaspersky Security Center gebeurtenis ID                 | 000003fa  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Error in interaction with Kaspersky Security Center](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1019  |
| Kaspersky Security Center gebeurtenis ID                 | 000003fb  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Not all components were updated](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1021  |
| Kaspersky Security Center gebeurtenis ID                 | 000003fd  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Update completed successfully, update distribution failed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1023  |
| Kaspersky Security Center gebeurtenis ID                 | 000003ff  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Internal task error](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 101   |
| Kaspersky Security Center gebeurtenis ID                 | 00000065  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Patch installation failed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2153  |
| Kaspersky Security Center gebeurtenis ID                 | 00000869  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |


#### [Patch rollback failed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2156  |
| Kaspersky Security Center gebeurtenis ID                 | 0000086c  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



#### [Error applying file encryption / decryption rules](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 904   |
| Kaspersky Security Center gebeurtenis ID                 | 00000388  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [File encryption / decryption error](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 912   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ENCRYPTION_ERROR  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is het pad naar het bestand.</li> <li>• GNRL_EA_PARAM_2 is de oorzaak van de fout</li> <li>• GNRL_EA_PARAM_3 is het type apparaat</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |


### [File access blocked](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 940   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is het doelobject.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe) dat probeert toegang te krijgen tot het bestand.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Error enabling portable mode](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 951   |
| Kaspersky Security Center gebeurtenis ID                 | 000003b7  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Error disabling portable mode](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 953   |
| Kaspersky Security Center gebeurtenis ID                 | 000003b9  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [Error creating encrypted package](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 931   |
| Kaspersky Security Center gebeurtenis ID                 | 000003a3  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Error encrypting / decrypting device](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1305  |
| Kaspersky Security Center gebeurtenis ID                 | 00000519  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Could not load encryption module](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1311  |
| Kaspersky Security Center gebeurtenis ID                 | 0000051f  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

[The task for managing Authentication Agent accounts ended with an error !\[\]\(d78c9078ee3cb2e4419b0f5e50b1709c\_img.jpg\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1340  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

[Policy cannot be applied !\[\]\(dff16eb91fad07a22c76e16adcd431cc\_img.jpg\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 1312  |
| Kaspersky Security Center gebeurtenis ID                 | 00000520  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


[FDE upgrade failed !\[\]\(7292cfeb0e02ff5cd8a27a6eab9e1e20\_img.jpg\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1342  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053e  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


[FDE upgrade rollback failed \(for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help\) !\[\]\(d38d40db5bb31e2db2f3490804bde37d\_img.jpg\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1344  |
| Kaspersky Security Center gebeurtenis ID                 | 00000540  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Kaspersky Anti Targeted Attack Platform server unavailable](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2100  |
| Kaspersky Security Center gebeurtenis ID                 | 00000834  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Failed to delete object](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2252  |
| Kaspersky Security Center gebeurtenis ID                 | 000008cc  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object not quarantined \(Kaspersky Sandbox\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2603  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a2b  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [An internal error occurred](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2607  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a2f  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [Invalid Kaspersky Sandbox server certificate](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2613  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a35  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [The Kaspersky Sandbox node is unavailable](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2614  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a36  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [An error occurred while processing the object in Kaspersky Sandbox](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2617  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a39  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [Maximale belasting van Kaspersky Sandbox is overschreden](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2618  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a3a  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


### [IOC gevonden](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2651  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a5b  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### [Kaspersky Sandbox license verification failed](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2620  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a3c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### [Object startup blocked](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2553  |
| Kaspersky Security Center gebeurtenis ID                 | 000009f9  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### [Opstart van proces geblokkeerd](#)




|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2551  |
| Kaspersky Security Center gebeurtenis ID                 | 000009f7  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Uitvoering van script geblokkeerd](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2559  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object not quarantined \(Endpoint Detection and Response\)](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2556  |
| Kaspersky Security Center gebeurtenis ID                 | 000009fc  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Error changing application components](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 1401  |
| Kaspersky Security Center gebeurtenis ID                 | 00000579  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

Functionele fout

### [Task cannot be performed](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 212   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d4  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Invalid task settings. Settings not applied](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 707   |
| Kaspersky Security Center gebeurtenis ID                 | 000002c3  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

## Waarschuwing

### [Programma gecrasht tijdens vorige sessie](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 237   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [License expires soon](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 204   |
| Kaspersky Security Center gebeurtenis ID                 | 000000cc  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### Databases are out of date

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 208   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d0  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### Automatic updates are disabled

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 210   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d2  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### Self-Defense is disabled

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 211   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d3  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### Protection components are disabled

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 214   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d6  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Computer is running in safe mode](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 215   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d7  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [There are unprocessed files](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 216   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d8  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Group policy applied](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 219   |
| Kaspersky Security Center gebeurtenis ID                 | 000000db  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Task stopped](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 222   |
| Kaspersky Security Center gebeurtenis ID                 | 000000de  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**Quit and reopen the application to complete updating** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 224   |
| Kaspersky Security Center gebeurtenis ID                 | 0000057b  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**Computer restart required** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 225   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e1  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**The license allows the use of components that have not been installed** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 226   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e2  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**Advanced Disinfection started** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 232   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e8  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Advanced Disinfection completed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 233   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e9  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



### [Incorrect reserve key](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 230   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e6  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Subscription expires soon](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 240   |
| Kaspersky Security Center gebeurtenis ID                 | 000000f0  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Geblokkeerd](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gedragdetectie<br>Exploit-preventie<br>Web Threat Protection                        |
| Windows-gebeurtenissen ID                                | 331   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |




#### [Cannot restore object from Backup](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 336   |
| Kaspersky Security Center gebeurtenis ID                 | 00000150  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### [Suspicious network activity detected](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2001  |
| Kaspersky Security Center gebeurtenis ID                 | 000007d1  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Encrypted connection terminated](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 250   |
| Kaspersky Security Center gebeurtenis ID                 | 000007d3  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Participation in KSN disabled](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2021  |
| Kaspersky Security Center gebeurtenis ID                 | 000007e5  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Processing of some OS functions is disabled.](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 245   |
| Kaspersky Security Center gebeurtenis ID                 | 000000f5  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Quarantine storage is almost out of space](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 344   |
| Kaspersky Security Center gebeurtenis ID                 | 00000158  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Verbinding geblokkeerd](#)



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 809   |
| Kaspersky Security Center gebeurtenis ID                 | 00000abe  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Cannot create a backup copy](#)




|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Gedragsdetectie<br>Host Intrusion Prevention<br>Virusscan |
| Windows-gebeurtenissen ID                                | 310   |
| Kaspersky Security Center gebeurtenis ID                 | 00000136  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |


[Object not processed](#) 

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>AMSI-bescherming<br>Virusscan  |
| Windows-gebeurtenissen ID                                | 314   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_REPORTED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |



### [Object encrypted](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Host Intrusion Prevention   |
| Windows-gebeurtenissen ID                                | 320   |
| Kaspersky Security Center gebeurtenis ID                 | 00000140  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [Object corrupted](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Virusscan |
| Windows-gebeurtenissen ID                                | 321   |
| Kaspersky Security Center gebeurtenis ID                 | 00000141  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



[Legitimate software that can be used by intruders to damage your computer or personal data was detected \(local bases\)](#)<sup>2</sup>

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>AMSI-bescherming<br>Gedragsdetectie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 303  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_SUSPICIOUS_OBJECT_FOUND  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |



[Legitimate software that can be used by intruders to damage your computer or personal data was detected \(KSN\)](#)<sup>2</sup>

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>AMSI-bescherming<br>Gedragsdetectie<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 303  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_SUSPICIOUS_OBJECT_FOUND  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |



[Object deleted](#) 

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>Exploit-preventie<br>Gedragsdetectie<br>Virusscan  |
| Windows-gebeurtenissen ID                                | 307   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_DELETED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |



[Object disinfected](#) 

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Mail Threat Protection<br>Host Intrusion Prevention<br>Virusscan  |
| Windows-gebeurtenissen ID                                | 306   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_CURED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |



### Object wordt gedesinfecteerd bij herstart

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Host Intrusion Prevention<br>File Threat Protection<br>Virusscan                      |
| Windows-gebeurtenissen ID                                | 324   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [Object wordt verwijderd bij herstart <sup>?</sup>](#)

|  |   |
|--|---|
| Status   |                      |
| Onderdeel  | Gedragdetectie<br>Exploit-preventie<br>Host Intrusion Prevention<br>File Threat Protection<br>Virusscan |
| Windows-gebeurtenissen ID                                | 323   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |                      |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [Object verwijderd volgens instellingen <sup>?</sup>](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Mail Threat Protection  |
| Windows-gebeurtenissen ID                                | 342   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |



### [Rollback completed <sup>?</sup>](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Gedragdetectie<br>Exploit-preventie<br>Virusscan            |
| Windows-gebeurtenissen ID                                | 455   |
| Kaspersky Security Center gebeurtenis ID                 | 000001c7  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Object download was blocked <sup>?</sup>](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Web Threat Protection   |
| Windows-gebeurtenissen ID                                | 341   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_BLOCKED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [Keyboard authorization error](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | BadUSB Attack Prevention  |
| Windows-gebeurtenissen ID                                | 2052  |
| Kaspersky Security Center gebeurtenis ID                 | 00000804  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [The object scan result has been sent to a third-party application](#)



|  |   |
|--|---|
| Status   |    |
| Onderdeel  | AMSI-bescherming  |
| Windows-gebeurtenissen ID                                | 1512  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_OBJECT_REPORTED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File.</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_8 is het type van de dreiging, bijvoorbeeld, Trojware.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.<br/> EDR-versie.<br/> Identificatie van dreiging in EDR.<br/> MD5 hash van het object.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [Task settings applied successfully](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Programmacontrole   |
| Windows-gebeurtenissen ID                                | 708   |
| Kaspersky Security Center gebeurtenis ID                 | 000002c4  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Warning about undesirable content \(local bases\)](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Webcontrole  |
| Windows-gebeurtenissen ID                                | 708  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_WEB_URL_WARNING  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de URL.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

#### [Warning about undesirable content \(KSN\)](#)

|  |  |
|--|--|
| Status   |    |
| Onderdeel  | Webcontrole  |
| Windows-gebeurtenissen ID                                | 708  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_WEB_URL_WARNING  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de URL.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

#### [Undesirable content was accessed after a warning](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Webcontrole   |
| Windows-gebeurtenissen ID                                | 754   |
| Kaspersky Security Center gebeurtenis ID                 | 000002f2  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### Temporary access to the device activated

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 803   |
| Kaspersky Security Center gebeurtenis ID                 | 000002f2  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### Operation cancelled by the user

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1016  |
| Kaspersky Security Center gebeurtenis ID                 | 000003f8  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### User has opted out of the encryption policy

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1306  |
| Kaspersky Security Center gebeurtenis ID                 | 0000051a  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### Toepassing van regels voor bestandsencryptie/-decryptie onderbroken

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 903   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### [Encryptie/decryptie van bestanden onderbroken](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 914   |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |


#### [Encryptie/decryptie van apparaat onderbroken](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1303  |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |




#### [Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1345  |
| Kaspersky Security Center gebeurtenis ID                 | 00000541  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




#### [Module signature check failed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Integriteitscontrole  |
| Windows-gebeurtenissen ID                                | 2002  |
| Kaspersky Security Center gebeurtenis ID                 | 000007d2  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



#### [Application startup was blocked](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2105  |
| Kaspersky Security Center gebeurtenis ID                 | 00000839  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




#### [Document opening was blocked](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2106  |
| Kaspersky Security Center gebeurtenis ID                 | 0000083a  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




#### [Proces is beëindigd door de beheerder van de Kaspersky Anti Targeted Attack Platform-server](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2112  |
| Kaspersky Security Center gebeurtenis ID                 | 00000840  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




#### [Het programma is beëindigd door de beheerder van de Kaspersky Anti Targeted Attack Platform-server](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2113  |
| Kaspersky Security Center gebeurtenis ID                 | 00000841  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




**Bestand of stream is verwijderd door de beheerder van de Kaspersky Anti Targeted Attack Platform-server** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2111  |
| Kaspersky Security Center gebeurtenis ID                 | 0000083f  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




**Bestand is door de beheerder teruggezet vanuit quarantaine op de Kaspersky Anti Targeted Attack Platform-server** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2110  |
| Kaspersky Security Center gebeurtenis ID                 | 0000083e  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




**Bestand is door de beheerder in quarantaine geplaatst op de Kaspersky Anti Targeted Attack Platform-server** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2109  |
| Kaspersky Security Center gebeurtenis ID                 | 0000083d  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### Netwerkactiviteit van alle programma's van andere leveranciers is geblokkeerd

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2107  |
| Kaspersky Security Center gebeurtenis ID                 | 0000083b  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### Netwerkactiviteit van alle programma's van andere leveranciers is gedeblokkeerd

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Endpoint Sensor  |
| Windows-gebeurtenissen ID                                | 2108   |
| Kaspersky Security Center gebeurtenis ID                 | 0000083c   |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




### Object will be deleted after restart (Kaspersky Sandbox)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2605  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a2d  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




### Total size of scan tasks exceeded the limit

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2612  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a34  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




### Object startup allowed, event logged

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2553  |
| Kaspersky Security Center gebeurtenis ID                 | 000009fa  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




### Process startup allowed, event logged

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Endpoint Detection and Response  |
| Windows-gebeurtenissen ID                                | 2554   |
| Kaspersky Security Center gebeurtenis ID                 | 000009f8   |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### Object will be deleted after restart (Endpoint Detection and Response)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2558  |
| Kaspersky Security Center gebeurtenis ID                 | 000009fe  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### Network isolation


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2700  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a8c  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



### [Termination of network isolation](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2701  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a8d  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



### [Restart required to complete the task](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 225   |
| Kaspersky Security Center gebeurtenis ID                 | 0000057b  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### [Application startup blockage message to administrator](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Programmacontrole   |
| Windows-gebeurtenissen ID                                | 503   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_AC_USER_REQUEST   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_DESCRIPTION is het bericht aan de gebruiker.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_6 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe).</li> <li>• GNRL_EA_PARAM_7 is het pad naar het uitvoerbare bestand.</li> <li>• GNRL_EA_PARAM_8 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_9 is de versie van het programma die de gebruiker probeert uit te voeren.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |



#### [Device access blockage message to administrator](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 804   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_DC_USER_REQUEST   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• c_er_descr is het bericht aan gebruiker.</li> <li>• GNRL_EA_PARAM_1 is de Hardware-ID (HWID).</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

#### [Web page access blockage message to administrator](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Webcontrole  |
| Windows-gebeurtenissen ID                                | 755  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_WC_USER_REQUEST  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_DESCRIPTION is het bericht aan de gebruiker.</li> <li>• GNRL_EA_PARAM_1 is de URL.</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

### Device connection blocked



|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 807   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_DEVCTRL_DEV_PLUG_DENIED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de Hardware-ID (HWID).</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### Application activity blockage message to administrator

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Adaptieve controle op afwijkingen  |
| Windows-gebeurtenissen ID                                | 503  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ADSEC_USER_REQUEST   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_DESCRIPTION is het bericht aan de gebruiker.</li> <li>• GNRL_EA_PARAM_1 is de naam van de regel voor Adaptieve controle op afwijkingen.</li> <li>• GNRL_EA_PARAM_2 is de ID van de heuristische regel.</li> <li>• GNRL_EA_PARAM_3 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_4 is het bronproces.</li> <li>• GNRL_EA_PARAM_5 is het bronobject.</li> <li>• GNRL_EA_PARAM_6 is het doelproces.</li> <li>• GNRL_EA_PARAM_7 is het doelobject.</li> <li>• GNRL_EA_PARAM_8 is bijkomende informatie over het gedetecteerde object:<br/>Hashes van bronproces / object en doelproces / object.<br/>Proces geblokkeerd (verdict_type): true of false.<br/>User security ID (SID).</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | -  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

## Informatieve berichten.

### [Application started](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 235   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


### [Application stopped](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 236   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [The operation with application resources is blocked by Self-Defense](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 213   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d5  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Report cleared](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 217   |
| Kaspersky Security Center gebeurtenis ID                 | 000000d9  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Group policy disabled](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 220   |
| Kaspersky Security Center gebeurtenis ID                 | 000000dc  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Application settings changed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 218   |
| Kaspersky Security Center gebeurtenis ID                 | 000000da  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### Task started

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 221   |
| Kaspersky Security Center gebeurtenis ID                 | 000000dd  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### Task completed

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 223   |
| Kaspersky Security Center gebeurtenis ID                 | 000000df  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### All application components that are defined by the license have been installed and run in normal mode

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 227   |
| Kaspersky Security Center gebeurtenis ID                 | 000000e3  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### Subscription settings have changed

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 238   |
| Kaspersky Security Center gebeurtenis ID                 | 000000ee  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Subscription has been renewed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 239   |
| Kaspersky Security Center gebeurtenis ID                 | 000000ef  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |


### [Object restored from Backup](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 335   |
| Kaspersky Security Center gebeurtenis ID                 | 0000014f  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [User name and password input](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2000  |
| Kaspersky Security Center gebeurtenis ID                 | 000007d0  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Participation in KSN enabled](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2020  |
| Kaspersky Security Center gebeurtenis ID                 | 000007e4  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |




**KSN servers available** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2022  |
| Kaspersky Security Center gebeurtenis ID                 | 000007e6  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**The application works and processes data under relevant laws and uses the appropriate infrastructure** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 2024  |
| Kaspersky Security Center gebeurtenis ID                 | 000007e8  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**Object restored from Quarantine** 


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 345   |
| Kaspersky Security Center gebeurtenis ID                 | 00000159  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**Object deleted from Quarantine** 




|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 347   |
| Kaspersky Security Center gebeurtenis ID                 | 0000015b  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



**A backup copy of the object was created** 

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | File Threat Protection<br>Mail Threat Protection<br>Gedragsdetectie<br>Host Intrusion Prevention<br>Kaspersky Sandbox<br>Virusscan |
| Windows-gebeurtenissen ID                                | 308  |
| Kaspersky Security Center gebeurtenis ID                 | 00000134   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓  |

**Overwritten by a copy that was disinfected earlier** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | File Threat Protection<br>Host Intrusion Prevention<br>Virusscan                      |
| Windows-gebeurtenissen ID                                | 327   |
| Kaspersky Security Center gebeurtenis ID                 | 00000147  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |


**Password-protected archive detected** 

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Virusscan   |
| Windows-gebeurtenissen ID                                | 322   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_PASSWD_ARCHIVE_FOUND  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is de naam van het object.</li> <li>• GNRL_EA_PARAM_3 is de datum van aanmaak van het object (optioneel).</li> <li>• GNRL_EA_PARAM_7 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object:<br/> Programmacomponent (<a href="#">engine</a>).<br/> Threat detection technology (<a href="#">methode</a>).<br/> Dreiging gedetecteerd door Privaat KSN (denylist): true of false.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [Information about detected object](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Virusscan |
| Windows-gebeurtenissen ID                                | 332   |
| Kaspersky Security Center gebeurtenis ID                 | 0000014c  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### [The object is in the Private KSN allowlist](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Host Intrusion Prevention<br>Virusscan |
| Windows-gebeurtenissen ID                                | 340   |
| Kaspersky Security Center gebeurtenis ID                 | 00000154  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


### Object renamed

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Mail Threat Protection<br>Exploit-preventie<br>Gedragsdetectie<br>Virusscan         |
| Windows-gebeurtenissen ID                                | 329   |
| Kaspersky Security Center gebeurtenis ID                 | 00000149  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



### Object processed

|  |   |
|--|---|
| Status   |                                |
| Onderdeel  | Host Intrusion Prevention<br>File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>Virusscan |
| Windows-gebeurtenissen ID                                | 301   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



### Object skipped

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Host Intrusion Prevention<br>File Threat Protection<br>AMSI-bescherming<br>Virusscan |
| Windows-gebeurtenissen ID                                | 315  |
| Kaspersky Security Center gebeurtenis ID                 | -  |
| Windows gebeurtenislogboek - EventLogItem.               |   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -  |

### [Archive detected](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Host Intrusion Prevention<br>File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Virusscan |
| Windows-gebeurtenissen ID                                | 318   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Packed object detected](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Host Intrusion Prevention<br>File Threat Protection<br>Web Threat Protection<br>Mail Threat Protection<br>AMSI-bescherming<br>Virusscan |
| Windows-gebeurtenissen ID                                | 319   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |    |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



### [Link processed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Web Threat Protection   |
| Windows-gebeurtenissen ID                                | 361   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [Application startup allowed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Programmacontrole   |
| Windows-gebeurtenissen ID                                | 701   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Update source is selected](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1001  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [Proxyserver is geselecteerd](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1002  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [The link is in the Private KSN allowlist](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Web Threat Protection   |
| Windows-gebeurtenissen ID                                | 370   |
| Kaspersky Security Center gebeurtenis ID                 | 00000172  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [Application placed in the trusted group](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Host Intrusion Prevention   |
| Windows-gebeurtenissen ID                                | 401   |
| Kaspersky Security Center gebeurtenis ID                 | 00000191  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



#### [Application placed in restricted group](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Host Intrusion Prevention   |
| Windows-gebeurtenissen ID                                | 402   |
| Kaspersky Security Center gebeurtenis ID                 | 00000192  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [Host Intrusion Prevention was triggered](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Host Intrusion Prevention   |
| Windows-gebeurtenissen ID                                | 403   |
| Kaspersky Security Center gebeurtenis ID                 | 00000193  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [File restored](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gedragsdetectie<br>Exploit-preventie<br>Host Intrusion Prevention                   |
| Windows-gebeurtenissen ID                                | 457   |
| Kaspersky Security Center gebeurtenis ID                 | 000001c9  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |



#### [Registry value restored](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gedragsdetectie<br>Exploit-preventie  |
| Windows-gebeurtenissen ID                                | 458   |
| Kaspersky Security Center gebeurtenis ID                 | 000001ca  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Registry value deleted](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gedragsdetectie<br>Exploit-preventie  |
| Windows-gebeurtenissen ID                                | 459   |
| Kaspersky Security Center gebeurtenis ID                 | 000001cb  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Process action skipped](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Adaptieve controle op afwijkingen  |
| Windows-gebeurtenissen ID                                | 2201   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_ADSEC_DETECT   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de naam van de regel voor Adaptieve controle op afwijkingen.</li> <li>• GNRL_EA_PARAM_2 is de ID van de heuristische regel.</li> <li>• GNRL_EA_PARAM_3 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_4 is het bronproces.</li> <li>• GNRL_EA_PARAM_5 is het bronobject.</li> <li>• GNRL_EA_PARAM_6 is het doelproces.</li> <li>• GNRL_EA_PARAM_7 is het doelobject.</li> <li>• GNRL_EA_PARAM_8 is bijkomende informatie over het gedetecteerde object:<br/>Hashes van bronproces / object en doelproces / object.<br/>Proces geblokkeerd (verdict_type): true of false.<br/>User security ID (SID).</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

### Keyboard authorized


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | BadUSB Attack Prevention  |
| Windows-gebeurtenissen ID                                | 2050  |
| Kaspersky Security Center gebeurtenis ID                 | 00000802  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### Network activity allowed




|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Firewall  |
| Windows-gebeurtenissen ID                                | 601   |
| Kaspersky Security Center gebeurtenis ID                 | 00000259  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [Application startup prohibited in test mode](#)

|  |  |
|--|--|
| Status   |   |
| Onderdeel  | Programmacontrole  |
| Windows-gebeurtenissen ID                                | 703  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_APP_LAUNCH_TESTED_DENIED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de handmatig aangemaakte categorie-ID.</li> <li>• GNRL_EA_PARAM_4 is de veiligheidsidentificatie van de account (SID).</li> <li>• GNRL_EA_PARAM_5 is informatie over de digitale handtekening van het programma.</li> <li>• GNRL_EA_PARAM_6 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe).</li> <li>• GNRL_EA_PARAM_7 is het pad naar het uitvoerbare bestand.</li> <li>• GNRL_EA_PARAM_8 is de hash van het object (SHA256).</li> <li>• GNRL_EA_PARAM_9 is de versie van het programma die de gebruiker probeert uit te voeren.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |   |

### [Application startup allowed in test mode](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Programmacontrole   |
| Windows-gebeurtenissen ID                                | 704   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_APP_LAUNCH_TESTED_ALLOW   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_3 is de handmatig aangemaakte categorie-ID.</li> <li>• GNRL_EA_PARAM_4 is de veiligheidsidentificatie van de account (SID).</li> <li>• GNRL_EA_PARAM_5 is informatie over de digitale handtekening van het programma.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |


#### [A page that is allowed was opened](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Webcontrole   |
| Windows-gebeurtenissen ID                                | 751   |
| Kaspersky Security Center gebeurtenis ID                 | 000002f4  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### [Operation with the device allowed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 801   |
| Kaspersky Security Center gebeurtenis ID                 | 00000321  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### [File operation performed](#)

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 808   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_USB_FILE_OPERATION  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de bestandsbewerking (schrijven of wissen).</li> <li>• GNRL_EA_PARAM_2 is het pad naar het bestand.</li> <li>• GNRL_EA_PARAM_3 is de naam van het apparaat.</li> <li>• GNRL_EA_PARAM_4 is de naam van de sessiegebruiker.</li> <li>• GNRL_EA_PARAM_5 is de Hardware-ID (HWID).</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### No available updates

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1020  |
| Kaspersky Security Center gebeurtenis ID                 | 000003fc  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### Update distribution completed successfully

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1022  |
| Kaspersky Security Center gebeurtenis ID                 | 000003fe  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

#### Bestanden downloaden

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1003  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Bestand gedownload](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1004  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Bestand geïnstalleerd](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1005  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Bestand geüpdatet](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1006  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Bestand teruggedraaid vanwege fout bij update](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1007  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Bestanden updaten](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1008  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Updates verspreiden](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1009  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Bestanden terugdraaien](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1010  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Lijst met te downloaden bestanden maken](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 1013  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Patches downloaden](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2150  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Patch installeren](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2151  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Patch geïnstalleerd](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2152  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Patch terugdraaien](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2154  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [Patch teruggedraaid](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Database-update   |
| Windows-gebeurtenissen ID                                | 2155  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



#### [Started applying file encryption / decryption rules](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 901   |
| Kaspersky Security Center gebeurtenis ID                 | 00000385  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Finished applying file encryption / decryption rules](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 902   |
| Kaspersky Security Center gebeurtenis ID                 | 00000386  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

#### [Toepassing van regels voor bestandsencryptie/-decryptie hervat](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 905   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



#### Bestandsencryptie/-decryptie is gestart

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 910   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### Encryptie/decryptie van bestanden voltooid

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 911   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### Bestand is niet geëncrypt omdat het een uitzondering is

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 913   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### Portable modus ingeschakeld



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 950   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



### [Portable modus uitgeschakeld](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 952   |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


### [Encryptie/decryptie van apparaat gestart](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1301  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Encryptie/decryptie van apparaat voltooid](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1302  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

### [Encryptie/decryptie van apparaat hervat](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1304  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [Apparaat is niet geëncrypt](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1307  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Encryptie/decryptie van apparaat is overgeschakeld naar actieve modus](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1308  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Encryptie/decryptie van apparaat is overgeschakeld naar passieve modus](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1309  |
| Kaspersky Security Center gebeurtenis ID                 | -   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Encryption module loaded](#)

|  |                   |
|--|-------------------|
| Status   | <a href="#">①</a> |
| Onderdeel  | Gegevensencryptie |
| Windows-gebeurtenissen ID                                | 1310              |
| Kaspersky Security Center gebeurtenis ID                 | 0000051e          |
| Windows gebeurtenislogboek - EventLogItem.               | -                 |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -                 |

#### [New Authentication Agent account created](#) <sup>?</sup>

|  |                   |
|--|-------------------|
| Status   | <a href="#">①</a> |
| Onderdeel  | Gegevensencryptie |
| Windows-gebeurtenissen ID                                | 1330              |
| Kaspersky Security Center gebeurtenis ID                 | 00000532          |
| Windows gebeurtenislogboek - EventLogItem.               | -                 |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -                 |

#### [Authentication Agent account deleted](#) <sup>?</sup>

|  |                   |
|--|-------------------|
| Status   | <a href="#">①</a> |
| Onderdeel  | Gegevensencryptie |
| Windows-gebeurtenissen ID                                | 1331              |
| Kaspersky Security Center gebeurtenis ID                 | 00000533          |
| Windows gebeurtenislogboek - EventLogItem.               | -                 |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -                 |

#### [Authentication Agent account password changed](#) <sup>?</sup>

|  |                   |
|--|-------------------|
| Status   | <a href="#">①</a> |
| Onderdeel  | Gegevensencryptie |
| Windows-gebeurtenissen ID                                | 1332              |
| Kaspersky Security Center gebeurtenis ID                 | 00000534          |
| Windows gebeurtenislogboek - EventLogItem.               | -                 |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -                 |

#### [Successful Authentication Agent login](#) <sup>?</sup>

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1333  |
| Kaspersky Security Center gebeurtenis ID                 | 00000535  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [Failed Authentication Agent login attempt](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1334  |
| Kaspersky Security Center gebeurtenis ID                 | 00000536  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Hard drive accessed using the procedure of requesting access to encrypted devices](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1335  |
| Kaspersky Security Center gebeurtenis ID                 | 00000537  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1336  |
| Kaspersky Security Center gebeurtenis ID                 | 00000538  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

#### [Account was not added. This account already exists](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1337  |
| Kaspersky Security Center gebeurtenis ID                 | 00000539  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |



**Account was not modified. This account does not exist** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1338  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053a  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |

**Account was not deleted. This account does not exist** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1339  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053b  |
| Windows gebeurtenislogboek - EventLogItem.               | -   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


**FDE upgrade successful** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1341  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053d  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

**FDE upgrade rollback successful** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1343  |
| Kaspersky Security Center gebeurtenis ID                 | 0000053f  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1346  |
| Kaspersky Security Center gebeurtenis ID                 | 00000542  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [BitLocker recovery key was changed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1370  |
| Kaspersky Security Center gebeurtenis ID                 | 0000055a  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [BitLocker password / PIN was changed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1371  |
| Kaspersky Security Center gebeurtenis ID                 | 0000055b  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [BitLocker-herstelsleutel is opgeslagen op verwisselbare schijf.](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevensencryptie   |
| Windows-gebeurtenissen ID                                | 1372  |
| Kaspersky Security Center gebeurtenis ID                 | 0000055c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


**Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2103  |
| Kaspersky Security Center gebeurtenis ID                 | 00000837  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



**Endpoint Sensor connected to server** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2101  |
| Kaspersky Security Center gebeurtenis ID                 | 00000835  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


**Connection to the Kaspersky Anti Targeted Attack Platform server restored** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2102  |
| Kaspersky Security Center gebeurtenis ID                 | 00000836  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



**Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed** 

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Sensor   |
| Windows-gebeurtenissen ID                                | 2104  |
| Kaspersky Security Center gebeurtenis ID                 | 00000838  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |


### [Object deleted](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevens wissen   |
| Windows-gebeurtenissen ID                                | 2251  |
| Kaspersky Security Center gebeurtenis ID                 | 000008cb  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

### [Wipe task statistics](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Gegevens wissen   |
| Windows-gebeurtenissen ID                                | 2253  |
| Kaspersky Security Center gebeurtenis ID                 | 000008cd  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Object quarantined \(Kaspersky Sandbox\)](#)


|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2602  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a2a  |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |  |

### [Object verwijderd \(Kaspersky Sandbox\)](#)




|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2604  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a2c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | -   |


#### [IOC Scan started](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2652  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a5c  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |


#### [IOC Scan completed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2653  |
| Kaspersky Security Center gebeurtenis ID                 | 00000a5d  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object quarantined \(Endpoint Detection and Response\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2555  |
| Kaspersky Security Center gebeurtenis ID                 | 000009fb  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

#### [Object deleted \(Endpoint Detection and Response\)](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Endpoint Detection and Response   |
| Windows-gebeurtenissen ID                                | 2557  |
| Kaspersky Security Center gebeurtenis ID                 | 000009fd  |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |

### [Application components successfully changed](#)

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Systeemaudit  |
| Windows-gebeurtenissen ID                                | 1402  |
| Kaspersky Security Center gebeurtenis ID                 | 0000057a  |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | ✓   |



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2606  |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2609  |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               | ✓   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |



|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2610  |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |

|  |   |
|--|---|
| Status   |  |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2616  |
| Kaspersky Security Center gebeurtenis ID                 | –   |
| Windows gebeurtenislogboek - EventLogItem.               |  |
| Kaspersky Security Center-gebeurtenislogboek (standaard) | –   |



### Asynchrone Kaspersky Sandbox-detectie

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Kaspersky Sandbox   |
| Windows-gebeurtenissen ID                                | 2619  |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_APP_INCIDENT_OCCURED  |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de Kaspersky Sandbox componentinstelling</li> <li>• GNRL_EA_PARAM_2 is het pad naar het object.</li> <li>• GNRL_EA_PARAM_3 is de incident-ID.</li> <li>• GNRL_EA_PARAM_4 is de hash van het object (SHA256).</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### Device is connected

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 805   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_DEVCTRL_DEV_PLUGGED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de Hardware-ID (HWID).</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

### Device is disconnected

|  |   |
|--|---|
| Status   |    |
| Onderdeel  | Apparaatcontrole  |
| Windows-gebeurtenissen ID                                | 806   |
| Kaspersky Security Center gebeurtenis ID                 | GNRL_EV_DEVCTRL_DEV_UNPLUGGED   |
| Gebeurtenisparameters                                    | <ul style="list-style-type: none"> <li>• GNRL_EA_PARAM_1 is de Hardware-ID (HWID).</li> <li>• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.</li> </ul> |
| Windows gebeurtenislogboek - EventLogItem.               | –   |
| Kaspersky Security Center-gebeurtenislogboek (standaard) |    |

## 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, Flash, Reader en Shockwave zijn gedeponeerde handelsmerken of handelsmerken van Adobe Systems Incorporated in de Verenigde Staten en/of andere landen.

Apple, FireWire, iTunes en Safari zijn handelsmerken van Apple Inc. in de Verenigde Staten en andere landen.

AutoCAD is een gedeponeerd handelsmerk of handelsmerk van Autodesk, Inc. en/of diens dochterondernemingen en/of gelieerde ondernemingen in de Verenigde Staten en andere landen.

Het woord Bluetooth, het merk en de logo's zijn eigendom van Bluetooth SIG, Inc.

Borland is een handelsmerk of gedeponeerd handelsmerk van Borland Software Corporation.

Android en Google Chrome zijn handelsmerken van Google, Inc.

Citrix en Citrix Provisioning Services en XenDesktop zijn handelsmerken van Citrix Systems, Inc. en/of een of meer van haar dochterondernemingen, en kunnen gedeponeerd zijn bij het United States Patent and Trademark Office en in andere landen.

Dell is een handelsmerk van Dell, Inc. of haar dochterondernemingen.

dBase is een handelsmerk van dataBased Intelligence, Inc.

EMC is een handelsmerk of gedeponeerd handelsmerk van EMC Corporation in de Verenigde Staten en/of andere landen.

Foxit is een gedeponeerd handelsmerk van Foxit Corporation.

Radmin is een gedeponeerd handelsmerk van Famatech.

IBM is een gedeponeerd handelsmerk van International Business Machines Corporation in veel jurisdicties wereldwijd.

Intel is een handelsmerk van Intel Corporation in de V.S. en/of andere landen.

IOS en Any Connect zijn gedeponeerde handelsmerken van Cisco Systems, Inc. en/of diens gelieerde ondernemingen in de Verenigde Staten en andere landen.

Lenovo en ThinkPad zijn handelsmerken van Lenovo in de Verenigde Staten en/of elders.

Linux is het gedeponeerde handelsmerk van Linus Torvalds in de VS en andere landen.

Logitech is een gedeponeerd handelsmerk of handelsmerk van Logitech in de Verenigde Staten en/of andere landen.

LogMeIn Pro en Remotely Anywhere zijn handelsmerken van LogMeIn, Inc.

Mail.ru is een gedeponeerd handelsmerk van Mail.Ru, LLC.

McAfee is een handelsmerk of gedeponeerd handelsmerk van McAfee, Inc. in de Verenigde Staten en andere landen.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface and Hyper-V zijn handelsmerken van Microsoft Corporation in de Verenigde Staten en andere landen.

Mozilla, Firefox en Thunderbird zijn handelsmerken van de Mozilla Foundation.

Java en JavaScript zijn gedeponeerde handelsmerken van Oracle en/of diens gelieerde ondernemingen.

VERISIGN is een gedeponeerd handelsmerk in de Verenigde Staten en elders, of een niet-gedeponeerd handelsmerk van VeriSign, Inc. en haar dochterondernemingen.

VMware, VMware ESX, VMware ESXi en VMware Workstation zijn gedeponeerde handelsmerken of handelsmerken van VMware, Inc. in de Verenigde Staten en/of andere rechtsgebieden.

Tor is een gedeponeerd handelsmerk van The Tor Project, U.S. Registration No. 3.465.432.

Thawte is een handelsmerk of gedeponeerd handelsmerk van Symantec Corporation of diens gelieerde ondernemingen in de VS en andere landen.

SAMSUNG is een handelsmerk van SAMSUNG in de Verenigde Staten en andere landen.